Nr. 5

Tätigkeits-Bericht

Datenschutzbeauftragter des Kantons Zürich

1999

Tätigkeitsbericht

Nr. 5
1999

Der Datenschutzbeauftragte erstattet dem Regierungsrat jährlich oder nach Bedarf einen Bericht über seine Tätigkeit (§ 23 Datenschutzgesetz). Der vorliegende Tätigkeitsbericht Nr. 5 deckt den Zeitraum vom 1. Januar 1999 bis 31. Dezember 1999 ab.

Zürich, Juni 2000

Der Datenschutzbeauftragte
des Kantons Zürich
Dr. Bruno Baeriswyl

Inhaltsverzeichnis

V. Datensicherheit

VI. Information

VII. Entwicklungen

Datenschutz: Eckpfeiler des Vertrauens

Fünf Jahre nach Einführung des Datenschutzgesetzes im Kanton Zürich zeigt sich, dass wir auf Grund der technologischen und gesellschaftlichen Entwicklungen mit wachsenden Herausforderungen für den Schutz der Privatsphäre der Bürgerinnen und Bürger rechnen müssen.

Als die Datenschutzgesetze in den 80er Jahren zum Schutz der Bürgerinnen und Bürger vor den wachsenden Gefahren der Informationstechnologie für die Privatsphäre konzipiert wurden, war die rasante Entwicklung der Informationstechnologie noch nicht voraussehbar. Der Wandel von der Grosstechnologie zur Mikro- und zur Nanotechnologie hat neue Möglichkeiten der Datenbearbeitungen eröffnet. Neue Architekturen mit verteilten Systemen und Datenbanken sowie die weltweite Vernetzung der Systeme hat die Situation für den Datenschutz stark verändert.

Informationsgesellschaft

Zugleich hat ein gesellschaftlicher Wandel in Richtung Informationsgesellschaft eingesetzt, der einen zunehmenden Bedarf an Informationen – Stichwort Information als Ressource – geltend macht. Gleich geblieben sind in dieser Zeit die rechtlichen Konzepte für den Schutz der Privatsphäre. Das Datenschutzgesetz des Kantons Zürich, das am 1. Januar 1995 in Kraft trat, konkretisiert – in Harmonie mit dem eidgenössischen Datenschutzgesetz – diese Konzepte. Viele der Fragestellungen, wie sie sich auch in der vorliegenden Berichtsperiode gezeigt haben, sind geprägt von den neuen technologischen und gesellschaftlichen Entwicklungen.

Entwicklungen in der Informatik

Im Bereich der Informationstechnik wird das Internet auch in der Verwaltung immer mehr zum bestimmenden Faktor. Wir beschäftigten uns sowohl aus datenschutzrechtlicher wie auch aus sicherheitstechnischer Sicht insbesondere mit den Internet-Auftritten der kommunalen Verwaltungen (siehe S. 31). Dabei stellten wir teilweise erhebliche Sicherheitsmängel fest. Sie waren grösstenteils auf eine mangelnde Beachtung der Sicherheitsaspekte des Internet-Auftritts zurückzuführen, das heisst, die Gefahren der neuen Technologien werden noch zu wenig zur Kenntnis genommen.

Ebenso sind wir bei geografischen Informationssystemen (GIS) mit einem sich rasch verbreitenden Konzept der Datenbearbeitung konfrontiert, dem so genannten «Data Warehousing»: Daten werden in einem Pool zusammengetragen und können beliebig kombiniert und verknüpft werden (siehe S. 19 ff.). Damit erlaubt die Technologie neue Eingriffe in die Privatsphäre betroffener Personen, indem durch Kombinationen neue Informationen – die bisher vielleicht unbekannt waren – entstehen.
Ebenfalls zeigte sich bei der Umsetzung der Informatiksicherheitsverordnung, dass das Bewusstsein der Sicherheitsrisiken der neuen Technologien für die Privatsphäre der betroffenen Bürgerinnen und Bürger teilweise noch wenig ausgeprägt ist (siehe S. 31).

Rolle des Datenschutzbeauftragten

Die neuen Herausforderungen für den Schutz der Privatsphäre der Bürgerinnen und Bürger bestimmen auch die Rolle und Funktion des Datenschutzbeauftragten bei der Umsetzung des Datenschutzgesetzes. Um einen wirksamen Datenschutz auch in der modernen Verwaltung – Stichwort «E-Government» – gewährleisten zu können, wird der Datenschutzbeauftragte vermehrt den Datenschutz und die Informationssicherheit als Teil der politischen Verantwortung in der Informationsgesellschaft thematisieren müssen. Dabei sind sowohl die Entwicklungen als auch der Handlungsbedarf, der für einen wirksamen Schutz der Privatsphäre notwendig ist, aufzuzeigen.
Viele Spannungsfelder, die sich bei der praktischen Umsetzung des Datenschutzgesetzes zeigen, können unter Umständen durch entsprechendes gesetzgeberisches Handeln vermieden respektive entschieden werden.
Des Weiteren ist der Datenschutzbeauftragte vermehrt gefordert, aktiv die Lösung von Sicherheitsproblemen anzugehen und an deren Realisierung mitzuwirken.
Damit sowohl im datenschutzrechtlichen wie im sicherheitstechnischen Bereich angemessene Lösungen entwickelt werden können, muss eine umfassende Information über die Anliegen des Datenschutzes und der Informationssicherheit gewährleistet werden.
Ebenso ist eine kompetente, anlassunabhängige Aufsichtstätigkeit, insbesondere im Informatikbereich sicherzustellen, wie auch die einzelfallweise Beratungs-, Auskunfts- und Unterstützungstätigkeit Bestandteil der Aufgaben ist.
In einer regelmässigen Berichterstattung wird vermehrt auf die Zielsetzungen des Datenschutzes hinzuweisen sein und die Wirkungsweise der Massnahmen und Instrumente ist konstant zu überprüfen, um auch eine Anpassung von Instrumenten und Ressourcen rechtzeitig planen zu können.

Überprüfung und Sensibilisierung

Diesen Entwicklungen kann nur mit neuen Methoden der Überprüfung und Kontrolle respektive der Sensibilisierung begegnet werden. Aus diesem Grund haben wir in der Berichtsperiode wiederum einen Sicherheits-Check durchgeführt, der im Rahmen der Grundschutzmassnahmen insbesondere die Qualität der Passwörter und den Umgang mit unsicheren E-Mails überprüfte (siehe S. 30). Des Weiteren erstellten wir im Rahmen des Datenschutz-Reviews ein Vorgehenskonzept für die systematische Überprüfung von sensiblen Datenbearbeitungen (siehe S. 32). Beide Massnahmen sollen nicht nur allfällige Schwachstellen aufzeigen, sondern gleichzeitig die betroffenen Verwaltungsstellen für die Anliegen angemessener Sicherheitsmassnahmen sensibilisieren.
Immer mehr sind heute aber konkrete Lösungen gefragt. Aus diesem Grunde haben wir auch die Initiative übernommen für den Vorschlag einer verwaltungsweiten Sicherheitsstrategie. Im Projekt SOPRANO wurden die Grundlagen für einen verwaltungsinternen wie -externen Datenaustausch erarbeitet, der vertraulich, authentisch, integer und nicht abstreitbar ist (siehe S. 22). Die Grundlage hierfür bildet eine Public Key Infrastructure (PKI) mit der Verwendung von digitalen Signaturen.

Datenschutzrechtliche Entwicklungen

Im datenschutzrechtlichen Bereich zeigt sich eine zunehmende Komplexität der Fragestellungen. Einerseits hängen diese Fragen stärker von der technologischen Entwicklung ab, wie dies die erwähnten geografischen Informationssysteme zeigen (siehe S. 19 ff.). Bisherige Rechtsgrundlagen sagen kaum etwas über die Kombinierbarkeit von Daten oder die Öffentlichkeit von Daten aus, wie sie heute das Internet ermöglicht. Ebenso wenig spricht sich das Datenschutzgesetz hierzu konkreter aus. Die Gesetze sind deshalb nach den ihnen zu Grunde liegenden Zwecken auszulegen und in der Praxis ist eine Interessenabwägung vorzunehmen. Die Interessenabwägungen in diesen Fällen sind oft schwierig, da sich meistens auf beiden Seiten grundsätzlich berechtigte Interessen gegenüberstehen.

Sensible Datenbekanntgaben

Weiter zeigt sich in verschiedenen Einzelfällen die erhöhte Sensibilität der Datenbekanntgaben. Die Zunahme der Datenbearbeitungen verläuft auch parallel zur Zunahme von Datenbekanntgaben. Obwohl für die Aufgabenerfüllung nicht notwendig, wird oftmals mit personenbezogenen Daten gearbeitet, da diese ohne zusätzlichen technischen Aufwand bekannt gegeben werden können, wohingegen eine Anonymisierung einen zusätzlichen Handlungsbedarf bedeuten würde.

Auch die Rechte der betroffenen Personen, insbesondere das Auskunftsrecht, das grundsätzlich ein Recht auf unbeschränkte Auskunft über die bearbeiteten Daten gibt, sind im konkreten Einzelfall oftmals schwierig zu handhaben (siehe S. 9). Angesichts der technischen Möglichkeiten verliert die betroffene Person sehr rasch den Überblick, wer welche Daten zu welchem Zweck über sie bearbeitet. Die Transparenz der Datenbearbeitungen ist indessen ein wesentliches Anliegen des Datenschutzes.

Sensibilisierung für den Datenschutz

Diese Entwicklungen erfolgen zwar sehr rasch, aber oftmals nur verdeckt und sind in Bezug auf die Auswirkungen auf den Schutz der Privatsphäre kaum transparent. Aus diesem Grunde ist sehr grosses Gewicht auf die Information und Sensibilisierung für die Anliegen des Datenschutzes zu legen. Diese Aufgabe obliegt dem Datenschutzbeauftragten nicht nur in Bezug auf den datenschutzrechtlichen Teil, sondern auch für die Informationssicherheit. Mit regelmässigen Informationsveranstaltungen und Symposien (siehe S. 35) wie auch mit gezielten Informationen für die PC-Benutzerinnen und -Benutzer im Bereich der Datensicherheit (siehe S. 34) versuchen wir, diese Bedürfnisse zu befriedigen.

Neue Herausforderungen

Fünf Jahre nach der Einführung des Datenschutzgesetzes zeigt sich, dass nicht zur Tagesordnung übergegangen werden kann. Einerseits bestehen wachsende Bedürfnisse der Verwaltungsstellen nach Beratung und Information im Bereich des Datenschutzes und der Informationssicherheit. Andererseits verlangen die technologischen und gesellschaftlichen Entwicklungen nach neuen angemessenen Lösungen, um den Schutz der Privatsphäre der Bürgerinnen und Bürger gewährleisten zu können. Rückblickend betrachtet können verschiedene Spannungsfelder, die sich mit der Einführung des Datenschutzgesetzes in den kantonalen und kommunalen Verwaltungen gezeigt haben, dadurch erklärt werden, dass das Datenschutzgesetz diesen zu wenig Rechnung trägt.

Neuer Datenschutz

Um einen wirksamen Datenschutz erreichen zu können, muss vermehrt an den grundlegenden Konzepten gearbeitet werden, und es sind allenfalls Schritte für deren Anpassung an die neuen Entwicklungen in die Wege zu leiten. Ebenso hat sich der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben immer wieder die Frage nach der Wirksamkeit seiner Mittel zu stellen und allenfalls Vorschläge für deren Verbesserung zu unterbreiten. Die Verwaltung wird unter dem Titel «E-Government» die neuen Technologien vermehrt auch im interaktiven Verkehr mit den Bürgerinnen und Bürgern nutzen wollen. Diese werden diesen Schritt aber nur mitmachen, wenn sie Gewissheit darüber haben, was mit ihren Daten geschieht, und wenn ihre Privatsphäre auch in diesem Umfeld einen gleichwertigen Schutz geniesst. Datenschutz ist deshalb auch ein Eckpfeiler für das Vertrauen der Bürgerinnen und Bürger in die moderne Verwaltung.

Zugriffe auf Datenbanken

Datenbearbeitungen werden kontinuierlich erweitert durch Zugriffsmöglichkeiten auf bestehende Datensammlungen.

1. Auskunftsrecht bei Krankengeschichten

Recht auf Auskunft, Berichtigung und Herausgabe

Verschiedene Anfragen betrafen Fragen rund um das Auskunftsrecht bei Krankengeschichten. Bei Krankengeschichten in Spitälern besteht ein Auskunftsanspruch gestützt auf § 17 DSG. Auch § 14 Patientenrechtverordnung sieht ein Recht auf Einsicht in die Krankengeschichte vor. Der Anspruch erstreckt sich auf sämtliche zur Krankengeschichte bzw. zum Patientendossier gehörenden Angaben, so auch auf Röntgen- und Laborbefunde, Aufzeichnungen über diagnostische, therapeutische und pflegerische Massnahmen usw., auch wenn diese handschriftlich sind. Nur persönliche Notizen des ärztlichen und des Pflegepersonals sind ausgenommen, sofern es sich dabei um Gedankenstützen oder Arbeitshilfen handelt. Als solche gelten etwa die Notiz über ein zu führendes Telefonat mit einer betroffenen Person oder die persönliche Agenda mit Einträgen über zu absolvierende Visiten. Hingegen sind so genannte Kardex-Einträge oder auch an anderen Stellen angebrachte Bemerkungen wie «Patient schlief unruhig, war schlecht gelaunt» u.ä. nicht persönlicher Natur und fallen unter das Auskunftsrecht. Dies sieht auch das Kreisschreiben der Gesundheitsdirektion zu §§ 13 – 17 Patientenrechtverordnung entsprechend vor. Einschränkungen sind bezüglich Angaben von Dritten zu machen, sofern eine Interessenabwägung ergibt, dass die Geheimhaltung ihrer Angaben und/oder ihrer Identität das Offenlegungsinteresse der betroffenen Person überwiegt (§ 18 DSG; der § 14 Abs. 1 lit. a Patientenrechtverordnung ist dagegen missverständlich und analog § 18 DSG anzuwenden).

Besonderheiten bei Krankengeschichten bestehen im Zusammenhang mit dem Berichtigungsanspruch, wonach unrichtige Daten zu berichtigen sind (§ 19 Abs. 2 lit. a in Verbindung mit § 4 Abs. 2 DSG). Soweit ärztliche Aufzeichnungen, z.B. im Rahmen einer Konsultation, Wertungen enthalten, ist es häufig nicht möglich, die Richtigkeit oder Unrichtigkeit der Daten nachzuweisen. Im Falle eines solchen Beweisnotstands hat die betroffene Person, die mit der Wertung nicht einverstanden ist, das Recht, dass ein entsprechender Vermerk angebracht wird (§ 19 Abs. 3 DSG; siehe auch Entscheid des Bundesgerichts 1P.150/1998 vom 15. Juli 1998, auszugsweise abgedruckt in ZBl 1999, S. 312 ff.). Ein besonderes Augenmerk ist der Mitteilung zu widmen. Nach § 19 Abs. 2 lit. b DSG kann die betroffene Person verlangen, dass der Entscheid oder die Berichtigung Dritten mitgeteilt oder veröffentlicht wird. So ist unter Umständen den Empfängern früherer ärztlicher Berichte eine entsprechende Korrektur weiterzugeben, insbesondere wenn die betroffene Person dies ausdrücklich verlangt.

Bisher ungeklärt geblieben ist die Frage nach der Herausgabe des Originals der Krankengeschichte. (Anspruch auf eine Kopie besteht auf Grund des Auskunftsrechts nach § 17 DSG.) Laut § 13 Patientenrechtverordnung steht die Krankengeschichte im Eigentum des Krankenhauses und ist nach Abschluss der Behandlung noch während zehn Jahren aufzubewahren. Im privatrechtlichen Verhältnis zwischen Patient und Arzt (oder Privatspital) besteht gemäss Bundesgericht ein Herausgabeanspruch auf Grund des Auftragsrechts (BGE 119 II 222). Der Arzt bzw. das Spital können während der Verjährungsfrist für allfällige Forderungen (z.B. Haftpflichtansprüche) Kopien aufbewahren, sofern der Patient nicht rechtsgültig auf die Geltendmachung der Ansprüche verzichtet. Fraglich ist, inwiefern das öffentlichrechtliche Behandlungsverhältnis anders zu beurteilen ist als das privatrechtliche. Diese Fragestellung wird (nebst anderen) durch das geplante Patientenrechtgesetz zu klären sein.

