Nummer 8

Tätigkeitsbericht 2002

dsb
datenschutzbeauftragter
kanton zürich

Nummer 8
Tätigkeitsbericht 2002

Der Datenschutzbeauftragte erstattet dem Regierungsrat jährlich oder nach Bedarf einen Bericht über seine Tätigkeit (§ 23 Datenschutzgesetz). Der vorliegende Tätigkeitsbericht 2002 Nr. 8 deckt den Zeitraum vom 1. Januar 2002 bis 31. Dezember 2002 ab.

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

Zürich, Juni 2003

Der Datenschutzbeauftragte des Kantons Zürich
Dr. Bruno Baeriswyl

Datenschutzbeauftragter des Kantons Zürich
Postfach, 8090 Zürich
Tel.: 043 259 39 99
Fax: 043 259 51 38
E-Mail: datenschutz@dsb.zh.ch
Web: www.datenschutz.ch

Inhaltsverzeichnis

Die Risiken für die Privatheit

Die Respektierung des Rechts der Bürgerinnen und Bürger auf Datenschutz ist nicht durchwegs gewährleistet, obwohl dies ein Grundrecht ist, das bei jeder Datenbearbeitung in Abwägung gezogen werden muss. Die Risiken für die Privatsphäre sind zunehmend.

Die Herausforderungen für den Schutz der persönlichen Freiheit der Bürgerinnen und Bürger haben im vergangenen Jahr erneut zugenommen. Die Risiken für das informationelle Selbstbestimmungsrecht verdeutlichten sich insbesondere in zwei Bereichen: Auf der einen Seite stellen wir fest, dass die Transparenz der Datenbearbeitungen für die betroffenen Personen wegen des Fehlens angemessener Rechtsgrundlagen in zahlreichen sensiblen Bereichen abnimmt. Auf der anderen Seite werden mit neuen Technologien neue Risikosituationen geschaffen, ohne dass die entsprechenden Sicherheitsmassnahmen getroffen werden.

Fehlen angemessener Rechtsgrundlagen

Das Ziel des Datenschutzes, den Bürgerinnen und Bürgern Transparenz über die Datenbearbeitungen durch die Verwaltung zu verschaffen, kann nur erreicht werden, wenn auf der rechtlichen Ebene die Grundlagen bestehen, welche die Rahmenbedingungen der Datenbearbeitungen abstecken. Im Mittelpunkt einer solchen Regelung müssen dabei der Zweck sowie der Umfang der Datenbearbeitung stehen. Erst dadurch wird auch die Möglichkeit gegeben, die Datenbearbeitung auf ihre Verhältnismässigkeit zu überprüfen. Seit einiger Zeit stellen wir die Tendenz fest, dass gerade bei Datenbearbeitungen mit hohen Risiken das Erfordernis einer angemessenen Rechtsgrundlage vernachlässigt wird. Vielfach wird in den entsprechenden Projekten zu wenig Aufwand in diese Fragen investiert. Das Projekt wird vorangetrieben und die Rahmenbedingungen werden definiert, ohne die (datenschutz)rechtlichen Erfordernisse zu berücksichtigen. Wenn dann Projekt und Vorgehen kritisiert und datenschutzrechtliche Anforderungen formuliert werden, wird ratloses Unverständnis gezeigt.

Dass eine vorgängige Berücksichtigung der datenschutzrechtlichen Anliegen effizienter wäre, liegt auf der Hand. Die Gründe, warum dies nicht geschieht, sind weniger offensichtlich und brauchen im Einzelnen nicht eruiert zu werden. Denn der Grundsatz, dass der Eingriff in die persönliche Freiheit der Bürgerinnen und Bürger einer angemessenen Rechtsgrundlage bedarf, ist unbestritten.

Im Berichtsjahr konnte ein solches Vorgehen vor allem im Bereich der Installation von Anlagen zur optischen Überwachung beobachtet werden. Dies veranlasste uns deshalb auch, einen grundlegenden Bericht mit Empfehlungen zu verfassen. Damit soll es den verantwortlichen Organen ermöglicht werden, diese sensiblen Datenbearbeitungen nach rechtsstaatlichen Grundsätzen zu projektieren.

Neue Technologien beinhalten neue Risiken

Im Bereich des Einsatzes neuer Technologien kommen immer mehr Systeme zum Einsatz, die umfassende Datenbearbeitungen erlauben, ohne über adäquate Sicherheitsmassnahmen zu verfügen. Die Systeme zeichnen sich durch grosse Datenmengen aus, die vielfach zu unterschiedlichen Zwecken Verwendung finden. Neben der Frage der klaren Zwecksetzung der Systeme stellen sich vermehrt Probleme in Bezug auf die Angemessenheit des Umfangs der Datenerfassung. Werden Personendaten zu unterschiedlichen Zwecken und in grossem Umfang bearbeitet, ist zu gewährleisten, dass die Daten nicht missbräuchlich Verwendung finden. Dies müsste wiederum über die Regelung der Zugriffe gesteuert werden.

Zwei im Berichtsjahr geprüfte Systeme zeigten die unterschiedlichen Ansätze auf. Während in einem Projekt die Fragestellung des Datenschutzes und der Sicherheit von Anfang mitberücksichtigt wurde – was notabene zu einer angemessenen Lösung geführt hat –, wurde im anderen Projekt ein System, das zur flächendeckenden Ausbreitung geplant ist, in Pilotprojekten eingeführt, ohne diese Fragestellung zu bearbeiten. Dass dieses System nun in der Praxis ein hohes Risikopotenzial für die Persönlichkeitsrechte der betroffenen Personen aufweist, ist offensichtlich.

Fehlender Grundschutz

Ebenfalls haben die Datenschutz-Reviews, die wir bei verschiedenen Stellen durchgeführt haben, gezeigt, dass oftmals auch die Grundschutzmassnahmen nicht getroffen wurden. Diese Nachlässigkeit zeigt, dass die Risiken der digitalen Welt noch zu oft verkannt werden. Diese Risiken können nur auf ein tolerierbares Mass reduziert werden, wenn auch die entsprechenden Sicherheitsmassnahmen getroffen werden. Um das gleiche Sicherheitsniveau in der digitalen Welt wie in der realen Welt zu erhalten, sind bei Informatiksystemen zusätzliche Massnahmen notwendig.

Zunehmende Risiken für die Privatheit

Die Entwicklungen illustrieren deutlich, dass die Datenbearbeitungen der Verwaltung die Privatsphäre der Bürgerinnen und Bürger zunehmenden Risiken aussetzen. Diesen stehen auf der anderen Seite vielfach keine ausreichenden Schutzmassnahmen gegenüber. Einerseits müssten auf der rechtlichen Ebene klare Rahmenbedingungen geschaffen werden, welche in Abwägung der Grundrechte der betroffenen Personen die Datenbearbei-

tungen auf das angemessene Ausmass festlegen. Auf der anderen Seite müssten die neuen Technologien datenschutzfreundlich ausgestaltet werden, was angemessene Sicherheitsmassnahmen beinhaltet. Fehlen diese beiden Voraussetzungen, so nehmen die Risiken für die betroffenen Personen laufend zu.

Die neuen Informations- und Kommunikationstechnologien, die insbesondere auch im Rahmen von E-Government-Projekten zunehmend zum Einsatz gelangen und längerfristig die elektronische Interaktion zwischen Verwaltung und Bürgerinnen und Bürger ermöglichen sollen, werden sich aber nur durchsetzen können, wenn sie transparent und sicher aufgebaut und betrieben werden. Fehlt die Transparenz oder die notwendige Sicherheit, werden sich die Bürgerinnen und Bürger dieser Mittel kaum bedienen, da ein Missbrauch ihrer Personendaten nicht ausgeschlossen wird.

Erarbeitung neuer Rahmenbedingungen

Auf diesem Weg in die Informations- und Kommunikationsgesellschaft soll deshalb das sich in Erarbeitung befindliche neue Informations- und Datenschutzgesetz die notwendigen Rahmenbedingungen schaffen. Mit einem konzeptionellen Ansatz, der die Transparenz zwischen Zugang und Nichtzugang zu Informationen und Daten in den Vordergrund stellt, soll ein angemessener Schutz der Grundrechte der Bürgerinnen und Bürgern gewährleistet werden. Ebenso sollen auf der technischen Ebene die Bedingungen geschaffen werden, die den Einsatz von datenschutzfreundlichen Technologien und von angemessenen Sicherheitsmassnahmen erleichtern. Mit diesem gesetzgeberischen Schritt würde den Herausforderungen für den Schutz der Privatsphäre besser begegnet werden können.

Schutz der Grundrechte

Die persönliche Freiheit ist eine wichtige Errungenschaft unserer liberalen Rechts- und Wirtschaftsordnung. Der Datenschutzbeauftragte setzt sich in seiner täglichen Arbeit für den Schutz der Grundrechte der Bürgerinnen und Bürger ein. Die Ressourcen, die ihm dabei zur Verfügung stehen, sind sehr beschränkt, weshalb es auf jede einzelne Verwaltungsstelle ankommt, ihre Verantwortung für den Schutz der Privatsphäre wahrzunehmen. Je weniger dabei die Grundsätze des Datenschutzes respektiert werden, desto schwieriger wird die Arbeit des Datenschutzbeauftragten. Die Entwicklungen im Berichtsjahr zeigten, dass seine Mittel nicht ausreichend waren, um dem notwendigen Schutz der Privatsphäre der Bürgerinnen und Bürger in der Verwaltung überall genügend Nachachtung zu schaffen.

Schwerpunkte des Tätigkeitsberichtes

Die Schwerpunkte im vorliegenden Tätigkeitsbericht widerspiegeln im Einzelnen diese generelle Entwicklung. Wie in einem umfangreichen Datenbearbeitungssystem die Anliegen des Datenschutzes und der Sicherheit

angemessen berücksichtigt werden können, zeigt das Customer-Relationship-Management-System beim Zürcher Verkehrsverbund (S. 10). Dagegen werden ebenso sensible Datenbearbeitungssysteme im Bereich der Pflegebedarfsabklärung eingesetzt, und dies ohne hinreichende Berücksichtigung der Grundrechte der betroffenen Personen (S. 13 f.).

Im Bereich der optischen Überwachung fehlen oftmals die rechtlichen Rahmenbedingungen, weshalb die Datenbearbeitungen nicht transparent sind und auch nicht überprüfbar werden (S. 28 ff.).

Im Weiteren geben Datenbekanntgaben immer wieder Anlass zur Überprüfung der Verhältnismässigkeit und der Zweckbindung (S. 12, 13, 14, 17). Daneben bleibt die Mitwirkung bei Vernehmlassungen und Gesetzgebungsvorhaben ein wichtiger Bereich der Tätigkeit (S. 16, 31).

Im Umfeld der Informatik stehen die Unterstützung bei der Gewährleistung eines angemessenen Sicherheitsstandards in der Verwaltung sowie die Überprüfung und Kontrolle einzelner Datenbearbeitungen im Vordergrund (S. 20 f., S. 23). Einen weiteren Schwerpunkt bildet die kontinuierliche Informations- sowie Aus- und Weiterbildungstätigkeit für die öffentlichen Organe mittels Seminarien und Referaten (S. 33 f.).

Datenbearbeitungen werden umfangreicher

Zahlreiche grosse Datenbearbeitungsprojekte standen im Mittelpunkt der Beratungs- und Kontrolltätigkeit.

