dsb

datenschutzbeauftragter
kanton zürich

2011

Tätigkeitsbericht

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.

«Sensitive Gesundheitsdaten sind wirksam zu schützen»

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 dritte, 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 2011 bis und mit 31. Dezember 2011 ab und wird auch im Internet unter www.datenschutz.ch veröffentlicht.

Zürich, März 2012

Der Datenschutzbeauftragte des Kantons Zürich
Dr. Bruno Baeriswyl

Überblick

Mit Kontrollen den Datenschutz stärken 06–07

Der Datenschutz verändert sich 08–09

Die Wirkung des IDG 10–11

Schwerpunkte

Formelle Empfehlungen gemäss IDG 12–13

Brennpunkt Gesundheitswesen 14–16

Beratung

Überblick 2011: Kurzberatungen liegen weiter im Trend 17

Ausgewählte Beratungsfälle

01 Datenfluss im Rahmen der Pflegefinanzierung 18

02 Weitergabe von Patientenadressen 18

03 Fragebogen über Gemeindeangelegenheiten 19

04 Sozialhilfeentscheide an Betreibungsamt 20

05 Bekanntgabe des Aufenthaltsorts eines Inhaftierten 20

06 Schülerbefragung zur Unterrichtsqualität 21

07 Biografische Texte von Lernenden 21

08 Informationsplattform über Lernende 22

09 Zugang zu eigenen Personendaten 22

10 Eigene Personendaten? 23

11 Elektronisches Personaldossier 23

12 Elektronische Verfügungen und Rechnungen 24

13 Abgrenzung von Drittangeboten auf Websites 25

14 Auslagerung von Datenbearbeitungen 25

15 Live-Übertragungen von Medienkonferenzen 26

16 Aktenbeizug für parlamentarische Oberaufsicht 27

17 Bezug von Fischerei- und Jagdbewilligungen über das Internet 27

Kontrollen

Überblick 2011: Systematische Auswertung der Kontrollresultate **28**

Aufsicht im Bereich des Staatsschutzes **29**

Informationssicherheit in Gemeinden **30**

Kontrolle der Registerharmonisierung **31**

Vernehmlassungen

Überblick 2011: Stellungnahmen zu Gesetzesvorhaben **32–33**

Personenkontrollen und Überwachungsmassnahmen **34**

Unklare Regelung des Krebsregisters **35**

Statistikidentifikator notwendig **35**

Regelung der Online-Zugriffe **36**

Freiwilliges elektronisches Patientendossier **36**

Kommunikation

Relaunch des Webauftritts im Fokus **37**

Aus- und Weiterbildung

Sensibilisierung durch Referate und Seminare **38**

Impressum **39**

Mit Kontrollen den Datenschutz stärken

Die Datenbearbeitungen nehmen in allen Bereichen laufend zu. Trotz der zunehmenden Sensitivität bestehen bei der Sicherheit der Daten nach wie vor grosse Defizite.

Erstmals hat der Datenschutzbeauftragte zwei formelle Empfehlungen ausgesprochen. Sie betreffen die Weitergabe von Unterschriftbogen einer Petition vom Kanton an eine Gemeinde. Unter Verletzung von Geheimhaltungsvorschriften gelangten sie auch an die Öffentlichkeit. Mit einer Empfehlung kann der Datenschutzbeauftragte verlangen, dass Massnahmen ergriffen werden, wenn eine Datenschutzverletzung vorliegt. Im vorliegenden Fall ging es um die Beseitigung der Folgen der rechtswidrigen Datenbekanntgaben. Während die Gemeinde die Empfehlung akzeptierte, wurde sie von der betroffenen Direktion abgelehnt. Um den datenschutzrechtlichen Anliegen Nachachtung zu verschaffen, hat der Datenschutzbeauftragte die Ablehnung angefochten. Das Verfahren ist noch hängig.

Wirksame Eingriffsbefugnisse

Die Empfehlung ist das einzige Instrument des Datenschutzbeauftragten, mit dem er verbindliche Massnahmen anordnen kann. Das öffentliche Organ, an das sich die Empfehlung richtet, kann sie annehmen, indem es die Massnahmen umsetzt. Lehnt es sie ab, hat es eine Verfügung zu erlassen, die der Datenschutzbeauftragte auf dem Rechtsweg anfechten kann. Die Möglichkeit, eine verbindliche gerichtliche Anordnung zu erlangen, ist eine Umsetzung der europarechtlichen Vorgaben aus dem Schengen-Assoziierungsabkommen und dem Zusatzprotokoll zur Europaratskonvention Nr. 108. Beide verlangen, dass der Datenschutzbehörde wirksame Eingriffsbefugnisse zur Verfügung stehen müssen.

Vertiefte Kontrolltätigkeit

Mit Kontrollen – sogenannten Datenschutz-Reviews – überprüft der Datenschutzbeauftragte die Datenbearbeitungen einzelner öffentlicher Organe. Die Kontrollen zeigen ein hohes Verbesserungspotenzial im Bereich der Informationssicherheit. Die Prüfungen, welche nach den anerkannten Audit-Standards erfolgen, zeigen bei allen geprüften Bereichen einen durchschnittlichen Umsetzungsgrad von weniger als 50 Prozent. Der Datenschutzbeauftragte gibt dabei Hinweise, welche Massnahmen zu treffen sind, um ein dem Stand der Technik angemessenes Sicherheitsniveau zu erlangen. Empfehlungen wurden dabei bisher keine ausgesprochen. Aufgrund der Zunahme der Datenbearbeitungen und der Sensitivität der bearbeiteten Personendaten bestehen heute in vielen Fällen hohe Risiken für die Persönlichkeitsrechte der Bürgerinnen und Bürger. Die Kontrollen tragen dazu bei, diese Risiken aufzudecken und entsprechende Massnahmen zu deren Minimierung einzuleiten. Da für die Kontrolltätigkeit aber nur unzureichende Ressourcen zur Verfügung stehen, sind sie nicht in einem regelmässigen Turnus möglich. Angesichts der Resultate der Kontrollen ist dies eine unbefriedigende Situation.

Mangelnder Geheimnisschutz im Gesundheitswesen

Nach wie vor gehört das Gesundheitswesen zu den sensitivsten Bereichen des Datenschutzes. Nicht nur das Datenvolumen und der Datenaustausch nehmen laufend zu, sondern mit den genetischen Befunden auch die Sensitivität dieser Daten. Gesundheitsdaten haben nicht nur eine grosse persönliche Bedeutung, sondern im gesellschaftlichen Umfeld auch ein hohes Diskriminierungspotenzial.

Obwohl im Gesundheitswesen von allen Beteiligten die grosse Bedeutung des Datenschutzes oder des Patientengeheimnisses unterstrichen wird, sind die Massnahmen zur Gewährleistung dieses Geheimnisschutzes in der Praxis oft ungenügend. Vielfach wird das Patientengeheimnis durch unzureichende Massnahmen ausgehöhlt. Dies trifft beispielsweise zu bei den nun eingeführten Fallkostenpauschalen (SwissDRG), bei denen medizinische Daten an die Versicherer weitergegeben werden, ohne dass in der überwiegenden Zahl der Fälle eine Notwendigkeit für detaillierte medizinische Angaben bestehen würde. Der Datenschutzbeauftragte hat sich dabei verschiedentlich dafür eingesetzt, dass das Patientengeheimnis auch bei den neuen Fallkostenpauschalen respektiert wird. Eine ausgewogene, die Interessen des Schutzes der Patientendaten gewährende Lösung kam aber nicht zu Stande.

Mit E-Health, dem elektronischen Patientendossier und der weiteren Informatisierung des Gesundheitswesens wird der Datenfluss nochmals stark wachsen. Um die Vorteile des elektronischen Datenflusses im Gesundheitswesen vollumfänglich nutzen zu können, werden von Anfang an die notwendigen Massnahmen zum Schutz der sensiblen Daten vorzusehen sein.

Elektronischer Datenaustausch

Zunehmend bietet die Verwaltung den Bürgerinnen und Bürgern ihre Dienstleistungen auch elektronisch an. Mit der elektronischen Rechnungsstellung (E-Rechnung) wird die Zahlungsabwicklung vereinfacht. Bei dieser Art der Zahlungsabwicklung in der öffentlichen Verwaltung ist aber zu berücksichtigen, dass solche Rechnungsstellungen auch Verfügungscharakter haben und besonderen Geheimhaltungsvorschriften unterliegen können – beispielsweise dem Steuergeheimnis. Wenn solche Dienstleistungen an ein Finanzinstitut ausgelagert werden, ist zudem zu beachten, dass die Daten und Informationen von diesem nicht zu eigenen (Marketing-)zwecken ausgewertet werden. Der Datenschutzbeauftragte hat in einem konkreten Projekt auf verschiedene zu beachtende Rahmenbedingungen hingewiesen.

Weitere Schwerpunkte

- Schülerbefragungen und Informationsplattform über Lernende
- Zugang zu eigenen Personendaten
- Informationssicherheit in Gemeinden
- Stellungnahmen zu Gesetzesvorhaben

Der Datenschutz verändert sich

Werden die Bürgerinnen und Bürger in der Zukunft noch wissen, wer ihre Daten bearbeitet? Welcher rechtliche Schutz wird für die Privatsphäre bestehen?

Umwälzungen in der Informationstechnologie sind nach wie vor die Treiber einer zunehmend umfassenderen Datenbearbeitung. Einerseits findet schon heute eine immer breitere Bearbeitung von Daten über die Bürgerinnen und Bürger statt, beispielsweise indem bei einer Hotelübernachtung auch schnell überprüft werden soll, ob die betreffende Person in einem Fahndungssystem der Polizei ausgeschrieben ist, und – auch wenn dies nicht der Fall sein sollte – die Information über die Hotelübernachtung bei der Polizei gespeichert bleiben soll (siehe Seite 34). Andererseits sollen im Rahmen der «personalisierten Medizin» immer mehr auch genetische Informationen über den Menschen gespeichert werden. Diese Informationen sind sehr sensitiv, haben sie doch eine grosse Bedeutung für den einzelnen Menschen, aber auch ein hohes Risikopotenzial für Diskriminierungen im gesellschaftlichen Umfeld. Das elektronische Patientendossier (siehe Seite 36) wird dadurch zu einer höchst sensitiven Datenbank. Die zukünftigen Datenbearbeitungen über die Bürgerinnen und Bürger zeichnen sich damit schon heute klar ab.

Daten in der Wolke

Dabei ist ein weiterer Trend auszumachen: Zunehmend werden Daten «ausgelagert», das heisst, ein Dritter bearbeitet und speichert die Daten im Auftrag der Verwaltung. Was sich auf den ersten Blick als ein klassisches Outsourcing präsentiert, zeigt sich bereits heute als «mäandrisches Gebilde»: Die Datenbearbeitung findet nicht mehr an einem bestimmten Ort statt, sondern schlängelt sich durch die virtuelle Welt und sucht ihren Platz dort, wo die Ressourcen am günstigsten sind. Hinter dem Stichwort «Cloud Computing» verbergen sich die unterschiedlichsten Gebilde von «Auslagerungen» in allen Bereichen. Für das öffentliche Organ, das für die Bearbeitung der Daten über die Bürgerinnen und Bürger verantwortlich ist, ist es eine Gratwanderung zwischen Verantwortlichkeit und Kontrolle diesbezüglicher Datenbearbeitungen. Es stellen sich technische wie datenschutzrechtliche Fragen, die zurzeit erst auf konzeptioneller Ebene berücksichtigt werden. Doch das Cloud Computing wächst ungebremst.

Keine Insel in der virtuellen Welt

Die technologischen Entwicklungen haben auch einen grossen Einfluss auf die Datenbearbeitungen der öffentlichen Organe im Kanton Zürich. Die technologischen Entwicklungen prägen die Art und Weise der Datenbearbeitung. Dabei erfolgt die Adaption neuer technologischer Möglichkeiten in der öffentlichen Verwaltung immer schneller. Und mit diesen Technologien lassen sich zusätzliche Datenbearbeitungen realisieren und beispielsweise Datenbestände schnell und automatisch miteinander abgleichen. Damit stellt sich für die öffentlichen

Organe zunehmend die Frage, wie mit diesen neuen Technologien umzugehen ist.
Die neuen Technologien verändern den Umgang mit den Daten der Bürgerinnen und Bürger und damit den Datenschutz. Von jeher ist der Datenschutz ein dynamisches Rechtsgebiet – wie die schnelle Entwicklung im Kanton Zürich vom Datenschutzgesetz (DSG) zum Informations- und Datenschutzgesetz (IDG) zeigt. In Zukunft wird sich vermehrt die Frage stellen, wie Informationen über die Bürgerinnen und Bürger effizient, aber unter Respektierung der berechtigten Anliegen auf Schutz der Privatsphäre bearbeitet werden sollen. Dazu gehört deshalb auch eine Analyse der Risiken der Datenbearbeitungen in Bezug auf ihre Auswirkungen auf die Rechte der betroffenen Personen.