2. Listen im Bereich der Arbeitslosenversicherung

Fehlen klarer Bestimmungen

Im Bereich des Vollzuges der Arbeitslosenversicherung werden Listen über Verstösse im Zusammenhang mit Einarbeitungszuschüssen und Ausländerbeschäftigung geführt. Die Liste im Bereich Einarbeitungszuschüsse bestand im Wesentlichen aus einer Zusammenstellung von Verdachtsmomenten gegenüber bestimmten Firmen, welche die Institution der Einarbeitungszuschüsse möglicherweise missbrauchten. Das Führen dieser Liste tangierte die Grundsätze der Integrität und der Verhältnismässigkeit von Datenbearbeitungen, da meist gar keine näheren Abklärungen erfolgten, der Verdacht aber trotzdem gespeichert blieb. Die Liste wurde inzwischen aufgehoben.

Bei Verstössen im Bereich der Ausländerbeschäftigung ergeht gegen den fehlbaren Arbeitgeber eine Sperre (Verweigerung von Bewilligungen zur Anstellung von Ausländern während einer bestimmten Frist); über diese Sperren wird ebenfalls eine Liste geführt. Wir konnten erwirken, dass der Verteiler dieser Liste auf einen verhältnismässigen Rahmen eingeschränkt und die Liste in ihrer Form offizialisiert wurde (Briefkopf, Datierung, Unterschrift). Dadurch wird klar, wer für die Datenbearbeitung verantwortlich ist (§ 6 DSG), und betroffene Personen können ihre Rechte ausüben.

In einem anderen Fall wandte sich ein Mitarbeiter eines Regionalen Arbeitsvermittlungszentrums (RAV) an uns, weil das RAV von den zur Vermittlung angemeldeten Personen eine Entbindung von der Schweigepflicht verlangt, um Daten an potenzielle Arbeitgeber weiterzuleiten. Die Verwendung einer solchen allgemein formulierten Einwilligung ist mangels Transparenz für die betroffene Person problematisch. In der Praxis wurden ausserdem mehr Daten (d.h. ganze Bewerbungsdossiers) statt nur die in der Vollmacht bezeichneten weitergeleitet, und als Kommunikationsmittel wurde das Telefax verwendet. Das Amt für Wirtschaft und Arbeit teilte diesbezüglich mit, dass die RAV bereits früher angewiesen worden seien, auf solche Vollmachten zu verzichten, und stellte eine erneute Anweisung an die RAV in Aussicht.

Meinungsverschiedenheiten bestehen dagegen immer noch bezüglich der Weiterleitung von Listen über arbeitslose Personen an die Gemeinden (vgl. Tätigkeitsberichte Nr. 2 [1996], S. 24 f. und Nr. 4 [1998], S. 40 f.). Zuletzt berichteten wir über eine «Praxisänderung» des Bundesamtes für Wirtschaft und Arbeit (neu: Staatssekretariat für Wirtschaft [seco]). Anlässlich einer Aussprache wurde auch diese Frage angesprochen, konnte aber nicht weiter geklärt werden, da die Abklärungen beim Bund noch im Gange waren (vgl. Tätigkeitsbericht Nr. 4 [1998], S. 40). Unsere Nachfrage beim Eidgenössischen Datenschutzbeauftragten hat ergeben, dass das seco das Kreisschreiben über den Datenschutz im Bereich der Informationssysteme AVAM/ASAL (Informationssysteme zur Vermittlung von arbeitslosen Personen respektive zur Auszahlung von Leistungen der Arbeitslosenversicherung) ergänzt hatte. Die RAV dürfen den Gemeindearbeitsämtern, die nicht an die erwähnten Informationssysteme angeschlossen sind, eine Liste sämtlicher in der Gemeinde wohnhafter Bezügerinnen und Bezüger von Arbeitslosenversicherungsleistungen zustellen. Adressaten der Listen waren im Kanton Zürich jedoch die Sozialvorstände der Gemeinden. Infolge der Regionalisierung des Vollzugs des Arbeitsvermittlungs- (AVG) und Arbeitslosenversicherungsgesetzes (AVIG) bestehen im Kanton Zürich faktisch keine Gemeindearbeitsämter mehr oder sie haben die Funktion und die Aufgaben eines Regionalen Arbeitsvermittlungszentrums (z.B. in der Stadt Zürich). Gemäss der Regelung in Art. 125 Arbeitslosenversicherungsverordnung (AVIV) dürfen den Sozialämtern im Einzelfall auf Anfrage Daten weitergegeben werden, wenn dies erforderlich ist. Wir forderten deshalb das Amt für Wirtschaft und Arbeit (AWA) auf, bei den RAV für die Einstellung dieser

Datenbekanntgaben zu sorgen. Das AWA hielt an seiner Praxis fest. Wir stellten fest, dass insbesondere die Gemeinden beim AWA in Bezug auf die regelmässige Zusendung der Listen insistiert hatten. Die Begründung war, dass mangels Informationen keine sinnvolle Planung der Beschäftigung und Unterstützung von ausgesteuerten Arbeitslosen möglich sei. Wir hatten nie bestritten, dass für eine sinnvolle Ressourcenplanung im Sozialhilfebereich auch Daten über die in naher Zukunft ausgesteuerten Personen notwendig sind. Hierfür genügen jedoch anonymisierte Listen, da für die Planung nicht relevant ist, wer arbeitslos gemeldet ist. Wir sahen uns daher veranlasst, vom AWA erneut eine Praxisänderung zu fordern, weil die fragliche Listenweitergabe für die Aufgabenerfüllung der Gemeinden nicht notwendig ist und lediglich der Befriedigung ihrer Neugier Vorschub leistet, da weniger als 10 Prozent der ausgesteuerten arbeitslosen Personen überhaupt Sozialhilfeleistungen beantragen. Unseres Erachtens stellt die Weitergabe auch eine Verletzung der arbeitslosenversicherungsrechtlichen Schweigepflicht dar, was strafrechtliche Sanktionen nach sich ziehen kann.

3. Zentrale Datenbanken und Vernetzung

Verhältnismässige Rechtsgrundlagen notwendig

Dem Regierungsrat wurden diverse Fragen betreffend Wünschbarkeit und Zulässigkeit einer zentralen Datenbank und der Vernetzung der kantonalen Polizeiorgane sowie zu den Risiken solcher Einrichtungen für den Persönlichkeitsschutz der betroffenen Personen vorgelegt. In einem Mitbericht befassten wir uns eingehend mit den einzelnen heiklen Punkten.
Der Aufbau zentraler Datenbanken bzw. die umfassende Vernetzung von Systemen im Sinne von Online-Zugriffsmöglichkeiten erfordert klare gesetzliche Grundlagen. Auf kantonaler Ebene fehlt es an genügenden Regelungen, weshalb die zürcherischen Systeme nicht ohne weiteres im vorgesehenen Umfang mit anderen Kantonen und/oder dem Bund gekoppelt werden können. Auf Bundesebene wurden für gesamtschweizerische polizeiliche Datenbanken ausdrückliche Rechtsgrundlagen in formellen Gesetzen geschaffen. Dabei wird allerdings oft nicht erkannt, dass das Datenschutzrecht zwar solche gesetzliche Grundlagen für Datenbearbeitungen verlangt, jedoch damit auch eine materielle Überprüfung hinsichtlich des öffentlichen Interesses und der Verhältnismässigkeit verlangt. Wir wiesen in unserem Mitbericht explizit auf diese Problematik hin und hielten fest, dass beispielsweise eine umfassende Registrierung von Zeugen und Anzeigeerstattern in einem der Ermittlung dienenden gesamtschweizerischen System dem Grundsatz der Verhältnismässigkeit widersprechen würde.
Beim Erlass von im öffentlichen Interesse liegenden, verhältnismässigen Rechtsgrundlagen ist auch der Grundsatz der Zweckbindung (§ 4 Abs. 4 DSG) zu berücksichtigen. Da ein vernetztes System hohe Risiken beinhaltet, sind ausserdem klare Bestimmungen in Bezug auf die organisatorischen und technischen Massnahmen zu erlassen. Systeme, die umfangreich vernetzt sind und in denen sensible Datenbearbeitungen erfolgen, sind in einem angemessenen Umfang regelmässig auch anlassunabhängig zu kontrollieren, weshalb auch hierfür die notwendigen Ressourcen für interne und externe Revisions- bzw. Aufsichtsstellen bereitzustellen sind. Die Mittel des Datenschutzbeauftragten reichen derzeit nicht aus, um die bereits bestehenden oder gar zukünftige Systeme ausreichend kontrollieren und die politischen Organe periodisch umfassend ins Bild setzen zu können.

4. Zweckbindung von Datensammlungen
Vernehmlassungen zu Gesetzesvorhaben

Zahlreiche Gesetzgebungsvorhaben auf bundesrechtlicher und kantonaler Ebene boten Gelegenheit, zu datenschutzrechtlichen Aspekten Stellung zu beziehen. Der Entwurf für ein Bundesgesetz über die Ausweise für Schweizer Staatsangehörige (Ausweisgesetz) warf Fragen zur Zweckbindung dieser zentralen Datensammlung auf. Das Gesetz formuliert als Zweck des zu Grunde liegenden Informationssystems die Verhinderung von Mehrfachausstellungen eines Ausweises für dieselbe Person und die Verhinderung missbräuchlicher Verwendung. Nach dieser Umschreibung ist das Informationssystem auf administrative Zwecke beschränkt. Weiter wird aber Behörden und Stellen, die polizeiliche Zwecke verfolgen, ein Zugriff im Abrufverfahren auf das Informationssystem gegeben. Diese Zugriffe sind durch die umschriebene Zweckbestimmung nicht abgedeckt. Sofern auf diese nicht verzichtet wird, ist im Sinne des Grundsatzes der Transparenz klar zu deklarieren, dass dieses Informationssystem auch polizeilichen Zwecken dient. Es ist auch zu prüfen, ob die geplanten Zugriffe im Abrufverfahren nach dem Prinzip der Verhältnismässigkeit für die erwähnten Behörden und Stellen erforderlich sind.

Eine gleiche Problematik stellt sich auch bei der mit der Änderung des Zivilgesetzbuches betreffend die Beurkundung des Personenstandes geplanten zentralen Datenbank (Personenstandregister, Infostar). Der Zweck dieses Informationssystems liegt in der Beurkundung des Personenstandes einer Person. Als Personenstand gelten die eine Person unmittelbar betreffenden Zivilstandstatsachen (Geburt, Heirat, Tod), die personen- und familienrechtliche Stellung (Mündigkeit, Abstammung, Ehe), die Namen und die Bürgerrechte bzw. die Staatsangehörigkeit (Art. 39 Abs. 2 ZGB). Nach dieser Umschreibung ist das Informationssystem auf administrative sowie auf beweisrechtliche (Art. 9 ZGB) Zwecke beschränkt. Weiter wird indessen Behörden und Stellen, die polizeiliche Zwecke verfolgen, ein Zugriff im Abrufverfahren auf das Informationssystem gegeben. Diese Zugriffe sind durch die umschriebene Zweckbestimmung nicht abgedeckt. Es ist deshalb zu prüfen, ob diese Zugriffe auch verhältnismässig sind: Welchen Zwecken dienen sie? Sind sie für die Erreichung dieser Zwecke geeignet, erforderlich und verhältnismässig, das heisst: Lassen sich die Zwecke mit diesen Zugriffen überhaupt erreichen? Liessen sie sich nicht auch mit weniger weit gehenden Massnahmen erreichen? Und stehen die Zugriffe in einem vernünftigen und vertretbaren Verhältnis zum Eingriff? Auffällig ist in diesem Zusammenhang, dass bei immer mehr gesamtschweizerisch geführten, elektronischen Informationssystemen die Polizeibehörden im Abrufverfahren angeschlossen werden. Begründet wird dies mit einem entsprechenden Bedürfnis nach raschen Verfahrensabläufen. Das Bedürfnis selbst wird jedoch nicht näher ausgewiesen; die erläuternden Berichte beantworten diese Fragen nicht überzeugend. Bereits der Bericht der Geschäftsprüfungskommission des Ständerates vom 19. November 1998 betreffend Einrichtung von Online-Verbindungen im Bereich des Polizeiwesens forderte beziehungsweise empfahl, dass solche Verbindungen auf ihre Notwendigkeit, Verhältnismässigkeit und Zweckbindung zu prüfen sind und dass dies entsprechend transparent zu machen ist (Ziff. 261 und 263 des Berichts).

Die Einrichtung eines automatisierten Strafregisters (Vostra) (vgl. Tätigkeitsbericht Nr. 2 [1996], S. 14 f.) führte in der Folge zu zwei neuen Verordnungen auf Bundes- sowie auf Kantonsebene, zu denen wir Stellung bezogen. Nicht Gegenstand des vorliegenden Projektes waren Fragen der Löschungen bzw. Entfernungen der Einträge im Strafregister, da lediglich die Schaffung ausreichender gesetzlicher Grundlagen für das Führen der Datenbank Ziel der Vorlage war; eine diesbezügliche materielle Diskussion hat daher nicht stattgefunden. Die Fragestellungen sollten deshalb im Rahmen der Revision des Allgemeinen Teils des Strafgesetzbuches diskutiert und gelöst werden. Unklar blieb die Regelung der Verantwortlichkeit. Es ist aber davon auszugehen, dass der Bund die Hauptverantwortung für die Datenbearbeitungen im automatisierten Strafregister zu übernehmen hat.

Dies ergibt sich einerseits aus der zentralen Regelung in Bezug auf die Datensicherheit. Andererseits führt das Bundesamt das Register und vergibt die individuellen Bearbeitungsrechte. Weiter ist vorgesehen, dass das Bundesamt Auszüge aus dem Register erstellt und das Auskunftsrecht gewährt.
Angesichts der Sensibilität der Datenbearbeitungen hätte auch den Verfahrensrechten der betroffenen Personen bereits auf Gesetzesstufe Rechnung getragen werden müssen. Die in der Verordnung vorgeschlagene Lösung vermag in verschiedener Hinsicht nicht zu genügen; sie erweist sich teilweise gar als gesetzeswidrig.
Art. 27 Abs. 3 sieht eine mündliche Auskunft über den vollständigen Strafregistereintrag vor. Dies wird damit begründet, dass eine zweckwidrige Verwendung vollständiger Strafregisterauszüge (etwa durch potenzielle Arbeitgeber) verhindert werden soll. Diese Auffassung ist äusserst fragwürdig. Nach Art. 8 DSG ist die Auskunft in der Regel schriftlich zu erteilen; eine mündliche Auskunft kann nicht zur Regel erklärt werden.

Die mündliche Auskunft unterläuft ausserdem die weiteren Ansprüche gemäss Datenschutzgesetz, insbesondere die Ansprüche auf Unterlassung, Feststellung, Beseitigung und Berichtigung (Art. 25 DSG; § 19 DSG-ZH), da die betroffene Person jeglicher Beweismittel beraubt wird. Ausserdem wäre eine Verweisung auf die Regelung dieser Rechte im DSG angemessen.
Im Weiteren ist es unzumutbar, dass eine betroffene Person den vollständigen Eintrag beim Bundesamt einsehen müsste. Diese Regelung würde es insbesondere nicht mobilen (z.B. gehbehinderten) Personen faktisch verunmöglichen, Auskunft über den vollständigen Eintrag zu erhalten.

Auf kantonaler Ebene war sodann aus datenschutzrechtlicher Sicht zu regeln, welches Organ die Aufgaben der kantonalen Koordinationsstelle (und damit die Verantwortung im Sinne von § 6 DSG) übernimmt, welche Organe an das automatisierte Strafregister angeschlossen werden und welche organisatorischen und technischen Massnahmen zu treffen sind.

Generell ist bei all diesen Datenbankprojekten mit Online-Anschlüssen zu bemängeln, dass jegliche Konkretisierung von Datensicherheitsmassnahmen fehlt. Die teilweise hohe Sensibilität dieser Datenbearbeitungen erfordert Regelungen auf gesetzgeberischer Ebene, nicht erst bei der Umsetzung des Projekts. Nach dem heutigen Stand der Technik können nur kryptografische Verfahren mit entsprechenden Authentisierungsmechanismen als angemessene Sicherheitsmassnahmen für den Transfer von sensiblen Personendaten betrachtet werden.

Im Weiteren nahmen wir auch Stellung zur Verordnung über die erkennungsdienstliche Identifizierung mit DNA-Profilen (siehe auch: Tätigkeitsbericht Nr. 4 [1998], S. 22 ff.) und auf kantonaler Ebene zur Revision des Gesundheitsgesetzes, des Gesetzes über die Finanzkontrolle sowie des Einführungsgesetzes zum Gleichstellungsgesetz.