KANTON

1. Kundenbindung in der öffentlichen Verwaltung

Customer Relationship Management beim Zürcher Verkehrsverbund

Der Zürcher Verkehrsverbund (ZVV) plante den Aufbau eines zentralen Contact Center. Das Contact Center soll einerseits die zentrale Anlaufstelle für alle Kundinnen und Kunden des öffentlichen Verkehrs im Kanton Zürich sein. Andererseits sollen die erfassten Daten die Grundlage für Optimierungs-, Qualitätssicherungs- und Verbesserungsmassnahmen bilden. Die Verkehrsbetriebe der Stadt Zürich (VBZ) erhielten den Auftrag für die Planung, den Aufbau und den Betrieb. Mit einem Konzept zur Informationssicherheit gelangte die Projektleitung an uns. Im Verlauf der Abklärungen stellte sich heraus, dass eine CRM-Lösung (CRM = Customer Relationship Management) vorgesehen war. Solche Lösungen werden vorzugsweise in der Privatwirtschaft zur Kundenbewertung und Kundenbindung eingesetzt. Es stellte sich die Frage, ob eine solche Datenbearbeitungsmethode für die Aufgabenerfüllung eines öffentlichen Organs geeignet und damit verhältnismässig ist beziehungsweise wie das System gegebenenfalls datenschutzkonform zu gestalten wäre. Ausserdem waren die Anforderungen an die Auftragsbearbeitung nach § 13 DSG zu erfüllen.

Da die Fragestellungen rund um CRM in der Verwaltung neu waren, führten wir mit interessierten Datenschutzbeauftragten anderer Kantone und der Stadt Zürich einen Workshop durch. Die Ergebnisse diskutierten wir mit der Projektleitung beziehungsweise mit dem ZVV als verantwortlichem Organ. Es stellte sich heraus, dass keine personenbezogenen Auswertungen (z.B. welche Personen beschweren sich regelmässig über welche Ereignisse?), sondern nur ereignisbezogene Auswertungen (z.B. welche Tram- und Buslinien sind oft verschmutzt?) vorgesehen sind und auch keine Data-Warehousing- und Data-Mining-Methoden eingesetzt werden. Unter dieser Einschränkung erachteten wir den Einsatz eines CRM-Systems zur optimierten Kundenbetreuung als zulässig. Hingegen würde – jedenfalls im Bereich der allgemeinen Transportpflicht – ein Verstoss gegen die Rechtsgleichheit vorliegen, wenn die einzelnen Kunden nach Rentabilität, Aufwand-Nutzen-Verhältnis oder ähnlichen Gesichtspunkten bewertet und eingestuft würden (z.B. Kunde mit Umsatz grösser X Franken wartet in der Hotline maximal Y Sekunden).

Die Aufbewahrungsdauer der Daten wurde nach Kategorien geregelt. Vorgesehen wurde, dass das System technisch so einzurichten ist, dass die Daten nach Ablauf dieser Fristen anonymisiert werden. Damit bleibt das Datenmaterial für Auswertungen und Langzeitbeobachtungen ohne Personenbezug erhalten. Für den Aspekt der Auftragsdatenbearbeitung durch die VBZ formulierte der ZVV eine Vereinbarung. Die Vereinbarung regelt den Zweck und Umfang der Datenbearbeitungen und verpflichtet die VBZ, die notwendigen Sicherheitsmassnahmen zu treffen sowie Vorkehrungen zu treffen, um die Rechtsansprüche betroffener Personen (Auskunft, Berichtigung, Löschung) erfüllen zu können.

Eine datenschutzfreundliche Technikgestaltung ermöglicht, die Rahmenbedingungen des Datenschutzgesetzes korrekt umzusetzen. Dabei kann einerseits der personenbezogene Zweck der Kundenbetreuung erfüllt werden. Andererseits kann auch das Ziel der Qualitätssicherung erreicht werden, indem Auswertungen mit anonymen (oder allenfalls pseudonymen) Daten erfolgen. Die transparente Zusammenarbeit der beteiligten Stellen mit dem Datenschutzbeauftragten bildete die Grundlage für eine erfolgreiche Projektdurchführung unter Wahrung der Privatsphäre.

2. Umgang mit gefährlicher Verwaltungskundschaft

Schutz des Personals und der Behörden

Nach dem Attentat im Zuger Kantonsrat im September 2001 wurden Massnahmen geprüft, welche dem Schutz der Verwaltungsangestellten und Behörden dienen. Zu diesem Zweck wurde eine Arbeitsgruppe «Risikoabschätzung», zusammengesetzt aus Personen verschiedener Gerichts- und Verwaltungsstellen, eingesetzt. Sie erarbeitete bis im Mai 2002 einen Bericht über mögliche Massnahmen sowie deren Notwendigkeit und Zulässigkeit.

Behörden und Verwaltungsstellen fühlen sich oftmals allein gelassen und überfordert im Umgang mit schwieriger Verwaltungskundschaft. Insbesondere geht es auch darum, nicht nur schwierige, sondern vor allem auch potenziell gefährliche Kundinnen und Kunden zu erkennen. Es wurden verschiedene Lösungsvarianten diskutiert:

Die Schaffung einer zentralen Datenbank wird verworfen, da eine solche datenschutzrechtlich nicht vertretbar wäre. Es fehlen die grundlegenden Voraussetzungen, insbesondere eine genügende Rechtsgrundlage, für eine entsprechende Erfassung.

Ein offener Informationsaustausch zwischen betroffenen Stellen wird unterstützt. Damit die involvierten Stellen, welche meistens aus schriftlichen Unterlagen bekannt sind, einen offenen Informationsaustausch pflegen können, müssen entsprechende Rechtsgrundlagen ebenfalls erst geschaffen werden. Dies soll im Rahmen der Revision des Datenschutzgesetzes (Informations und Datenschutzgesetz, vgl. dazu Seite ••) erfolgen.

Durch zusätzliche Beratungsstellen, zusammengesetzt aus Fachleuten mit konkretem Fallwissen, soll ausserdem verwaltungsinternes Know-how über potenziell gefährliche Personen zusammengeführt werden.

Bereits verwirklicht wurde der Vorschlag, ein zusätzliches Ausbildungsangebot (ein zweitägiger Kurs «Aggression und Gewalt im Arbeitsumfeld») für die Mitarbeitenden im Rahmen der Kantonalen Aus- und Weiterbildung anzubieten.

Das Bedürfnis nach einem intensiven Datenaustausch betreffend «schwierige Verwaltungskundschaft» zwischen verschiedenen Verwaltungsstellen ist ausgewiesen. Für einen spezifischen Datenaustausch fehlen zurzeit jedoch die gesetzlichen Grundlagen, sie sind in Bearbeitung.

3. Sicheres Abstimmen über Internet

Datenschutz und Sicherheit als kritische Erfolgsfaktoren

Der Kanton Zürich ist einer von drei Kantonen, in denen das E-Voting in einem Pilotprojekt getestet wird. Auf Grund einer Vereinbarung mit dem Bund wurde eine Projektorganisation aufgebaut mit dem Ziel, einen entsprechenden Pilotversuch durchzuführen. Die Projektleitung liegt beim Statistischen Amt, und der Datenschutzbeauftragte ist im Projektausschuss vertreten. Schwerpunkte bildeten in der Berichtsperiode die Modalitäten der Ausschreibung, die Erarbeitung eines Pflichtenhefts und die Evaluation eines geeigneten Realisierungspartners.

Datenschutz und Datensicherheit gehören zu den kritischen Erfolgsfaktoren in diesem Projekt, die schliesslich darüber entscheiden werden, ob die mit dieser neuen Technologie verbundenen Chancen für die Demokratie auch realisiert werden können. Aus unserer Sicht ging es deshalb darum, dass eine seriöse Risikoabschätzung zur Grundlage genommen wird, um die technische Lösung aufzubauen. Erst damit lässt sich ein umfassendes Sicherheitskonzept erarbeiten, das den Anforderungen an die Geheimhaltung und an die Sicherheit genügen kann. Zahlreiche sicherheitstechnische Fragen sind heute ungelöst. So beispielsweise das Problem der unsicheren Plattformen, die sichere Authentifikation des Abstimmungsservers oder die fehlende Nachvollziehbarkeit oder Beweisbarkeit. Dagegen liegen für die Authentifikation und Autorisation der Stimmberechtigten oder für die sichere Übertragung mittels Verschlüsselung praktikable Ansätze vor. In der Praxis wird aber oftmals vergessen, dass alle Komponenten berücksichtigt werden müssen, damit ein System sicher wird. Aus diesem Grunde ist aus dem Pilotversuch im Kanton Zürich diesbezüglich zusätzliche Erkenntnis zu erlangen, bevor die Einführung des E-Voting diskutiert werden kann. Das Vertrauen, das in die heutigen Abstimmungsmechanismen besteht, muss auch gleichwertig bei den elektronischen Mechanismen bestehen. Dies bedeutet aber, dass angesichts der Risiken im elektronischen Bereich die Anforderungen an die Sicherheit um einiges höher sind.

Das E-Voting-Pilotprojekt ermöglicht, Chancen und Risiken des elektronischen Abstimmungsverfahrens zu prüfen und entsprechende Lösungsansätze für eine sichere und vertrauenswürdige Systemgestaltung zu entwickeln.

4. Bewilligung als allgemein zugängliches Datum

Möglichkeit der Bekanntgabe durch die Verwaltung

Auf Grund einer Anfrage beurteilten wir die Frage, ob die Weitergabe einer Liste über Ärzte, die eine Bewilligung zur Medikamentenabgabe besitzen (so genannte Selbstdispensation), durch die Gesundheitsdirektion zulässig ist. Die Gesundheitsdirektion hatte die Anfrage eines Arztes erhalten, welche Ärztinnen und Ärzte in den Städten Zürich und Winterthur eine solche Bewilligung zur Selbstdispensation haben. Es stellte sich die Frage, ob diese Daten herausgegeben werden dürfen.

Die Bewilligung zur Selbstdispensation ist Voraussetzung, dass eine Ärztin oder ein Arzt Medikamente abgeben darf. Sie wird von der Gesundheitsdirektion nach den gesetzlichen Kriterien erteilt und kann bei Entfallen bestimmter Voraussetzungen auch wieder entzogen werden.

Ein Bewilligungsnehmer kann sich in Bezug auf die Tatsache des Bestehens einer Bewilligung nicht auf den Schutz seiner Privatsphäre berufen, da die Ausübung dieser Tätigkeit in der Öffentlichkeit eben gerade vom Bestehen der Bewilligung abhängig ist. Vielmehr macht der Bewilligungsnehmer mit der Ausübung der bewilligungspflichtigen Tätigkeit die Daten allgemein zugänglich, indem er eine unbestimmte Anzahl Personen anspricht. Im konkreten Fall bedeutet dies, dass jeder Patient einer Ärztin mit einer Bewilligung zur Selbstdispensation diese Tatsache auch erfährt, sobald er die Medikamente direkt von der betreffenden Ärztin erhält. Es erscheint damit offensichtlich, dass sich jede Person über das Bestehen einer solchen Bewilligung bei der Bewilligungsbehörde erkundigen kann und die Daten gestützt auf § 8 litera c DSG (Bekanntgabe von allgemein zugänglich gemachten Daten) weitergegeben werden können.

Über die Frage, ob eine ganze Liste von bestimmten Bewilligungsnehmern an Dritte weitergegeben werden darf, äussert sich das DSG nicht weiter. Für den einzelnen Bewilligungsnehmer bedeutet vorliegend die Bekanntgabe in einer Liste keinen schwereren Eingriff in seine Privatsphäre. Daher stellt sich hier einzig die Frage, ob es sich bei einer solchen Liste um ein Geheimnis im Sinne des Amtsgeheimnisses (Art. 320 StGB) handelt, weshalb dadurch eine Weitergabe allenfalls unterbunden wird. Auf jeden Fall kann die Bekanntgabe einer solchen Liste nicht auf Grund des Datenschutzgesetzes verweigert werden.

Soweit eine Bewilligung zu einer öffentlich ausgeübten Tätigkeit führt, besteht für eine Verwaltungsbehörde die Möglichkeit zur Bekanntgabe dieser Tatsache.

PERSONALBEREICH

5. Unterlagen in Personalakten

Beachtung der Zweckbindung

Eine im öffentlichen Dienst beschäftigte Person hatte Anhaltspunkte über mögliche Datenschutzverletzungen bei der Handhabung ihres Personaldossiers. Gemäss den Bestimmungen des Personalrechts dürfen nur Personendaten bearbeitet werden, die für das Arbeitsverhältnis notwendig und geeignet sind.