Neuer Datenschutz

In diese Richtung gehen die neuen Rechtsentwicklungen in Europa. Sowohl in der EU als auch im Europarat sind Anpassungen der Datenschutzgesetzgebung an die neuen Entwicklungen vorgesehen. Über die Abkommen von Schengen/Dublin für den Justiz- und Polizeibereich sowie durch die Konvention 108 des Europarates sind diese Rechtsentwicklungen für die Schweiz und den Kanton Zürich mittel- oder unmittelbar verbindlich. Die europäischen Vorhaben zeigen auf, wo der Datenschutz Verstärkung braucht, um die Risiken für die Privatsphäre auch bei der Verwendung neuer Technologien zu minimieren. Um die Persönlichkeitsrechte auch in der digitalen Welt zu gewährleisten, müssen die Datenbearbeitungen für die Bürgerinnen und Bürger transparenter gemacht werden. Das bedeutet beispielsweise, dass in der virtuellen Welt Daten konsequent gelöscht werden müssen, um das «Recht auf Vergessen» auch hier zu verwirklichen. Damit soll sichergestellt werden, dass alle über ihre eigenen Personendaten tatsächlich selber bestimmen können.
Besonders sensitiv ist der internationale Austausch von Daten im Bereich der polizeilichen und justiziellen Zusammenarbeit. Mit den Abkommen von Schengen/Dublin sind die Schweiz und der Kanton Zürich in ein klares Rechtssystem eingebunden. Dennoch stellen sich auch hier aufgrund der technologischen Entwicklungen neue (datenschutz)rechtliche Herausforderungen, denen mit entsprechenden rechtlichen Anpassungen zu begegnen sein wird.
In diesem Rahmen wird der Datenschutz für die zukünftigen Herausforderungen anzupassen sein. Die vorgeschlagenen Rechtsänderungen auf europäischer Ebene werden deshalb in der Schweiz wie auch im Kanton Zürich näher zu prüfen sein.

Die Wirkung des IDG

Die Berichterstattung über die Wirkung des Informations- und Datenschutzgesetzes gemäss § 39 IDG wird systematisiert und damit aussagekräftig.

Für die Berichterstattung des Datenschutzbeauftragten über die Wirkung des IDG bestehen unzureichende Grundlagen. Die bisherigen Feststellungen beruhen auf unterschiedlichen Dokumenten in verschiedenen Bereichen wie Statistiken über Gesuche auf Informationszugang oder Wirkungsindikatoren des Datenschutzbeauftragten im KEF. Aus diesen lassen sich keine verlässlichen Aussagen über die Wirkung des IDG ableiten. Aus diesem Grund hat der Datenschutzbeauftragte zusammen mit der ZHAW (Zürcher Hochschule für Angewandte Wissenschaften) ein Projekt initiiert mit dem Ziel, eine systematische und aussagekräftige Evaluation des IDG zu ermöglichen.

Erstellung eines Konzepts

Hierfür wird ein Konzept erstellt für eine regelmässige Evaluation des IDG im Rahmen der Berichterstattung des Datenschutzbeauftragten. Dabei sollen die Wirkungen des Gesetzes bezogen auf die in § 1 IDG beschriebenen Zwecke erfasst werden. Dazu gehören die Bereiche des Datenschutzes und des Informationszuganges. Gegenstand der Evaluation sind dabei die beabsichtigten, aber unter Umständen auch die unbeabsichtigten Wirkungen. Soweit für die Beurteilung der Wirkung notwendig, werden auch die Vollzugsinstrumente und das tatsächliche Verhalten der öffentlichen Organe einbezogen.

Kriterien des Konzepts

Die Darstellung der Wirkung des IDG erfolgt im Rahmen der Berichterstattung des Datenschutzbeauftragten, weshalb das Konzept die tatsächlichen Ressourcen des Datenschutzbeauftragten zu berücksichtigen hat. Dabei soll eine Auslagerung von bestimmten Aufgaben, beispielsweise Umfragen oder Auswertungen, möglich sein. Die Evaluation der Wirkung soll mit einem verhältnismässigen Aufwand durchgeführt werden können und deshalb auch bereits bestehende Statistiken und Befragungen benutzen.

Eine kontinuierliche Darstellung der Wirkung im Rahmen der Berichterstattung muss über die Jahre vergleichbar bleiben, das heisst, die Indikatoren müssen so ausgewählt sein, dass sie regelmässig erfasst werden können. Die Entwicklung des Konzeptes erfolgt deshalb in drei Schritten. Zuerst soll ein Wirkungsmodell für das IDG erstellt werden – ähnlich wie dies für die Tätigkeiten des Datenschutzbeauftragten im Rahmen des KEF besteht. Daraus werden die Wirkungsindikatoren abgeleitet und ihre empirische Erfassung definiert. Im letzten Schritt entsteht daraus das definitive Evaluationskonzept.

Datenschutzbeauftragter

Nr. 9071
Funktionale Gliederung: 0

Finanzierung

Erfolgsrechnung (in Mio. Fr.)	R 10	B 11	Δ(P 12)	P 12	Δ(P 13)	P 13	Δ(P 14)	P 14	P 15	Δ%(10-15)
Ertrag	0.0	0.1	0.1	0.2	0.0	0.1	0.0	0.1	0.1	
Aufwand	-2.1	-2.2	0.1	-2.4	-0.1	-2.5	-0.1	-2.5	-2.5	21.9
Saldo	-2.0	-2.0	0.2	-2.2	-0.1	-2.4	-0.0	-2.4	-2.4	
Investitionen (in Mio. Fr.)										Ø (10 -15)
Einnahmen										
Ausgaben	0.0									0.0
Nettoinvestitionen	0.0									0.0
Personal (Beschäftigungsumfang)	8.3	8.2	0.0	9.2	0.0	9.2	0.0	9.2	9.2	

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	Kontrolle: Verstärkung in den Bereichen "Bearbeitung besonderer Personendaten" und "Schengen"	2012	0
E2	Datenschutzfreundliche Technologien: Förderung der Entwicklung und des Einsatzes von datenschutzfreundlichen Technologien	2012	0
E3	Begleitung und Überprüfung der Gesetzesanpassungen an die Vorgaben des IDG (Übergangsfrist)	2013	0
E4	Gesetzeskonformer Umgang mit Personendaten in sensitiven Bereichen fördern und fordern (Gesundheitswesen, Schule, Sozialbereich etc.)	2014	0

Indikatoren

		Art	R 10	B 11	P 12	P 13	P 14	P 15
Wirkungen								
W1	Kundenbeurteilung der Qualität der Leistungen	min.	-	-	gut	-	gut	-
W2	Anteil umgesetzter Hinweise (%)	P	79	60	60	60	60	60
Leistungen								
L1	Anteil komplexer Beratungen von öffentlichen Organen (%)	P	22	33	33	33	33	33
L2	Anteil aufwändiger Beratungen von Privatpersonen (%)	P	7	15	15	15	15	15
L3	Anzahl Grundsatzfragen u. Stellungnahmen	max.	15	25	25	25	25	25
L4	Anzahl Datenschutz-Reviews	min.	9	20	35	35	35	35
L5	Zuwachs Besuche auf Internetangeboten (%)	P	-	5	5	5	5	5
L6	Anzahl Teilnehmerstunden an Weiterbildungsangeboten	min.	450	500	500	500	500	500
Wirtschaftlichkeit								

Leistungsgruppe 9071	Budgetentwurf 2012
Budgetkredit Erfolgsrechnung (in Mio Fr.)	-2.245
Budgetkredit Investitionsrechnung (in Mio. Fr.)	
Leistungsindikatoren L3, L4 und L6	

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

Anhang 1-10

Formelle Empfehlungen gemäss IDG

Der Datenschutzbeauftragte hat die Möglichkeit, verbindliche Empfehlungen abzugeben und – falls das betroffene öffentliche Organ diese nicht akzeptiert – den Rechtsweg zu beschreiten. Im Berichtsjahr fand dieses Instrument erstmals Anwendung.

Zu den Aufgaben des Datenschutzbeauftragten gehört die Aufsicht über die korrekte Anwendung der Vorschriften über den Datenschutz durch die öffentlichen Organe. Kontrollen dienen einerseits der systematischen Überprüfung der Einhaltung von Datenschutzvorschriften, anderseits erfolgen sie auf einen konkreten Anlass hin. Die Kontrolltätigkeit mündet in der Regel in eine Stellungnahme oder einen Bericht zu Handen des öffentlichen Organs. Stellt der Datenschutzbeauftragte fest, dass Bestimmungen über den Datenschutz verletzt wurden, kann er eine Empfehlung abgeben.

Rechtlich verbindliches Instrument

Bei der Empfehlung handelt es sich um ein formelles Instrument mit Rechtswirkungen. Das öffentliche Organ, an das sich die Empfehlung richtet, ist zu verbindlichem Handeln angehalten: Es hat die Empfehlung entweder anzunehmen oder abzulehnen. Die Annahme erfolgt durch Umsetzung der mit der Empfehlung abgegebenen Handlungsanweisungen oder Massnahmen. Ist das öffentliche Organ mit der Empfehlung nicht einverstanden, hat es innert 60 Tagen eine Verfügung zu erlassen. Der Datenschutzbeauftragte kann die Verfügung auf dem Rechtsweg gemäss Verwaltungsrechtspflegegesetz anfechten.

Die Terminologie des Gesetzes darf als nicht besonders gelungen bezeichnet werden, stellt sich der Rechtsunterworfene doch unter dem Begriff der «Empfehlung» etwas eher Unverbindliches vor. Spricht der Datenschutzbeauftragte eine Empfehlung aus, muss er deshalb sicherstellen, dass der Adressat deren Verbindlichkeit erkennt. Die Empfehlung ist deshalb als solche zu bezeichnen, und sie hat klare Handlungsanweisungen sowie eine Rechtsbelehrung bezüglich Annahme oder Ablehnung zu enthalten.

Diese Einwirkungsbefugnisse, einschliesslich der Möglichkeit, den Rechtsweg zu beschreiten, sind als Folge von neuen europarechtlichen Vorgaben ins IDG aufgenommen worden. Damit wird den Anforderungen des Zusatzprotokolls zur Europaratskonvention Nr. 108 und des Schengen-Assoziierungsabkommens entsprochen. Der Datenschutzbeauftragte hat neu also die Möglichkeit, strittige Datenbearbeitungen auf dem Rechtsweg klären zu lassen.

Verbreitung von Petitionsunterschriften

Während auf Bundesebene das Instrument der Empfehlung schon lange gesetzlich vorgesehen war und durch den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten wiederholt eingesetzt wurde, hat der Datenschutzbeauftragte des

Kantons Zürich im Berichtsjahr die ersten Empfehlungen abgegeben. Dabei ging es um den Fall der Weiterverbreitung von unterschriebenen Petitionsbogen durch den Kanton und Behördenvertreter einer politischen Gemeinde.

Die Petition richtete sich an die Baudirektion und hatte zum Gegenstand, dass für ein Strassenbauprojekt des Kantons (Ortsumfahrung von Ottenbach) eine andere Variante gewählt werden sollte als die vom Kanton geplante. Die Baudirektion lud die Gemeinde Ottenbach zu einer Stellungnahme zur Petition ein und sandte ihr die eingescannten Unterschriftenbogen zu. Die Unterschriftenbogen wurden den Mitgliedern der vom Gemeinderat für das Umfahrungsprojekt eingesetzten Kommission weitergegeben und aus dieser Kommission heraus weiterverbreitet. Die Petitionsbogen gelangten schliesslich zu einer Privatperson, die sich an den Datenschutzbeauftragten wandte.

Der Datenschutzbeauftragte klärte den Sachverhalt ab und stellte fest, dass bereits die Weitergabe der eingescannten Unterschriftenbogen von der Baudirektion an die Gemeinde unverhältnismässig war, da die Gemeinde die Unterschriftenbogen für ihre Aufgabe – Stellungnahme zum Petitionsbegehren – nicht benötigte. Erst recht stellte die Weiterverbreitung der Unterschriftenbogen aus der Kommission an Private eine Verletzung von Geheimhaltungsvorschriften dar. Diese Feststellungen veranlassten den Datenschutzbeauftragten dazu, gegenüber der Baudirektion und der Gemeinde Ottenbach je eine Empfehlung für die Wiederherstellung des rechtmässigen Zustands und die Vermeidung künftiger Rechtsverletzungen abzugeben. Während die Gemeinde Ottenbach die Empfehlung des Datenschutzbeauftragten annahm, lehnte die Baudirektion diese ab und erliess eine Verfügung. Gegen diese Verfügung hat der Datenschutzbeauftragte seinerseits beim Regierungsrat Rekurs eingelegt.

Das Verfahren ist noch hängig.

§ 36 IDG

Brennpunkt Gesundheitswesen

Datenschutz und Arztgeheimnis bilden die Grundlage des medizinischen Behandlungsverhältnisses. Der Schutz dieses Vertrauensverhältnisses steht immer mehr unter Druck.

Informationen über die Gesundheit eines Menschen gehören zu den sensibelsten Daten überhaupt. Das IDG ordnet die Gesundheitsdaten deshalb den sogenannten besonderen Personendaten zu, was erhöhte Anforderungen für die Bearbeitung nach sich zieht. Im Zusammenhang mit Gesundheitsinformationen besteht die Gefahr der Stigmatisierung eines Menschen, sei es wegen einer Behinderung, eines psychischen Leidens oder einer bestimmten Krankheit. Trotz dieser Sensibilität ist der Schutz der Privatsphäre und der Gesundheitsdaten kaum angemessen präsent. Angesichts der komplexen Fragestellungen geht die Thematik des Datenschutzes oft unter oder wird anderen Interessen geopfert.