5. Daten im Ermittlungs- und Strafuntersuchungsverfahren

Nur verhältnismässige und integre Bearbeitung

Ein Mann war im Zusammenhang mit einer Strafuntersuchung wegen Sittlichkeitsdelikten gegenüber Kindern zu einer DNA-Analyse aufgeboten worden, obwohl er wesentlich älter als der im Steckbrief gesuchte Verdächtigte war und zudem mit dem Robotbild nur eine vage Ähnlichkeit aufwies. Anlass für die angeordnete Analyse war unter anderem, dass dieser Mann bereits vor ein paar Jahren verdächtigt worden war, am Verschwinden eines Kindes beteiligt zu sein; später war seine Unschuld festgestellt worden. Mit Vorliegen des Ergebnisses der DNA-Analyse war die Täterschaft in Bezug auf die neuerlichen Verdächtigungen eindeutig auszuschliessen.
In der Beurteilung des Sachverhalts stellten wir fest, dass gemäss bundesgerichtlicher Rechtsprechung (BGE 124 I 80 ff.) eine Ähnlichkeit einer

betroffenen Person mit der steckbrieflich gesuchten Person ausreicht, damit eine DNA-Analyse durchgeführt werden kann. Dabei ist zwar die Beurteilung der Ähnlichkeit eine Ermessensfrage. Jedoch ist von den zuständigen Behörden mit der angemessenen Sorgfalt zu prüfen, ob eine Übereinstimmung im erforderlichen Umfang vorliegt. Der Umstand, dass sowohl Robotbild wie verdächtigte Person Männer sind, reicht somit für sich allein nicht aus (zur DNA-Analyse vgl. auch Tätigkeitsbericht Nr. 4 [1998], S. 22 ff.).
Des Weiteren wiesen wir darauf hin, dass die auf Grund einer hinfällig gewordenen Verdächtigung erhobenen Daten von Amtes wegen zu vernichten sind. Die praktische Umsetzung dieses klaren Grundsatzes ist heute nicht gewährleistet, da der anderslautende § 8 der «Verordnung über die erkennungsdienstliche Behandlung von Personen» aus dem Jahre 1960 – wie von der Polizeidirektion (heute Direktion für Soziales und Sicherheit) bereits 1996 in Aussicht gestellt (vgl. Tätigkeitsbericht Nr. 2 [1996], S. 11 sowie Tätigkeitsbericht Nr. 4 [1998], S. 18 f.) – bisher nicht angepasst worden ist.
Im Übrigen haben sich auch Ermittlungsberichte der Polizei nach den Grundsätzen der Datenintegrität (§ 4 Abs. 2 DSG) und Verhältnismässigkeit (§ 4 Abs. 3 DSG) auszurichten. Insbesondere ist auf nicht nachprüfbare Werturteile zu verzichten. Stattdessen sind in sachlichen Worten die konkreten objektiven Umstände aufzuführen. Sind Werturteile in einem Fall unumgänglich, ist dies bei der Abfassung des Berichts entsprechend transparent zu machen. Selbstverständlich dürfen dabei nur Informationen festgehalten werden, welche zur Erfüllung der konkreten polizeilichen Aufgabe geeignet und erforderlich sind; weitere Lebensumstände der betroffenen Person dürfen nicht erhoben werden.

6. Volkszählung 2000

Vorbereitung der datenschutzrechtlichen Rahmenbedingungen

Auf Bundesebene wurden mit dem Volkszählungsgesetz (siehe auch Tätigkeitsbericht Nr. 2 [1996], S. 14), einer entsprechenden Verordnung und konkretisierenden Weisungen die rechtlichen Rahmenbedingungen für die Durchführung der Volkszählung 2000 geschaffen. Die Gewährleistung des Datenschutzes sowie der Kontrolle sind die Anliegen des Datenschutzbeauftragten, der entsprechende Vorbereitungen traf.
Die Volkszählung 2000 hat aus verschiedenen Gründen eine besondere Bedeutung: Erstmals werden nicht mehr nur Daten von den betroffenen Personen selber erhoben, sondern auch die bestehenden Einwohnerregister werden für einen Vordruck der Personenfragebogen verwendet. Des Weiteren werden in der von den meisten Gemeinden gewählten Variante der Durchführung die Daten in einem externen Dienstleistungszentrum bearbeitet. Und schlussendlich fliessen die Daten der Volkszählung in einem gewissen Rahmen wieder zurück in die Register der Gemeinden. Diese Ausgangslage für die Volkszählung 2000 soll für die im Jahre 2010 geplante Volkszählung zu einem vollkommen automatisierten System führen. Hierzu sind allerdings noch einige weitere Voraussetzungen wie die Harmonisierung der Register zu gewährleisten.
Die Volkszählung ist auf Grund ihrer Grösse besonders sensibel. Zwar sind die einzeln erhobenen Datenkategorien grösstenteils nicht besonders schützenswert, doch liessen sich durch ihre Kombination zahlreiche neue Erkenntnisse über Personen finden. Sensibel ist auch die Tatsache, dass die Auswertungen der Fragebogen in einem zentralen Dienstleistungszentrum erfolgen, das auch andere Aufgaben im Bereich der Adressverwaltung erfüllt.
Der Datenschutzbeauftragte wird in Zusammenarbeit mit den involvierten kantonalen und kommunalen Stellen die Volkszählung 2000 aus datenschutzrechtlicher Sicht begleiten. In Zusammenarbeit mit weiteren Datenschutzbeauftragten soll auch die Aufsichtstätigkeit in Bezug auf das Dienstleistungszentrum wahrgenommen werden.

7. Online-Zugriffe auf das Handelsregister

Anforderungen an Rechtsgrundlagen bei Abrufverfahren

Eine Abteilung der Kantonspolizei sowie die Staatsanwaltschaft beantragten umfassende Online-Anschlüsse an die Datenbank des Handelsregisteramtes. Zu beurteilen war, ob ausreichende Rechtsgrundlagen hierfür bestehen.
Das Datenschutzgesetz (DSG) ist auf öffentliche Register des Privatrechtsverkehrs, wie zum Beispiel das Handelsregister, nicht anwendbar. Dieser Ausschluss ergibt sich aus Art. 2 Abs. 2 lit. d Bundesdatenschutzgesetz. Ebenfalls nicht anwendbar ist es in hängigen Verfahren der Strafrechtspflege (§ 3 Abs. 2 lit. b DSG).
Das Anliegen des DSG ist der Schutz der Grundrechte von Personen, über die Daten bearbeitet werden. Das DSG entspricht einem verfassungsrechtlichen Anliegen. Gemäss Art. 13 der Bundesverfassung vom 18. April 1999 sowie der bundesrätlichen Botschaft dazu darf der Staat Personendaten nur bearbeiten, soweit dies gesetzlich vorgesehen und notwendig ist und die Datenbearbeitungen zweckgebunden erfolgen und verhältnismässig sind. Ob eine gesetzliche Grundlage den verfassungsrechtlichen Anforderungen genügt, beurteilt sich nach der Schwere des Grundrechtseingriffs. Nach der Praxis des Bundesgerichts lassen sich den Datenschutzgesetzen von Bund und Kantonen Hinweise zu den verfassungsrechtlichen Mindestanforderungen an die gesetzliche Grundlage entnehmen; die den Datenschutzgesetzen zu Grunde liegenden allgemeinen Grundsätze stellen weitgehend Konkretisierungen der verfassungsrechtlichen Anforderungen in diesem Bereich dar (BGE 122 I 364). Nach dieser Praxis sind die datenschutzrechtlichen Grundsätze auch in Bereichen analog anwendbar, in welchen die direkte Geltung des DSG ausgeschlossen ist.

Bei so genannten Abrufverfahren werden Daten nach dem Selbstbedienungsprinzip bekannt gegeben, d.h., die empfangende Stelle entscheidet selbständig und ohne Intervention der bekannt gebenden Stelle über die Bekanntgabe. Eine Interessenabwägung im Einzelfall kann naturgemäss nicht mehr erfolgen. Dies beinhaltet eine besondere Gefährdung für die Persönlichkeitsrechte der Betroffenen. Bei der Bekanntgabe von Personendaten im Abrufverfahren sind die Tatsache des Abrufverfahrens, die berechtigten Behörden, der Umfang der abrufbaren Daten sowie der Zweck der Datenbearbeitung durch den Empfänger ausdrücklich zu regeln, wobei eine Delegationsverordnung genügen kann. Hingegen reicht eine allgemeine Vollzugskompetenz in einer Verordnung nicht aus, wenn das Gesetz über die Bekanntgabe von Daten nichts aussagt. Werden besonders schützenswerte Personendaten im Abrufverfahren bekannt gegeben, ist ein Gesetz im formellen Sinn erforderlich.

Mit der Bekanntgabe geht im beurteilten Fall auch eine Zweckänderung einher; die ursprünglich zu registerrechtlichen Zwecken bearbeiteten Daten sollen neu Zwecken der polizeilichen Prävention und Ermittlung bzw. der strafprozessualen Untersuchung dienen. Mit dem neuen Bearbeitungszweck würden die Daten ausserdem zu besonders schützenswerten Daten im Sinne von § 2 lit. d Ziff. 4 DSG.

Auf Grund der Kumulation dieser Punkte war von einem schweren Grundrechtseingriff auszugehen, der entsprechend klare gesetzliche Grundlagen erfordert. Weder im polizeilichen Ermittlungsverfahren noch in der Strafprozessordnung findet sich diesbezüglich eine ausreichende Rechtsgrundlage. Möglich bleibt dabei die Datenbekanntgabe im Einzelfall im Rahmen der Amtshilfe.

Nicht geklärt ist, ob eine Bestimmung, welche eine Veröffentlichung von Daten vorsieht, hierfür genügt. Die Direktion der Justiz und des Innern kam zum Schluss, dass der Grundsatz der Öffentlichkeit des Handelsregisters sowohl Online-Anschlüsse der erwähnten Behörden als auch die Möglichkeit der personenbezogenen Abfrage ermöglicht.

8. Outsourcing der Verwaltungsinformatik

Umsetzung bezüglich Geheimhaltung und Datenschutz

Der Kantonsrat hat die Vorlage des Regierungsrates für ein Gesetz über die Auslagerung von Informatikdienstleistungen angenommen. Das Gesetz trat am 1. Januar 2000 in Kraft (vgl. Tätigkeitsbericht Nr. 4 [1998], S. 10 f.). Das kantonale Amt für Informatikdienste (AID) wurde in die privatrechtlich organisierte Firma Abraxas AG überführt; der Kanton Zürich ist an dieser Unternehmung beteiligt.
In rechtlicher Hinsicht besteht ein grosser Umsetzungsbedarf, da das Auslagerungsgesetz (zu) rudimentäre materielle Regelungen enthält. Die Umsetzung erfolgt auf verschiedenen Ebenen. Einerseits musste eine Übergangsregelung für die bestehenden Auftragsverhältnisse mit dem AID getroffen werden; die Abraxas AG führt die bestehenden Aufträge befristet weiter. Andererseits sind vertragliche Grundlagen für neue Projekte und Aufträge notwendig. Die Kommission für strategische Informatikführung (KOSIF) hat eine Arbeitsgruppe damit beauftragt, entsprechende Lösungen zu erarbeiten. Der Datenschutzbeauftragte wurde in diese Arbeitsgruppe einbezogen, um Lösungsvorschläge betreffend Geheimhaltungspflichten und Datenschutz einzubringen.
Die besondere Problematik beim Outsourcing zeigte sich anhand zweier Anfragen beim Datenschutzbeauftragten. Die Verwaltungsrechenzentrum AG St. Gallen (VRSG), welche u.a. Informatikdienstleistungen für Zürcher Gemeinden erbringt, überarbeitete ihre Allgemeinen Geschäftsbedingungen. Der Abschnitt über «Datenschutz, Daten- und Betriebssicherheit» wurde uns zur Beurteilung unterbreitet. Im Projekt NAPEDUV des Steueramtes (EDV-Lösung zur Veranlagung natürlicher Personen) wurde uns das Kapitel «Datenschutz, Daten- und Betriebssicherheit» des Betriebsvertrages zur Stellungnahme vorgelegt. In beiden Fällen fehlten wesentliche Regelungen. Wir wiesen auf diese Mängel hin.
Es erscheint wenig sinnvoll, in sämtlichen Betriebsverträgen Regelungen über Datenschutz und Datensicherheit zu treffen. Daher entschied die Arbeitsgruppe, der KOSIF den Erlass von «Allgemeinen Geschäftsbedingungen des Kantons Zürich über die Geheimhaltung, den Datenschutz und die Daten- und Informationssicherheit bei der Erbringung von Informatikdienstleistungen» vorzuschlagen. Diese AGB wären allen Dienstleistungserbringern aufzuerlegen und würden ein hohes Datenschutzniveau garantieren. Zugleich könnten verschiedene Probleme in Bezug auf das Amtsgeheimnis und die besonderen Schweigepflichten gelöst werden. Die diesbezüglichen Lücken im Auslagerungsgesetz würden dadurch mehrheitlich geschlossen.

9. Erfassung der Gewerkschaftszugehörigkeit

Verzicht im Rahmen des GAV für Assistenzärztinnen und -ärzte

Der Kanton Zürich sowie der Verband Zürcher Krankenhäuser schloss mit der Sektion Zürich des Verbandes Schweizerischer Assistenz- und Oberärztinnen und -ärzte einen Gesamtarbeitsvertrag ab (GAV; siehe Offizielle Gesetzessammlung Bd. 56, S. 15). Während der Vorbereitung wurden wir vom Personalamt kontaktiert, um verschiedene Fragestellungen aus datenschutzrechtlicher Sicht zu begutachten.
Die allgemeinen Bestimmungen zum Datenschutz wären aus unserer Sicht nicht nötig gewesen; ein Verweis auf die detaillierten Bestimmungen im kantonalen Personalrecht hätte genügt. Dass die Regelung dennoch in der definitiven Fassung des GAV beibehalten wurde, ist aus Gründen der Transparenz zu begrüssen: die Anliegen des Datenschutzes erhalten einen angemessenen Stellenwert im Personalwesen (vgl. auch Tätigkeitsberichte Nr. 1 [1995], S. 14; Nr. 3 [1997], S. 41 und Nr. 4 [1998], S. 14).
Als eigentliche Knacknuss entpuppte sich dagegen die Frage, ob im Personalinformationssystem die Gewerkschaftszugehörigkeit von

Angestellten vermerkt werden dürfe. In der Praxis ist es üblich, dass diejenigen Angestellten, welche nicht Mitglied der beteiligten Gewerkschaft sind, einen Solidaritätsbeitrag leisten, da sie ebenfalls von den Vorteilen des ausgehandelten GAV profitieren. In der Fachliteratur wird denn auch die Meinung vertreten, dass zu diesem Zweck die Gewerkschaftszugehörigkeit durch die Arbeitgeberin oder den Arbeitgeber erfasst werden dürfe.
Entsprechend dem Verhältnismässigkeitsgrundsatz sind von der Arbeitgeberin bzw. vom Arbeitgeber nur Daten zu führen, die zur Durchführung des Arbeitsverhältnisses geeignet und erforderlich sind. Bei der Gewerkschaftszugehörigkeit handelt es sich um ein besonders schützenswertes Datum (§ 2 lit. d Ziff. 1 DSG); das Bearbeiten dieses Datums durch die Arbeitgeberin oder den Arbeitgeber kann sich als sehr sensibel erweisen (vgl. Tätigkeitsberichte Nr. 3 [1997], S. 13 und Nr. 4 [1998], S. 42).
Wir erwogen daher eine Lösung, welche die Erfassung dieses Datums erübrigen würde. Nach unserem Lösungsvorschlag würde bei sämtlichen Angestellten ein Solidaritätsabzug gemacht und dem Verband überwiesen. Diesem obläge es, intern den eigenen Mitgliedern den entsprechenden Betrag zurückzuerstatten. Bei mehreren beteiligten Verbänden würde der Ablauf über einen zu bildenden Fonds erfolgen. In beiden Fällen könnte auf die Erfassung der Gewerkschaftszugehörigkeit verzichtet werden. Da wir jedoch nicht sämtliche Praktikabilitätsüberlegungen einbeziehen konnten, verzichteten wir in diesem Fall auf eine Empfehlung. Der Kanton Zürich hat unseren Argumenten Rechnung getragen und die von uns vorgeschlagene Lösung gewählt; der Solidaritätsbeitrag wird bei sämtlichen dem GAV unterstellten Angestellten erhoben.