Für alle Angestellten wird ein Personaldossier geführt. Es umfasst sämtliche Personalakten über diese Person. Ausserhalb der Haupt- und Nebendossiers dürfen keine Personalakten geführt werden. Daten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, der aus den Umständen ersichtlich ist oder der gesetzlich vorgesehen wird. Werden Personendaten systematisch, namentlich mit Fragbogen, erhoben, so müssen Rechtsgrundlage und Zweck der Bearbeitung bekannt gegeben werden.

Das Personaldossier der von uns beratenen Person enthielt einen Fragebogen, worin eine Abschlussklasse zu Berufstreue und Berufsbild sowie zur Bewertung der praktischen Ausbildung im Betrieb und der theoretischen Fachausbildung an der Berufsschule befragt wurde. Im Personaldossier befand er sich jedoch zur Beurteilung des Unterrichts dieser Person. Eine solche Verwendung widerspricht dem ursprünglichen Zweck. Es liegt eine Verletzung der Zweckbindung vor. Zudem sind auf dem Fragebogen weder Rechtsgrundlage noch Zweck genannt.

Weiter befand sich im Personaldossier eine Mitteilung betreffend einen zu erledigenden Telefonanruf, welcher längst nicht mehr aktuell war, sowie eine längere Zeit zurückliegende Entschuldigung für eine Absenz. Wir

gelangten zum Schluss, dass der Fragebogen sowie die beiden Mitteilungen aus dem Personaldossier zu entfernen und somit zu vernichten sind.

Die Angestellten haben das Recht auf Berichtigung oder Vernichtung unrichtiger Personendaten. Kann weder die Richtigkeit noch die Unrichtigkeit von Personendaten bewiesen werden, kann ein entsprechender Vermerk angebracht werden. Wir rieten der betroffenen Person, die Berichtigung oder Löschung der ihres Erachtens unrichtigen Personendaten in denjenigen Unterlagen zu verlangen, welche weiterhin im Personaldossier verbleiben.

Personaldossiers sind periodisch auf die Aktualität ihres Inhaltes zu überprüfen. Nicht mehr benötigte Unterlagen sind zu vernichten.

6. Auskünfte an Unfallversicherungen

Mitwirkungspflicht der Arbeitnehmer und Arbeitgeberinnen

Oft stellt sich nach dem Unfall eines Angestellten die Frage, welche Auskunftspflicht die Arbeitgeberin gegenüber der Unfallversicherung hat. Die Rechtslage in Bezug auf diese Frage hat sich zu Beginn des Jahres 2003 geändert. Während bisher das Unfallversicherungsgesetz die Arbeitgeberin explizit zur Auskunft verpflichtete, wurde diese Regelung per 1. Januar 2003 aufgehoben. Dies heisst nun nicht, dass eine Arbeitgeberin bei der Ermittlung des Sachverhaltes nicht mehr mitwirken muss. Das (neue) Bundesgesetz über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG, SR 830.1) statuiert für den Arbeitnehmer wie auch für die Arbeitgeberin eine Mitwirkungspflicht beim Vollzug der Sozialversicherungsgesetze. Die Mitwirkungspflicht berechtigt die Arbeitgeberin aber noch nicht zur Auskunftserteilung. Vielmehr muss auf Grund der neuen Rechtslage die betroffene versicherte Person die Arbeitgeberin zuerst dazu ermächtigen. Erst wenn eine solche Vollmacht vorliegt, ist eine Arbeitgeberin verpflichtet, Auskünfte zu erteilen. Da eine Vollmacht auch allgemein formuliert sein kann («die notwendigen Auskünfte»), sollten Informationen immer mit einer gewissen Zurückhaltung weitergegeben werden. Es sind nur diejenigen Tatsachen mitzuteilen, die für den Schadenfall auch wirklich relevant sind.

Nach dem Grundsatz, dass die Daten in der Regel bei der betroffenen Person zu beschaffen sind (§ 7 DSG), wäre z.B. ein Lohnausweis durch die Versicherung direkt bei der betroffenen Person zu verlangen. Hat allerdings die betroffene Person eine Vollmacht für eine konkrete Frage ausgestellt (Herausgabe der Lohnausweise), so ist die Erteilung der Auskunft in dieser Frage unproblematisch.

Die Arbeitgeberin darf Informationen an die Unfallversicherung oder eine andere Sozialversicherung weitergeben, wenn ein Arbeitnehmer eine Vollmacht erteilt hat.

GESUNDHEITSWESEN

7. Pflegebedarfsabklärungssysteme

Zu umfangreiche Datenerhebung

Das Krankenversicherungsgesetz (KVG) verlangt, dass in der Langzeitpflege Untersuchungen, Behandlungen und Pflegemassnahmen gestützt auf eine Bedarfsabklärung zu erbringen sind. Die Abklärung muss nach einheitlichen Kriterien erfolgen und zu einer Einstufung führen, wobei mindestens vier Pflegebedarfsstufen bestehen müssen.

Im Kanton Zürich war ein Pilotprojekt zur Einführung eines solchen neuen Systems (genannt RAI/RUG) im Gang. Die Anbieterin des Systems RAI/RUG gelangte zusammen mit einer Vertreterin der Gesundheitsdirektion an uns. Sie wollte ein Merkblatt zum Datenschutz in diesem System verfassen, das von uns genehmigt und anschliessend an die Leistungserbringer (Heime) verteilt werden sollte. Zwar sind die Heime als Daten bearbeitende Stellen für die Einhaltung der datenschutzrechtlichen Rahmenbedingungen verantwortlich. Da aber die Fragestellungen bei der Einführung neuer Pflegebedarfsabklärungssysteme für alle Heime gleich sind und wir keine einzelnen Produkte oder Systeme von privaten Anbieterinnen prüfen, regten wir eine Koordination durch die Gesundheitsdirektion an und boten unsere Unterstützung an.

Gleichzeitig befasste sich die Arbeitsgruppe Gesundheit (AGX) der Vereinigung der Schweizerischen Datenschutzbeauftragten (DSB+CPD.CH) mit diesem System. Eine Prüfung durch diese Arbeitsgruppe ergab verschiedene Unzulänglichkeiten. So besteht RAI/RUG aus einem so genannten «Minimum Data Set» mit rund 250 Fragen an die Pflegeheimbewohner und -bewohnerinnen. Die Informatiklösung ist so angelegt, dass alle Fragen beantwortet

werden müssen, auch wenn einzelne nicht relevant sind. Ausserdem dient das System nebst der Pflegebedarfsabklärung auch der Tarifierung, der Personaleinsatzplanung und dem Qualitätsmanagement, also verschiedenen Zwecken. Im RAI/RUG-System fehlt es an der notwendigen Transparenz und Verhältnismässigkeit. Weiter stellte die Arbeitsgruppe fest, dass verschiedene Mängel in punkto Sicherheit bestehen und dass die Anonymisierung für die Qualitätsmessungen unzureichend durchgeführt wird. Die Arbeitsgruppe verfasste einen Bericht über ihre Feststellungen, den sie der Anbieterin von RAI/RUG zur Verfügung stellte. Offenbar fühlt sich die Anbieterin des Systems nicht verpflichtet, die Mängel zu beheben und Verbesserungen vorzunehmen, sind doch keinerlei Bemühungen diesbezüglich ersichtlich.

Wir stellten diesen Bericht auch der Gesundheitsdirektion zur Verfügung und verlangten Vorschläge für das weitere Vorgehen. Die Gesundheitsdirektion leitete den Bericht an die Projektleitung zur Stellungnahme weiter und versprach, uns über die Lösungsvorschläge zu informieren. Nach einiger Zeit erkundigten wir uns nach dem Stand und stellten weitere konkrete Fragen. In der Folge stellte sich die Gesundheitsdirektion auf den Standpunkt, die Verantwortung für die Einführung eines Pflegebedarfsabklärungssystems liege bei den Leistungserbringern.

Da auch ein anderes, summarisch geprüftes Pflegebedarfsabklärungssystem verschiedene Mängel in Bezug auf den Schutz der Persönlichkeitsrechte und die Sicherheit aufweist, gingen wir davon aus, dass die evaluierten Pflegebedarfsabklärungssysteme zu unverhältnismässigen und intransparenten Datenbearbeitungen führen und die Privatsphäre der betroffenen Personen (Bewohnerinnen und Bewohner von Heimen) verletzen. Der Datenschutzbeauftragte hat die verantwortlichen Stellen mehrfach auf den Handlungsbedarf aufmerksam gemacht und seine Unterstützung angeboten. Mangels Handlungs- und Kooperationswillen dieser Stellen wandten wir uns deshalb mit einer Empfehlung direkt an die Leistungserbringer und empfahlen, von der Einführung eines solchen neuen Systems abzusehen, bis die datenschutzrechtlichen Fragestellungen gelöst sind, und bei den Systemlieferanten auf eine datenschutzfreundliche Systemgestaltung hinzuwirken.

Pflegebedarfsabklärungssysteme sind so zu gestalten, dass die Datenbearbeitungen transparent und verhältnismässig sind. Es sind nur die im Einzelfall zur Pflege jeweils erforderlichen Daten zu erfassen. Die Leistungserbringer sowie die Koordinations- und Aufsichtsstellen haben bei den Lieferanten darauf hinzuwirken, dass datenschutzkonforme Lösungen angeboten und eingerichtet werden.

8. Auskünfte an Betreibungsämter

Keine Bekanntgabe des Klinikaufenthaltes

Eine Klinik fragte uns an, wie sie mit zunehmenden Anfragen von Betreibungsämtern umzugehen habe, welche zwecks Zustellung von Betreibungsurkunden wissen wollen, ob sich eine bestimmte Person in der Klinik aufhalte.

Ärztinnen und Ärzte unterstehen einer gesetzlichen Schweigepflicht, deren Verletzung strafbar ist (Artikel 321 StGB). Auskünfte dürfen nur mit Zustimmung der Patientin bzw. des Patienten oder gestützt auf ein gesetzliches Mitteilungsrecht erteilt werden. Fehlen Rechtsgrundlagen, ist die Einwilligung der betroffenen Person einzuholen. Von einer stillschweigenden Einwilligung kann nur ausgegangen werden, wenn die ausdrückliche Zustimmung gar nicht oder nur erschwert eingeholt werden kann und die Bekanntgabe im Interesse der betroffenen Person liegt. Im konkreten Fall wäre dies nicht erfüllt, weshalb die Klinik eine ausdrückliche Einwilligung einholen muss. Wird auch keine Einwilligung zur Bekanntgabe des Klinikaufenthalts erteilt, kommt ersatzweise der Mechanismus der Entbindung von der Schweigepflicht in Frage. Dazu nimmt die Aufsichtsbehörde, in diesem Fall die Gesundheitsdirektion, eine Interessenabwägung vor. Damit ein Arzt oder eine Ärztin von der Schweigepflicht entbunden wird, muss das Interesse des Gläubigers gegenüber dem Interesse der Patientin an der Geheimhaltung ihres Klinikaufenthalts überwiegen.

Dem Betreibungsamt, welches eine Bestätigung dieser Praxis verlangte, teilten wir die rechtlichen Grundlagen, die sich aus Artikel 321 StGB ergeben, mit. Gleichzeitig wiesen wir darauf hin, dass eine Rechtsänderung in Betracht zu ziehen wäre, sofern die bestehenden Möglichkeiten (Einwilligung bzw. Entbindung von der Schweigepflicht) in der Praxis nicht genügen sollten.

Eine Klinik darf einem Betreibungsamt den Klinikaufenthalt eines Patienten mitteilen, sofern sie von ihm dazu ermächtigt oder durch die Gesundheitsdirektion von der Schweigepflicht entbunden wurde. Dies gilt gleichermassen auch für andere Institutionen, die einer besonderen gesetzlichen Schweigepflicht unterliegen.

9. Abklärungen bei fürsorgerischer Freiheitsentziehung

Auskünfte nur bei Einwilligung

Nach der Einweisung in eine psychiatrische Klinik auf Grund einer fürsorgerischen Freiheitsentziehung muss die eingewiesene Person ärztlich untersucht werden, da die Klinik die Voraussetzungen für die fürsorgerische Freiheitsentziehung zu prüfen verpflichtet ist, ansonsten die eingewiesene Person aus der Klinik entlassen werden muss. Bei diesen Abklärungen spielen Auskünfte von Drittpersonen eine wichtige Rolle.