Verhältnismässige Datenbekanntgaben

Information ist ein Gut mit einem grossen wirtschaftlichen Wert geworden. Auch im Gesundheitsmarkt ist es attraktiv, Informationen über die Gesundheit der aktuellen und der potenziellen Patientinnen und Patienten zu kennen. Die Gesundheitsdaten sind jedoch durch das Arztgeheimnis geschützt, so dass sie nur für die Behandlung, allenfalls auch für die Forschung, verwendet, aber sonst nicht weitergegeben werden dürfen. Damit entsteht ein Spannungsfeld zum Informationsbedürfnis der Versicherer. Letztere möchten sich von Kosten für vermeintlich unnötige Behandlungen befreien. Die Leistungserbringer müssen deshalb immer mehr Daten an die Versicherer liefern. Mit der Einführung der Fallkostenpauschalen (SwissDRG) per 2012 sollten in allen Fällen detaillierte Diagnosen und Therapien mit der Rechnung an die Versicherer geliefert werden. Zur Überprüfung der Wirksamkeit, Zweckmässigkeit und Wirtschaftlichkeit einer Behandlung sind jedoch nur in Einzelfällen (5–10 Prozent aller Fälle) solch detaillierte Daten erforderlich. Der Datenschutzbeauftragte setzte sich bei der Gesundheitsdirektion sowie über die Vereinigung der Schweizerischen Datenschutzbeauftragten (privatim) beim Bundesamt für Gesundheit und beim zuständigen Bundesrat dafür ein, eine verhältnismässige Lösung zu finden, welche dem Schutz der Privatsphäre der Patientinnen und Patienten ebenso Rechnung trägt wie den Interessen der Versicherer. Die mangelnde Bereitschaft der Versicherer, ihre Position zu überdenken, hat bis anhin eine Lösung verhindert. Wegweisend ist hingegen ein Entscheid des Regierungsrates vom Herbst 2011: Er hat die neuen Tarifverträge im Spitexbereich genehmigt, jedoch denjenigen Tarifbestimmungen die Genehmigung versagt, die einen umfassenden Datentransfer der Spitex an die Versicherer vorsahen.

Aktuelle Themen im Gesundheitswesen

Neues Tarifsystem (SwissDRG)

Im Akutspitalbereich wurde auf 2012 ein neues Tarifsystem mit Fallkostenpauschalen eingeführt. Der Datenschutzbeauftragte unterstützte die Vereinigung privatim bei deren Vorstössen beim Bundesamt für Gesundheit und beim zuständigen Bundesrat und wirkte bei der Gesundheitsdirektion darauf hin, dass anlässlich der Genehmigung von Tarifverträgen auf die korrekte Umsetzung der datenschutzrechtlichen Rahmenbedingungen geachtet wird. Es gilt sicherzustellen, dass das Arztgeheimnis nicht durch übertriebene Mitteilungspflichten ausgehöhlt wird. Für die Prüfung der Rechnungen benötigen die Versicherer keine systematischen Meldungen aller Diagnosen und Therapien.

Geltungsbereich IDG

Einzelne Spitäler wehren sich gegen die Anwendung des IDG. Mit dem Argument, sie ständen mit anderen Spitälern, insbesondere Privatspitälern, im wirtschaftlichen Wettbewerb, versuchen sie, sich von der Anwendung des IDG und den Kontrollen des Datenschutzbeauftragten auszunehmen. Die sich stellenden Fragen sollen im Rahmen eines Rechtsgutachtens im Auftrag von privatim geklärt werden.

Spitalplanungs- und -finanzierungsgesetz (SPFG) und Pflegegesetz

Das SPFG wurde 2011 vom Kantonsrat verabschiedet. In der Praxis stellten sich Fragen nach der Datenweitergabe von Leistungserbringern an die Gesundheitsdirektion im Rahmen von Kostenübernahmen, Qualitätssicherungen und Wirtschaftlichkeitsprüfungen. Ähnliche Fragen stellten sich bei der Umsetzung des Pflegegesetzes bezüglich Datenaustausch zwischen Leistungserbringern der Langzeitpflege (Alters- und Pflegeheime) und der Spitex in den Gemeinden. Der Datenschutzbeauftragte beriet die Gesundheitsdirektion und einzelne Leistungserbringer und intervenierte in einem Fall bei einer Gemeinde, die von Pflegeheimen unverhältnismässig viele Daten über Bewohnerinnen und Bewohner verlangte. Auch hier sind dem Datenaustausch durch das Arztgeheimnis enge Grenzen gesetzt.

E-Health

Unter diesem Schlagwort arbeitet eine Projektgruppe von Bund und Kantonen daran, die Medizin mit Informations- und Kommunikationstechnologien (IKT) zu modernisieren. Kern ist das elektronische Patientendossier. Als Voraussetzung für den Datenaustausch in und zwischen Versorgungsgemeinschaften werden IKT-Standards und IKT-Architektur definiert. Der Datenschutzbeauftragte wirkt über die Vereinigung privatim bei diesen Arbeiten mit und hat einen Mitbericht zum Entwurf des Bundesgesetzes über das elektronische Patientendossier abgegeben.

Schwarze Listen von Prämienzahlern

Anlässlich einer Teilrevision des Krankenversicherungsgesetzes (KVG) wurden das Verfahren und die Kostenbeteiligung bei Nichtbezahlung von Prämien neu geregelt. Die Versicherer haben die Möglichkeit, 85 Prozent der Prämienforderungen für die ein Verlustschein besteht, auf die Kantone ab-

zuwälzen. Im Gegenzug können die Kantone eine Liste über Prämienschuldner führen, die Gemeinden und Leistungserbringern zugänglich ist. In der Teilrevision des kantonalen Einführungsgesetzes zum KVG hat der Regierungsrat darauf verzichtet, eine solche schwarze Liste einzuführen. Im Berichtsjahr beriet der Datenschutzbeauftragte die Gesundheitsdirektion bei der Überarbeitung der Vorlage nach der Vernehmlassung.

Medizinische Forschung

Im Bereich der Forschung bestehen oft Unsicherheiten über das anwendbare Recht. Hier gilt eine Verordnung des Bundes über die Offenbarung des Berufsgeheimnisses in der medizinischen Forschung. Diese wird künftig abgelöst durch das neue Humanforschungsgesetz, das von den Eidgenössischen Räten im Herbst 2011 verabschiedet wurde. Grundsätzlich muss der Patient oder die Patientin aufgeklärt und dessen bzw. deren Einwilligung eingeholt werden, bevor seine oder ihre Daten zu Forschungszwecken bekannt gegeben werden dürfen. Der Datenschutzbeauftragte beriet Forschende und wirkte in einem Modul eines Weiterbildungslehrgangs des Universitätsspitals mit.

Pilotprojekt Case Management

In einem Pilotprojekt eines Leistungserbringers der Psychiatrie soll das (patientenbezogene) Case Management breiter abgestützt und auf weitere Kostenträger, insbesondere Kranken- und Sozialversicherungen, ausgeweitet werden. Der Datenschutzbeauftragte überprüfte ein umfangreiches Vertragskonstrukt zwischen dem Leistungserbringer und einem grossen Versicherer hinsichtlich der vorgesehenen Datenbearbeitungen sowie der Transparenz und Verhältnismässigkeit der Einwilligungserklärungen. Zum Vertragskonstrukt gab es nur vereinzelte Hinweise anzubringen; die Rechtmässigkeit der Datenbearbeitungen steht und fällt mit der umsichtigen Umsetzung in der Praxis.

Kurzberatungen liegen weiter im Trend

Die Beratungen von Privatpersonen und öffentlichen Organen inklusive der durchgeführten Vorabkontrollen sind ein konstanter Schwerpunkt in der Tätigkeit des Datenschutzbeauftragten. Am aufwändigsten ist die Beurteilung neuer Technologien mit Blick auf die datenschutzrechtlichen Rahmenbedingungen.

Ein grosser Teil der Beratungstätigkeit des Datenschutzbeauftragten liegt bei Kurzberatungen per Mail oder Telefon mit über tausend Anfragen pro Jahr. Diese nehmen im Durchschnitt 30 Minuten in Anspruch und weisen thematisch eine grosse Bandbreite auf. Am meisten personelle Ressourcen beanspruchen jedoch die Vorabkontrollen sowie die Beurteilung komplexer Sachgeschäfte.

Schwerpunktthemen Beratungstätigkeit

Die von Anfragen am meisten betroffenen Themenbereiche waren Datenbearbeitungen und Datenbekanntgaben im Schul- und im Sozialhilfebereich. Ungebrochen war auch die Nachfrage nach der Beurteilung im Zusammenhang mit Videoüberwachungen, seien dies umfassende Konzepte wie dasjenige der Universität Zürich und des kantonalen Immobilienamtes oder kleinere Einsätze dieser Technologie im Bereich von Schulen und Kirchen. Wesentlich angestiegen sind zudem Anfragen im organisatorisch-technischen Bereich.

Beurteilung eingesetzter Technologien

Bei den komplexen Sachgeschäften finden sich zunehmend Sachverhalte, welche die Beurteilung detaillierter technischer Vorgänge bedingen, um anschliessend die Einbettung in den rechtlichen Rahmen zu analysieren. Im Berichtsjahr waren dies beispielsweise die Beurteilung der Nutzung von Inlineframes durch öffentliche Organe (dienen der Strukturierung von Websites), die Begutachtung technischer Lösungen betreffend E-Government oder auch die Auslagerung von Datenbearbeitungen ins Ausland. Generell immer wieder ein Thema sind die Nutzung von Drittangeboten auf Websites und deren Zulässigkeit respektive die Umsetzung der dazu notwendigen Anforderungen.

Vorabkontrollen

Die Sensibilität der öffentlichen Organe in Bezug auf das Vorlegen von geplanten Datenbearbeitungen zwecks Beurteilung der datenschutzrechtlichen Anforderungen hat nachgelassen. So wird der Datenschutzbeauftragte im Rahmen von anderweitigen Beratungen immer wieder mit Fragen zum Einsatz neuer Software konfrontiert, die eigentlich im Rahmen einer Vorabkontrolle hätten beurteilt werden müssen.

01
Datenfluss im Rahmen der Pflegefinanzierung

Eine Gemeinde verlangte von einem Pflegeheim mittels eines Fragebogens Auskunft darüber, aus welchem Grund zwei bestimmte Bewohner in das Heim eingetreten sind, wie die Auswahl des Heims erfolgte und ob es Gründe gab, warum die Personen nicht in einem Heim gepflegt werden konnten, mit dem die Gemeinde eine Leistungsvereinbarung abgeschlossen hatte.
Der Datenschutzbeauftragte klärte die Rechtslage ab und nahm dazu Rücksprache mit der Gesundheitsdirektion.
Die Gemeinden haben für eine bedarfs- und fachgerechte stationäre und ambulante Pflegeversorgung ihrer Einwohnerinnen und Einwohner zu sorgen. Sie betreiben zu diesem Zweck eigene Einrichtungen oder beauftragen Dritte. Eine pflegebedürftige Person kann grundsätzlich frei wählen, ob sie ambulant oder in einem Pflegeheim und durch einen Leistungserbringer aus dem kommunalen Angebot oder einen anderen Leistungserbringer gepflegt werden will. Die Gemeinde darf deshalb nicht generell überprüfen, ob der Aufenthalt eines Gemeindeeinwohners oder einer Gemeindeeinwohnerin im jeweiligen Heim indiziert ist und ob kostengünstigere Möglichkeiten bestehen. Wählt eine Person einen Leistungserbringer ohne Gemeindeauftrag, hat die Gemeinde grundsätzlich pauschale Beiträge an die ungedeckten Kosten der Pflegeleistungen zu bezahlen, wobei höchstens Beiträge im Umfang des kantonal festgelegten Normdefizits übernommen werden müssen.
Auf Verlangen hat die Gemeinde einer pflegebedürftigen Person einen geeigneten Leistungserbringer zu vermitteln, wenn die erforderlichen Leistungen nicht durch einen von der Gemeinde betriebenen oder beauftragten Leistungserbringer erbracht werden können.
Die für die Vermittlung erforderlichen Informationen über die Gesundheit müssen direkt beim Leistungsbezüger eingeholt werden.
Nachdem der Datenschutzbeauftragte auf die beschriebene Rechtslage hingewiesen hatte, beschloss die Gemeinde, den Fragebogen nicht mehr zu verwenden.
In der Zwischenzeit hat der Datenschutzbeauftragte zu einem von der Gesundheitsdirektion erarbeiteten Empfehlungskatalog über die Anwendung des neuen Pflegegesetzes zu Handen von Gemeinden und Leistungserbringern Stellung genommen.