10. Einsicht in archivierte Akten

Akten eines längst abgeschlossenen Vaterschaftsverfahrens

Ein Bezirksgericht hatte ein Akteneinsichtsgesuch einer Person zu beurteilen, welche vor über vierzig Jahren als Kind in einem Vaterschaftsprozess involviert gewesen war. Bei der Beurteilung stellte es sich die Fragen, ob die betroffene Person überhaupt ein Einsichtsrecht hat, ob eine Offenlegungspflicht besteht und wie allenfalls eine Interessenabwägung vorzunehmen ist.
Die Anwendbarkeit des Datenschutzgesetzes (DSG) war ohne weiteres gegeben, da das Verfahren abgeschlossen war und die Akten nach wie vor (d.h. über das Inkrafttreten des DSG) aufbewahrt wurden. Ebenfalls zur Anwendung gelangte das Archivgesetz, in diesem Fall § 14 der Verordnung des Obergerichts über die Archive der Gerichte, Friedensrichter-, Gemeindeammann-, Stadtammann- und der Betreibungsämter. Nach dieser Bestimmung sind Akten während zwanzig Jahren nach Abschluss des Verfahrens aufzubewahren, bevor sie zu archivieren sind. Diese Frist war längst verstrichen, weshalb die Akten unter dem Gesichtspunkt der (spezialrechtlichen) Archivregelung zu betrachten waren.
Im Folgenden wäre zu prüfen, ob die Akten noch in die Schutzfrist fielen. Dies war im zu beurteilenden Fall anzunehmen. (Eine nähere Prüfung war mangels Angaben nicht möglich.) Im Ergebnis zeigte sich, dass diese Frage im Einzelfall irrelevant war. Eine Ausnahme für eine Einsichtnahme vor Ablauf der Schutzfrist ist nämlich gegeben, wenn – wie in diesem Fall – eine betroffene Person ein Auskunfts- (bzw. Akteneinsichts-)Begehren stellt.
In diesem Fall ist eine Einsichtnahme grundsätzlich möglich, auch wenn noch Schutzfristen laufen.
Der Anspruch auf Akteneinsicht beurteilt sich einerseits nach dem DSG, andererseits nach der Akteneinsichtsordnung des anwendbaren Verfahrensgesetzes bzw. des Art. 4 der Bundesverfassung (BV) von 1874 (neu: Art. 29 BV vom 18. April 1999). Das Auskunftsrecht gemäss § 17 DSG und das Akteneinsichtsrecht sind nicht deckungsgleich (zur Unterscheidung vgl. Tätigkeitsbericht Nr. 1 [1995], S. 15). Insbesondere setzt das Akteneinsichtsrecht einen Interessennachweis voraus.

In diesem Zusammenhang war auf die bundesgerichtliche Praxis hinzuweisen. Im Entscheid BGE 115 Ia 234 berücksichtigte das Bundesgericht bei der Beurteilung einer kantonalen Regelung der modernen Fortpflanzungsmedizin einen Entscheid des (deutschen) Bundesverfassungsgerichts, welches aus dem allgemeinen Persönlichkeitsrecht ein Recht auf Kenntnis der eigenen Abstammung ableitet, und schloss nicht aus, dass ein Samenspender in einem Verfahren allenfalls seine Anonymität nicht wahren könne. In einem neueren Entscheid zur gleichen Thematik (BGE 119 Ia 460) wurde auf Art. 24novies BV 1874 (neu: Art. 119 BV 1999) hingewiesen, der jeder Person ein Recht auf Zugang zu den Daten über ihre Abstammung einräumt (Art. 119 Abs. 2 lit. g BV 1999).
Wird ein Interessennachweis als ausreichend erachtet, stellt sich in der Folge die Frage von Einschränkungen auf Grund überwiegender entgegenstehender Interessen Dritter. So könnten etwa Interessen der direkt betroffenen Personen, aber auch von Zeugen, Sachverständigen usw. einer Einsicht entgegenstehen. Diese Interessen sind im Einzelfall gegeneinander abzuwägen. In einem älteren Entscheid hatte das Bundesgericht die Interessen von Vater, Mutter und Pflegeeltern an der Geheimhaltung noch höher gewichtet (BGE 112 Ia 97). Inwieweit dieser Entscheid vor dem neueren Verfassungsartikel noch Bestand hätte, ist offen.
Im konkreten Fall erübrigte sich für das Bezirksgericht die Einzelfallbeurteilung, da das Begehren zurückgezogen wurde. In Zukunft steht ihm nun aber eine Zusammenstellung der neueren gesetzlichen Regelung sowie der Praxis zur Interessenabwägung als Beurteilungsgrundlage für ähnlich gelagerte Fälle von Akteneinsichtsgesuchen zur Verfügung.

11. Aufsicht über den Regierungsrat

Keine Zuständigkeit des Datenschutzbeauftragten

Im Rahmen der Beantwortung einer kantonsrätlichen Anfrage erteilte der Regierungsrat den Medien umfangreiche Auskünfte über den Inhalt eines Sachgeschäftes. Dabei wurden die betroffenen Personen namentlich genannt, und es wurden Einzelheiten zum Sachgeschäft bekannt gegeben. Eine betroffene Person fühlte sich in ihren Persönlichkeitsrechten verletzt und wandte sich an den Datenschutzbeauftragten.
In Zusammenhang mit den materiellen Abklärungen stellte sich die Frage, ob der Datenschutzbeauftragte auch für eine datenschutzrechtliche Aufsicht über den Regierungsrat zuständig ist. Weder die Gesetzesmaterialien des Kantons Zürich noch ein Quervergleich mit anderen Kantonen liessen eine eindeutige Schlussfolgerung zu. Beim Erlass des DSG wurde diese Frage weder in der Kommission noch im Kantonsrat ausdrücklich diskutiert; lediglich die Frage nach der Wahlbehörde (Regierungsrat oder Kantonsrat) wurde ausführlich besprochen, wobei letztlich ein knapper Entscheid zugunsten des Regierungsrates als Wahlinstanz gefällt wurde.
Im Bund und in anderen Kantonen sind verschiedene Lösungen vorgesehen, die von der Zuständigkeit bis zur ausdrücklichen Ausnahme der Aufsicht über die Exekutive reichen.
Da es nicht Aufgabe des Datenschutzbeauftragten sein kann, in diesem Bereich über seine Aufsichtskompetenz zu entscheiden, stellten wir im Rahmen der materiellen Abklärungen dem Regierungsrat vorfrageweise die Frage nach der Zuständigkeit bzw. den Aufsichtsrechten. Der Regierungsrat kam zum Schluss, dass dem Datenschutzbeauftragten keine Vermittlungs- und Aufsichtsfunktion gegenüber dem Regierungsrat zukommt. Bei einer Anfrage einer betroffenen Person, ob ein konkretes Handeln des Regierungsrates mit den Anforderungen des Datenschutzes übereinstimme, kann er deshalb lediglich eine Rechtsauskunft erteilen. Sofern dies nicht genügt, besteht die Möglichkeit, die betroffene Person an den kantonalen Ombudsmann zu verweisen, der auf Grund seiner Stellung und seiner Aufgaben auch den Regierungsrat überprüfen kann.

(Kein) Datenschutz bei geografischen Informationssystemen?

In geografischen Informationssystemen (GIS) werden auch Personendaten bearbeitet. Der Persönlichkeitsschutz ist daher sowohl auf konzeptioneller als auch auf regulatorischer Ebene zu berücksichtigen und angemessen umzusetzen.

Informationssysteme zur Bewirtschaftung raumbezogener Daten – geografische Informationssysteme oder kurz GIS – sind als Instrumente für die Raumplanung und den Umweltschutz konzipiert worden. Es handelt sich dabei vor allem um raumbezogene Daten, wie sie aus den klassischen gedruckten kartografischen Werken (Stadtpläne, Landeskarten, Atlasse usw.) bekannt sind. Heutzutage sind diese Informationen in GIS weitgehend digitalisiert. Auf Grund der technologischen Entwicklungen ist es ohne weiteres möglich, die Ebenen verschiedener einzelner Pläne und Karten zu verknüpfen und/oder mit Daten aus der Statistik oder aus anderen Datenbanken zu verbinden. So können auch neue Informationen gewonnen und neue Funktionalitäten (z.B. Suchfunktionen) zur Verfügung gestellt werden. Das Potenzial von GIS wird erst ersichtlich, wenn man sich die konkreten Anwendungsmöglichkeiten vor Augen führt (siehe Kasten nebenan).

Datenschutzrechtliche Relevanz

Die datenschutzrechtliche Relevanz von GIS wird häufig verkannt, weil davon ausgegangen wird, es handle sich lediglich um raumbezogene Daten ohne Personenbezug. Bei einem grundstücksgenauen Detaillierungsgrad von GIS-Daten und/oder ihrer Verknüpfung mit anderen Datenbanken werden jedoch einzelne Personen bestimmbar (z.B. Eigentümer oder Bewohner), wodurch die Informationen zu Personendaten werden.
Die vielfältigen Verknüpfungsmöglichkeiten in GIS führen dazu, dass in den meisten Fällen von einem Personenbezug der Daten ausgegangen werden muss. Der Datenschutzbeauftragte hat die verantwortlichen Stellen bereits früher auf diese Problematik hingewiesen (vgl. Tätigkeitsbe-

Potenzial von GIS

Das Potenzial von GIS wird bei den wachsenden Anwendungen ersichtlich. GIS sind als Instrumente für Raumplanung und Umweltschutz konzipiert. Spezifische Anwendungsmöglichkeiten sind etwa die Planung der Besiedlung oder der Bewirtschaftung des Landes, Massnahmen zum Schutz von Pflanzen und Tieren, ein Rohstoff- bzw. Ressourcenmanagement (z.B. bezüglich Grundwassernutzung) oder eine Notfall- und Katastrophenplanung (z.B. bezüglich Überschwemmungen).
Es bestehen aber auch viel weiter gehende Möglichkeiten. GIS-Anwendungen können für die Beurteilung von Gesundheitsrisiken (Luft- und Lärmbelastung, Altlastenverdachtsflächen usw.) genutzt werden, wenn Luft- und Lärmbelastungskarten, Altlastenverdachtsflächenkataster usw. gezielt ausgewertet werden. Geodemografische Studien zeigen, dass trotz Mobilität die wirtschaftliche und soziale Struktur der meisten Quartiere und Zonen relativ stabil ist. In Verbindung mit Daten der Volkszählung können soziale und wirtschaftliche Klassen definiert und Persönlichkeitsprofile erstellt werden. Die Verknüpfung von GIS-Daten mit statistischen Daten über das Stimmverhalten kann für gezielte politische Kampagnen genutzt werden. Moderne militärische Kriegführung beruht zu einem grossen Teil auf GIS-Anwendungen, wie der Golfkrieg der Vereinten Nationen gegen den Irak und der Luftkrieg des Nordatlantischen Bündnisses gegen Serbien gezeigt haben. Auf Grund solcher Informationen wurden Ziele ausgewählt. Falsche Daten können in solchen Fällen schwere Folgen haben. So erfolgte die Zerstörung der chinesischen Botschaft in Belgrad durch die Nato im Mai 1999 auf Grund falscher GIS-Daten. Die Technologie kann auch zum Schaden der eigenen Bevölkerung und des eigenen Staates eingesetzt werden, wenn terroristische oder kriminelle Organisationen GIS-Informationen für ihre Zwecke verwenden.

richt Nr. 2 [1996], S. 16 f.). In der Folge wurde eine Verordnung über geografische Informationssysteme erlassen. Wir bezweifelten, dass diese Verordnung eine ausreichende Rechtsgrundlage für die Datenbearbeitungen in GIS darstellt, und regten (erneut) eine umfassende Abklärung der Rechtslage an (vgl. Tätigkeitsbericht Nr. 4 [1998], S. 41).

Grundlagenpapier

Im Berichtsjahr wurden wir mit weiteren Einzelanfragen konfrontiert. Der Zürcher Verkehrsverbund wollte sein Internet-Angebot um GIS-Funktionalitäten erweitern. Durch Eingabe von Ausgangs- und Zieladresse im Fahrplan sollten Start- und Zielhaltestellen nach Berechnung der Verbindung mit einer Karte visualisiert werden können.
Das «Programm 2010» der (ehemaligen) Flughafendirektion befasst sich mit der Planung und Umsetzung von Schallschutzmassnahmen im Rahmen der 5. Bauetappe des Flughafens und beinhaltet auch eine entsprechende Information der Bevölkerung. Dabei sollten GIS-Daten verwendet werden, indem mittels Abfragemöglichkeit nach Adressen bzw. Gebäuden ersehen werden kann, welche Lärmbelastung besteht und ob bzw. wann Sanierungsmassnahmen geplant sind.
In beiden Fällen besteht ein öffentliches Interesse an den Datenbearbeitungen bzw. -veröffentlichungen. Die datenschutzrechtlichen Fragen konnten jedoch nicht abschliessend geklärt werden, was zu einer Rechtsunsicherheit bei allen Beteiligten führte. Insbesondere blieb offen, ob die bestehenden Rechtsgrundlagen für den Zweck der vorgesehenen Datenbearbeitungen ausreichen.
Wir entschlossen uns daher, ein Grundlagenpapier zuhanden der verantwortlichen Stellen zu erstellen, das die Problematik der Datenbearbeitungen in GIS und die sich stellenden Fragen aufzeigt. Das Grundlagenpapier soll die Fragestellungen veranschaulichen und als Diskussionsbasis dienen. Es enthält auch Empfehlungen in Bezug auf das Vorgehen und die zu beantwortenden Fragestellungen bei GIS-Datenbearbeitungen (vgl. Kasten, S. 21).

Zweckbindung und Öffentlichkeit von GIS-Daten

Auszugehen ist von den verschiedenen einzelnen Bearbeitungen raumbezogener Daten. In verschiedenen Gesetzen finden sich Bestimmungen über bestimmte Kataster und Pläne, z.B. Heimatschutzinventar, Haltestellen des öffentlichen Verkehrs, Lärmemissionskataster, Übersichtsplan, amtliche Vermessung usw.
Einzelne Erlasse bestimmen, dass diese Pläne «öffentlich» oder zu veröffentlichen sind, wobei Umfang und Form der Öffentlichkeit nicht oder nur in allgemeiner Weise umschrieben sind. Herkömmlicherweise wurden gedruckte Pläne erstellt und abgegeben.
Die Digitalisierung dieser Informationen bietet neue Möglichkeiten. Veröffentlichungen erfolgen in neuen Formen und Medien (z.B. CD-ROM, Internet usw.). Die Informationen können auf Grund von Schnittstellen oder standardisierten Applikationen verknüpft werden. Die Daten erhalten damit eine neue Qualität und ein neues Potenzial in Bezug auf Eingriffe in Persönlichkeitsrechte.
Werden Daten in einem Pool zusammengeführt, wird der Grundsatz der Zweckbindung tangiert. Dieser Grundsatz besagt, dass Daten nur zu einem Zweck bearbeitet werden dürfen, der bei der Beschaffung angegeben wurde, der aus den Umständen ersichtlich ist oder der gesetzlich vorgesehen wird (§ 4 Abs. 4 DSG). Die einzelnen Pläne bzw. Daten dienen ganz bestimmten Zwecken, die sich aus den jeweiligen bereichspezifischen Erlassen herleiten lassen. In geografischen Informationssystemen ist nicht mehr gewährleistet, dass die Daten nur dem ursprünglichen Bearbeitungszweck dienen. Aus diesem Grund ist davon auszugehen, dass die bereichspezifischen Rechtsgrundlagen nicht ausreichen, da der Gesetzgeber bei deren Erlass die neuen Bearbeitungsformen nicht hatte einbeziehen können.
In Bezug auf die «Öffentlichkeit» stellt sich die Frage, ob die neuen technologischen Möglichkeiten (z.B. Internet) überhaupt vom Gesetz erfasst sind. Auch hier hatte der Gesetzgeber beim Erlass der Normen mangels Kenntnis der neuen Technologien meist noch keine Gelegenheit, die Aspekte der

neuen Medien und die damit verbundenen neuen Gefahren für den Persönlichkeitsschutz zu berücksichtigen und seine Wertungen in angemessene Rechtsgrundlagen einfliessen zu lassen.

Ansatz einer Lösung?