Das Einholen von Auskünften bei Drittpersonen kann eine Verletzung des Patientengeheimnisses bedeuten. Angaben, welche dem Patientengeheimnis unterstehen, dürfen nur mit Einwilligung der betroffenen Person gemacht werden. Dieser Grundsatz findet sich auch in der Patientenrechtsverordnung, welche die Auskunfterteilung an Dritte von einer Einwilligung der betroffenen Person abhängig macht. Bei den nächsten Angehörigen wird dabei von einer stillschweigenden Einwilligung ausgegangen.

Aus datenschutzrechtlicher Sicht gelangten wir zum Schluss, dass keine gesetzliche Grundlage besteht, welche der Klinik die Einholung von Auskünften bei Drittpersonen ermöglicht. Offenbar war der Gesetzgeber der Ansicht, der Klinik sollten im Verfahren nicht dieselben Abklärungsrechte und -pflichten zukommen wie der Vormundschaftsbehörde, welche im Einführungsgesetz zum ZGB eine gesetzliche Grundlage zur Anhörung von der betroffenen Person nahe stehenden Personen sowie von Behörden und Stellen hat, welche sich mit dieser Person befasst haben.

Nach datenschutzrechtlichen Grundsätzen ist bei Fehlen einer gesetzlichen Grundlage eine Datenbekanntgabe nur bei Einwilligung durch die betroffene Person möglich. Wir erläuterten die Voraussetzungen, welche erfüllt sein müssen, damit von einer Einwilligung ausgegangen werden kann, die nach den Umständen vorausgesetzt werden darf. Diese muss sich auf einen konkreten Fall beziehen. Betrifft die Bekanntgabe besonders schützenswerte Daten wie beispielsweise medizinische Daten, ist eine ausdrückliche Einwilligung nötig. Eine nach den Umständen vorausgesetzte Einwilligung darf nur angenommen werden, wenn es sich als unmöglich oder äusserst schwierig erweist, die Einwilligung der betroffenen Person einzuholen. Auf jeden Fall müssen die Umstände klar erkennen lassen, dass die Person die Bekanntgabe gutgeheissen und diese auch eindeutig in ihrem Interesse stattgefunden hätte. Diese Sachlage bezieht sich indes nur auf ganz wenige Fälle.

Abklärungen im Zusammenhang mit einer fürsorgerischen Freiheitsentziehung bei Drittpersonen, die nicht zu den nächsten Angehörigen gehören, sind mangels gesetzlicher Grundlage von einer entsprechenden Einwilligung abhängig, welche in ganz wenigen Fällen als nach den Umständen vorausgesetzt betrachtet werden kann.

POLIZEI UND JUSTIZ

10. Unschuldig registriert

Einträge in Polizeidatenbank nicht gelöscht

Zahlreiche Personen haben sich beim Datenschutzbeauftragten beschwert, dass Angaben über sie, die in der Datenbank der Polizei geführt werden, nicht korrekt sind respektive nicht gelöscht wurden, nachdem sich eine Anschuldigung als haltlos erwiesen hat. In dieser Angelegenheit haben wir auch mit dem Ombudsmann zusammengearbeitet, bei dem ebenfalls Beschwerden im gleichen Sinne eingegangen sind.

Wir haben bereits früher festgestellt (vgl. Tätigkeitsbericht Nr. 7 [2001], S. 11), dass das von der Kantonspolizei geführte Informatiksystem (Joufara II respektive Polis) auf mangelnden gesetzlichen Grundlagen beruht. Einerseits soll mit einem Polizeiorganisationsgesetz und einer entsprechenden Verordnung hier Abhilfe geschaffen werden. Andererseits wurde angekündigt, dass in einer Arbeitsgruppe die konkreten Probleme aus der Praxis angeschaut werden sollen. Leider hat nach einer ersten Sitzung mit den betroffenen Stellen, wo über den Handlungsbedarf in diesem Bereich weitgehend Einigung erreicht wurde, im Berichtszeitraum keine weitere Sitzung mehr stattgefunden.

Insbesondere zeigte sich in den im vergangenen Jahr von betroffenen Personen eingereichten Beschwerden, dass die Polizei sich weigert, Einträge, die sich im Nachhinein als falsch erwiesen, zu löschen. So bleibt ein Tatverdacht in der polizeilichen Datenbank bestehen, obwohl das Verfahren gegen die betroffene Person eingestellt wurde. Die betroffene Person verlangte nach der Einstellung die Löschung des Eintrages, doch die Polizei zeigte sich

lediglich bereit, den Eintrag mit der zusätzlichen Bemerkung der Einstellung des Verfahrens zu versehen. Zwar können wir den Ausführungen der Polizei so weit zustimmen, dass es im Rahmen der Geschäftskontrolle notwendig ist, die polizeiliche Fallbearbeitung zu dokumentieren. Diese Einträge dürfen jedoch gleichzeitig nicht auch für Fahndungszwecke und Recherchen zur Verfügung stehen. Hierfür fehlen die gesetzlichen Grundlagen, weshalb auch der Registereintrag mit dem angefügten Vermerk zu beanstanden ist.

Es ist zu hoffen, dass die erwähnte Arbeitsgruppe nunmehr bald konkrete Resultate erarbeiten kann, die einen Ausgleich zwischen den polizeilichen Interessen und den Interessen der betroffenen Personen an der Respektierung ihrer Grundrechte bringen.

Einträge in der Polizeidatenbank müssen richtig sein und dürfen nur zweckgemäss verwendet werden.

11. Neues Polizeiorganisationsgesetz

Gesetzliche Grundlagen für polizeiliche Datensammlungen

Bei den Vorarbeiten für den neusten Entwurf für ein Polizeiorganisationsgesetz (POG), der nunmehr in die Vernehmlassung geschickt wurde, war auch der Datenschutzbeauftragte involviert.

Auf Grund unserer Hinweise in früheren Vernehmlassungen (August 2000) wurde in die neue Fassung ein Artikel aufgenommen, in welchem der Zweck der polizeilichen Datensammlungen festgehalten wird. Damit wird die dringend notwendige Transparenz geschaffen, auch wenn die Formulierungen im Gesetzesentwurf sehr allgemein gehalten sind. Die Möglichkeit, polizeiliche Leistungen durch Dritte erledigen zu lassen (Outsourcing von polizeilichen Leistungen), wird mehrmals erwähnt, ohne dass die Details geregelt werden. Ebenso fehlen genauere Angaben, wie der Informationsaustausch zwischen den verschiedenen Polizeiorganen bzw. Behörden stattfinden soll.

Hier besteht demnach ein grosser Handlungsbedarf bei der Ausarbeitung der entsprechenden Verordnungen durch den Regierungsrat. Im Bereich der polizeilichen Datenbanken sind insbesondere Konkretisierungen zu folgenden Punkten notwendig: Zugriffe (insbesondere auch online), Datenkategorien, Aufbewahrung, Vernichtung und Löschung, Fristen sowie die Verantwortlichkeiten. Bei den Themen Outsourcing und Informationsaustausch sind ebenfalls Präzisierungen notwendig, welche die datenschutzrechtlichen Aspekte berücksichtigen.

Das im Entwurf vorliegende Polizeiorganisationsgesetz bringt vermehrte Transparenz. Wichtig wird die Detailarbeit bei der Ausarbeitung der entsprechenden Verordnung sein, welche dem Datenschutz Rechnung tragen muss.

12. Elektronisches Rechtsinformationssystem

Klare Rahmenbedingungen zu setzen

Bei der Direktion der Justiz und des Innern (JI) soll für die meisten Amtsstellen das «Rechtsinformationssystem RIS» eingeführt werden. Damit wird einerseits das bisherige Geschäftskontrollsystem JUSTITIA abgelöst, andererseits sollen auch Amtsstellen angeschlossen werden, welche bisher andere Systeme verwendet haben.

Für die Einführung, den Aufbau und Betrieb eines solch umfassenden elektronischen Informationssystems, bei welchem der Zugriff der beteiligten Stellen «online» erfolgt, müssen die Voraussetzungen, Rahmenbedingungen und Verantwortlichkeiten klar formuliert werden. Es sind zahlreiche Fragen betreffend die erfassten Personen, die einzelnen Datenkategorien, den Zweck, die Notwendigkeit etc. zu klären. Weiter müssen Regelungen für die Bearbeitung der Daten, die Weitergabe und die Zugriffsberechtigungen getroffen werden. Nicht zuletzt sind für die Aufbewahrung und Löschung bzw. Vernichtung klare Vorgaben zu machen.

Die JI legte einen Entwurf für ein Reglement für das RIS vor, in welchem gute Ansätze vorhanden sind. Wir haben jedoch gewisse unklare Formulierungen bemängelt, und die Regelungen sind noch unvollständig. Um die notwendige Transparenz zu schaffen, muss insbesondere mittels einer Verfügung geregelt werden, welche Daten(kategorien) zu welchem Zweck erfasst werden und was mit den erfassten Daten weiter geschieht. Wesentlich ist auch die Ausformulierung von detaillierten Zugriffsberechtigungen. Dabei ist zu berücksichtigen, dass ein Datenaustausch basierend auf dem Verhältnismässigkeitsprinzip nur in einem

engen Rahmen zur Erfüllung der gesetzlichen Aufgaben möglich sein darf.

Bereits in Vorbereitung war der elektronische Datenaustausch zwischen dem RIS und dem automatisierten Strafregister VOSTRA mittels einer Schnittstelle. Wir haben auch hier auf die Notwendigkeit einer datenschutzkonformen Umsetzung seitens der Justizvollzugsdienste hingewiesen.

Die datenschutzrechtlichen Anforderungen an ein umfassendes Rechtsinformationssystem wie das RIS sind ausserordentlich hoch. Die Grundlagen sollten bereits bei der Systemkonfiguration und vor der geplanten Einführung detailliert ausgearbeitet werden.

13. Einsicht in archivierte Strafakten

Einsicht in Strafakten des verstorbenen Vaters

Vom Staatsarchiv wurden wir angefragt, ob dem Gesuch einer Person, welche Einsicht in die beim Staatsarchiv archivierten Strafakten ihres 1987 verstorbenen Vaters wünscht, stattzugeben sei.

Für Akten in den Archiven mit Personendaten gelten Amtsgeheimnis und Datenschutz während einer Schutzfrist von 30 Jahren seit dem Tod. Während der Schutzfrist können die öffentlichen Organe aus wichtigen Gründen die Akteneinsicht bewilligen. Wichtige Gründe liegen vor, wenn die Einsichtnahme im überwiegenden Interesse der betroffenen Person erfolgt oder diese zugestimmt hat oder ihre Zustimmung nach den Umständen vorausgesetzt werden kann oder wenn die Akten für Gesetzgebung, Rechtsprechung, statistische oder wissenschaftliche Zwecke oder einen Entscheid über die Rechte der betroffenen Person benötigt werden.

Im konkreten Fall machte die anfragende Person geltend, die Akten für eine berufsbedingte Diplomarbeit persönlich-familiengeschichtlicher Art zu benötigen. Wir gelangten zum Schluss, dass im vorliegenden Fall die Zustimmung der betroffenen Person nach den Umständen vorausgesetzt werden kann, da es sich nicht um eine schwere Straftat handelte und sich diese zudem nicht gegen die Familie richtete. Zudem diente die Einsichtnahme in die Akten auch wissenschaftlichen Zwecken.

Eine Einsicht in im Staatsarchiv archivierte Strafakten ist – nach Abdeckung von Personendaten Dritter – bei Vorliegen einer nach den Umständen zu vermutenden Zustimmung der betroffenen Person oder eines wissenschaftlichen Zweckes mit den üblichen Auflagen zu gewähren.