§ 5 Abs. 1 Pflegegesetz
§ 6 Pflegegesetz
§ 15 Pflegegesetz

02
Weitergabe von Patientenadressen

Ein ehemaliger Arzt eines öffentlichen Spitals machte nach Absprache mit dem Spital in einem Werbebrief an frühere Patienten und Patientinnen auf die Aufgabe seiner Tätigkeit im Spital und die Eröffnung einer eigenen Praxis aufmerksam. Eine betroffene Person wollte vom Datenschutzbeauftragten wissen, ob dieses Vorgehen rechtmässig ist.
Nach dem Austritt gilt der Arzt als Drittperson. Die Weitergabe der Daten durch das Spital an einen ausgetretenen Arzt stellt demnach eine Datenbekanntgabe dar, für die eine gesetzliche Grundlage oder die Einwilligung der betroffenen Person erforderlich ist. Da vorliegend beides nicht gegeben ist, handelt es sich um eine unzulässige Datenbekanntgabe.
Personendaten dürfen nur zu dem Zweck bearbeitet werden, zu dem sie erhoben worden sind, soweit nicht eine rechtliche Bestimmung ausdrücklich eine weitere Verwen-

dung vorsieht oder die betroffene Person im Einzelfall einwilligt.
Daten von Patientinnen und Patienten werden zum Zwecke einer Behandlung im Spital erhoben und bearbeitet. Die Weitergabe der Adressen an einen ehemaligen Arzt, damit dieser über seine neue Tätigkeit informieren kann, verstösst gegen das Zweckbindungsgebot.
Betroffene Personen können vom Spital verlangen, dass es solche widerrechtlichen Datenbearbeitungen zukünftig unterlässt und die Folgen des widerrechtlichen Bearbeitens beseitigt, indem es den Arzt auffordert, die Adressen aus seiner Kartei zu löschen.
Einem Spital stände es frei, die Patientinnen und Patienten selbst anzuschreiben und über den Stellenwechsel eines Arztes zu informieren, wenn es dies im Interesse der Patienten und Patientinnen für notwendig erachtet. So wäre dem Interesse der Patientinnen und Patienten am Schutz ihrer Daten Rechnung getragen.
Zulässig wäre es auch, wenn ein Arzt in einem Spital eine privatärztliche Praxis mit einer eigenen Praxisbewilligung führt und nur die Adressen jener Patienten und Patientinnen mitnimmt, die er in seiner Tätigkeit als Privatarzt behandelt hat.

§ 17 IDG
§ 9 IDG
§ 21 lit. b und c IDG

03
Fragebogen über Gemeindeangelegenheiten

Eine Gemeinde organisierte zum Thema Ortsplanung eine Ausstellung. Die Bevölkerung wurde auf freiwilliger Basis aufgerufen, per Fragebogen zu verschiedenen Zielsetzungen und Massnahmen Stellung zu nehmen. Mit dem Fragebogen war die Teilnahme an einem Wettbewerb verknüpft. Anonym eingereichte Fragebogen wurden in die Auswertung nicht einbezogen.
Das öffentliche Organ darf Personendaten bearbeiten, soweit dies zur Erfüllung der gesetzlich umschriebenen Aufgaben geeignet und erforderlich ist. Zu den Aufgaben der Gemeindevorsteherschaft gehört unter anderem die Information der Bevölkerung über wesentliche Gemeindeangelegenheiten. Im Rahmen der Aufgabenerfüllung kann die Gemeindevorsteherschaft auch die Meinung der Bevölkerung zu wichtigen Themen einholen. Führt eine Gemeinde eine solche Konsultativumfrage durch, stellt sich die Frage, ob der Umfragezweck nur erreicht werden kann, wenn die teilnehmenden Personen ihre Personalien angeben. Im vorliegenden Fall ergab die Rücksprache mit der Gemeinde, dass bei der Umfrage im Vordergrund stand, aus welchem Ortsteil die Antworten zur Ortsplanung kamen. Die Namen der an der Umfrage teilnehmenden Personen wurden nur zwecks Teilnahme am Wettbewerb und allfälliger Rücksprache mit den betreffenden Personen erhoben. Der Zweck der Umfrage, nämlich die Meinung der Bevölkerung zur Ortsplanung zu erfragen, konnte also auch erreicht werden, wenn auf die Erhebung von Namen verzichtet wurde. Die Rücksprache mit an der Umfrage teilnehmenden Personen war weder geeignet noch erforderlich, um den Zweck der Umfrage zu erfüllen, und die Teilnahme am Wettbewerb konnte auch auf andere Weise als durch Angabe von Namen und Adressen auf dem Fragebogen organisiert werden. Die Gemeinde erklärte sich daher bereit, auch anonym eingereichte Fragebogen auszuwerten.
Führt eine Gemeinde eine Konsultativumfrage durch, hat sie dafür zu sorgen, dass Einsichtsgesuche behandelt werden können. Dies bedingt, dass die Fragebogen noch während einer angemessenen Zeit nach der Auswertung aufbewahrt werden.

§§ 8 und 20 IDG
§ 68b Gemeindegesetz

04
Sozialhilfeentscheide an Betreibungsamt

Bei einer Sozialhilfebehörde bestand die Praxis, alle Beschlüsse bzw. Leistungsentscheide jeweils dem Betreibungsamt derselben Gemeinde im Dispositiv mitzuteilen. Die Zustellung hatte zum Zweck, dem Betreibungsamt allfällige Abklärungen im Zusammenhang mit der Berechnung des Existenzminimums zu erleichtern, wenn bei einem Sozialhilfebezüger eine Pfändung vollzogen wurde. Bestanden gegen einen Sozialhilfebezüger keine Pfändungen, wurden die Entscheide nach kurzer Zeit vernichtet. Ein betroffener Sozialhilfebezüger wandte sich mit dem Anliegen an den Datenschutzbeauftragten, die Zulässigkeit solcher Entscheidzustellungen an das Betreibungsamt zu überprüfen.

Die Zustellung eines Sozialhilfeentscheides an das Betreibungsamt bedarf einer gesetzlichen Grundlage. Im Rahmen einer Pfändung oder eines Konkurses ist die Sozialbehörde gegenüber dem Betreibungsamt aufgrund des Bundesgesetzes über Schuldbetreibung und Konkurs zur Auskunft verpflichtet. Für eine Mitteilung der Sozialbehörde an das Betreibungsamt ausserhalb eines Betreibungsverfahrens besteht hingegen keine gesetzliche Grundlage. Nachdem der Datenschutzbeauftragte auf die fehlende gesetzliche Grundlage hingewiesen hatte, beschloss die Sozialbehörde, dem Betreibungsamt – ausgenommen in den vom Bundesgesetz über Schuldbetreibung und Konkurs geregelten Fällen – in Zukunft keine Entscheiddispositive mehr mitzuteilen und das Betreibungsamt anzuweisen, bereits zugestellte Entscheide aus den Akten zu entfernen, sofern die Zustellung nicht aufgrund des Bundesgesetzes über Schuldbetreibung und Konkurs erfolgt war.

§ 17 Abs. 1 lit. a IDG
Art. 91 Abs. 5 SchKG
Art. 222 Abs. 5 SchKG

05
Bekanntgabe des Aufenthaltsorts eines Inhaftierten

Für die Bekanntgabe des Aufenthaltsortes eines Inhaftierten durch die Einwohnerkontrolle an eine Inkassofirma fehlt es an einer gesetzlichen Grundlage. Die Bekanntgabe ist nicht notwendig. Auskünfte über den Aufenthaltsort von Untersuchungshäftlingen und Strafgefangenen gehören zu den besonderen Personendaten, da über eine strafrechtliche Sanktion informiert wird. Besondere Personendaten dürfen nur an Privatpersonen bekannt gegeben werden, wenn eine hinreichend bestimmte Regelung in einem formellen Gesetz dazu ermächtigt, eine ausdrückliche Einwilligung des Betroffenen vorliegt, eine unmittelbar drohende Gefahr für Leib und Leben besteht oder der notwendige Schutz anderer wesentlicher Rechtsgüter höher zu gewichten ist.

Eine gesetzliche Grundlage war vorliegend nicht ersichtlich. Da bei Anfragen von Inkassofirmen selten eine der übrigen Voraussetzungen erfüllt ist, darf der Aufenthaltsort eines Insassen einer Strafanstalt im Normalfall nicht bekannt gegeben werden. Eine Inkassofirma kann ihre Forderung ohne Kenntnis des Aufenthaltsortes durchsetzen, da ein Schuldner am Wohnsitz zu betreiben ist.

Wenn sich ein Betreibungsamt an die Einwohnerkontrolle wendet, ist die Möglichkeit der Amtshilfe zu prüfen. Der Datenschutzbeauftragte hat sich im Tätigkeitsbericht 2005 (Seite 69ff.) zu dieser Thematik geäussert und die Zulässigkeit der Bekanntgabe des Aufenthaltsortes eines inhaftierten Schuldners an ein Betreibungsamt bejaht.

§ 3 Abs. 4 lit. a Ziff. 4 IDG
§ 17 Abs. 1 und 2 IDG
Art. 46 Abs. 1 SchKG

06
Schülerbefragung zur Unterrichtsqualität

Ein Fachlehrer einer kantonalen Berufsschule beanstandete die Art und Weise einer durchgeführten Schülerbefragung. Die Befragung zu seiner Person und seinem Unterricht wurde im Auftrag des gemeinsamen Vorgesetzten durch Arbeitskollegen des Lehrers und ohne dessen Kenntnis durchgeführt; zudem wurde dem Lehrer die Einsicht in die erhobenen Daten verweigert. Seine Kollegen hingegen erhielten Einblick in die ausgefüllten Fragebogen.
Im Bereich der Berufsfachschulen bestehen keine expliziten Rechtsgrundlagen, die Lehrer- und Unterrichtsevaluation regeln. Hingegen sind die Schulleitungen solcher Institutionen aufgrund gesetzlicher Vorgaben verpflichtet, ein schulinternes Qualitätsmanagement zu unterhalten. Das kantonale Mittelschul- und Berufsbildungsamt (MBA) begleitet und kontrolliert die dazu notwendigen Prozesse. Das MBA hält in der auf seiner Website publizierten Weisung vom Januar 2010 fest, dass jegliche Aufzeichnungen oder Äusserungen über die Ergebnisse durchgeführter Individualfeedbacks unter den Persönlichkeitsschutz fallen und nicht veröffentlicht werden dürfen.
Bei der Schülerbefragung werden Daten erhoben, die ein nicht geringes Risiko einer Persönlichkeitsverletzung für die betroffenen Lehrkräfte bergen. Die Erhebungsblätter sind deshalb mit der entsprechenden Sorgfalt auszugestalten und die einzelnen Bearbeitungsschritte durch unmissverständliche Regelungen festzuhalten. Dabei ist den Grundsätzen der Verhältnismässigkeit, Transparenz und Vertraulichkeit Beachtung zu schenken.
Vorliegend wurde aus Zeitgründen auf das standardisierte Vorgehen verzichtet. Die Schulleitung hielt den fehlbaren Vorgesetzten dazu an, die Vorgaben zur Evaluation künftig strikte einzuhalten.

§ 8 Abs. 1 BBG
§§ 3 lit. b, 12 Abs. 4 lit. d und 35 Abs. 1 lit. 3 EG BBG
§ 2 Abs. 1 VEG BBG
§§ 7 Abs. 2 lit. a, 8 Abs. 1 und 12 IDG

07
Biografische Texte von Lernenden

Schülerinnen und Schüler im ersten Lehrjahr einer Berufsschule sahen sich mit folgender biographischen Aufgabe konfrontiert: Im Rahmen eines zweiseitigen Textes mussten sie möglichst viel Persönliches aus ihrem Leben aufschreiben und den Text danach ihren Mitschülerinnen und Mitschülern zur Durchsicht und Bewertung abgeben. Eine Lehrperson äusserte Bedenken zur gestellten Aufgabe und zur Preisgabe der zum Teil sehr persönlichen Informationen. Der Datenschutzbeauftragte wurde um eine Stellungnahme gebeten. Zur Veranschaulichung erhielt er das Dokument einer Schülerin mit Beschreibung und Bebilderung des an Krebs erkrankten Bruders.
Bei der gestellten Aufgabe werden (besondere) Personendaten der Schülerinnen und Schüler bzw. ihres nahen Umfelds bearbeitet und bekannt gegeben. Für die Bekanntgabe besonderer Personendaten ist bei fehlender gesetzlicher Regelung die Einwilligung der betroffenen Person notwendig. Bereits bei der Aufgabenstellung muss also klar sein, was mit den zu verfassenden Texten geschieht und wer Kenntnis vom Inhalt erhält. Nur so können die Schreibenden kritisch abwägen, welche Informationen sie an einen grösseren Adressatenkreis bekanntgeben möchten und welche nicht. Dies auch mit Blick auf die möglicherweise ebenfalls tangierten Persönlichkeitsrechte von Drittpersonen.

Die Lehrperson muss sich bewusst sein, dass die Einwilligung der noch sehr jungen Menschen durch deren Abhängigkeitsverhältnis zu ihrer Ausbildungsstätte und deren Lehrpersonen eingeschränkt sein kann. Für die Lernenden ist es möglicherweise schwierig, sich über die persönlich zu steckenden Grenzen bei der gestellten Aufgabe klar zu werden. Es ist nicht auszuschliessen, dass relativ unreflektiert (allzu) Persönliches preisgegeben wird, sei es um den Klassenkameraden zu imponieren oder um eine gute Bewertung zu erhalten. Zur Wahrung des Grundsatzes der Verhältnismässigkeit sollte den Lernenden daher ein zweites Thema zur Auswahl gestellt werden.