Das DSG statuiert Rahmenbedingungen für Datenbearbeitungen, insbesondere das Erfordernis gesetzlicher Grundlagen. Dabei geht es darum, für die betroffenen Personen, deren Persönlichkeitsrechte auf dem Spiel stehen, Transparenz zu schaffen, indem die Datenbearbeitungen auf demokratisch ausreichend legitimierten Rechtsgrundlagen beruhen. Der Datenschutzbeauftragte erachtet es als notwendig, dass Möglichkeiten und Folgen geografischer Informationssysteme öffentlich diskutiert werden. Darauf basierend sind die notwendigen gesetzlichen Grundlagen, die im öffentlichen Interesse liegen und verhältnismässig sind, zu erlassen.

Empfehlungen des Datenschutzbeauftragten zu GIS*

Bei Projekten im Zusammenhang mit der Bewirtschaftung von Raumdaten ist den Persönlichkeitsrechten betroffener Personen die notwendige Aufmerksamkeit zu widmen. Insbesondere sind die Risiken und Gefahren durch angemessene Rechtsgrundlagen über die Verwendung der Daten zu minimieren. Aus diesem Grund empfiehlt der Datenschutzbeauftragte, folgende Überlegungen in die Konzeption solcher Projekte einzubeziehen:

1. Datenvermeidung und Datensparsamkeit
Gemäss den Grundsätzen der Datenvermeidung und der Datensparsamkeit haben geografische Informationssysteme wenn immer möglich anonymisierte Daten zu verwenden, d.h., es ist so weit als möglich auf Personendaten respektive auf einen Personenbezug der Daten zu verzichten.

2. Schaffung von im öffentlichen Interesse liegenden, verhältnismässigen Rechtsgrundlagen
Soweit ein solcher Verzicht nicht möglich oder nicht gewünscht ist, sind ausreichende Rechtsgrundlagen für die Datenbearbeitungen im Rahmen solcher Systeme und Projekte zu schaffen.
Die Rechtsgrundlagen haben folgende Fragen zu regeln:

- Welche Zwecke werden mit der jeweiligen Datenbearbeitung verfolgt?
- Welche Daten werden für welchen Zweck benötigt?
- Wie werden die Daten bearbeitet?
- Werden Daten kombiniert bzw. Kombinationen ermöglicht und wenn ja, wie?
- Wer ist für welche Datenbearbeitungen verantwortlich?
- Welchen Stellen/Personen werden welche Daten regelmässig (online) weitergegeben?
- Welchen Stellen/Personen werden welche Daten im Einzelfall weitergegeben?
- Welche Rechtsansprüche haben die betroffenen Personen?
- Dürfen Daten kommerzialisiert werden und wenn ja, welche Daten auf welche Weise?

Angesichts der Tragweite der Datenbearbeitungen und der absehbaren künftigen Entwicklungen scheint der Erlass eines Gesetzes im formellen Sinn notwendig und sinnvoll.

3. Überprüfung bestehender Systeme
Bestehende Konzepte, Technologien, Projekte und Rechtserlasse sind in Bezug auf die rechtlichen Erfordernisse und die Angemessenheit zu überprüfen.

**aus: Datenschutzbeauftragter des Kantons Zürich, Bewirtschaftung raumbezogener Daten (GIS, GeKaGe usw.) und Datenschutz-Grundlagenpapier, Zürich, 20. Januar 2000 (siehe www.datenschutz.ch, Rubrik «Publikationen»)*

Sicherheitsstrategie für die Informatik

Mit dem Projekt SOPRANO wurden die Vorbereitungsarbeiten für eine sichere Informatik-Infrastruktur geleistet. Als Ergebnis wurde ein Strategiebericht erarbeitet, der die Einführung einer Public Key Infrastructure (PKI) vorsieht.

Eine verwaltungsweite Sicherheitsstrategie hat die folgenden Anforderungen abzudecken:
1. Die Vertraulichkeit der Datenübermittlung, damit keine unbefugten Personen die Daten lesen können.
2. Die Echtheit von Absender und Empfänger, damit einwandfrei feststellbar wird, wer mit wem kommuniziert.
3. Die Feststellung allfälliger Veränderungen, damit keine verfälschten Informationen verarbeitet werden.
4. Die Verbindlichkeit der Kommunikation, damit nicht später die Datenübermittlung abgestritten werden kann.

Eine sichere Kommunikation ist dabei nicht nur innerhalb der Verwaltung für die Optimierung der internen Abläufe, sondern auch für den elektronischen Kontakt zwischen der Verwaltung und den Bürgerinnen und Bürgern sowie mit der Wirtschaft und anderen Verwaltungen vorzusehen. Dies beinhaltet insbesondere die folgenden Möglichkeiten:

Verwaltungsintern:
- Vertraulicher Datenaustausch und vertrauliche Datenbearbeitung in dezentralen Anwendungen (wie zum Beispiel im Personalprojekt PALAS).
- Sichere E-Mail: E-Mails mit vertraulichem Inhalt können verschlüsselt und elektronisch unterschrieben (authentisiert) werden (auch solche an Adressaten ausserhalb der Verwaltung).
- Vertraulicher und verbindlicher Datenaustausch zwischen Gemeinden und kantonaler Verwaltung (zum Beispiel Übermittlung von Abstimmungsresultaten via Internet).

Verwaltungsextern:
- Elektronisches Einreichen von Gesuchsformularen, Anträgen, Abrechnungen etc. (Passbestellungen, Führer- und Fahrzeugausweise, Einreichen von Bauabrechnungen usw.).
- Übermittlung von Steuererklärungen via Internet und Möglichkeit der automatischen Weiterverarbeitung in den internen Systemen. Dabei können die Vertraulichkeit und die Echtheit des Absenders sichergestellt werden.

Alle diese Aktivitäten verlangen eine vertrauliche, verbindliche, inhaltlich nicht veränderte und nicht abstreitbare Kommunikation. Dies ist heute auf der Basis einer Public Key Infrastructure (PKI) als technologischer Standard möglich. Die PKIs werden sowohl in der Privatwirtschaft wie auch in der Verwaltung weltweit zur umfassenden Lösung der bestehenden und zukünftigen Sicherheitsanforderungen eingesetzt. PKIs sind deshalb Grundlage für sicheres E-Business und sicheres E-Government.

Ausgangslage für das Projekt SOPRANO

Im Rahmen der Einführung des Personalinformationssystems PALAS hatte der Regierungsrat entschieden, die Sicherheitsaspekte dieses Projektes nicht losgelöst zu betrachten, sondern sie im Rahmen einer verwaltungsweiten Sicherheitsstrategie zu lösen. Hierzu wurde eine Projektgruppe unter der Leitung des Datenschutzbeauftragten bestimmt, welche diese Strategie zu erarbeiten hatte (Projekt SOPRANO). In diesem Projekt waren alle interessierten Direktionen und Stellen vertreten, insbesondere die Finanzdirektion, die Direktion der Justiz und des Innern, die Direktion für Soziales und Sicherheit, die Gesundheitsdirektion, die Bildungsdirektion und das Notariatsinspektorat. Ausgangslage waren dabei die rechtlichen Rahmenbedingungen (Datenschutzgesetz und Informatiksicherheitsverordnung) wie auch bestehende Sicherheitslösungen.

Erfahrungen aus dem Pilot-Projekt Digitale Signatur

Der Datenschutzbeauftragte hat mit der Teilnahme am Pilot-Projekt Digitale Signatur (siehe Tätigkeitsbericht Nr. 4 [1998], S. 34) notwendige Erfahrungen beim Einsatz einer Public Key Infrastructure gesammelt. Die technische Funktionalität wurde für alle Testfälle unter den Teilnehmern wie auch zwischen den Teil-Piloten erfolgreich bewiesen. Die wichtigsten voneinander abhängigen Problemkreise waren Administration/Verzeichnisse, Kosten/Umfeld und Ausbreitung/Bedienung. Sie wurden vom Projekt SOPRANO wie folgt beachtet: Die Anforderung, dass ein zentrales Verzeichnis die Speicherung der Zertifikate sowie den zentralen Rückruf nicht mehr gültiger Zertifikate übernimmt, ist erkannt worden (Projekt für ein zentrales Directory). Das Speichern der persönlichen Schlüssel (Private Keys) auf einer Smart Card ist für diejenigen PCs vorgesehen, die gemäss Informatiksicherheitsverordnung den Sicherheitsstufen 2 und 3 zugewiesen werden.

Im Projekt SOPRANO wurden drei verschiedene Anbieter von PKIs evaluiert. Auf Grund zweier Workshops und von Referenzbesuchen wurden die Voraussetzungen für eine PKI in der kantonalen Verwaltung abgeklärt. Dabei hat sich gezeigt, dass die beiden bis zum Schluss evaluierten PKI-Angebote die allgemeinen Bedürfnisse nach einer sicheren und vertraulichen Kommunikation verwaltungsintern wie -extern abdecken können. Sie unterstützen die vorhandenen Informatikprozesse in der kantonalen Verwaltung, sind kompatibel mit bestehenden Sicherheitslösungen und erfüllen die Sicherheitsanforderungen der Stufe 2 und 3 gemäss Informatiksicherheitsverordnung (ISV). Eine PKI gibt eine technische und organisatorische Infrastruktur vor, die von verschiedenen Applikationen und E-Mail-Systemen mit geringem Integrationsaufwand genutzt werden kann. Bestehende Host-Applikationen können ebenfalls weitgehend integriert werden. Neue Projekte können auf dieser Infrastruktur aufbauen, bereits bestehende Lösungen können in die PKI eingebunden werden.
Die Kosten des Einsatzes einer PKI wurden ebenfalls durch das Projekt abgeklärt. Es hat sich gezeigt, dass dank einem modularen Aufbau der Infrastruktur die Investitions- und Betriebskosten für diese gezielten Massnahmen für die Informatiksicherheit sich je nach Sicherheitsstufe und Softwareausstattung in einem akzeptablen Rahmen bewegen.

Der Nutzen des Aufbaus einer zentralen Public Key Infrastructure liegt dabei insbesondere in den folgenden Punkten:

1. Basisinfrastruktur für alle E-Government-Projekte.
2. Kosteneinsparungen (werden durch die Möglichkeit des elektronischen Datenaustausches in den einzelnen Projekten realisiert).
3. Grundlage für die Erfüllung der Sicherheitsanforderungen gemäss ISV.
4. Modulare Aufbaumöglichkeit.
5. International anerkannte und implementierte Standards für den sicheren Datenaustausch mit Unternehmen sowie mit Bürgerinnen und Bürgern.

Als Grundlage für die Lösung der internen Sicherheitsanforderungen und unentbehrlich für sicheres E-Government ist der Aufbau einer PKI unverzüglich in Angriff zu nehmen. Daher soll das Projekt SOPRANO weitergeführt werden.

Sensible Datenbekanntgaben

Das Festlegen des Umfanges und der Grenzen von Datenbekanntgaben ist in der Praxis immer wieder heikel.

1. Publikation von Vormundschaftssachen

Beachtung des Verhältnismässigkeitsgrundsatzes

Eine Person machte uns auf die teilweise sehr weit gehende Publikationspraxis aufmerksam, welche eine zürcherische Gemeinde in Bezug auf Vormundschaftsdaten verfolgte. In der Folge konnten wir auf Grund eigener Abklärungen feststellen, dass mehrere Gemeinden im Amtsblatt jeweils neben Name und Adresse der betroffenen Person sowie des Vormundes weitere Informationen aus deren persönlichem Umfeld der Öffentlichkeit zugänglich machten, so beispielsweise Hinweise zum aktuellen Aufenthaltsort in einer psychiatrischen Klinik oder in einer Anstalt.

Einschlägig für die Publikation von Bevormundungsfällen ist Art. 375 ZGB sowie § 88 EG zum ZGB. Mit einer Publikation soll die Schaffung der erforderlichen Transparenz im Geschäftswesen erreicht werden: Potenzielle Geschäftspartner müssen informiert sein, dass sie mit der betroffenen Person ohne Mitwirkung des Vormundes keine Geschäfte abwickeln können. Entsprechend lässt Art. 375 Abs. 2 ZGB denn auch einen Verzicht auf die Publikation zu, sofern die psychische Krankheit offenkundig oder die betroffene Person in einer Anstalt untergebracht ist. Folgerichtig dürfen nicht mehr als die zur Identifikation der betroffenen Person und des zuständigen Vormundes erforderlichen Personendaten sowie ein Hinweis auf Art und Beginn der vormundschaftlichen Massnahme veröffentlicht werden. Die Angabe des zivilrechtlichen Wohnsitzes reicht aus, weshalb weitergehende Kenntnisse über den aktuellen Aufenthaltsort nicht vonnöten und somit unzulässig sind. Darüber hinaus handelt es sich beim Hinweis auf den Aufenthalt beispielsweise in einer psychiatrischen Klinik um Angaben zur Gesundheit und deshalb um besonders schützenswerte Personendaten. Ebenso wenig ist aufzuführen, wenn zwischen bevormundeter Person und Vormund ein allfälliges familienrechtliches Verhältnis besteht, weshalb auf solche Informationen zu verzichten ist.

Wir wandten uns an die Verwaltungskommission des Obergerichtes des Kantons Zürich als der in zweiter Instanz zuständigen Aufsichtsbehörde im Vormundschaftswesen mit der Bitte, zur Publikationspraxis Stellung zu nehmen. Diese befand es als vertretbar, auf die Bekanntgabe des genauen Aufenthaltsortes zu verzichten. Sie führte jedoch aus, dass es im Allgemeinen erforderlich sei, neben dem zivilrechtlichen Wohnort auch den faktischen Wohnort zu nennen. Im Übrigen verwies sie auf ein Kreisschreiben der Justizdirektion aus dem Jahre 1967, welches den wesentlichen Anliegen des Datenschutzes bereits Rechnung trage.

Wir konnten uns mit dem Inhalt des erwähnten Kreisschreibens einverstanden erklären. Dieses hält nämlich in vorbildlicher Weise fest, dass ausschliesslich die getroffene vormundschaftliche Massnahme und die genauen Angaben über die bevormundete Person sowie den Vormund zu veröffentlichen sind. «Hingegen sind Angaben über den Anstaltsaufenthalt eines Entmündigten nicht nötig und haben zu unterbleiben», wodurch «eine dem Zweck der Veröffentlichung fremde diffamierende Wirkung für den Bevormundeten und seine Angehörigen vermieden werden» soll. Folgerichtig besteht für die betroffenen vormundschaftlichen Stellen richtigerweise kein Spielraum, ob in einem einzelnen Fall neben dem zivilrechtlichen Wohnsitz zusätzliche Angaben zum Aufenthaltsort veröffentlicht werden.

Eine Verletzung des Verhältnismässigkeitsgrundsatzes ist als noch gravierender zu bewerten, seit das Amtsblatt im Internet veröffentlicht wird, da die bekannt gegebenen Personendaten weltweit sowie auf unabsehbare Zeit abrufbar und ausserdem für beliebige Zwecke weiter verwertbar geworden sind.

2. Datenfluss von der Einwohnerkontrolle zur Schulpflege

Angaben über noch nicht schulpflichtige Kinder

Gemäss § 38 Volksschulverordnung haben die Einwohnerkontrollen den Schulpflegen rechtzeitig vor Beginn des Schuljahres die neu in die Schulpflicht eintretenden sowie jeweils die zu- und weggezogenen schulpflichtigen Kinder zu melden. Folgerichtig haben wir in unserem Rundschreiben an die Einwohnerkontrollen (vgl. Tätigkeitsbericht Nr. 4 [1998], S. 28 f.) entsprechende Mutationsmeldungen ausdrücklich als zulässig aufgeführt. In einer Anfrage wurden wir daraufhin ersucht, nochmals zu überprüfen, ob den Schulpflegen nicht ein weiterer Kreis von Daten zugänglich zu machen sei. Denn um ihre Aufgaben pflichtgemäss und im Interesse der Öffentlichkeit erfüllen zu können und insbesondere um eine sorgfältige, langfristige Planung und gut strukturierte Organisation zu ermöglichen, müsse bekannt sein, wie sich die Kinderzahl in einer Gemeinde pro Jahrgang entwickle. In unserer Antwort hielten wir fest, dass gesetzliche Grundlagen für eine automatische Übermittlung von Daten noch nicht schulreifer Kinder nicht vorhanden sind. Ebenso wenig erscheinen solche Angaben als zur Aufgabenerfüllung notwendig. Zwar hat die Schulpflege dafür zu sorgen, dass jedes Kind später bei Eintritt in die Schulpflicht in geeigneten Räumen durch eine kompetente Lehrkraft unterrichtet werden kann; ebenso hat sie einen zumutbaren Schulweg zu gewährleisten. Hierbei handelt es sich indessen um typische Planungsdaten: bekannt sein muss nur die (anonymisierte) Kinderzahl eines Jahrgangs, allenfalls aufgeschlüsselt nach Quartieren oder Dorfteilen. Aus diesen nicht personenbezogenen und daher auch nicht dem Datenschutzgesetz unterstellten Informationen, welche die Einwohnerkontrolle jederzeit liefern darf, lässt sich die mutmassliche Entwicklung im Schulwesen und damit der Bedarf an Schulräumen und Lehrkräften für die Zukunft ohne weiteres extrapolieren. Zudem wäre eine bedarfsgerechtere Planung angesichts der allgemein feststellbaren zunehmenden Mobilität der Bevölkerung auch mit Hilfe der gewünschten Personendaten nicht zu erwarten.