GEMEINDEN

14. Datenerfassung und -weitergabe durch die Einwohnerkontrolle

Automatische Mutationsmeldungen

Durch verschiedene Hinweise und Beanstandungen aus der Bevölkerung sowie durch Anfragen von Einwohnerkontrollen wurden wir auf die in der Praxis unvollständig umgesetzten datenschutzrechtlichen Vorgaben bei automatischen Mutationsmeldungen der Einwohnerkontrollen aufmerksam. Wir führten umfangreiche Abklärungen in einzelnen Gemeinden durch und stellten eine sehr unterschiedliche Umsetzung unseres Rundschreibens vom Januar 1999 zu Datenerfassungen und -weitergaben fest (vgl. Tätigkeitsbericht Nr. 4 [1998], S. 28). So erfolgen beispielsweise automatische Mutationsmeldungen an Polizei-, Sozialhilfe- und Vormundschaftsbehörden, an Betreibungsämter sowie an politische Parteien.

Welche automatischen Mutationsmeldungen zu machen sind, ergibt sich aus dem geltenden eidgenössischen, kantonalen sowie kommunalen Recht.

Wir wandten uns in einem weiteren Rundschreiben an sämtliche Einwohnerkontrollen des Kantons Zürich, machten auf die unvollständige Umsetzung der datenschutzrechtlichen Vorgaben aufmerksam und wiesen erneut auf unser Rundschreiben von Januar 1999 hin.

Zulässig sind insbesondere folgende automatischen Mutationsmeldungen je mit den folgenden Datenkategorien:

- Steueramt: Dieses erhält sowohl die zur Identifizierung dienenden Angaben sowie die Konfession (sofern es sich um eine der Konfessionen handelt, für die Kirchensteuern erhoben werden) und alle Mutationen des Zivilstandes.
- Militärsektion/Sektionschef: Zu melden sind je die bundesrechtlich vorgegebenen Daten der stellungspflichtigen Personen.

- Zivilschutzstelle: Zu liefern sind die identifizierenden Angaben der zivilschutzpflichtigen Personen.
- Anerkannte (Landes-)Kirchen (evangelisch-reformiert, römisch-katholisch und christkatholisch): Mitzuteilen sind Name, Vorname, Adresse, Geschlecht, Geburtsdatum, Zivilstand, Heimatort bzw. Nationalität bei Ausländern, Aufenthalts- bzw. Niederlassungsstatus, Zuzugs- und Wegzugs- bzw. Todesdatum, Zuzugs- und Wegzugs- bzw. Todesort, Bevormundung/Entmündigung mit Namen und Adresse der zuständigen Vertretung. Über konfessionsfremde Familienmitglieder wie Ehepartner und Kinder dürfen keine Angaben weitergegeben werden.
- Schulpflegen: Gemeldet werden die neu in die Schulpflicht eintretenden sowie die neu zugezogenen schulpflichtigen Kinder mit deren gesetzlicher Vertretung.
- AHV-Zweigstellen: Sie erhalten die identifizierenden Angaben, welche sie brauchen, um die Erfüllung der Beitragspflicht zu überprüfen.
- Migrationsamt: Zu melden sind die in der Verordnung über das Zentrale Ausländerregister ausdrücklich aufgeführten Datenkategorien.

Die einzelnen Einwohnerkontrollen geben in unterschiedlichem Umfang Mutationsmeldungen automatisch weiter. In einem Rundschreiben weisen wir auf die gesetzlich zulässigen Datenkategorien sowie auf die zulässigen automatischen Mutationsmeldungen hin.

15. Privatisierung städtischer Werke

Bezug von Adressdaten bei der Einwohnerkontrolle

Von einer Gemeinde wurden wir angefragt, ob die Einwohnerkontrolle den Gemeindewerken nach deren Privatisierung weiterhin die Daten der Einwohnenden automatisch zur Verfügung stellen kann.

Die Gemeindewerke wurden in einer Werke AG verselbständigt. Somit gehören sie nicht mehr der Organisationsstruktur der Gemeindeverwaltung an. Öffentliche Organe dürfen Personendaten bei Vorliegen einer gesetzlichen Grundlage bekannt geben. Eine solche lag in der betreffenden Gemeinde nicht vor. Bei der Schaffung einer Grundlage für die Bekanntgabe von Adressdaten von Einwohnenden an die Werke AG ist eine gesetzliche Grundlage zu schaffen, welche die wöchentlichen Mutationsmeldungen von der Gemeindeverwaltung an die Werke AG regelt, indem sie ausdrücklich die regelmässige Bekanntgabe der Adressdaten sowie den Datenempfänger nennt sowie Zweck und Ausmass der Bekanntgabe umschreibt. Ist diese Grundlage geschaffen, dürfen nach dem Grundsatz der Verhältnismässigkeit nur die zur Aufgabenerfüllung geeigneten und erforderlichen Personendaten bekannt gegeben werden, weshalb nicht die Daten sämtlicher Einwohnenden, sondern nur derjenigen, welche bei der Werke AG als Kunden gemeldet sind, bekannt gegeben werden dürfen.

Nach der Privatisierung der Gemeindewerke in einer Werke AG sind diese nicht mehr Teil der Gemeindeverwaltung. Benötigt die Werke AG regelmässig Angaben zu Einwohnenden der Gemeinde, ist eine entsprechende gesetzliche Grundlage zu schaffen. Zudem darf die Gemeindeverwaltung der Werke AG nur die Daten ihrer Kunden bekannt geben.

16. Mitteilungen des Sozialamtes an das Steueramt

Anzeigepflicht bei unvollständiger Besteuerung

Das Steueramt einer Gemeinde verlangte vom Sozialamt, dass es regelmässig Meldungen über steuerpflichtige Ereignisse und Tatsachen zu erstatten habe, beispielsweise wenn Liegenschaften veräussert oder Pensionskassenguthaben infolge Invalidität ausbezahlt werden. Es berief sich dabei auf eine Weisung der Finanzdirektion über das Meldeverfahren der gegenüber Steuerbehörden zur Auskunft und Anzeige verpflichteten Verwaltungsbehörden, Strafuntersuchungsbehörden und Gerichte. Das Sozialamt stellte sich auf den Standpunkt, dass eine Anzeigepflicht erst gegeben sei, wenn es im Rahmen seiner Aufgabenerfüllung Kenntnis von einer unvollständigen Besteuerung erlangt.

Gemäss § 121 Steuergesetz sind Verwaltungsbehörden auf Anfrage zur Auskunftserteilung über steuerlich relevante Tatsachen an das Steueramt verpflichtet. Darüber hinaus sind sie verpflichtet, von sich aus Meldung zu machen, wenn sie Kenntnis von einer unvollständigen Veranlagung haben. Das Sozialamt trifft demnach erst im Falle einer unvollständigen Besteuerung eines Klienten von Amtes wegen eine Anzeigepflicht. Dies ist dann der Fall, wenn das Sozialamt im Rahmen seiner Aufgaben (Abklärung der wirtschaftlichen Verhältnisse für finanzielle Unterstützungsleistungen) feststellt, dass steuerpflichtige Tatsachen gegenüber dem Steueramt nicht deklariert wurden. Dagegen kann beispielsweise

bei einer Auszahlung von Pensionskassenguthaben, die das Sozialamt zur Kenntnis erhält, nicht von einer automatischen und vorgängigen Meldepflicht ausgegangen werden. Dafür fehlen gesetzliche Grundlagen. Ausserdem widerspräche die automatische Meldung von steuerlich relevanten Vorgängen dem Prinzip der Selbstdeklaration der Steuergesetzgebung.

Falls die Voraussetzungen für eine Meldung erfüllt sind, ist zu prüfen, ob überwiegende öffentliche Interessen der meldenden Behörde entgegenstehen (§ 10 DSG). Keine Rolle spielen dagegen Geheimhaltungspflichten, da diese in § 121 Steuergesetz explizit ausgenommen werden. Auch die Interessen der betroffenen Person an einer Unterlassung der Meldung dürften in der Regel nicht höher zu gewichten sein als die öffentlichen Interessen an einer korrekten Besteuerung.

Verwaltungsstellen dürfen Informationen über Ereignisse und Tatsachen, die allenfalls steuerlich relevant sein können, nicht ohne Weiteres von Amtes wegen dem Steueramt anzeigen. Sie haben dem Steueramt erst Meldung zu machen, wenn sie im Rahmen ihrer Aufgaben von einer unvollständigen Besteuerung Kenntnis erhalten.

17. Konfessionsangaben in den Einwohnerkontrollen

Weitergabe an staatlich anerkannte Kirchgemeinden

Im vergangenen Jahr richtete sich die Israelitische Gemeinde Winterthur mit der Bitte an die Einwohnerkontrollen verschiedener Gemeinden in ihrer Umgebung, ihnen eine Liste der in den jeweiligen Gemeinden wohnhaften Personen israelitischen Glaubens zukommen zu lassen.

Laut dem Gemeindegesetz erhalten staatlich anerkannte Kirchen aus dem Einwohnerregister der Niederlassungsgemeinde die Mitteilungen, deren sie zur Erfassung ihrer Mitglieder bedürfen. Der Regierungsrat kann unter bestimmten Voraussetzungen anderen religiösen Gemeinschaften christlicher oder jüdischer Zugehörigkeit das gleiche Recht einräumen.

Mit einem Regierungsratsbeschluss aus dem Jahre 1991 wurde ein Gesuch der Israelitischen Cultusgemeinde Zürich diesbezüglich bewilligt. Gestützt auf diesen Regierungsratsbeschluss erteilten einzelne Gemeinden im Raum Winterthur auch der Israelitischen Gemeinde Winterthur die gewünschten Angaben.

Zu beachten ist in diesem Zusammenhang, dass das Gesuch ausschliesslich für die Israelitische Cultusgemeinde Zürich bewilligt wurde. Der Israelitischen Gemeinde Winterthur wurde bislang keine entsprechende Bewilligung erteilt. Deshalb können ihr die gewünschten Angaben aus den Einwohnerregistern nicht erteilt werden.

Eine weitere Frage im Zusammenhang mit der Konfession war, ob die Einwohnerkontrolle abzuklären hat, ob Mitglieder der Evangelisch-reformierten Kirchgemeinde zugleich Mitglieder der Französischen Kirchgemeinschaft sind (siehe auch Tätigkeitsbericht Nr. 7 [2001], S. 18). Als Begründung für diese Abklärungen verwies die Einwohnerkontrolle auf das Statistische Amt, das diese Angaben jeweils Ende Jahr von den Einwohnerkontrollen einfordere. Auf dem entsprechenden Formular des Statistischen Amtes wird auf die Vorschriften des Finanzausgleichs verwiesen. Der Umstand, ob jemand ein Mitglied der Evangelisch-reformierten Landeskirche und gleichzeitig auch Mitglied der Französischen Kirchgemeinschaft ist, ist für den Finanzausgleich indessen unerheblich. Die Unterscheidung dieser beiden Religionsgemeinschaften ist jedoch relevant für die Synodalwahlen. Da die Mitglieder der französischen Kirche sich aber selber bei der Einwohnerkontrolle als solche anmelden, braucht die Einwohnerkontrolle diese Frage nicht von sich aus abzuklären. Sie hat lediglich die Zugehörigkeit zu der französischen Kirche zu führen. Da auch keine gesetzliche Grundlage existiert, welche die Erhebung dieser Angaben für Statistikzwecke erlaubt, sind die entsprechenden Fragebögen anzupassen.

Die Einwohnerkontrollen führen Angaben zu der Konfession der Einwohnerinnen und Einwohner. Sie dürfen nur in den gesetzlich vorgesehenen Fällen weitergegeben werden.