§§ 17 Abs. 1 lit. a, b und 8 Abs. 1 IDG

08
Informationsplattform über Lernende

Ein Verband von überkantonal organisierten Berufsschulen plante, für sämtliche Ausbildungsverhältnisse eine internetbasierte Kommunikationsplattform für die berufliche Grundbildung einzurichten. Lernende, Lehrbetriebe, Berufsfachschulen und Anbieter von überbetrieblichen Kursen sollten einen schnellen Zugriff auf alle ausbildungsrelevanten Informationen erhalten, wie beispielsweise Prüfungsnoten, Absenzen, praktische Fähigkeiten oder das Lernverhalten der Auszubildenden.
Mit der Erfassung der Daten sämtlicher Ausbildungsverhältnisse wurde angestrebt, Ausbildungslücken der Schülerinnen und Schüler frühzeitig zu erkennen und Unterstützung anzubieten.
Der Leiter einer der vom Projekt betroffenen Berufsschulen gelangte an den Datenschutzbeauftragten mit der Bitte um Klärung der Rechtmässigkeit des Vorhabens.
Die Zusammenstellung oben erwähnter Daten erlaubt eine Beurteilung wesentlicher Aspekte der Persönlichkeit der betroffenen Personen und birgt das Risiko einer Diskriminierung oder Persönlichkeitsverletzung. Für das gemeinsame Bearbeiten und das gegenseitige Bekanntgeben dieser Daten bedarf es einer hinreichend bestimmten Regelung in einem formellen Gesetz. Vorliegend erwiesen sich die vorhandenen Rechtsgrundlagen als ungenügend. Auch aus Gründen der Verhältnismässigkeit wäre es fraglich, alle Daten der Schülerinnen und Schüler auf einer Informationsplattform zu speichern und allen Ausbildungsbeteiligten zur Verfügung zu stellen. Dies auch deshalb, weil es sogar Eltern bereits mündiger Schülerinnen und Schüler nur unter bestimmten Voraussetzungen möglich ist, Einblick in die entsprechenden Daten ihrer Kinder zu erhalten.

§§ 8 und 17 Abs. 1 lit. a IDG
Art. 16 und 21 je Abs. 5 BBG
Art. 17 Abs. 3 BBV
§§ 22 Abs. 2 und 51 Abs. 3 VEG BBG

09
Zugang zu eigenen Personendaten

Ein Mitarbeitender eines kantonalen Spitals, welcher selbst als Patient dort behandelt wurde, wollte wissen, welche anderen Mitarbeitenden auf sein Patientendossier Zugriff genommen hatten, und verlangte Einsicht in die Zugriffsprotokolle. Gleichzeitig stellte sich die Frage, ob Einträge im Patientendossier einer Berichtigung zugänglich sind und ob für die Abgabe von Kopien eine Gebühr verlangt werden kann.
Das Auskunftsrecht vermittelt den Anspruch auf Zugang zu den eige-

nen Personendaten. Zugriffsprotokolle sind Aufzeichnungen darüber, welcher Mitarbeitende zu welcher Zeit das Dossier eines bestimmten Patienten geöffnet hat. Sie gelten als Personendaten. Daher werden sie vom Auskunftsrecht des Patienten erfasst. Der Datenschutzbeauftragte hielt in seiner Stellungnahme fest, dass, wenn das Spital die Zugriffe in einer Logdatei aufzeichnet und der Einsichtnahme keine überwiegenden Interessen entgegenstehen, den Patienten auf Gesuch hin Einsicht in die Zugriffsprotokolle zu gewähren ist. Enthält das Patientendossier Auskünfte Dritter, kann die Interessenabwägung dazu führen, dass eine Patientin oder ein Patient nicht in alle Teile ihres bzw. seines Dossiers Einsicht erhält. Für die Abgabe von Kopien aus dem Patientendossier wird eine kostendeckende Gebühr erhoben. Enthält das Patientendossier Diagnosen, mit denen die Patientin oder der Patient nicht einverstanden ist, kann sie oder er verlangen, dass ein entsprechender Vermerk angebracht wird. Eine eigentliche Berichtigung erfolgt hingegen nicht.

§§ 20, 21 und 23 IDG
§ 19 Patientinnen- und Patientengesetz
§ 13 Abs. 4 Gesundheitsgesetz

10
Eigene Personendaten?

Ein ehemaliger Mitarbeitender der kantonalen Verwaltung verlangte, gestützt auf das Auskunftsrecht, Einsicht in Dokumente, welche er während seiner Tätigkeit für die Verwaltung selbst erstellt hatte.
Mitarbeitende eines öffentlichen Organs oder Behördenmitglieder bearbeiten im Rahmen ihrer Funktion Personendaten. Sie handeln dabei in ihrer Funktion als Teil des öffentlichen Organs. Der Datenschutzbeauftragte hielt daher in seiner Stellungnahme fest, dass Informationen, die Mitarbeitende eines öffentlichen Organs oder Behördenmitglieder im Rahmen ihrer Arbeitstätigkeit erstellt haben, keine eigenen Personendaten sind. Möchten ehemalige Mitarbeitende Auskunft über alle von ihnen erstellten Daten erhalten, müssen sie ein schriftliches Informationszugangsgesuch einreichen.

§§ 20, 23, 26 und 27 IDG

11
Elektronisches Personaldossier

Der Datenschutzbeauftragte prüfte im Rahmen einer Vorabkontrolle die Einführung eines elektronischen Personaldossiers unter Einbezug der Möglichkeit, dass Mitarbeitende über das Internet ihr Dossier einsehen. Die beiden Aspekte sind aus datenschutzrechtlicher Sicht gesondert zu beurteilen.
Was die Bearbeitung der Daten und insbesondere die Aufbewahrung betrifft, so ergeben sich durch das Einsetzen eines neuen technischen Hilfsmittels allein keine weiteren Anforderungen aus gesetzgeberischer Sicht. Die bestehenden Rechtsgrundlagen umfassen auch die Bearbeitung mit technischen Hilfsmitteln, sofern Datenbearbeitungen weiter innerhalb des gesetzlichen Rahmens stattfinden. Hingegen müssen technische und organisatorische Sicherheitsmassnahmen getroffen werden. Im konkreten Fall stand die elektronische Bearbeitung allerdings im Widerspruch zum noch geltenden Recht, das in der Vollzugsverordnung zum Per-

sonalgesetz festhält, dass Mitarbeiterbeurteilungen im Original zu bearbeiten resp. aufzubewahren sind. Diese Verordnung soll diesbezüglich geändert werden. Was die organisatorischen und technischen Massnahmen betrifft, so ist sicherzustellen, dass insbesondere die Vertraulichkeit und die Integrität gewährleistet sind, ein detailliertes Rollen- und Berechtigungskonzept vorliegt sowie eine Protokollierung besteht. Weiter verlangt das Bearbeiten besonderer Personendaten ein Managementsystem und eine Verschlüsselung oder eine starke Authentifizierung.
Der Zugang zu den eigenen Personendaten beinhaltet im heutigen Rechtsrahmen eine Interessenabwägung durch das öffentliche Organ, denn überwiegende öffentliche oder private Interessen können eine allumfassende Auskunft einschränken. Aus diesem Grund ist der Zugriff über das Internet auf eng begrenzte Kategorien wie Adresse und Mitarbeiterbeurteilung zu beschränken. Der direkte Zugriff darf nur auf die eigenen Daten und nicht auf Daten Dritter erfolgen. Der alle Daten umfassende Zugang kann nur im Einzelfall auf nicht elektronischem Weg oder in anderer Form, beispielsweise durch vom öffentlichen Organ freigegebene temporäre Links, wahrgenommen werden.

§ 21 lit. g Vollzugsverordnung zum Personalgesetz

12
Elektronische Verfügungen und Rechnungen

Ein öffentliches Organ möchte den Bürgerinnen und Bürgern die elektronische Rechnungsstellung (E-Rechnung) anbieten. Dabei soll ein Portal eines Finanzinstituts eingesetzt werden, auf dem der gesamte Prozess elektronisch abgewickelt wird, so dass Zustellungen auf dem Postweg komplett entfallen.
Solche E-Rechnungen werden heute zunehmend eingesetzt. Im staatlichen Bereich ist jedoch zu beachten, dass nicht nur Rechnungen, sondern auch Verfügungen versandt werden. Zudem können die übermittelten Daten besonderen Geheimhaltungsbestimmungen wie dem Steuergeheimnis unterstehen. Im konkreten Projekt wies der Datenschutzbeauftragte auf die zu beachtenden rechtlichen und vertraglichen Rahmenbedingungen hin.
Die elektronische Zustellung und Rechnungsstellung ist nur auf Wunsch des Bürgers oder der Bürgerin, das heisst mit seiner bzw. ihrer schriftlichen Einwilligung, vorzunehmen. Wer nicht einwilligt, bleibt bei der Zustellung per Post und darf keine Nachteile erleiden; so darf die Wahlfreiheit nicht durch Gebühren eingeschränkt werden. Aus dem Einwilligungsformular müssen die geplanten Datenbekanntgaben an die beteiligten Finanzinstitute klar ersichtlich sein. Die Einwilligung kann jederzeit widerrufen werden. Das öffentliche Organ muss sicherstellen, dass das Finanzinstitut die Daten nicht auswertet oder ins Ausland übermittelt. Im beurteilten Fall wird beabsichtigt, mit dem Finanzinstitut eine schriftliche Vereinbarung abzuschliessen, die diese Garantien festhält. Das öffentliche Organ muss die Vereinbarung von der vorgesetzten Stelle genehmigen lassen, wenn es sich um sensible Daten handelt.
Öffentliche Organe stellen auch Verfügungen zu, gegen die der Bürger oder die Bürgerin Einsprache erheben kann. Das anwendbare Verfahrensrecht bezieht sich auf den herkömmlichen Postweg; so dass die elektronische Zustellung rechtlich nicht klar geregelt ist. Im beurteilten Projekt wird beabsichtigt, eine Verordnung zu erlassen, welche die Wirkungen der elektronischen Zustellung regelt. Festzulegen sind beispielsweise die regelmässige Leerung des Postfachs und der Zeitpunkt, in dem die Einsprachefrist zu laufen beginnt. Für die Übertragungssicherheit müssen elektronische Signaturen und eine verschlüsselte Übermittlung zum Einsatz kommen.

13
Abgrenzung von Drittangeboten auf Websites

Eine Gemeinde beauftragte einen privaten Dienstleister mit der Betreuung von Inhalten auf ihrer Website. Die Öffentlichkeit sollte über möglichst aktuelle Freizeit-, Kultur- und andere Angebote in der Region informiert werden. Zur Umsetzung des Auftrags war vorgesehen, dass der Dienstleister Inhalte seiner eigenen Website über ein sogenanntes iFrame (eine Art Website in der Website) direkt in den Webauftritt der Gemeinde integriert.
Ein Besucher der gemeindeeigenen Website wird je nach Surfverhalten auf die Website des Dienstleisters gelenkt und gibt dabei automatisch seine IP-Adresse bekannt. Gemäss bundesgerichtlicher Rechtsprechung können IP-Adressen nach Prüfung der tatsächlichen Verhältnisse als Personendaten qualifiziert werden.
Auch wenn ein öffentliches Organ seine gesetzlichen Aufgaben an Dritte auslagert, bleibt es für den Umgang mit den Informationen verantwortlich. Mit dem Dienstleister ist ein schriftlicher Vertrag nach den gesetzlichen Vorgaben abzuschliessen.
Der Datenschutzbeauftragte wies die Gemeinde an, mittels einer Vereinbarung sicherzustellen, dass die IP-Adressen ausschliesslich zwecks Aufrechterhaltung und Erbringung des technischen Betriebs bearbeitet werden und die Verknüpfung mit anderen Daten ausgeschlossen wird. Im Sinne des Zweckbindungsgebotes müssen die Verantwortlichen technisch sicherstellen, dass keine Cookies zum Einsatz kommen. Aus Gründen der Transparenz wurde weiter empfohlen, die Abgrenzung zwischen dem Angebot der Gemeinde einerseits und jenem des Dienstleisters andererseits für die Nutzerinnen und Nutzer auf der Website besser sichtbar zu machen.