Die Frage, ob die Schulbehörden nebst Angaben zu den neu in die Schulpflicht eintretenden sowie den neu zu- beziehungsweise weggezogenen Kindern nicht weitere Daten haben müsse, wurde schliesslich in einer kantonsrätlichen Anfrage dem Regierungsrat vorgelegt. Der Regierungsrat führte in seiner Antwort aus, dass zur Aufgabenerfüllung der Schulbehörden – obwohl einschlägige Rechtsgrundlagen nicht vorhanden sind – einer Weitergabe von Daten über alle Kinder und bezüglich unterschiedlichster Bereiche nichts entgegenzusetzen sei; allerdings müssten längerfristig die erforderlichen Gesetzesgrundlagen für einen solchen Datenfluss geschaffen werden.

Anlässlich einer weiteren Anfrage stellten wir präzisierend fest, dass die Namen der neu zum Kindergartenbesuch berechtigten Kinder im Rahmen einer einmaligen Datenbekanntgabe weiterzugeben sind. Denn gemäss § 74 Volksschulgesetz muss die zuständige Schulbehörde gewährleisten, dass jedes Kind ein bis zwei Jahre lang den Kindergarten besuchen kann. Dieser Pflicht kann sie nur nachkommen, wenn sie die betroffenen Eltern rechtzeitig kontaktieren und auf die Möglichkeit des Kindergartenbesuchs hinweisen kann.

3. Personendaten an die Polizei

Datenschutzrechtliche Rahmenbedingungen zu beachten

In unserem Rundschreiben an die Einwohnerkontrollen (vgl. Tätigkeitsbericht Nr. 4 [1998], S. 28 f.) listeten wir diejenigen Stellen auf, welche automatisch mit Mutationsmeldungen bedient werden dürfen. Die Polizei ist dabei nicht als berechtigte Datenempfängerin aufgeführt. In der Folge wurden wir gebeten zu prüfen, ob die Kantons- und Stadtpolizei nicht zur Erfüllung ihrer Aufgaben auf automatische Mutationsmeldungen angewiesen sei.

Wir stellten fest, dass der Polizei zwar durch die §§ 22 und 23 der Strafprozessordnung gewisse Aufgaben im Hinblick auf die Aufklärung von Delikten überbunden worden sind. Beispielsweise muss sie nach ausgeschriebenen Personen fahnden. Daraus ist jedoch keine Berechtigung der zuständigen Polizeistellen abzuleiten, grundsätzlich die Daten der Gemeindeeinwohnerinnen und -einwohner zu erhalten. Damit wird lediglich zu amtshilfeweisen Abklärungen im konkreten Einzelfall ermächtigt. Im Übrigen würde die Weitergabe von Angaben zur gesamten Einwohnerschaft auch dem Verhältnismässigkeitsprinzip widersprechen, ist doch für die Polizei nur ein kleiner Bruchteil aller betroffenen Personen tatsächlich von Interesse. Ausserdem wäre ein solches Vorgehen auch wenig effizient, indem sich polizeilich gesuchte Personen wohl mehrheitlich nicht ordnungsgemäss bei der jeweiligen Einwohnerkontrolle an- und abmelden.

Um einen noch weiter gehenden Datenfluss wurde eine Einrichtung ersucht, welche physisch oder psychisch behinderte Menschen betreut und ausbildet: Sie wurde um Listen aller neu eingetretenen Personen zwecks polizeilicher Überprüfung angefragt.
Allein durch die Herausgabe von Listen der Neueintritte an die zuständige Polizeistelle würde indessen bekannt gegeben, dass die betroffenen Personen in irgendeiner Form gesundheitlich angeschlagen und daher betreuungsbedürftig sind, weshalb besonders schützenswerte Daten gemäss § 2 lit. d Ziff. 2 DSG tangiert wären. Eine Weitergabe von Daten müsste infolgedessen die qualifizierten Anforderungen von § 5 DSG erfüllen.
Wir stellten fest, dass für einen solchen Datentransfer keine Rechtsgrundlagen im erforderlichen Präzisierungsgrad vorhanden sind. Abgesehen davon wäre auch hier bei Meldungen aller neu eingetretenen Personen die Verhältnismässigkeit nicht gewahrt. Immerhin kann die Polizei bei der Betreuungsstelle amtshilfeweise um die erforderlichen Angaben nachsuchen, wenn in Bezug auf eine konkrete Person polizeiliche Abklärungen getroffen werden müssen.

4. Weitergabe von Schätzungsanzeigen

Verwendung für Wasserversorgung und Eigenmietwertberechnung

Einige Privatpersonen gelangten an uns, weil sie mit der Weitergabe von Schätzungsanzeigen der Gebäudeversicherung an die Wasserversorgungsgenossenschaft bzw. an das Steueramt nicht einverstanden waren. Sie beanstandeten, dass die Schätzwerte für die Berechnung von Wasser- und Abwasseranschlussgebühren bzw. des Wasserverbrauchs sowie zur Berechnung der Eigenmietwerte bzw. Liegenschaftssteuerwerte verwendet werden.
Die Schätzungen der Gebäudeversicherung dienen der Berechnung der Versicherungswerte von Gebäuden; sie werden den Gemeinden mittels Schätzungsanzeigen mitgeteilt. Auf Grund des Gebäudeversicherungsgesetzes dürfen diese Daten im Zusammenhang mit der Gebäudeversicherung, dem Brandschutz und der Brandbekämpfung bearbeitet werden. Für eine Bearbeitung der Daten zu anderen Zwecken sind gesetzliche Grundlagen erforderlich.
Die Verwendung der Schätzwerte für die Berechnung von Wasser- und Abwasseranschlussgebühren bzw. des Wasserverbrauchs stellt eine Zweckänderung dar. Das Wasserwirtschaftsgesetz (§ 29) bzw. das Einführungsgesetz zum Gewässerschutzgesetz (§ 42) lassen offen, auf welcher Grundlage diese Gebühren berechnet werden. Die Gemeinden haben in diesem Bereich demnach eine Rechtssetzungskompetenz. Die Frage, ob die Schätzwerte der Gebäudeversicherung für die genannten Zwecke Verwendung finden dürfen, ist daher auf Grund des kommunalen Rechts zu beantworten. Häufig sehen kommunale Wasserversorgungs- bzw. Kanalisationsverordnungen eine Berechnung auf dieser Grundlage vor; in diesem Fall beruht die Verwendung der Daten auf gesetzlichen Grundlagen. Soweit die Aufgaben (z.B. im Falle der Wasserversorgung)

an eine private Genossenschaft delegiert wurden, gelten deren Statuten und Reglemente in Verbindung mit dem Delegationsbeschluss als entsprechende Rechtsgrundlagen.
Das Steuergesetz (§ 39) ermächtigt den Regierungsrat zum Erlass von Bestimmungen über die Bewertung von Grundstücken, wobei eine schematische, formelmässige Bewertung vorgesehen werden kann. Die Weisung über die Bewertung von Liegenschaften und die Festsetzung der Eigenmietwerte (Ziff. 31 und 52) sieht vor, dass als Berechnungsgrundlage auf die von der Gebäudeversicherung festgelegten Basiswerte abgestützt wird. Diese Bestimmungen stellen gesetzliche Grundlagen für die Verwendung der Schätzungsanzeigen zu steuerrechtlichen Zwecken dar. Da es sich nicht um sensible Personendaten handelt, scheint die amtliche publizierte Weisung des Regierungsrates, die sich auf eine Ermächtigung im Steuergesetz stützt, als eine ausreichende Rechtsgrundlage.

5. Bekanntgabe von Todesfällen?

Datenfluss zwischen Zivilstands- und Sozialamt

§ 27 Sozialhilfegesetz nennt mehrere Gründe, welche zur Rückerstattung von rechtmässig bezogener wirtschaftlicher Hilfe verpflichten. Unter anderem besteht eine Rückerstattungspflicht, wenn sich die finanziellen Verhältnisse der unterstützten Person infolge Erbschaft verbessern. Folgerichtig hat das Sozialamt ein faktisches Interesse, das Ableben der gemäss Art. 328 f. ZGB unterstützungspflichtigen Angehörigen vom zuständigen Zivilstandsamt gemeldet zu erhalten, um entsprechende Abklärungen vornehmen zu können.
Wir stellten fest, dass eine gesetzliche Grundlage im Sinne von § 8 DSG für einen Datenfluss vom Zivilstands- zum Sozialamt nicht vorhanden ist. Insbesondere reicht hierfür der erwähnte § 27 Sozialhilfegesetz, welcher lediglich unter bestimmten Umständen die Rückforderung von rechtmässig bezogenen Leistungen zulässt, nicht aus.
Amtshilfe kann definitionsgemäss nur im Einzelfall geleistet werden, weshalb automatisierte Meldungen jeweils beim Tod einer unterstützungspflichtigen Person von vornherein ausser Betracht fallen. Des Weiteren können gemäss § 25 Sozialhilfegesetz auch lebende Verwandte zur Unterstützung herangezogen werden, weshalb das Sozialamt nicht zwingend vom Ableben dieser Personen in Kenntnis gesetzt werden muss. Sodann würde durch entsprechende Meldungen auch der Verhältnismässigkeitsgrundsatz (§ 4 Abs. 3 DSG) verletzt, indem sich die finanziellen Verhältnisse der unterstützten Person durch den Todesfall von unterstützungspflichtigen Personen und ein damit allenfalls verknüpftes Erbe nicht zwingend solcherart verbessern, dass eine Rückforderung bisheriger Leistungen durch das Sozialamt ins Auge gefasst werden könnte.
Zentrale Datenquelle im Sozialbereich ist in Übereinstimmung mit § 7 DSG die betroffene Person. Diese ist gemäss § 18 Sozialhilfegesetz zu wahrheitsgetreuer Auskunft verpflichtet. Bei unwahren oder unvollständigen Angaben kann ihr gestützt auf § 24 Sozialhilfegesetz die Leistung gekürzt werden. Daher kann ihr auferlegt werden, den Tod von unterstützungspflichtigen Personen zu melden, selbst wenn sie zu diesem Zeitpunkt keine Unterstützungsleistungen mehr bezieht.

6. Namen von Erben bzw. Erbenvertretung an Gläubiger

Begrenzter Datenfluss Steueramt - Einwohnerkontrolle

Hinterlässt eine verstorbene Person offene Verbindlichkeiten, können sich die Gläubiger auf Grund der Regelungen des Zivilgesetzbuches über die Gesamtnachfolge an die Erben halten und von ihnen Befriedigung verlangen. Voraussetzung ist allerdings, dass die Gläubiger Informationen über die Erben oder zumindest über die Erbenvertretung haben. Entsprechend müssen sie – sollen die materiellrechtlichen Bestimmungen des Zivilgesetzbuches nicht faktisch unterlaufen werden - die erforderlichen Angaben an geeigneter Stelle einholen können.

Für Adressbekanntgaben ist gemäss § 9 DSG die Einwohnerkontrolle zuständig. Sie wäre denn auch gestützt auf § 9 Abs. 4 DSG berechtigt, bei Gelingen eines entsprechenden Interessennachweises durch die um Auskunft ersuchenden Gläubiger nähere Angaben zu den für die Erbmasse verantwortlichen Personen zu machen. Jedoch verfügt sie selber im Normalfall über keinerlei Angaben zu den Erben. Üblicherweise kann sie nicht einmal mit Informationen über die nächsten Verwandten dienen (abgesehen davon, dass die Verwandtschaft nicht deckungsgleich sein muss mit der Erbenstellung).

Demgegenüber sind dem Steueramt notwendigerweise Informationen über die für eine Erbmasse verantwortlichen Hinterbliebenen bekannt. Es muss im Hinblick auf die Erledigung der Erbschaftssteuern zumindest wissen, wer die Erbschaft im Todesfall vertritt; allenfalls hat es sogar sämtliche Erben aufgelistet. Jedoch darf gerade das Steueramt angesichts des Steuergeheimnisses den anfragenden Gläubigern keine Auskunft geben.

Mehrere Anfragen haben uns auf diesen Widerspruch hingewiesen und uns ersucht, einen Ausweg zu finden. Wir wandten uns daher an das kantonale Steueramt mit dem Vorschlag, dass den Steuerämtern die Befugnis verliehen werden sollte, im Bedarfsfall die erforderlichen Angaben an die Einwohnerkontrolle weiterzuleiten. Die um Befriedigung ihrer Forderungen nachsuchenden Gläubigerinnen und Gläubiger könnten diese Informationen dann bei der Einwohnerkontrolle abholen. Ein solcher Datenfluss hätte sich auf die unabdingbar notwendigen Angaben zu beschränken. Konkret mitzuteilen wären ausschliesslich die Namen der Erben oder zumindest der Erbenvertretung und selbstverständlich keine weiteren Informationen über den Erbfall.

Das kantonale Steueramt war mit unserem Vorschlag einverstanden. Es subsumierte einen entsprechenden Datenfluss unter § 120 Abs. 2 des Steuergesetzes (StG). Diese Bestimmung lässt eine Auskunft aus Steuerakten zu, wenn und soweit dies im öffentlichen Interesse geboten ist. In der Folge waren nur noch die Gemeindesteuerämter zu informieren, dass sie künftig die Erben bzw. Erbenvertretungen auf Verlangen an die Einwohnerkontrolle weiterzumelden haben.

7. Durchbrechung von Datensperren

Voraussetzungen zum Erhalt von gesperrten Steuerdaten

Eine als Verein konzipierte religiöse Gemeinschaft auferlegt jeder Person mit dem Erwerb der Mitgliedschaft eine Beitragspflicht. Berechnet wird der Beitrag dabei auf Grund der Kennzahlen Reineinkommen und Reinvermögen im Steuerausweis. Folgerichtig ist die Gemeinschaft daran interessiert, von den zuständigen Steuerämtern die Steuerausweise ihrer Mitglieder zu erhalten, auch in solchen Fällen, wo gestützt auf § 122 Abs. 2 Steuergesetz eine Datensperre errichtet worden ist. Dabei stellt sich die Frage, ob der Hinweis auf die Berechnung der Mitgliederbeiträge als Grund zur Durchbrechung einer Datensperre ausreiche. Ausgangspunkt bildet dabei § 11 Abs. 2 lit. b DSG: Eine Sperre kann durchbrochen werden, wenn die gesuchstellende Person oder Organisation glaubhaft macht,

dass sie ohne die verlangten Daten in der Verfolgung eigener Rechte gegenüber der betroffenen Person behindert wäre.
Indem sich die Beitragshöhe aus den im Steuerausweis aufgeführten Kennzahlen Reineinkommen und -vermögen berechnet, stehen für die Gemeinschaft in den geschuldeten Mitgliedschaftsbeiträgen eigene Rechte auf dem Spiel. Weniger klar ist dagegen, ob eine Behinderung in der Rechtsdurchsetzung tatsächlich vorliegt. Denn es bestehen diverse andere Möglichkeiten, um zu den angemessenen Mitgliedschaftsbeiträgen zu kommen: Die Gemeinschaft könnte entweder jedes Mitglied von Anfang an verpflichten, nicht nur eine Selbstdeklaration vorzunehmen, sondern auch einen aktuellen Steuerausweis einzureichen. Zudem kann sie gemäss ihren Statuten bei Fehlen der zur Einschätzung erforderlichen Unterlagen auf eine Ermessenseinschätzung ausweichen (womit jedoch ein erheblicher Aufwand verbunden ist). Als letzten Ausweg sehen die Statuten vor, ein Mitglied, welches die erforderlichen Angaben zur Einschätzung verweigert, aus der Gemeinschaft auszuschliessen (was aber dem Ziel der Gemeinschaft, alle Religionsangehörigen zu umfassen, entgegenwirkt).
Ob die aufgezeigten Behinderungen in der Praxis zur Durchbrechung einer Datensperre ausreichen würden, war nicht abschliessend zu beurteilen. Immerhin scheint dies wahrscheinlich, indem das Gesetz lediglich eine glaubhaft gemachte Behinderung verlangt und nicht eine massive Behinderung oder gar eine Verunmöglichung der Rechtsdurchsetzung.
Es empfiehlt sich daher, von den Mitgliedern die ausdrückliche Einwilligung zum Bezug von Steuerausweisen einzuholen. Damit würde die pauschal gegenüber allen Dritten errichtete Datensperre partiell aufgehoben. Schwierigkeiten ergäben sich lediglich, wenn ein Mitglied seine Einwilligung verweigern würde.
In beiden Fällen, nämlich sowohl bei Durchbrechung der Sperre wie bei erteilter Einwilligung durch die Mitglieder, bleibt ein Problem bestehen: Durch die Anfrage beim zuständigen Gemeindesteueramt wird zwangsläufig offenkundig, dass die nachgefragte Person dieser religiösen Gemeinschaft angehört. Hierdurch werden indirekt Angaben über die religiösen Ansichten und infolgedessen besonders schützenswerte Personendaten preisgegeben. Umgehen lässt sich diese Konsequenz nur, wenn die Mitglieder aufgefordert werden, von sich aus einen Steuerausweis beizubringen.