18. Gesuchsformular Zusatzleistungen zur AHV und IV

Abklärungen der finanziellen Verhältnisse

Eine Gemeinde wandte sich an uns mit dem Anliegen, eine Überprüfung ihres Gesuchsformulars zu den Zusatzleistungen zur AHV und IV aus datenschutzrechtlicher Sicht vorzunehmen. Wir stellten fest, dass der Fragenkatalog im Vergleich mit demjenigen anderer Zürcher Gemeinden sowohl sehr umfangreich als auch sehr detailliert ist. In unserer Antwort wiesen wir darauf hin, dass sämtliche Fragen auf einer gesetzlichen Grundlage beruhen müssen und das Erfragen der Personendaten nach dem Grundsatz der Verhältnismässigkeit für die Erfüllung der Aufgabe, diesfalls die Abklärung der Einkommens- und Vermögensverhältnisse von gesuchstellenden Personen, geeignet und erforderlich sein muss. Diese Voraussetzungen waren bei den meisten Fragen erfüllt. Nicht erfüllt waren sie jedoch bei Fra-

gen über Drittpersonen wie beispielsweise Familienangehörige. Hier empfahlen wir deren Streichung. Wir wiesen zudem darauf hin, dass bei Unklarheiten in einem weiteren Abklärungsschritt bei tatsächlichem Bedarf weitere Angaben erfragt werden könnten. Mit diesem Vorgehen kann ein unnötiges Datensammeln auf Vorrat vermieden werden. Im Weiteren wiesen wir darauf hin, dass aus Gründen der Transparenz auf dem Fragebogen selber der Zweck sowie die jeweiligen Rechtsgrundlagen anzugeben sind.

Für die Zukunft regten wir die Schaffung eines einheitlichen Gesuchsformulars für Zusatzleistungen im Kanton Zürich an. Diese Idee wurde vom Vorstand des Fachverbandes der Zusatzleistungen aufgenommen, und die Erarbeitung eines einheitlichen Formulars wurde in Aussicht gestellt.

Bei Gesuchsformularen für Zusatzleistungen darf nur nach den Einkommens- und Vermögensverhältnissen gefragt werden, welche für die Berechnung des Anspruchs auf Zusatzleistungen massgebend sind. Angaben über Drittpersonen sind nicht zu erfragen. Bei der Abklärung von Einkommens- und Vermögensverhältnissen ist verhältnismässig vorzugehen.

INFORMATIONSSICHERHEIT

19. Einheitliche Sicherheitsinfrastruktur

Projekt Soprano weitergeführt

Im vergangenen Jahr wurden die Ausschreibung für die definitive Public-Key-Infrastruktur (PKI) abgeschlossen und der Vergabeentscheid gefällt.

Mit der PKI wird die Einführung einer Informatik-Sicherheitsinfrastruktur bezüglich Vertraulichkeit, Authentizität, Integrität und Nicht-Abstreitbarkeit innerhalb der kantonalen Verwaltung und den Gemeinden ermöglicht. Damit wird ein einheitlicher Sicherheitsstandard gewährleistet, auf dem die einzelnen Anwendungen der Verwaltung modular aufbauen können und der kompatibel zu externen Stellen ist (Bund, Kantone).

In Pilotprojekten (vgl. Tätigkeitsbericht Nr. 7 [2001], Seiten 34 f.) konnte der Nachweis über die Funktionstüchtigkeit einer PKI als wirkungsvoller Schutz von Applikationen erbracht werden.

Die dadurch gewonnenen Erkenntnisse in verschiedenen Einsatzgebieten, erleichtern das Vorgehen für den Einsatz mit der definitiven PKI-Lösung.

Soprano hat das Ziel, in einem ersten Schritt flächendeckend in der kantonalen Verwaltung Secure E-Mail einzuführen. Auch Gemeinden setzen in einzelnen Projekten auf die Technologie der Verschlüsselung mit Soprano-Zertifikaten.

Der Bundesrat hat am 3. Juli 2002 ebenfalls die vielfältigen Vorteile einer PKI anerkannt (rechtsverbindlicher elektronischer Verkehr, komfortable Anmeldung bei Computersystemen) und beschlossen, für die Bundesverwaltung eine PKI aufzubauen. Damit wird auch die Strategie des Kantons Zürich zur Einführung einer PKI unterstützt und die Einführung von E-Government-Anwendungen, mit welchen Interaktionen mit den Bürgern ermöglicht werden, gefördert.

Das Projekt Soprano legt die Grundlagen für eine verwaltungsweite einheitliche Sicherheitsinfrastruktur. Eine schrittweise Umsetzung soll in den kommenden Jahren folgen.

20. Beratungsstelle für Informatiksicherheit

Erfolgreicher Datenschutz durch Informatiksicherheit

Verwaltungsstellen und öffentliche Institutionen sind verpflichtet, mit Personendaten rechtlich korrekt und sicher umzugehen. Es wird damit eine Grundlage für das Vertrauen der Bürgerinnen und Bürger in die Datenbearbeitungen der Verwaltung geschaffen. Um Schäden zu verhindern, muss die Erreichung der strategischen Sicherheitsziele gewährleistet werden. Dazu ist ein Sicherheitsmanagement mit einer verbindlichen Informatiksicherheitspolitik notwendig. Die Informatiksicherheitspolitik legt die grundsätzlichen Regeln zum sicheren Umgang mit Informatikmitteln fest. Die gesetzlichen Bestimmungen geben vor, wie mit Informationen und mit allfälligen Risiken umzugehen ist (Sicherheitsdispositiv).

Die wiederkehrende Überprüfung der Informatik auf Einhaltung der Vorgaben des Sicherheitsmanagements ist ein wichtiges Element der Führung. Der spezifische Sicherheitsbedarf wird auf der Basis der Anforderungen, Prozesse und Informatikumgebung individuell ermittelt und priorisiert. Dies ist eine Voraussetzung für die Kosteneffizienz und die Wirksamkeit aller Massnahmen. Zum Sicherheitsbedarf gehören sowohl die betriebsspezifische Sicherheit als auch der Einbezug der gesetzlichen

Rahmenbedingungen. Der Ist-Zustand wird mittels einer IT-Risikoanalyse und einer darauf aufbauenden Sicherheitsanalyse erhoben. Anhand der Feststellungen werden Massnahmen zur Behebung der allfälligen Schwachstellen definiert.

Mittels einer allgemeinen Katastrophenplanung, der Planung von baulichen Massnahmen (physische Sicherheit) und der Beübung des Ernstfalles können Ausfälle der Informatikmittel auf ein definiertes Mass reduziert werden. Damit alle relevanten Daten und Akten ohne Aufwand innert kürzester Zeit wieder zur Verfügung gestellt werden können, müssen diese Übungen in regelmässigen Abständen erfolgen.

Durch den Schutz von Informationen und Daten wird eine der wichtigsten Ressourcen der Verwaltungsstellen und öffentlicher Institutionen gesichert. Um deren wachsende Bedürfnisse im Bereich der Informations- und Informatiksicherheit abdecken zu können, hat der Datenschutzbeauftragte die Beratungsstelle für Informatiksicherheit aufgebaut. Die Beratungsstelle für Informatiksicherheit bietet umfassende, praxisorientierte Beratungsleistungen zu allen Themen der Informationssicherheit und des technischen Datenschutzes. Sie fördert das Bewusstsein über die Zusammenhänge von Informatiksicherheit und Datenschutz.

Die Beratungsstelle für Informatiksicherheit begleitet schrittweise in allen Phasen eines Projektlebenszyklus, berät in allen Belangen der Informatiksicherheit, evaluiert und implementiert Sicherheitslösungen und führt Evaluationen, Bewertungen oder Schulungen durch.

21. Richtlinien zur Nutzung der Informatik

Erarbeitung von Weisungen, Richtlinien oder Verordnungen

Wir wurden von verschiedenen Stellen angefragt, deren Entwürfe von Weisungen, Richtlinien oder Verordnungen zur Nutzung der Informatik zu beurteilen. Insgesamt erachteten wir alle abgegebenen Vorschläge als brauchbare Grundlage, auf der weiter aufgebaut werden konnte. Im Sinne der nachfolgenden Ausführungen bestand jedoch noch Bedarf an Anpassungen und Ergänzungen.

Generell waren die Entwürfe der Weisungen zu wenig präzise formuliert und die einzelnen Regelungen vermischten zu viele verschiedene Elemente der Informationstechnologie. Wir empfahlen deshalb die Auftrennung der teilweise umfangreichen Dokumente in einzelne Weisungen, Richtlinien oder Verordnungen mit möglichst einheitlichen Zwecken. Weiter haben wir eine Hilfestellung «Gestaltung von Weisungen» geschaffen, welche die bereits entwickelten Checklisten aus unserer Publikation «Fakten», Nummer 3/99, ergänzt. Im Vordergrund steht dabei die generelle Erarbeitung von Informatikweisungen mit möglichen Inhalten und wie diese strukturiert bzw. gestaltet werden sollen.

Um eine Weisung formell durchsetzen zu können, müssen in der Weisung die Verantwortlichkeiten, die Inkraftsetzung, die Regelung der Empfangsbestätigung, der Geltungsbereich und die Abgrenzungen niedergeschrieben werden. Diese organisatorischen Aspekte wurden meist zu wenig explizit definiert.

In manchen Weisungen waren die Begriffe nicht konsistent. Zum Beispiel wurde unter der Definition «Datenschutz» eigentlich die Datensicherheit behandelt und inhaltlich bezog sich der Abschnitt schliesslich wiederum nur auf den Zugriffsschutz. Die einzelnen Begriffe sind sorgsam zu wählen, damit die Kernaussage der Weisung nicht missverstanden werden kann. Der Datenschutz bezieht sich nicht nur auf Informatikmittel bzw. auf deren Benutzung, sondern generell auf die Handhabung personenbezogener Daten. Eine Abhandlung innerhalb der Weisung ist deshalb nicht notwendig, da die Rahmenbedingungen durch die Gesetze und Verordnungen geregelt werden.

Die meisten der an uns abgegebenen Dokumente enthielten eine Anordnung wie: «Office-Dokumente mit vertraulichem bzw. schützenswertem Inhalt sollen zusätzlich mit einem Passwort geschützt werden.» Grundsätzlich müssen alle Personendaten vor unbefugtem Zugriff geschützt werden. Das Passwort der Office-Dokumente kann leicht umgangen werden und bietet somit keinen echten Schutz. Aus diesem Grund empfehlen wir auch, sensible Daten mit einer starken Verschlüsselung abzusichern.

Einige der Weisungen trugen der Tatsache zu wenig Rechnung, dass der elektronische Mailverkehr mit der gleichen Sorgfalt zu behandeln ist wie der papierbezogene Schriftverkehr und dass E-Mails ohne digitale Signaturen formelle Dokumente nicht ersetzen können. Zudem fehlte bei allen Weisungen eine eindeutige Regelung, wie mit E-Mails bei Abwesenheiten umgegangen werden soll. Das automatische Weiterleiten von E-Mails und das Freigeben der persönlichen Mailbox an Drittpersonen ist nicht angemessen. Damit bei mehrtägigen Absenzen die ordentliche Geschäftsabwicklung gewährleistet werden kann, empfehlen wir die Funktion des Abwesenheitsassistenten (mit dem Hinweis, an wen man sich in dringenden Fällen wenden kann) zu nutzen.

Die Informatiksysteme sind Eigentum der Arbeitgebenden. Bei deren Gebrauch sollte sich jeder Anwendende bewusst sein, dass die Arbeitgebenden das Recht und die Pflicht haben, ihre Systeme zu schützen. Bei begründetem Verdacht oder klaren Hinweisen auf Missbrauch oder Zuwiderhandlungen gegen die erstellten Richtlinien sowie die unverhältnismässige Nutzung können, nach entsprechender Vorankündigung und Information der betroffenen Personen, gezielte Stichproben und Kontrollen durchgeführt werden. Entgegen der gängigen Meinung bleibt das Recht auf Sanktionen jederzeit bestehen und muss somit nicht explizit in den Weisungen aufgeführt werden.

Richtlinien zur Nutzung der Informatik sind ein wichtiges Instrument, den konkreten Umgang mit Informatikmitteln den Benutzenden zu erklären. Sie sind deshalb klar und zweckgerichtet zu formulieren.

22. Ausstellung von Jagd-Gästepässen via Internet

Zu umfassende Zugriffsrechte

Die Fischerei- und Jagdverwaltung hatte eine technische Lösung eingerichtet, bei der via Internet von Jagdrevierpächtern Gästepässe für die Jagd ausgestellt und direkt via Browser ausgedruckt werden konnten. Betroffene Personen hatten festgestellt, dass Jagende, welche eine Berechtigung für diese Applikation besassen, auch auf Daten anderer Jägerinnen und Jäger zugreifen und diese sogar mutieren konnten.