§§ 6 IDG i.V.m. 25 IDV und 9 IDG

14
Auslagerung von Datenbearbeitungen

Ein öffentliches Organ erkundigte sich beim Datenschutzbeauftragten, ob und wenn ja unter welchen Voraussetzungen es einen Dritten mit einer Datenbearbeitung beauftragen darf, wenn dieser bei der Erfüllung des Auftrages seinerseits die Dienste einer im Ausland domizilierten Firma in Anspruch nimmt.
Öffentliche Organe können Informationen durch Dritte bearbeiten lassen, wenn keine rechtlichen Bestimmungen, wie beispielsweise das Berufsgeheimnis oder vertragliche Vereinbarungen, entgegenstehen.
Aufträge betreffend eine Auslagerung, welche das Bearbeiten von Personendaten beinhalten, müssen in schriftlicher Form und mit einem definierten minimalen Inhalt erfolgen. Je sensitiver die Daten sind, desto umfassender müssen die Informationssicherheitsmassnahmen sein und desto detaillierter muss der Vertrag ausgestaltet sein. Weiter gelten die allgemeinen datenschutzrechtlichen Grundsätze. Es sind also auch Massnahmen zu prüfen, mit denen die Weitergabe von Daten vermieden oder diese anonymisiert resp. pseudonymisiert werden können. Das Amtsgeheimnis steht grundsätzlich einer Auslagerung nicht entgegen. Es ist aber in jedem Einzelfall zu prüfen, wie weit die Schweigepflicht geht, etwa im Falle von absoluten Schweigepflichten. Die Geheimhaltungspflichten sind stets Vertragsbestandteil.
Das öffentliche Organ als Auftraggeber bleibt auch bei der Auslage-

rung von Datenbearbeitungen für diese verantwortlich. Analog zur Haftung des Geschäftsherrn hat es die Sorgfaltspflichten in Bezug auf Auswahl, Instruktion und Kontrolle des Auftragnehmenden zu beachten. Dieser darf die Daten nur so bearbeiten, wie es das ihn beauftragende öffentliche Organ auch dürfte.
Nicht grundsätzlich ausgeschlossen ist, dass der Auftragnehmende seinerseits die Datenbearbeitung an einen Dritten auslagert. Ein solches Double-Outsourcing führt aber zu erhöhten Risiken in Bezug auf Verfügbarkeit, Integrität und Vertraulichkeit. Die Kontrollpflicht des öffentlichen Organs als Auftraggeber könnte erschwert werden. Diesem Punkt ist im Vertrag und auch in der Praxis besondere Beachtung zu schenken. Unterauftragsverhältnisse dürfen nur mit ausdrücklicher schriftlicher Genehmigung des originären Auftraggebers erfolgen.
Bei einer Auslagerung von Datenbearbeitungen ins Ausland entstehen höhere Risiken. Dabei muss sichergestellt sein, dass im Empfängerstaat ein angemessener Schutz für die Datenübermittlung gewährleistet ist und vom auslagernden öffentlichen Organ angemessene vertragliche Sicherheitsvorkehrungen getroffen wurden.

§ 6 IDG
§ 19 IDG
§ 25 IDV
Art. 55 OR

15
Live-Übertragungen von Medienkonferenzen

Im Berichtsjahr wurden erstmals Medienkonferenzen des Regierungsrates via Live-Stream ins Internet übertragen. Auf den Aufnahmen waren auch Medienschaffende sowie weitere anwesende Personen zu sehen. Ein teilnehmender Journalist war damit nicht einverstanden und gelangte an den Datenschutzbeauftragten.
Die Live-Übertragung von Medienkonferenzen ist ein geeignetes Mittel, um die Informationsansprüche der Bevölkerung zu erfüllen und dem Transparenzprinzip gemäss Artikel 49 der Kantonsverfassung gerecht zu werden. Sie lässt sich auf entsprechende im Organisationsgesetz definierte Aufgaben und auf die Leitlinien zur Information und Kommunikation abstützen, wonach der Regierungsrat frühzeitig, aktiv und umfassend informiert und dem Internet als Kommunikationsmittel zunehmende Bedeutung zukommt.
Der Datenschutzbeauftragte erachtet die Live-Übertragung von Medienkonferenzen grundsätzlich als zulässig. Dem Willen einzelner Personen, nicht Teil der Aufzeichnung/Übertragung sein zu wollen, ist jedoch Rechnung zu tragen. Teilnehmende Medienschaffende und Gäste müssen die Möglichkeit haben, sich mittels eines Opting-out einer solchen Aufzeichnung/Übertragung zu entziehen. Sie sind vorgängig darüber zu informieren, dass die Medienkonferenz live übertragen wird. Weiter ist ihnen die Möglichkeit zu geben, sich an einem Platz aufzuhalten, wohin keine Kameras gerichtet werden. Wenn eine teilnehmende Person eine Frage stellt oder eine Bemerkung macht und dabei nicht aufgezeichnet werden möchte, ist dies zu respektieren, und Kameras und Mikrofone sind entsprechend auszuschalten bzw. nicht auf diese Person zu richten. Soll die Frage oder Bemerkung dennoch Eingang in die Aufzeichnung/Übertragung finden, kann sie von der Regierungsrätin, dem Amtschef oder der Kommunikationsbeauftragten wiederholt werden.

16
Aktenbeizug für parlamentarische Oberaufsicht

Der Kantonsrat übt die Oberaufsicht über die kantonalen öffentlichen Organe aus. Im Rahmen von Abklärungen strebte die zuständige Aufsichtskommission des Kantonsrates den Beizug von Akten an und gelangte mit der Frage an den Datenschutzbeauftragten, wie weit sie Akten ohne Zustimmung betroffener Personen erhalten könne.

Aus datenschutzrechtlicher Sicht handelt es sich beim Aktenbeizug um eine Datenbekanntgabe, die sich im vorliegenden Fall auf eine Grundlage im Kantonsratsgesetz abstützen lässt. Dadurch wird die Aufsichtskommission ermächtigt, beim zuständigen Organ die Herausgabe aller mit der Beurteilung des Finanzhaushaltes beziehungsweise der Geschäftsführung in Zusammenhang stehenden Amtsakten zu verlangen. Eine Zustimmung betroffener Personen ist nicht notwendig. Das angefragte Organ ist gemäss den allgemeinen Regeln des IDG allerdings verpflichtet, eine Interessenabwägung vorzunehmen. Gemäss dem Kantonsratsgesetz kann das Organ die Aktenherausgabe verweigern, soweit dies zur Wahrung schutzwürdiger privater Interessen, zum Schutz der Persönlichkeit oder aus Rücksicht auf ein hängiges justizförmiges Verfahren unerlässlich ist. Stattdessen hat es einen besonderen Bericht zu erstatten. Die Aufsichtskommission hat demnach einen Anspruch auf Aktenherausgabe oder, im Falle überwiegender entgegenstehender Interessen, mindestens einen Anspruch auf einen besonderen Bericht.

§§ 17 und 23 IDG, § 34e KRG

17
Bezug von Fischerei- und Jagdbewilligungen über das Internet

Die kantonale Fischerei- und Jagdverwaltung (FJV) betreibt ein Online-System zur Verwaltung von Jagd- und Fischereibewilligungen. Sie plante eine Nachfolgelösung und fragte den Datenschutzbeauftragten an, welche datenschutzrelevanten Massnahmen zu treffen seien.

Das System wird gemeinsam mit anderen Kantonen entwickelt, soll aber für den Kanton Zürich separat betrieben werden. Es soll den Jägern und Fischern beispielsweise erlauben, Tagesbewilligungen über das Internet zu kaufen.

Der Datenschutzbeauftragte liess sich das bestehende und das geplante System durch die Verantwortlichen erklären und vor Ort demonstrieren. Zudem erhielt er Einsicht in die Dokumentation der Nachfolgelösung und des Ausschreibungsverfahrens. Aufgrund der Angaben der FJV waren keine Hinweise auf besondere datenschutzrechtliche Risiken erkennbar.

Bei den bearbeiteten Daten handelt es sich überwiegend um Sachdaten sowie gewöhnliche Personendaten. Erfasst werden die Personalien der Jäger und Fischer sowie die Voraussetzungen für deren Zulassung. Dabei wird ein abgestuftes Zugriffs- und Rollenkonzept zugrundegelegt, unter anderem mit einer Beschränkung auf einzelne Reviere.

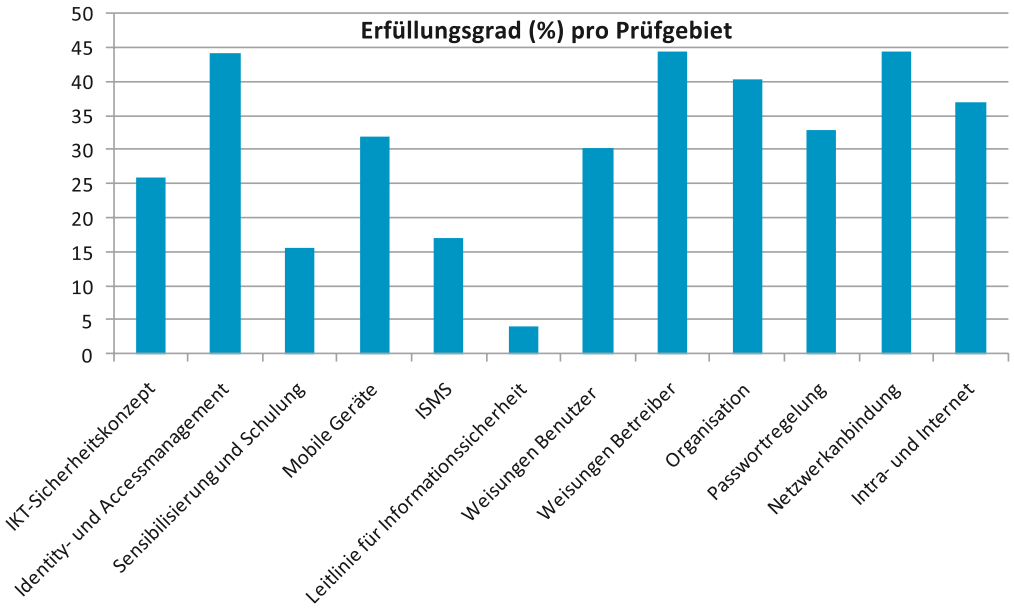
Eine erhöhte Sensibilität ergab sich im Zusammenhang mit der Sperrung von Personen, die wegen Nichtbezahlung, eines Gerichtsurteils oder administrativer Massnahmen keine Bewilligungen erhalten. Nähere Abklärungen haben ergeben, dass die Sperrgründe im System bloss stichwortartig erfasst werden und dies für Aussenstehende nicht ersichtlich ist. Heikle Daten werden ausserhalb des Systems gehalten. Die Datenbearbeitungen im Zusammenhang mit den Sperrungen erwiesen sich als verhältnismässig.

Systematische Auswertung der Kontrollresultate

Eine detaillierte Auswertung der Kontrollresultate ergibt klare Aussagen zur Umsetzung der wichtigsten Massnahmen für die Informationssicherheit der kantonalen Verwaltung, der Gemeinden und der übrigen öffentlichen Organe.

Das IDG fordert von den öffentlichen Organen das Umsetzen von angemessenen organisatorischen und technischen Massnahmen zum Schutz der Informationen. Diese sind den neuen Technologien und Dienstleistungen anzupassen.
Der Datenschutzbeauftragte hat die wichtigsten Prüfkriterien im Bereich Informationssicherheit definiert und seine Kontrolltätigkeit fokussiert. Zu diesen Kriterien gehören ein Sicherheitskonzept, ein Identity- und Accessmanagement, die Planung und Durchführung von Sensibilisierungsmassnahmen sowie Vorkehrungen zur Sicherheit von mobilen Arbeitsplätzen und Datenträgern. Öffentliche Organe, die der Sicherheitsstufe 3 nach Informationssicherheitsverordnung (höchstes Risiko bezüglich sensibler Daten) zugeordnet sind, müssen zusätzlich ein Managementsystem für Informationssicherheit (ISMS) einrichten.

Erfüllungsgrad pro Prüfgebiet



Die Resultate zeigen, dass die zentralen Massnahmen für die sichere Bearbeitung der Daten noch nicht den gesetzlichen Anforderungen entsprechend umgesetzt wurden. Bei den fünf wichtigsten Prüfgebieten wurde ein durchschnittlicher Umsetzungsgrad von 24 Prozent erreicht. Über alle Prüfgebiete war es ein Wert von 42 Prozent Die drei öffentlichen Organe mit dem besten Prüfungsresultat erreichten einen durchschnittlichen Erfüllungsgrad von 55 Prozent die drei schlechtesten einen solchen von 28 Prozent.
Als eine der Hauptursachen für diese mangelnde Umsetzung konnte das Fehlen eines Sicherheitsverantwortlichen im Bereich Informatik eruiert werden. Dieser ist für den korrekten Informationsfluss und die Ressourcenzuteilung zur Behebung der Schwachstellen verantwortlich.
Die Umsetzung der Sicherheitsmassnahmen für die Gemeinden wird neu durch Leitfäden und Hilfestellungen des Datenschutzbeauftragten erleichtert.

§ 7 IDG
§ 8 ISV

Aufsicht im Bereich des Staatsschutzes

Die nach durchgeführter Kontrolle des Staatsschutzes noch offenen Fragen wurden seitens der Kantonspolizei mit Blick auf die datenschutzrechtlichen Anforderungen grösstenteils zufriedenstellend beantwortet. Dennoch bleibt ein Unbehagen mit Blick auf die unklare Regelung der Aufsicht.

Die Kontrolltätigkeit des Datenschutzbeauftragten beschränkt sich auf das Einhalten der datenschutzrechtlichen Bestimmungen im Rahmen der Datenbearbeitungen und der vom Gesetz geforderten angemessenen organisatorischen und technischen Massnahmen im Bereich der nformationssicherheit. Der Datenschutzbeauftragte gibt dem geprüften Organ eine Stellungnahme respektive einen Prüfbericht ab. Er kann Empfehlungen aussprechen und auf Massnahmen hinweisen, welche es dem kontrollierten öffentlichen Organ erlauben, Schwachstellen zu minimieren. Die im Prüfbericht festgehaltenen Hinweise und Bemerkungen wurden durch die Kantonspolizei zum grossen Teil bereinigt. Nicht abschliessend beantwortet wurden allerdings Fragen wie beispielsweise diejenige in Bezug auf die Kontrolle der Löschung der elektronischen Daten.