Überprüfungen und Beratung

Die Sicherheit im Informatikbereich erfordert systematische Überprüfungen und kontinuierliche Beratung.

1. Sicherheits-Check deckt Handlungsbedarf auf

Überprüfung ausgewählter Sicherheitskomponenten

Der Datenschutzbeauftragte hat im Anschluss an einen früheren Sicherheits-Check (vgl. Tätigkeitsbericht Nr. 3 [1997], S. 34 ff.) erneut Teilbereiche der Informatik einer Sicherheitsüberprüfung unterzogen. Ziel dieser Überprüfungen ist einerseits die Eruierung von möglichen Schwachstellen und andererseits das gezielte Aufzeigen der diesbezüglichen Verbesserungspotenziale in der gesamten Verwaltung.
Unterstützt durch die Finanzkontrolle wurden mit Hilfe von externen Spezialisten folgende Bereiche untersucht und bewertet:

- die Passwortwahl
- der Umgang mit E-Mail und angehängten Dateien
- die Verbindungen zum Netzwerk (Verwendung von Modems)

Die Auswahl der Bereiche erfolgte unter der Berücksichtigung von neuen, aktuellen Gefahren (Umgang mit elektronischer Post und angehängten Dateien), der wichtigsten benutzerbezogenen Sicherheitsmassnahme (Wahl des Passwortes) sowie der neuerlichen Überprüfung der Verwendung von Modems.
Der Aufwand wurde in finanzieller, personeller und zeitlicher Hinsicht limitiert, um rasch neue Erkenntnisse und Schwachstellen zu finden und kommunizieren zu können.
Der Beizug von externen Spezialisten mit praxisbezogenem Know-how unterstützte diesen Prozess.

Im ersten Teil wurden die Passwortdateien einzelner Server einer Überprüfung unterzogen, um die Qualität der durch die Benutzerinnen und Benutzer verwendeten Passwörter herauszufinden. Ein Programm verglich die gewählten Passwörter mit speziell erstellten Wortlisten aus Wörterbüchern und Listen von Namen und Begriffen aus Lexika. Der Prozess wurde so gewählt, dass er nach zirka fünfzehn bis dreissig Minuten abgeschlossen werden konnte.
Die Überprüfung der Passwörter hat ergeben, dass im Durchschnitt 61 Prozent der Benutzenden ein leicht herauszufindendes Passwort gewählt haben. Im Bereich der E-Mail-Accounts waren sogar 91 Prozent der Mail-Konten mit einem äusserst schwachen Passwort definiert. Insgesamt lagen rund drei Viertel der Passwörter der gesamten Stichprobe nach einer Rechenzeit von fünfzehn bis dreissig Minuten im Klartext vor.

Im zweiten Teil wurde an ausgewählte E-Mail-Adressen ein Mail mit einem entsprechend präparierten Anhang geschickt, welcher beim Öffnen eine Virenwarnung auslösen sollte. Geprüft wurde die Bereitschaft der Benutzerinnen und Benutzer, Inhalte aus unbekannten Quellen zu akzeptieren und sogar Attachments zu öffnen. Ebenso sollten die Reaktionen der Benutzenden sowie die Massnahmen der Betreiber im Bereich der Aktualisierung von Virensignaturen sowie das Funktionieren der Meldewege bei Virenbefall geprüft werden.
Die Reaktionen der Benützenden zeigten, dass der Anhang zu bereitwillig geöffnet wurde (17 Prozent) und der Inhalt des E-Mail trotz offensichtlicher Mängel von den beteiligten Personen nicht angezweifelt wurde. Auch einzelne Betreiber hatten die aktuellen Virensignaturen noch nicht geladen oder nicht vom Hersteller der Virensoftware erhalten.

Wie bereits beim vorgängigen Sicherheits-Check wurden die Telefonnummernbereiche der kantonalen Verwaltung auf Zugriffswege ausserhalb des Firewalls des verantwortlichen Betreibers systematisch durch ein entsprechendes Programm abgesucht.
Die Resultate sind unverändert ausgefallen. Immer noch wurden Modems entdeckt, deren Zuordnung zur verantwortlichen Person in den Direktionen oder Ämtern sich sehr schwierig gestaltete.
Auf Grund dieser Resultate gaben wir generelle Empfehlungen ab und wiesen einzelne direkt betroffene Amtsstellen darauf hin, wie die wichtigsten Grundschutzmassnahmen der Informatiksicherheit (Passwörter, Virenabwehr und Sensibilisierung) angemessen zu realisieren sind.

2. Internet-Angebote in den Gemeinden

Handlungsbedarf in Bezug auf die Sicherheit

Der Anschluss von Behörden an das Internet beinhaltet auch zahlreiche Fragen der Informatiksicherheit (siehe auch Tätigkeitsbericht Nr. 4 [1998], S. 25 ff.).Wir beschäftigten uns daher mit dem zu erstellenden Sicherheitskonzept speziell im Umfeld der Gemeinden und liessen das Sicherheitskonzept und die ergriffenen Massnahmen einer Gemeinde überprüfen. Diese wurde anschliessend im Detail über die zu treffenden technischen Massnahmen orientiert, auch die zu ergänzenden Punkte des Sicherheitskonzepts wurden ausführlich aufgeführt. Nach neun Monaten kündigte die Gemeinde erhebliche Verbesserungen an, die der Datenschutzbeauftragte seinerseits auf ihre Wirksamkeit überprüfen liess. Es zeigte sich, dass die konzeptionellen Arbeiten noch verbessert und ergänzt werden müssen und dass auch den technischen Belangen noch mehr Aufmerksamkeit geschenkt werden muss.

Aus der Sicht des Datenschutzbeauftragten wurde in zwei Stossrichtungen an dem Problem gearbeitet. Erstens wurden die Grundlagen für eine sichere und vertrauenswürdige Informatik-Infrastruktur mit dem Projekt SOPRANO (siehe S. 22 ff.) erarbeitet, die später auch von den Gemeinden für ihre E-Government-Projekte genützt werden kann, um die Schwachstellen, wie sie bei der Überprüfung vorgefunden wurden, mittelfristig zu eliminieren. Zweitens erarbeitete der Datenschutzbeauftragte ein Seminar für die Informatik-Verantwortlichen von Gemeinden, die sich speziell mit dem Aufbau von Angeboten im Internet zu beschäftigen haben. Das Seminar vermittelt das nötige konzeptionelle und technische Rüstzeug, um die organisatorischen und technischen Sofortmassnahmen im laufenden Betrieb der Internet-Angebote zeitlich und sachlich korrekt zu ergreifen. Die Ausschreibung des Seminars wurde mit der Interessengemeinschaft IG-EDV der Gemeinden koordiniert.

3. Umsetzung der Informatiksicherheitsverordnung

Begleitete Umsetzung in den Amtsstellen und Gemeinden

Das von der Abteilung für Informatikplanung (AIP) und vom Datenschutzbeauftragten angebotene Beratungspaket, das den Amtsstellen und den Gemeinden die begleitete Umsetzung der Informatiksicherheitsverordnung für die Sicherheitsstufe 1 ermöglicht, ist insbesondere von Gemeinden in Anspruch genommen worden. Es ermöglicht, nach Abschluss der Arbeiten (Erarbeitung einer System- und Risikoanalyse, Festsetzung der Schutzziele und der Massnahmenpläne für den vollständigen Grundschutz) für die Sicherheitsstufe 1 die Dokumentation von einer unabhängigen Fachperson beurteilen zu lassen. Im Quervergleich ergaben sich für alle Beteiligten wertvolle Hinweise, vor allem konnten in den meisten Fällen nicht berücksichtigte Massnahmen noch eingebunden werden. Auch die Begleitung von Amtsstellen in der Pilotphase hat die gute Anwendbarkeit der Intranet-Applikation «Leitfaden zur Umsetzung der Informatiksicherheitsverordnung» bestätigt. Die Angebote «Sicherheit in Informatiksystemen» und der «Leitfaden» wurden laufend erweitert, damit die Verantwortlichen für die Umsetzung der Informatiksicherheit über die notwendigen Hilfsmittel und Informationen verfügen.

4. Datenschutz-Review

Vorbereitungsarbeiten zur systematischen Prüftätigkeit

Der Datenschutzbeauftragte hat im Tätigkeitsbericht Nr. 2 [1996], S. 34, sein Konzept für eine systematische und periodische Aufsichts- und Kontrolltätigkeit vorgestellt. Der erste Schritt einer Priorisierung wurde nun durchgeführt, um angesichts der beschränkten Ressourcen die Aufsichtstätigkeit auf die sensiblen Datenbearbeitungen fokussieren zu können. Die wichtigsten Prüfgebiete wurden auf Grund von Angaben im Register der Datensammlungen und qualitativen Einschätzungen des Datenschutzbeauftragten bestimmt. Im Jahr 2000 wird der Datenschutzbeauftragte systematisch Prüfungen vornehmen können. Der Schwerpunkt der Prüfungen liegt im Bereich der vollständigen Grundschutzmassnahmen (Sicherheitsstufe 1 der Informatiksicherheitsverordnung), wobei ausgewählte Stichproben aus den Massnahmenplänen und deren Umsetzung auch spezifische Aussagen und einen Quervergleich ermöglichen werden.

5. Diagnose per E-Mail

Verschlüsselungsmassnahmen erforderlich

Ein Institut eines öffentlichrechtlichen Spitals beabsichtigte, Diagnosen per E-Mail an die Auftraggeber zu liefern. Dabei sollten die Patientennamen durch Initialen und Geburtsdatum ersetzt werden.
Medizinische Daten sind besonders schützenswert und erfordern in Bezug auf die Datensicherheit angemessene Massnahmen, die dem Stand der Technik zu entsprechen haben. Beim Versand von solchen Daten über das Internet sind Massnahmen der Vertraulichkeit (Schutz vor Kenntnisnahme durch Unberechtigte), der Integrität (Schutz vor Verfälschung) und der Authentizität (Identifizierbarkeit von Absender und Empfänger) zu treffen. Das vorgeschlagene Vorgehen genügt hierfür nicht, da eine Identifikation der betroffenen Person nicht auszuschliessen ist.
Nach dem heutigen Stand der Technik sind Verschlüsselungsmechanismen zu wählen, welche die erwähnten Massnahmen gewährleisten können. Eine Möglichkeit wäre auch, die Daten so zu anonymisieren, dass z.B. der Bericht mit einer Nummer versehen wird, die auf einem separaten Kanal (per Telefon oder Fax) in nicht anonymisierter Form (Name und Nummer) übermittelt würde. Dies könnte jedoch lediglich eine Übergangslösung darstellen, bis die Verschlüsselungslösung eingerichtet wäre.

6. Browser-Test im Web-Angebot

Überprüfung der Browser-Einstellungen und der Systemumgebung

Erstmals stellte der Datenschutzbeauftragte den Benutzerinnen und Benutzern des Internets auf seinem Web-Angebot (www.datenschutz.ch) einen so genannten Browser-Test zur Verfügung, der es ermöglicht, die Sicherheit des eigenen PC beim Anschluss an das Internet zu überprüfen. Viele Surferinnen und Surfer sind sich nicht bewusst, dass beim Anschluss an das Internet auf den eigenen PC von Dritten zugegriffen werden kann, wenn Einstellungen unsorgfältig gesetzt werden. In einem solchen Fall könnten bei Rechnern mit den Betriebssystemen Windows 95/98 und NT Dateien gelesen oder sogar Verzeichnisse beschrieben werden. Weiter eröffnet sich damit die Möglichkeit der Installation von fremden Programmen auf dem Rechner, die dann Informationen an unbekannte Dritte liefern. Um vor solchen Gefahren zu schützen, überprüft der Test, ob die notwendigen Einstellungen korrekt vorgenommen wurden. Der Browser-Test wurde in zahlreichen Fachzeitschriften oder Sonderbeilagen zur Tagespresse immer wieder als Möglichkeit für die Benutzerinnen und Benutzer zur eigenen ersten Kurzprüfung der Informatiksicherheit am PC aufgeführt. Die Kommentare per E-Mail zum Browser-Test waren sehr positiv und konstruktiv. Der Browser-Test beweist durch die Häufigkeit seines Aufrufs, dass Sicherheitsmassnahmen für Informatiksicherheit am Arbeitsplatz oder häuslichen PC auch vom Laien beachtet werden, vorausgesetzt man unterstützt und führt die Benutzerinnen und Benutzer zielgruppengerecht und stellt entsprechende Erklärungen zur Thematik bereit.

Mit einer Mousepad und einer Informationsbroschüre zur Sicherheit am PC-Arbeitsplatz wurde sehr grosse Aufmerksamkeit für diesen Themenbereich geschaffen.

Notwendigkeit kontinuierlicher Informationen

Mit Publikationen, Spezialaktionen, Veranstaltungen und Referaten reagierten wir auf ein zunehmendes Informationsbedürfnis.

1. Sichere Informatik-Arbeitsplätze

Ausführliche Checklisten

Mit der Sondernummer 3/1999 von «Fakten» stellte der Datenschutzbeauftragte erstmals Checklisten für das Erstellen von Richtlinien und Weisungen in Bezug auf sichere Informatik-Arbeitsplätze zur Verfügung. In der Praxis bestehen unterschiedliche Formen von Richtlinien und Weisungen, die sich auch inhaltlich unterscheiden. Verschiedene Amtsstellen sind an den Datenschutzbeauftragten mit der Bitte herangetreten, die wesentlichen Punkte zusammenfassend zu publizieren.
Bei der Erstellung von Richtlinien geht es nicht nur um die Vollständigkeit und Richtigkeit in Bezug auf den anvisierten Themenbereich, sondern ebenso um die Form, wie den Benutzerinnen und Benutzern der für sie wichtige Inhalt vermittelt wird. Das Vorgehen kann von Organisationseinheit zu Organisationseinheit unterschiedlich sein, Musterlösungen sind auf Grund der vielfältigen Bedürfnisse (unterschiedliche Sicherheitsstufen und Informatikumgebungen) nicht sinnvoll. Die Checklisten basierten auf den Erfahrungen im Kanton Zürich mit der Umsetzung der Informatiksicherheitsverordnung (ISV). Die wichtigste Quelle für die Massnahmenempfehlungen war dabei das «IT-Grundschutzhandbuch» des Bundesamtes für Sicherheit in der Informationstechnologie (BSI) in Bonn. Einzelne Regelungen und Weisungen sind auch beispielhaft skizziert, damit ein möglicher Inhalt benutzerspezifisch abgeleitet werden kann.
Im Vordergrund steht die Erarbeitung der Richtlinie für eine spezifische Organisationseinheit mittels der bereitgestellten Checklisten, die sich deshalb in erster Linie an die Betreiber und die Verantwortlichen von Informatiksystemen richten. Sie kommentieren die einzelnen Punkte, die zum Inhalt einer Weisung im eigenen organisatorischen und technischen Umfeld gehören, ohne diese im Einzelnen (technisch) vorzuschreiben. Die Sondernummer 3/1999 von «Fakten» beinhaltet folgende vier Hauptbereiche:

1. Allgemeine Grundsätze:
   Checkliste für die allgemein zu regelnden Punkte wie Zielgruppendefinition, Abgrenzungsfragen, Einsatz von Virenschutzprogrammen usw.
2. Spezifische Checklisten:
   Empfehlungen für Richtlinien in den Bereichen PC-Arbeitsplatz, Notebook und Benutzung von E-Mail.
3. Glossar:
   Erklärung der wichtigsten verwendeten Begriffe.
4. Beispiel einer ausformulierten E-Mail-Weisung.