Wir teilten der Fischerei- und Jagdverwaltung unsere Feststellungen mit und verlangten eine umgehende Behebung der Mängel. Die Fischerei- und Jagdverwaltung liess die Applikation vorübergehend sperren und erarbeitete mit der Informatik-Dienstleisterin, welche die Lösung eingerichtet hatte, einen neuen Ablauf. Die Ausstellung eines Gästepasses ist mit der neuen Lösung nur noch möglich, wenn vorab mehrere Informationen über Formularfelder eingegeben werden. Dies löst eine Suche in der Datenbank aus. Wird eine Person gefunden, können die Informationen übertragen und der Gästepass kann ausgestellt werden. Ist die Person nicht in der Datenbank vorhanden oder stimmen die Eingaben nicht, muss ein Gästepass bei der Fischerei- und Jagdverwaltung beantragt werden, welche auch die Neuerfassung oder eine Mutation der Person vornimmt.

Unsere Intervention hatte dazu geführt, dass Jagende keinen unbeschränkten Zugriff auf Daten mehr haben.

Eine Internet-Applikation, die eine Interaktion mit einem öffentlichen Organ auslöst, muss so eingerichtet werden, dass nur diejenigen Daten aus einer Datenbank an einen Benutzer beziehungsweise eine Benutzerin geliefert werden, die für die Interaktion im Einzelfall notwendig sind. Mit Authentifizierungsverfahren ist sicherzustellen, dass die Identität der Benutzenden geklärt wird.

23. Fussnotentext in E-Mail

Keine ausreichende Sicherheitsmassnahme

In der elektronischen Post (E-Mail) sind häufig Fussnotentexte (so genannte «Disclaimer») zu finden, die in etwa wie folgt lauten: «Diese E-Mail enthält vertrauliche und/oder rechtlich geschützte Informationen. Wenn Sie nicht der richtige Adressat sind oder diese E-Mail irrtümlich erhalten haben, informieren Sie bitte sofort den Absender und vernichten Sie diese E-Mail. Das unerlaubte Kopieren oder die unbefugte Weitergabe dieser E-Mail ist nicht gestattet.» Der Informatikverantwortliche einer Gemeinde fragte uns an, ob solche Fussnotentexte empfohlen werden können und welche rechtliche Bedeutung sie haben.

Aus rechtlicher Sicht stellt ein solcher Text keine ausreichende Sicherheitsmassnahme dar, um die Vertraulichkeit und Integrität von E-Mails zu wahren. Dazu sind kryptografische Verfahren notwendig (siehe Tätigkeitsbericht Nr. 5 [1999], S. 32). Vertrauliche Informationen beziehungsweise sensible Daten sollten nicht per E-Mail ausgetauscht werden, solange keine Verschlüsselungsmöglichkeit eingerichtet ist. (Es fällt ja auch niemandem ein, Informationen, die vertraulich bleiben müssen, offen per Postkarte zu verschicken und einen ähnlichen Text anzufügen.) Ein Fussnotentext kann beim Austausch von nicht sensiblen Daten sinnvoll sein, um einen irrtümlichen Empfänger zu ermahnen, den Absender zu informieren, damit der Versand wiederholt werden kann. Ein solcher Text ist bereits heute häufig auf Telefaxen zu finden. (Das Telefax ist ebenfalls nur zum Versand nicht sensibler Informationen zu verwenden.) Andererseits kann er auch dazu verleiten, dennoch sensible Daten per E-Mail zu verschicken. Zum Sicherheitsstan-

dard gehören deshalb auch entsprechende Schulungs- und Sensibilisierungsmassnahmen.

Die Verwendung eines E-Mail-Disclaimers ist keine angemessene Sicherheitsmassnahme zur Wahrung der Vertraulichkeit von E-Mail. Vielmehr sind Verschlüsselungsmassnahmen zu treffen. Ein Disclaimer ist nützlich, um beim Versand von nicht sensiblen Informationen einen falschen Empfänger zur Löschung der E-Mail und um eine Information des Absenders anzuhalten.

DATENSCHUTZREVIEW

24. Überprüfungen bestätigen Defizite

Informatiksicherheit mangelhaft

Der Datenschutzbeauftragte hat wie in den Vorjahren bei ausgewählten Amtsstellen (siehe Tätigkeitsbericht Nr. 2 [1996], S. 34, Nr. 5 [1999], S. 32, Nr. 6 [2000], S. 32, und Nr. 7 [2001], S. 29) Datenschutzreviews durchgeführt. Das Ziel der Reviews sind die Überprüfung von Grundschutzmassnahmen sowie die Sensibilisierung für den Datenschutz und die Informatiksicherheit. Praxisbezogene Massnahmenempfehlungen für die geprüften Stellen sind ein erster Schritt zu verantwortungsbewusstem Umgang mit Personendaten und zu einem geordneten und sicheren Informatikbetrieb.

Die bereits in früheren Tätigkeitsberichten aufgeführten Mängel sind mit den vorgenommenen Prüfungen bestätigt worden. Die wichtigsten empfohlenen Massnahmen sind:

- Festlegen der Verantwortlichkeiten für den IT-Betrieb und insbesondere für Informatiksicherheit:
Nur durch die Zuweisung der Aufgaben können anschliessend auch die Mittel zur Erreichung der gemäss Informatiksicherheitsverordnung bestimmten Sicherheitsstufe festgelegt werden. In der Folge ist die Umsetzung der Massnahmenpläne durch den so bestimmten Verantwortlichen konkret an die Hand zu nehmen.

- Sensibilisieren der Benützenden für Informatiksicherheit:
Sporadische Meldungen sind zwingend in eine Planung überzuführen, um die Mitarbeitenden gezielt in allen Themen aus- oder weiterzubilden.

- Ergänzen der meist zu rudimentären Weisungen an die Benützenden (speziell zur Benützung PC, E-Mail und Internet). Alle ergänzten Weisungen sind nach der Überarbeitung zur Sensibilisierung der Benützenden zu verwenden.

- Dokumente zur Umsetzung der Informatiksicherheitsverordnung sind meist nur in Ansätzen oder nicht nachgeführt vorhanden:
Die Massnahmenpläne zur Erreichung der Sicherheitsstufe sind für eine korrekte und konsistente Umsetzung unverzichtbar. Der Plan soll Auskunft über den Stand, die Verantwortlichkeiten und Kosten im Bereich Informatiksicherheit geben und ist somit ein Nachweis einer verantwortungsvollen Führung der Stelle.

- In den Vertragsbestimmungen fehlen Klauseln für Geheimhaltung und Sicherheit:
Zumindest die Allgemeinen Geschäftsbedingungen über die Geheimhaltung, den Datenschutz und die Daten- und Informationssicherheit bei der Erbringung von Informatikdienstleistungen (AGB Sicherheit vom September 2001) sind den Dienstleistenden zu überbinden.

- Zugriffskonzepte sind mangelhaft:
Nebst der Differenzierung der Zugriffsberechtigungen sind die Auswertungen angepasst an die Stellengrösse zu kontrollieren.

Die Datenschutzreview als Überprüfungs- und Sensibilisierungsinstrument des Datenschutzbeauftragten ist weiterhin dringend nötig. Die Amtsstellen und Gemeinden haben den Bereichen Datenschutz und Informatiksicherheit einen den Risiken angemessenen Stellenwert in ihrem Aufgabenportfolio zuzuweisen.

FORSCHUNG UND STATISTIK

25. Vorgehen bei Forschungsprojekten

Merkblatt und Checkliste

Wir erhalten regelmässig Anfragen von öffentlichen Organen, welche wissen möchten, wie sie vorzugehen haben, wenn forschende Personen und Institutionen um Bekanntgabe von Personendaten ersuchen. Zugleich fragen auch forschende Personen oder Institutionen nach den datenschutzrechtlichen Voraussetzungen bei Forschungsprojekten.

Wir haben ein Merkblatt verfasst, welches sich an forschende Personen und Institutionen richtet, die zu Forschungszwecken Personendaten benötigen. Es soll aufzeigen, welche Rahmenbedingungen einzuhalten sind, wenn öffentliche Organe Personendaten für Forschungszwecke weitergeben sollen.

Personendaten dürfen für nicht personenbezogene Zwecke in der Forschung, Planung und Statistik bearbeitet werden, wenn

- die Daten anonymisiert werden, sobald es der Zweck des Bearbeitens erlaubt, und
- die Ergebnisse so veröffentlicht werden, dass die betroffenen Personen nicht bestimmbar sind.

Öffentliche Organe dürfen für nicht personenbezogene Zwecke Personendaten bekannt geben, wenn

- keine Geheimhaltungspflicht oder andere Bestimmung dies ausschliesst,
- Rückschlüsse auf die betroffenen Personen möglichst erschwert sind und
- die forschende Person oder Organisation für die Einhaltung der Bearbeitungsvorschriften Gewähr bietet und die Daten nur mit Zustimmung des verantwortlichen Organs weitergibt.

Für den Datenschutz ist das Organ verantwortlich, das die Personendaten zur Erfüllung seiner Aufgaben bearbeitet oder bearbeiten lässt. Bei der Erhebung von Personendaten muss den Befragten der Zweck der Erhebung dargelegt werden, ebenso allfällige Rechtsgrundlagen, Beschlüsse usw., welche zur Erhebung der genannten Personendaten berechtigen. Die erhobenen Daten sind mittels technischer und organisatorischer Massnahmen vor dem Zugriff Unbefugter zu schützen. Der Kreis der Personen, welche Zugang zu den Personendaten haben, muss auch innerhalb der Forschungsstelle möglichst klein sein. Die Personendaten dürfen nur für den bei der Erhebung angegebenen Zweck verwendet und nicht weitergegeben werden. Sie sind zu anonymisieren, sobald es der Zweck des Bearbeitens erlaubt. Nicht mehr benötigte Daten sind zu vernichten.

Werden beim Forschungsprojekt medizinische Daten bearbeitet, die unter das ärztliche Berufsgeheimnis fallen, so muss ein besonderes bundesrechtliches Verfahren eingehalten werden.

Zieht die forschende Person oder Institution einen Dritten bei, ist der Datenschutz durch Auflagen, Vereinbarungen oder auf andere Weise sicherzustellen. Ohne anders lautende ausdrückliche Ermächtigung darf die beauftragte Stelle Personendaten nur für die Auftraggeberin verwenden und nur dieser bekannt geben. Diese Bestimmung ist durch eine Muster-Vereinbarung für den Kanton Zürich konkretisiert worden.

Bei Gesuchen stellt die forschende Person/Institution beim öffentlichen Organ schriftlich und detailliert Antrag. Das öffentliche Organ überprüft als potenzieller Datenlieferant die Rechtmässigkeit der Datenbekanntgabe. Dazu ist es nur in der Lage, wenn es von der anfragenden Forschungsstelle ausreichende Angaben über das Forschungsvorhaben erhält. Sind sämtliche Voraussetzungen erfüllt, kann das öffentliche Organ der Forschungsstelle die gewünschten Personendaten bekannt geben. Die Bekanntgabe ist mit der Auflage zu versehen, die Daten nur für diesen Zweck zu verwenden.

Werden Daten direkt bei betroffenen Personen mittels Fragebogen erhoben, muss über Folgendes informiert werden:

- Nennung der forschenden Person/Institution und des Zwecks des Projekts,
- Kurzbeschreibung des Ablaufs der Datenbearbeitung (Auswertung, Anonymisierung usw.),
- Hinweis auf Freiwilligkeit der Teilnahme und Recht auf Verweigerung (besteht eine Mitwirkungspflicht, ist dies zu erwähnen, und es sind die gesetzlichen Grundlagen sowie die Folgen bei einer Verweigerung anzugeben).

Für die öffentlichen Organe haben wir eine Checkliste geschaffen. Sie konkretisiert die Voraussetzungen, welche erfüllt sein müssen, damit ein öffentliches Organ Personendaten zu Forschungszwecken bekannt geben darf. Die öffentlichen Organe müssen in jedem Fall die Einhaltung der gesetzlichen Vorschriften vor der Datenbekanntgabe überprüfen. Das von der Forschungsstelle zu stellende Gesuch muss dafür die notwendigen Angaben enthalten.