Weiterhin offene Punkte

Offen und nicht zufriedenstellend ist nach wie vor die Rechtslage im Hinblick auf die kantonale Aufsichtstätigkeit. Neue Bestimmungen regeln zwar die Dienstaufsicht. Ob, durch wen und wie diese wahrgenommen wird, wirft aber immer noch Fragen auf. Die rechtliche Einschränkung der Einsichtnahme durch die kantonalen Kontrollorgane trägt wesentlich zur unbefriedigenden Lage bei.
Ebenfalls nicht geklärt wurden im Rahmen der neuen Bestimmungen die Kompetenzen der Datenschutzbeauftragten. So behindern die unterschiedlichen Rechtsauffassungen nach wie vor eine uneingeschränkte und unabhängige Kontrolltätigkeit.

§ 34 lit. c IDG
§ 7 IDG
Art. 35, 35a Verordnung über den Nachrichtendienst des Bundes

Informationssicherheit in Gemeinden

Die durchgeführten Kontrollen haben gezeigt, dass in vielen Gemeinden gleiche Mängel im Bereich Informationssicherheit bestehen. Dies hat den Datenschutzbeauftragten veranlasst, diverse Hilfestellungen für die Gemeinden zu erstellen.

Im Berichtsjahr bildete die Kontrolle der Informationssicherheit in den Gemeinden einen Arbeitsschwerpunkt des Datenschutzbeauftragten. Dabei wurden diverse Aspekte anhand einer Schwachstellenanalyse überprüft. Es hat sich gezeigt, dass bei vielen Gemeinden dieselben Schwachstellen in der Informationssicherheit bestehen und die Ressourcen zur Schliessung der Sicherheitslücken nicht vorhanden sind. Einerseits fehlen Grundlagendokumente wie beispielsweise ein Sicherheitskonzept, andererseits werden Massnahmen im organisatorischen und im technischen Bereich wie etwa die Regelung und Umsetzung des Passwortgebrauchs, nicht oder nur mangelhaft umgesetzt.

Hilfestellungen für Gemeinden publiziert

Um den Aufwand für die Gemeinden zu minimieren, stellt der Datenschutzbeauftragte diverse Anleitungen, Vorlagen, Beispiele und Checklisten zur Verfügung. Diese erleichtern die Umsetzung der gesetzlichen Anforderungen an die Informationssicherheit.
Je nach Art der Vorlage wurden diese bereits an die spezifischen Bedürfnisse der Gemeinde angepasst.
Die Dokumente (Einführung und Übersicht, Leitlinie zur Informationssicherheit, Aufbau Organisationsstruktur Informationssicherheit, Rollen- und Berechtigungskonzept, Weisung Informationssicherheit, Sensibilisierung der Mitarbeitenden für Informationssicherheit, Glossar und Abkürzungen Informationssicherheit usw.) richten sich hauptsächlich an mittelgrosse Gemeinden mit rund 4000 Einwohnerinnen und Einwohnern. Teilbereiche der Dokumentation können – mit geringen Anpassungen – auch von grösseren und kleineren Gemeinden genutzt werden.
Zusätzlich hat der Datenschutzbeauftragte ein Modell erstellt, das auf dem Grundschutztool des Deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI) basiert. Dieses enthält ein Inventar, eine Schutzbedarfsfeststellung und einen Massnahmenkatalog für mittelgrosse Gemeinden. Damit lässt sich relativ einfach ein Sicherheitskonzept erstellen.

Support für kleinere Gemeinden geplant

Die Informationssicherheit in kleineren Gemeinden mit rund 1000 Einwohnerinnen und Einwohnern muss – aufgrund des geringeren Risikos – anders angepackt werden. Um diesem Sachverhalt gerecht zu werden, wird der Datenschutzbeauftragte entsprechend angepasste Hilfestellungen publizieren.

Kontrolle der Registerharmonisierung

Die Direktion der Justiz und des Innern beauftragte die Schweizerische Post, die Erstzuweisung des eidgenössischen Wohnungsidentifikators im Rahmen der Registerharmonisierung vorzunehmen. Der Datenschutzbeauftragte kontrollierte das Einhalten des Dienstleistungsvertrags.

Das für die Volkszählung lancierte Projekt der Registerharmonisierung beinhaltete die Harmonisierung der Einwohnerregister, der Personenregister des Bundes sowie des eidgenössischen Gebäude- und Wohnungsregisters. An der Zuweisung des eidgenössischen Wohnungsidentifikators waren im Kanton Zürich das Statistische Amt als Vertreterin der Direktion der Justiz und des Innern sowie Gemeinden, Grundeigentümer und Liegenschaftenverwaltungen beteiligt. Seitens der Auftragnehmerin waren dies die Swiss Post Solutions AG und die Schweizerische Post. Der Schwerpunkt der Leistung der Swiss Post Solutions AG lag in der Beschaffung der Wohnungs- und Bewohnerlisten, im Abgleich der Daten mit jenen aus den Gebäude- und Einwohnerregistern sowie in der Rücklieferung der konsolidierten Daten.
Kontrolliert wurden ausgewählte rechtliche, organisatorische und technische Aspekte, wie die erfolgten Datenflüsse zwischen dem Statistischen Amt und der Swiss Post Solutions AG. Aber auch die damit verbundenen Massnahmen in den Bereichen Organisation und Technik beim Statistischen Amt und bei der Swiss Post Solutions AG und, soweit sie in Anspruch genommen wurden, auch die Rechenzentrumsdienste der Schweizerischen Post.

Keine wesentlichen Beanstandungen

Zusammenfassend ist festzuhalten, dass keine gravierenden Mängel festgestellt wurden. Mittels Stichproben wurde die Vorgehensweise der Postboten, die teilweise Daten im Rahmen einer Gebäudebegehung bearbeiteten, auf ihre Verhältnismässigkeit überprüft. Es zeigte sich, dass die hierzu ausgehändigten Listen nur so viele Daten wie nötig enthielten. Weiter wurden die Postboten vorgängig bezüglich Klassifizierung und Handhabung der Daten sensibilisiert. Auch die Auswertung der vom Datenschutzbeauftragten initiierten Umfrage bei 20 zufällig ausgewählten Gemeinden ergab weder Anhaltspunkte für eine unverhältnismässige oder zweckwidrige Datenbearbeitung noch solche für eine Verletzung der Geheimhaltungsvorschriften. Einzig die Verantwortlichkeit für das Beantworten eventueller Auskunftsersuchen betroffener Personen konnte nicht klar zugewiesen werden.
Im organisatorischen und im technischen Bereich wurde darauf hingewiesen, dass bei der Datenbearbeitung festgestellte Sicherheitslücken nur teilweise geschlossen wurden und deren Überprüfung durch die Auftraggeberin zu spät erfolgte. Das Identity- und Accessmanagement zeigte Verbesserungspotenzial, indem das Rollen- und Berechtigungskonzept verfeinert werden musste. Die Kontrolle der Löschung aller Daten bei Projektabschluss gab seitens des Datenschutzbeauftragten zu keinen Bemerkungen Anlass.

§ 20 Abs. 2 IDG

Stellungnahmen zu Gesetzesvorhaben

In Gesetzesvorhaben werden die Grundlagen für die konkreten Datenbearbeitungen der Verwaltung gelegt. Sensitive Datenbearbeitungen stehen vermehrt im Fokus.

Für die Erfüllung der meisten Staatsaufgaben werden Daten über betroffene Personen bearbeitet. Das Bearbeiten von Daten über eine Person stellt einen Eingriff in eine grundrechtlich geschützte Position dar, es bedarf deshalb immer einer gesetzlichen Grundlage und muss verhältnismässig sein. Es ist Aufgabe des Gesetzgebers, die notwendigen gesetzlichen Grundlagen zu schaffen, damit der Staat diejenigen Daten beschaffen und bearbeiten darf, die zur Erfüllung der im öffentlichen Interesse liegenden Aufgaben geeignet und erforderlich sind.

Genauso wie klar sein muss, welche Gebühren in welchen Fällen auferlegt werden dürfen oder welche Verfahrensrechte einer betroffenen Person zukommen, muss durch gesetzliche Grundlagen transparent werden, in welchen Fällen eine betroffene Person damit rechnen muss, dass Daten über sie bearbeitet werden. Selbst im Umfeld von weniger bekannten Staatsaufgaben wie Statistik, Archivwesen usw. kommt es zu Datenbearbeitungen. Um sicherzustellen, dass das Gesetz angemessene und transparente Datenbearbeitungsbestimmungen enthält, ist der Datenschutzbeauftragte bei Gesetzgebungsvorhaben einzubeziehen – spätestens in der Vernehmlassung.

Schwerpunkte im Gesundheits- und im Polizeiwesen

Der Datenschutzbeauftragte hat sich im Berichtsjahr zu verschiedenen Gesetzesvorhaben geäussert. Im Vordergrund standen entsprechend den Entwicklungsschwerpunkten im Konsolidierten Entwicklungs- und Finanzplan (KEF) Bereiche mit sensiblen Datenbearbeitungen, etwa das Gesundheits- oder das Polizeiwesen. Infolge eines Bundesgerichtsurteils musste das Polizeigesetz teilrevidiert werden (siehe auch Seite 34). Die Gesundheitsdirektion hat 2012 eine kantonale Verordnung zum Krebsregister ausgearbeitet, und auf Bundesebene wurde ein Entwurf für ein Gesetz über das elektronische Patientendossier vorgelegt (siehe auch Seite 36). Die Statistik soll mit einem kantonalen Statistikgesetz ausreichende gesetzliche Grundlagen erhalten, und das kantonale Gemeindegesetz, das in die Jahre gekommen ist, soll mittels Totalrevision modernisiert werden (siehe auch Seite 36). Zu diesen und weiteren Vorhaben hat der Datenschutzbeauftragte im Berichtsjahr eine Stellungnahme abgegeben.

Der Datenschutzbeauftragte hat 2011 unter anderem zu folgenden Gesetzgebungsprojekten Stellung bezogen:

Kanton

- Anpassung des kantonalen Rechts an die Änderung des Zivilgesetzbuches (Entwurf für ein Einführungsgesetz zum Kindes- und Erwachsenenschutzrecht)
- Revision Polizeigesetz
- Statistikgesetz
- Gemeindegesetz
- Krebsregisterverordnung
- Verordnungen zum Kinder- und Jugendhilfegesetz
- Verordnungen zum Geoinformationsgesetz
- Gesetz über den Beitritt zum Konkordat über Sicherheitsdienstleistungen
- Änderung Archivgesetz

Bund

- Anhörung zum E-Health-Teilprojekt «Öffentliches Gesundheitsportal»
- Teilrevision Betäubungsmittelgesetz
- Änderung der Bundesverfassung, des Strafgesetzbuches, des Militärstrafgesetzes und des Jugendstrafgesetzes (Tätigkeitsverbot sowie Kontakt- und Rayonverbot)
- Direkter Gegenentwurf zur Volksinitiative «Ja zur Hausarztmedizin»
- Änderung des Nationalstrassenabgabegesetzes (E-Vignette)
- Änderung ZEMIS-Verordnung
- E-Health Suisse, Standards und Architektur, Anhörung zu den Empfehlungen III (Personenidentifikation und Berechtigungssystem)
- Genehmigung und Umsetzung des Übereinkommens des Europarates zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch (Lanzarote-Konvention)
- Bundesgesetz über das elektronische Patientendossier

Personenkontrollen und Überwachungsmassnahmen

Eine Teilrevision des Polizeirechts wurde in die Vernehmlassung gegeben. Im Mittelpunkt der datenschutzrechtlichen Beurteilung standen die Überwachungsmassnahmen.