2. Mehr Sicherheit am PC-Arbeitsplatz

Informationsbroschüre und Mousepad

Für eine Sensibilisierung der Benutzerinnen und Benutzer im sicheren Umgang mit dem PC erarbeiteten wir – zusammen mit dem Datenschutzbeauftragten des Kantons Basellandschaft – eine Mousepad und eine Broschüre mit Sicherheitstipps, die allen kantonalen und kommunalen Verwaltungen sowie interessierten Personen abgegeben wurde.
Mit dem wachsenden Einsatz von Informatikmitteln haben die Gefahren für den Datenschutz und die Datensicherheit stark zugenommen. Die meisten Computer sind heute in Netzwerke eingebunden oder auch ans Internet angeschlossen. Die komplexe Technik birgt jedoch Sicherheitsrisiken, deren sich die Benutzerinnen und Benutzer zu wenig bewusst sind.
Mit der Aktion «Sicher ist sicher…» machten wir auf diese Risiken und Gefahren aufmerksam und leisteten gleichzeitig einen Beitrag zur Verbesserung der Sicherheit des PC-Arbeitsplatzes. Die Mousepad soll mit einem

Augenzwinkern daran erinnern, wie wichtig Sicherheit im Umgang mit dem PC ist. Die übersichtliche Broschüre enthält die wichtigsten Sicherheitstipps für den PC-Arbeitsplatz.

Die Informationsbroschüre mit Mousepad wurde den interessierten Stellen und Personen gratis abgegeben. Dieser Sensibilisierungsaktion war ein sehr grosser Erfolg beschieden. Wir erhielten von vielen Seiten Anerkennung und – nachdem Broschüre und Mousepad innert weniger Wochen vollständig vergriffen waren – den Wunsch, eine Nachfolgeauflage in die Wege zu leiten.

3. Viertes Symposium für Datenschutz und Informationssicherheit

Neue Herausforderungen für den Schutz der Privatsphäre

Das vierte Symposium für Datenschutz und Informationssicherheit, das der Datenschutzbeauftragte zusammen mit dem Departement Informatik der ETH Zürich veranstaltete, ist auf ungebrochen grosses Interesse gestossen. Wiederum konnten über 350 Teilnehmerinnen und Teilnehmer begrüsst werden. Schwerpunktthemen bildeten dieses Mal Konzepte im «Data Mining / Data Warehousing» sowie Lösungsansätze im Bereich der digitalen Signaturen.
Prof. Dr. Olaf Kübler, Präsident der ETH, und Regierungsrat Dr. Markus Notter begrüssten die Teilnehmenden und versuchten die Fragen zu beantworten, ob die Folgen der Technik abschätzbar seien respektive ob Datenschutz realisierbar sei. Dabei zeigte sich, dass Recht und Technik im Bereich des Datenschutzes und der Informationssicherheit untrennbar verbunden sind und Lösungen beide Aspekte einbeziehen müssen.

Dass die Technik nicht nur eine Gefährdung der Privatsphäre beinhaltet, sondern auch ein Mittel für mehr Persönlichkeitsschutz darstellt, zeigte Dr. Marc Rotenberg in seinem Referat über «New Challenges for Privacy».
Die Thematik von «Data Mining» und «Data Warehousing» wurde von Mario Lütolf anhand eines Konzepts einer Grossunternehmung dargestellt, während Dr. Bruno Baeriswyl aus datenschutzrechtlicher Sicht die nicht gelösten Fragestellungen aufzeigte.
Im zweiten Schwerpunktbereich erläuterte Peter Fischer die Rahmenbedingungen für eine Public Key Infrastructure (siehe dazu auch S. 22) in der Schweiz. Barbara Meister brachte einen Praxisbericht über sichere E-Mail im Universitätsspital mit.
Ein Beispiel für die Anwendung digitaler Signaturen sind Abstimmungen über das Internet.
Prof. Dr. Ueli Maurer analysierte dazu die Problematik und zeigte mögliche Lösungsansätze aus technischer, rechtlicher und politischer Sicht auf.
Aus der Sichtweise der Ökonomie referierte Prof. Dr. Bernd Schips über die Auswirkungen des Electronic Business auf die Wirtschaft.

Weitere Themen des Symposiums waren der Datenschutz in der Psychiatrie (Markus Siegenthaler) und das Outsourcing von Informatikleistungen (Dr. Beat Rudin).
Wie bereits bei den früheren Symposien publizierten wir wiederum einige der Referate als «Beiträge 99 zum Datenschutz» in der Sondernummer 4/1999 von «Fakten».
Grossen Anklang fand die erstmals organisierte Fachausstellung. Parallel zur Veranstaltung zeigten verschiedene Unternehmungen Lösungen im Bereich der Informationssicherheit. Damit soll das Symposium auch in Zukunft noch mehr Praxisnähe bieten.
Das nach wie vor sehr grosse Interesse an der Veranstaltung zeigt das steigende Bedürfnis nach neuen Lösungen im Bereich von Recht und Technik der Informationssicherheit. Das fünfte Symposium für Datenschutz und Informationssicherheit findet am 26. Oktober 2000 statt.

4. Entwicklungen des Datenschutzes

Informationsaustausch mit Geschäftsprüfungskommission

Neben zahlreichen einzelfallbezogenen Anfragen der Geschäftsprüfungskommission ergab sich im vergangenen Jahr die Möglichkeit eines Informationsaustausches über die Verwirklichung des Datenschutzes im Kanton Zürich. Aus Sicht des Datenschutzbeauftragten war insbesondere auf die heutigen (rasanten) Entwicklungen im Bereich der Technik hinzuweisen, die eine hohe Sensibilität für den Schutz der Privatsphäre aufweisen. Ebenso zeigt sich, dass die Informationsgesellschaft neue Bedürfnisse nach Informationen schafft. Um die Grundanliegen des Datenschutzes - den Schutz der Privatsphäre der Bürgerinnen und Bürger – verwirklichen zu können, braucht es einen kontinuierlichen Prozess.

Die Einführung des Datenschutzgesetzes im Kanton Zürich hat zu einer Sensibilisierung sowohl bei den Verwaltungsstellen als auch bei den Bürgerinnen und Bürgern geführt. Das wachsende Bewusstsein wie auch die technologische und gesellschaftliche Entwicklung bedingen deshalb einen kontinuierlichen Entwicklungsprozess im Bereich des Datenschutzes. Dies zeigt sich sowohl im (vermehrten) Bereitstellen von datenschutzkonformen Lösungen im Bereich der Informatik als auch im Bestreben, angemessene gesetzliche Grundlagen für die Datenbearbeitungen zu schaffen. Dennoch ist nicht zu übersehen, dass teilweise dem Datenschutz nicht die notwendige Beachtung geschenkt wird. Der Datenschutzbeauftragte braucht deshalb auch entsprechende Ressourcen, um seine Beratungs- und Aufsichtsfunktionen im Bereich des Datenschutzes und der Informationssicherheit wahrnehmen zu können. Datenschutz trägt nicht nur zur Bildung des Vertrauens in die Verwaltung bei, sondern ist ein Grundrecht der Bürgerinnen und Bürger, weshalb dessen Verwirklichung das Anliegen aller Verwaltungsstellen sein muss.

5. Datenschutz in den Medien

Medienberichte über Datenschutzanliegen

Die in der Bevölkerung zunehmend feststellbare Sensibilisierung in Bezug auf die Datenbearbeitungen zeigt sich auch in den Medien, die vermehrt über Aspekte des Datenschutzes berichten.

Einerseits berichten die Medien regelmässig über Anliegen der Informationssicherheit. Dabei wurden sowohl unser «Browser-Test» (siehe S. 32) als auch die Informationsbroschüre mit Mousepad (siehe S. 34) von zahlreichen Medien als ausgezeichnetes Hilfsmittel für die Benutzerinnen und Benutzer ausführlich präsentiert.

Immer wieder werden auch Themen aufgenommen wie die Schulstatistik, die Volkszählung 2000, die geografischen Informationssysteme, die Überwachung am Arbeitsplatz, die DNA-Datenbanken oder generell die Videoüberwachung, mit denen sich der Datenschutzbeauftragte schon länger beschäftigte oder die zu Anfragen von interessierten Stellen und Personen führen.

In einem Medienseminar in Zusammenarbeit mit den Datenschutzbeauftragten der Kantone Bern und Basellandschaft konnten wir den interessierten Medienleuten zahlreiche Grundlageninformationen zu den Anliegen des Datenschutzes und der Informationssicherheit geben.

Datenbearbeitungen im Bildungsbereich

Die Bearbeitung von Daten über Lehrpersonen und über Schülerinnen und Schüler erlangen in der Praxis sehr hohe Aufmerksamkeit.

1. Leistungsbeurteilung von Lehrpersonen

Klare Rahmenbedingungen notwendig

Im Rahmen einer lohnwirksamen Beurteilung von Lehrkräften wird eine grosse Zahl besonders sensibler Daten beziehungsweise insgesamt ein Persönlichkeitsprofil bearbeitet. Das Risiko einer Persönlichkeitsverletzung der betroffenen Lehrkräfte ist deshalb als erheblich einzustufen. Folgerichtig sind gemäss § 5 DSG für die einzelnen Bearbeitungsschritte qualifizierte Anforderungen zu beachten. Als Konsequenz hat das verantwortliche Organ die zu verwendenden Erhebungsblätter mit entsprechender Sorgfalt auszugestalten sowie bei der praktischen Umsetzung von vornherein mit flankierenden Massnahmen auf eine rechtskonforme Abwicklung der Beurteilungsverfahren hinzuwirken.
Die von der Bildungsdirektion herausgegebenen Unterlagen zur Qualifikation von Lehrpersonal tragen diesen Anforderungen nicht ausreichend Rechnung, worauf wir schon im letzten Tätigkeitsbericht hingewiesen haben (Tätigkeitsbericht Nr. 4 [1998], S. 12 f.).

In der Praxis zeigt sich, dass Verletzungen der geltenden datenschutzrechtlichen Grundsätze sowie Eingriffe in die geschützte Persönlichkeitssphäre anlässlich des Beurteilungsverfahrens vorkommen. Wir hatten verschiedentlich betroffene Einzelpersonen zu beraten.

Demgegenüber wandte sich eine Berufsschule in Anbetracht der Sensibilität der zu bearbeitenden Daten mit dem Entwurf einer Leistungsbeurteilung von Lehrpersonen an uns mit der Bitte, das Material vorgängig unter datenschutzrechtlichem Aspekt zu überprüfen. Wir stellten fest, dass die Leistungsbeurteilung in § 4 Abs. 2 Berufsschullehrerverordnung eine ausreichende gesetzliche Grundlage hat. Auch das Verhältnismässigkeitsprinzip war angemessen berücksichtigt worden, indem die Datenerfassung ausdrücklich auf schulrelevante Kriterien beschränkt wird. Zur Schaffung der erforderlichen Transparenz für Lehrkräfte wurden zwei Mittel eingesetzt: Zum einen wurde klargestellt, dass eine Lehrperson mit ihrer Unterschrift nicht die Richtigkeit des Inhalts, sondern lediglich die Tatsache des geführten Beurteilungsgesprächs bestätigt. Andererseits wurde das gestützt auf § 17 DSG voraussetzungslos bestehende Auskunftsrecht des beurteilten Lehrpersonals deutlich für das Verfahren der Leistungsbeurteilung bestätigt. Transparenz wurde auch geschaffen durch unmissverständliche Regelungen, wie mit den anfallenden Unterlagen umzugehen ist und insbesondere welche davon später zu vernichten und welche in die Akten der jeweiligen Lehrperson zu legen sind. Betreffend den Beizug von Fachexperten empfahlen wir eine präzisierende Ergänzung, dass dies nur unter der Voraussetzung der Wahrung des Amtsgeheimnisses zulässig ist.

2. Schulstatistische Erhebung

Neue rechtliche Rahmenbedingungen

Die Kontakte mit der Bildungsdirektion zum Thema Bildungsstatistik (vgl. Tätigkeitsbericht Nr. 4 [1998], S. 13) wurden weitergeführt. Als Ergebnis konnte schliesslich eine neue Verordnung ausgearbeitet werden, welche die Datenbearbeitungen nicht nur für den Statistikbereich, sondern für den ganzen Bildungsbereich (das heisst die Vorschul- und Volksschulstufe, die Mittel- und Berufsschulstufe sowie die Hochschulstufe und den tertiären Bildungsbereich) in wichtigen Grundzügen regelt.
Die so genannte Bildungsdatenverordnung wurde auf den 15. August 1999 in Kraft gesetzt. Gestützt darauf wurden die ebenfalls mit uns vorbesprochenen Erfassungs-

blätter für die Schulstatistik an die einzelnen Schulgemeinden verschickt.
Auf den Versand der Unterlagen erfolgten ausgesprochen viele Reaktionen. So ging auch bei uns innert kurzer Zeit eine sehr grosse Zahl von schriftlichen wie telefonischen Anfragen ein.
Dabei wurde immer wieder die Befürchtung geäussert, die zu erhebenden Merkmale seien als zu weit gehend zu beurteilen, weshalb die Blätter insgesamt als datenschutzwidrig nicht oder zumindest nicht vollständig ausgefüllt werden dürften.
In der Beantwortung der einzelnen Anfragen wiesen wir einleitend auf § 12 DSG hin, welcher für die Datenbearbeitung zu statistischen Zwecken gewisse Lockerungen gegenüber den allgemein geltenden Datenschutzgrundsätzen zulässt. Voraussetzung ist allerdings, dass die Daten anonymisiert werden, sobald der Bearbeitungszweck dies erlaubt. Für Langzeiterhebungen kann naturgemäss erst anonymisiert werden, nachdem die betroffene Person aus dem statistisch erfassten Bereich ausgetreten ist. Gerade in solchen Fällen ist sowohl für die Gewährleistung der angemessenen Datensicherheit wie auch für eine strikte Beachtung der Zweckbindung der für statistische Zwecke erhobenen Daten zu achten.
Inhaltlich schreibt bereits das Bundesrecht die Erfassung gewisser schulischer und auch soziodemografischer Merkmale sowohl in Bezug auf die Personen in Ausbildung als auch in Bezug auf das Lehrpersonal vor. Dabei ist eine obligatorische Auskunftspflicht ausdrücklich festgehalten. Ausserdem werden die Kantone durch das Bundesrecht ermächtigt, ihre Erhebungen auf weitere Aspekte auszuweiten. Von dieser Möglichkeit hat die erwähnte Bildungsdatenverordnung Gebrauch gemacht. In deren beiden Anhängen wird im Detail ausgeführt, welche Daten zuhanden der Bildungsstatistik zu erheben sind. Da die verschickten Fragebogen ausschliesslich die in den Anhängen aufgeführten Daten enthalten, waren sie unter datenschutzrechtlichem Aspekt nicht zu beanstanden. Immerhin wiederholten wir die Notwendigkeit der Einhaltung der allgemeinen Bearbeitungsgrundsätze von § 4 DSG und vor allem das Verbot einer zweckwidrigen Nutzung der gesammelten Daten.
Zuständig für die Einhaltung der datenschutzrechtlichen Bestimmungen ist primär die Bildungsdirektion. Sie hat daher die mit der Erhebung betrauten Personen über das Zweckbindungsgebot zu informieren. Ausserdem hat sie durch geeignete flankierende Massnahmen einen datenschutzkonformen Umgang mit den Daten zu gewährleisten.

Datenschutzbeauftragter
Kanton Zürich
Postfach
8090 Zürich
Tel.: 01/259 39 99
Fax: 01/259 51 38
E-Mail: datenschutz@dsb.zh.ch
Homepage: http://www.datenschutz.ch
http://www.zh.ch/dsb

Datenschutzbeauftragter:
Dr. iur. Bruno Baeriswyl

Juristisches Sekretariat:
Dr. iur. Esther Hefti-Knellwolf
lic. iur. Marco Fey
lic. iur. Ratna Schemmekes (ab 1.6.2000)

IT-Sicherheitsberatung und -Revision:
Andrea C. Mazzocco, CISA

Sekretariat:
Tanja Blass

Tätigkeitsbericht Nr. 5 (1999)
ISSN 1422-5816

Konzeption und Produktion:
creactiva ender für Frontpage AG, Zürich

Druck:
KDMZ
Gedruckt auf Recyclingpapier

Bezug:
KDMZ
Räffelstrasse 32
8090 Zürich
Tel.: 01/468 68 68
Fax: 01/468 68 69
E-Mail: kdmz@zh.ch