Auslöser der Teilrevision des kantonalen Polizeirechts waren der Bundesgerichtsentscheid in Bezug auf die ungenügende Bestimmtheit der Regelung der Videoüberwachung im Polizeigesetz, das Inkrafttreten der eidgenössischen Strafprozessordnung sowie der Beitritt des Kantons Zürich zum Konkordat über die computergestützte Zusammenarbeit der Kantone bei der Aufklärung von Gewaltdelikten. In der Vernehmlassung hielt der Datenschutzbeauftragte fest, dass in diesen Bereichen mit grossem Verletzungspotenzial für die Persönlichkeitsrechte dem Erfordernis einer hinreichend bestimmten gesetzlichen Grundlage sowie dem Verhältnismässigkeitsprinzip besondere Bedeutung zukommt.
Drei Bereiche standen im Mittelpunkt der datenschutzrechtlichen Beurteilung: die Personenkontrolle in Hotels und Beherbergungsbetrieben, die Überwachungsmassnahmen und die formellgesetzliche Regelung der POLIS-Datenbank.
Die geplante Regelung des automatisierten, systematisierten Abgleichs aller Hotelgäste mit dem Schengener Informationssystem (SIS) entspricht nicht den Vorgaben des Schengener Durchführungsübereinkommens. Die Verwendungszwecke der im SIS erfassten Daten sind mit den Zwecken, zu welchen die Daten der ausländischen Hotelgäste erfasst werden, nicht identisch. Weiter muss eine solche Regelung des Abgleichs mit dem nationalen Fahndungsbestand (Ripol) so gestaltet werden, dass die Eingriffe in die Persönlichkeitsrechte der Betroffenen möglichst gering sind. Das heisst, dass die Abfrage auf eine bestimmte Schwere von Delikten zu beschränken ist und die Daten derjenigen Personen, gegen die kein Verdacht vorliegt, also die «No Hits», bei der Polizei sofort zu löschen sind.
Die Überwachungsmassnahmen, wie Videoüberwachung, Observation und technische Überwachung bei Grossveranstaltungen, sind so zu regeln, dass eine Zweck-Mittel-Relation überprüft werden kann. Präzise Regelungen beinhalten Faktoren, beispielsweise wann eine personenbezogene Auswertung erfolgen kann oder bei welcher Schwere von Delikten solche Massnahmen eingesetzt werden dürfen. Eine zeitliche Begrenzung sowie eine angemessene Bewilligungsinstanz sind vorzusehen.
Die Art der Überwachungen muss präzise aufgeführt sein, die Abgrenzungen zu anderen Einsatzmitteln müssen klar und die Einsätze selbst den Erfordernissen angemessen abgestuft sein.
Die Regelung des Datenbearbeitungs- und Informationssystems POLIS auf formell-gesetzlicher Stufe muss mindestens das verantwortliche Organ, den Zweck, Online-Zugriffe sowie die Aufbewahrung und die Löschung von Daten enthalten. Alles Weitere, wie die Datenkategorien, die Datenbekanntgabe sowie organisatorische und technische Massnahmen, kann in der Verordnung festgehalten werden.

Unklare Regelung des Krebsregisters

Der Kanton Zürich führt ein Krebsregister, in dem Angaben über krebskranke Menschen gesammelt werden. Für den Umgang mit solchen besonderen Personendaten schreibt das IDG zwingend eine Grundlage in einem formellen Gesetz vor. Heute beruht das Krebsregister auf einem Regierungsratsbeschluss. Aufgrund der Übergangsbestimmungen des IDG sind Datenbearbeitungen ohne formellgesetzliche Grundlagen nur noch bis Ende September 2013 zulässig. In der Vernehmlassung wies der Datenschutzbeauftragte darauf hin, dass die präsentierte Verordnung kein formelles Gesetz und daher keine hinreichende Rechtsgrundlage für das Krebsregister ist.
Im Weiteren bemängelte der Datenschutzbeauftragte die vorgeschlagene Verordnung auch dahingehend, dass das Krebsregister Angaben über alle Einwohnerinnen und Einwohner des Kantons Zürich erhalten soll. Dies ist unverhältnismässig, weil im Krebsregister bloss ein kleiner Teil der Einwohnerinnen und Einwohner erfasst wird. Ungeklärt ist schliesslich das Verhältnis der vorgeschlagenen kantonalen Verordnung zum Bundesgesetz über die Forschung am Menschen. Mit Inkrafttreten des Bundesgesetzes Mitte 2013 werden entgegenstehende kantonale Regeln nämlich ungültig.

Statistikidentifikator notwendig

Im Rahmen der Vernehmlassung zum Statistikgesetz hat sich der Datenschutzbeauftragte für einen datenschutzfreundlichen Statistikidentifikator ausgesprochen. Der Gesetzesentwurf sieht den Einsatz der Sozialversicherungsnummer vor. Aufgrund der weiten Verbreitung dieser Nummer ist ein statistischer Datensatz, der Sozialversicherungsnummern enthält, nicht missbrauchssicher. Es ist sehr leicht, die betroffenen Personen zu identifizieren und die statistischen Angaben mit weiteren Datenbanken zu verknüpfen. Die fehlende Anonymisierung weckt zudem die Begehrlichkeit anderer Behörden, bei den Statistikorganen Daten zu beziehen und diese für andere Zwecke zu verwenden. Solche Zweckänderungen sind nur auszuschliessen, wenn ein anonymer, nicht rückführbarer Identifikator verwendet wird. Es ist daher zwingend ein Identifikator zu wählen, der zwar die Verknüpfung von Datensätzen ermöglicht, eine Identifizierung der betroffenen Person jedoch ausschliesst. Die Anonymisierung des Identifikators ist derart wichtig, dass sie im Statistikgesetz ausdrücklich erwähnt werden muss.

Regelung der Online-Zugriffe

Die Vorlage zur Revision des Gemeindegesetzes gab zu Bemerkungen in Bezug auf die Verbesserung der Rechtsgrundlagen für die elektronische Abfrage von Daten Anlass. Zum einen sollen die an der finanztechnischen Prüfung beteiligten Personen besondere Personendaten und Steuerdaten elektronisch abrufen können. Diese Absicht lässt sich dem Gesetzestext aber nicht entnehmen. Eine hinreichend bestimmte Gesetzesgrundlage muss das elektronische Abrufverfahren ausdrücklich als solches bezeichnen, die Kategorien der Personendaten nennen sowie den Verwendungszweck umschreiben. Neben der vorgesehenen Geheimhaltungspflicht und der Zugriffskontrolle sollte der elektronische Zugriff zudem auf eine bestimmte Zeitdauer eingeschränkt werden (beispielsweise Gewährung nur für die Dauer der Prüfung, höchstens aber für 3 Monate).
Ebenfalls zu präzisieren sind die Anforderungen an die Rechtsgrundlage für den Online-Zugriff auf das Einwohnerregister. Im vorgeschlagenen Gesetz über die Einwohnerkontrolle ist transparent zu machen, dass ein dauerhafter elektronischer Zugriff auf das Einwohnerregister möglich ist. Die rechtliche Bestimmung sollte die zum Zugriff berechtigte Behörde, den Zweck des Zugriffs, die für den Zugriff freigegebenen Datenkategorien sowie geeignete Sicherheitsmassnahmen, Kontrollen und Sanktionen regeln.

Freiwilliges elektronisches Patientendossier

Der Bund gab einen Entwurf für ein neues Bundesgesetz über das elektronische Patientendossier (EPD) in die Vernehmlassung. Der Datenschutzbeauftragte nahm im internen Mitberichtsverfahren zu Handen der Gesundheitsdirektion Stellung.
Abgesehen von der Frage, ob der Bund überhaupt eine ausreichende Verfassungskompetenz zur Legiferierung in diesem Bereich hat, stellte sich insbesondere die Frage nach der Freiwilligkeit. Das Konzept, dass das EPD für die Patientinnen und Patienten freiwillig sein soll, war zu begrüssen. Absehbar ist, dass die Versicherer künftig Versicherungsmodelle anbieten werden, die Anreize enthalten, ein EPD einzurichten. Der Datenschutzbeauftragte forderte daher, zu prüfen, wie einem faktischen Zwang zur Teilnahme entgegengewirkt werden kann; auch müsse eine mehrstufige Einwilligung gewährleistet sein: für die Errichtung des EPD, für die Aufnahme der einzelnen Daten ins EPD sowie bezüglich der einzelnen Zugriffsrechte. Darüber hinaus wies der Datenschutzbeauftragte auf verschiedene weitere ungeklärte Fragen hin und empfahl, auf die Verwendung der Sozialversicherungsnummer (AHVN13) als Patientenidentifikator zu verzichten.

Relaunch des Webauftritts im Fokus

Im Zentrum der Informationstätigkeit des Datenschutzbeauftragten standen 2011 die Integration des Webauftritts in das kantonale Internetportal sowie die Bearbeitung von zahlreichen Medienanfragen.

Wie bereits in den Vorjahren lud der Datenschutzbeauftragte die Medien im April 2011 zur Jahrespressekonferenz ein. Im Zentrum der Ausführungen stand dabei der Schutz des Patienten- und Arztgeheimnisses, das immer stärker unter Druck gerät. Mit der zunehmenden Anzahl Stakeholder im Gesundheitswesen, die heute von kantonalen und kommunalen Behörden über öffentliche wie private Gesundheits- und Pflegeanbieter sowie Versicherern, bis zum Hausarzt reichen, wächst der Datenaustausch, und sensitive Gesundheitsdaten gelangen auch in die administrativen Bereiche von Kanton und Gemeinden.
Im Berichtsjahr verzeichnete der Datenschutzbeauftragte zudem über hundert Anfragen von Medienschaffenden aus der ganzen Schweiz. Die Themen Gesundheitsdaten, Videoüberwachung, neue technologische Entwicklungen und Social Media standen dabei im Mittelpunkt des Interesses.

Mobile Daten als Symposium-Thema

Die nunmehr bereits 16. Ausgabe des Symposiums on Privacy and Security im September 2011 hatte das Thema «Mobile Daten» zum Gegenstand. Die heutigen Informatikgeräte werden immer kleiner und mobiler – wie Smartphones, Memory Sticks oder Tablets. Die Daten werden auf den kleinen Geräten gespeichert oder zunehmend bei Dienstleistern im Internet abgelegt (Cloud Computing). Mit der zunehmenden Mobilität der Informationstechnologie nehmen die Risiken für die Privatsphäre zu. Das Symposium bietet Gelegenheit, solche Fragen interdisziplinär zu betrachten. Referenten aus den Disziplinen Recht, Computerwissenschaften und Ethik zeigten in ihren Beiträgen die künftig zu lösenden Fragestellungen sowohl aus wissenschaftlicher wie aus Praxissicht auf.

Einbindung in kantonalen Internetauftritt

Das zentrale Kommunikationsprojekt des Berichtsjahrs war die Integration der Website des Datenschutzbeauftragten in den Webauftritt des Kantons Zürich. Anlass für diesen Schritt waren folgende Überlegungen: hohe Qualität des Webauftritts bezüglich Gestaltung, Technik, Zugänglichkeit und Benutzerfreundlichkeit, ein einfach und unkompliziert handhabbares Contentmanagementsystem mit sehr hohem Standardisierungsgrad, die Möglichkeit, eine breite Palette von Themen zu präsentieren, sowie die Nutzung von Synergien in den Bereichen Technologie und Design. Selbstverständlich war die Umstellung auch Anlass, die Webinhalte einer generellen Aktualisierung zu unterziehen.

Sensibilisierung durch Referate und Seminare

Kurse und Seminare ermöglichen es den Mitarbeitenden von öffentlichen Organen, Datenschutzfragen in ihrem Arbeitsalltag zu lösen. Mit Referaten und Anlässen zum Thema Datenschutz werden Entscheidungsträger und interessierte Personen sensibilisiert.

Das Anbieten von Aus- und Weiterbildungen gehört zu den gesetzlich verankerten Aufgaben des Datenschutzbeauftragten. Mit über die Website allgemein zugänglichen Lernprogrammen werden den Mitarbeitenden von öffentlichen Organen und interessierten Dritten die Grundlagen des Datenschutzes vermittelt. Im Rahmen von Vertiefungsseminaren werden Fachpersonen und Sachbearbeitende in spezifischen Bereichen, wie Gesundheitswesen und Soziales, geschult. Auch der Kurs IKT-Sicherheit für Gemeinden steht weiterhin im Angebot.

Ausgewählte Referate 2011

- Datenschutzgesetzgebung in der Schweiz – Standortbestimmung und Ausblick
- Wie gläsern dürfen Patientinnen und Patienten sein? (Patientengeheimnis und Fallkostenpauschalen)
- Datenschutz in der digitalen Welt
- Selbstverantwortung und Regulierung (im Rahmen des Zyklus «Auf dem Weg zum gläsernen Menschen»)
- Der Fall «Google Street View»
- Datenschutz in der Schule
- Überwachung von Mitarbeitenden mittels GPS (Global Positioning System)
- Videoüberwachung am Arbeitsplatz
- Aktuelle datenschutzrechtliche Fragen im Polizeibereich

Neues Konzept für Seminare

Das Konzept für Seminare wurde überarbeitet. Das Angebot soll künftig kontinuierlich und zielgruppenspezifisch ausgebaut werden. Ziel ist es, ein Grundangebot für Juristinnen und Juristen sowie Mitarbeitende von Gemeinden und Informatikverantwortliche zur Verfügung zu stellen und in sensiblen Bereichen, wie Sozial-, Gesundheits- und Personalwesen sowie Polizei oder Bildung, spezifische Vertiefungsseminare anzubieten.

Auf Anfrage bietet der Datenschutzbeauftragte auch Kurse und Seminare für einzelne öffentliche Organe oder Betriebe an oder hält Referate zum Thema Datenschutz und Informationssicherheit in Lehrgängen. Der modulartige Aufbau des Weiterbildungsangebots ermöglicht es, auf die Bedürfnisse der jeweiligen Institution einzugehen und die Inhalte entsprechend zusammenzustellen. Dies erhöht den Nutzen für die Teilnehmenden und die Wirkung des Datenschutzbeauftragten.

Impressum

Herausgeber: Datenschutzbeauftragter des Kantons Zürich, Postfach, 8090 Zürich
Redaktion: Team des Datenschutzbeauftragten des Kantons Zürich
Schlussredaktion: Isabel Garcia
Korrektorat: Text Control, Zürich
Layout: René Habermacher, Visuelle Gestaltung, Flurstrasse 50, 8048 Zürich
Druck: Kantonale Druck- und Materialien Zentrale, KDMZ, 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 «Über uns».

dsb

datenschutzbeauftragter
kanton zürich

www.datenschutz.ch

Datenschutz mit Qualität