Die Anfrage muss Angaben über die folgenden Punkte enthalten:

- Name und Inhalt des Forschungsprojektes
- Angaben zur forschenden Person/Institution (inkl. Kurzvorstellung der Person/Institution sowie Funktion der Leitung und der Mitarbeitenden) sowie Angaben zu einem allfälligen Auftraggeber der Studie
- Gesetzliche Grundlagen (soweit vorhanden)

- Zweck der Studie (genauer Forschungszweck) mit dem Nachweis, dass das Ziel in Auswertungen bzw. Resultaten besteht, die von einzelnen Personen losgelöst sind (nicht personenbezogener Zweck)
- Beschreibung der Forschungsmethode
- Darlegung der Notwendigkeit sämtlicher verlangter Personendaten
- Nennung der zu bearbeitenden Personendaten
- Beschreibung des Kreises der untersuchten Personen
- Art der Bearbeitung (Design des Ablaufs der Datenbearbeitung mit Beschreibung der Methoden der Beschaffung und Auswertung der Personendaten)
- Zugang zu den Personendaten (Kreis der Personen, welche Zugang zu den Personendaten haben)
- Anonymisierung der Daten (Zeitpunkt, Vorgehen)
- Art der Veröffentlichung der Ergebnisse (Anonymisierung ohne Rückschlussmöglichkeiten auf Betroffene)
- Organisatorische und technische Massnahmen für die sichere Aufbewahrung und korrekte Vernichtung der Personendaten
- Datenschutz-Revers mit den beteiligten Personen sowie Vereinbarung mit allfällig beigezogenen Dritten

Forschende Personen und Institutionen sowie öffentliche Organe erhalten mit dem Merkblatt und der Checkliste Anleitungen für das Vorgehen bei Forschungsprojekten, bei welchen Personendaten bearbeitet werden. Das Merkblatt ist publiziert auf der Homepage des Datenschutzbeauftragten.

26. Evaluation der Mitarbeiterbeurteilung

Transparenz der Datenerhebung

Die Pädagogische Hochschule Zürich führte im Auftrag der Bildungsdirektion bei Lehrerinnen und Lehrern eine Evaluation der Mitarbeiterinnen- und Mitarbeiterbeurteilung (MAB) durch. Neben Fragen zur MAB enthielt der Fragebogen verschiedene andere Teile, u.a. einen, in dem die Lehrpersonen über ihre Lebensqualität in den letzten zwei Wochen befragt wurden. Auf Grund dieser zum Teil sehr persönlichen Fragen trafen heftige Reklamationen ein. Der Datenschutzbeauftragte wurde um eine Stellungnahme gebeten.

Die vorliegende Datenbearbeitung richtet sich nach den Grundsätzen von § 12 DSG.

In den Erklärungen zum Erhebungsbogen wurden der Zweck und das Ziel der Befragung dargelegt. Es wurde ausgeführt, die Befragung erfolge auf freiwilliger Basis, die erhobenen Personendaten würden vertraulich behandelt und baldmöglichst anonymisiert. Im Einführungsteil zu den Fragen zur Lebensqualität wurde darauf hingewiesen, dass Fragen, die den Befragten zu persönlich erscheinen, nicht zu beantworten sind. Zur Erklärung des Fragenkatalogs wurde ausgeführt, dass sämtliche Fragen auf einer international geeichten Skala der Weltgesundheitsorganisation beruhen würden.

Aus datenschutzrechtlicher Sicht war die Befragung nicht zu beanstanden, da die nötigen Vorkehrungen wie z.B. die ausdrückliche Freiwilligkeit oder die Anonymisierung vorgesehen waren. Fraglich erschien einzig, ob die Angaben zum Privatleben für die Evaluation der Mitarbeiterbeurteilung überhaupt geeignet und erforderlich sind.

Bei Evaluationen und Forschungsprojekten ist für die betroffenen Personen die notwendige Transparenz zu schaffen, wie ihre Daten bearbeitet werden.

27. Forschungsprojekt «Kinderpornographie im Internet»

Rahmenbedingungen für Befragung von Angeschuldigten

Der Psychiatrisch-Psychologische Dienst des Amtes für Justizvollzug bat den Datenschutzbeauftragten, zum geplanten Forschungsprojekt «Kinderpornographie im Internet» Stellung zu nehmen. Zweck des Forschungsprojektes ist die Erforschung der Persönlichkeit der Konsumenten von kinderpornographischem Material.

Wir unterscheiden zwischen der Bearbeitung von Personendaten im Rahmen eines laufenden Strafverfahrens und nach dem Abschluss eines solchen Verfahrens. Im laufenden Verfahren ist das Datenschutzgesetz nicht anwendbar, es gelten vielmehr die – für diesen Bereich noch zu schaffenden – gesetzlichen Bestimmungen der Strafprozessordnung. Für die Bearbeitung von Personendaten bei einem abgeschlossenen Verfahren gelangt das Datenschutzgesetz zur Anwendung. Dient die Bearbeitung einem Forschungszweck, gelten die erleichterten Voraussetzungen von § 12 Datenschutzgesetz.

Wir gelangten zum Schluss, dass die beim Forschungsprojekt «Kinderpornographie im Internet» des Psychiatrisch-Psychologischen Dienstes erhobenen Personendaten der Forschung dienen. Dabei dürfen jedoch im Rahmen der Verhältnismässigkeit nur die zur Erreichung dieses Zweckes absolut notwendigen Personendaten zur Person des Angeschuldigten erhoben werden.

Zudem müssen sie vertraulich behandelt werden. Die Angaben zur Person sind von den Auswertungen strikt getrennt aufzubewahren, so dass eine persönliche Identifikation nicht möglich ist. Zudem sind die Daten sobald als möglich zu anonymisieren und nach Ende des Forschungsprojekts zu vernichten.

Unter Beachtung der gesetzlichen Voraussetzungen dürfen Personendaten nach abgeschlossenem Verfahren zu Forschungszwecken bearbeitet werden.

INDIVIDUALRECHTE

28. Herausgabe eines psychiatrischen Gutachtens

Grundsatz der vollumfänglichen Einsicht

Von einem Bezirksrat wurden wir um Stellungnahme zur Herausgabe eines psychiatrischen Gutachtens durch eine Vormundschaftsbehörde ersucht.

Wir wiesen auf den Grundsatz der uneingeschränkten Einsicht in die eigenen Daten sowie auf die Voraussetzungen einer Aufschiebung, Einschränkung oder Verweigerung hin. Es war zu prüfen, ob ein überwiegendes öffentliches Interesse eine Verweigerung oder Einschränkung des Einsichtsrechts rechtfertigt. Die Vormundschaftsbehörde hatte die Einsicht in das psychiatrische Gutachten verweigert, der betroffenen Person jedoch angeboten, sich das Gutachten durch die behandelnden Ärzte der Klinik erklären zu lassen. Die betroffene Person verlangte jedoch vollständige Einsicht in das Gutachten und Zustellung einer Kopie.

Wir gelangten zum Schluss, dass grundsätzlich ein uneingeschränktes Einsichtsrecht besteht. Bei Gesundheitsdaten kann in Anlehnung an eine bundesrechtliche Vorschrift eine Spezialbestimmung zur Anwendung gelangen, wonach der Inhaber der Datensammlung der betroffenen Person Daten über die Gesundheit durch einen von ihr bezeichneten Arzt mitteilen lassen kann. Das Motiv dieser Regelung besteht darin, den Gesuchsteller vor Schaden zu bewahren, der ihm durch eine unmittelbare und unvorbereitete Einsicht in die medizinischen Daten entstehen könnte. Der Arzt soll auf Grund seiner Ausbildung und Erfahrung eher in der Lage sein, den Betroffenen so zu orientieren, dass dieser nicht noch zusätzlichen Schaden (sog. Aufklärungsschaden) nimmt. Weil diese Regelung indessen paternalistisch anmutet und zur Eigenverantwortung des Betroffenen in einem Spannungsfeld steht, ist sie restriktiv anzuwenden. Sie hat sich auf Fälle zu beschränken, bei denen die Möglichkeit einer Schädigung nahe liegt; ein temporäres Unwohlbefinden reicht nicht. Die Regelung dürfte damit regelmässig nur für einen Teil aller Daten über die Gesundheit zutreffen.

Wir boten dem Bezirksrat Entscheidungsgrundlagen, welche ihm ermöglichten, im zu beurteilenden Fall zu entscheiden, ob das öffentliche Interesse an der Verhinderung eines Aufklärungsschadens die Einschränkung oder Verweigerung der Einsicht rechtfertigt. Wir vertraten die Meinung, zumindest teilweise Einsicht sei zu gewähren. Sollte der Bezirksrat jedoch zur Auffassung gelangen, bei Gewährung der direkten Einsicht in einen Teil des Gutachtens bestehe die hohe Wahrscheinlichkeit eines Aufklärungsschadens, wäre der betroffenen Person indirekt auf dem Weg der Einsichtnahme über einen von ihr bezeichneten Arzt ihres Vertrauens Einsicht in diese Teile des Gutachtens zu gewähren.

Grundsätzlich besteht ein vollumfängliches Einsichtsrecht. Steht diesem ein überwiegendes öffentliches Interesse gegenüber, ist der betroffenen Person bei Gesundheitsdaten indirekt auf dem Weg der Einsichtnahme über einen Arzt Einsicht zu geben.

29. Verfahren der Personalschlichtung

Mangelnde Geheimhaltung

An einer höheren Ausbildungsstätte bestand ein Konflikt zwischen einer Lehrkraft und einer Mitarbeiterin, wobei der Konflikt offenbar auf geschäftlicher wie auf privater Ebene stattfand. Der Rechtsvertreter der Lehrkraft wandte sich mit verschiedenen datenschutzrechtlich relevanten Aspekten an uns.

Vorab beanstandete der Rechtsvertreter, dass die Ausbildungsstätte trotz mehrfacher Interventionen das Auskunftsrecht nicht gewährte bzw. nicht gewillt sei, Kopien des Personaldossiers anzufertigen. Im Sinne unserer Vermittlungsfunktion gelangten wir an die Ausbildungsstätte und konnten bewirken, dass dem Rechtsanwalt vollständige Auskunft über das Personaldossier seiner Mandantin erteilt wurde und er Kopien aller Dokumente erhielt. Ausserdem hatte er eine ungeeignete Führung des Personaldossiers moniert. Die Ausbildungsstätte teilte uns diesbezüglich mit, dass die Dossierführung im Rahmen der Umsetzung des neuen Personalrechts ohnehin überprüft und an die gesetzlichen Vorgaben angepasst werde. Diese Umsetzung sei im Gange.

Das Personalrecht der Ausbildungsstätte sieht vor, dass eine Kommission Schlichtungsverfahren durchführen kann, wenn es zu Konflikten unter den Mitarbeitenden oder zwischen Mitarbeitenden und Vorgesetzten kommt. Das Schlichtungsverfahren zeichnet sich durch eine strenge Geheimhaltungspflicht aller Beteiligten aus. Geschäftsstelle der Kommission ist eine Stabsstelle der Ausbildungsstätte. Der Konflikt hatte bereits zu einem Schlichtungsverfahren vor der Kommission geführt. Die Mitarbeiterin reichte im Rahmen eines Schlichtungsverfahrens private Briefe als Beweismittel ein, leitete diese Briefe gleichzeitig aber auch der Leitung der betreffenden Abteilung zu. Damit verstiess sie gegen die Geheimhaltungspflicht. Wir teilten der Ausbildungsstätte deshalb mit, dass die Briefe von der Abteilungsleitung zu vernichten sind, da sie im Rahmen des Schlichtungsverfahrens eingereicht worden waren. Es stellte sich auch die Frage nach der Verwendung von privaten Briefen im Rahmen eines personalrechtlichen Schlichtungsverfahrens. Da wir die Bedeutung dieser Briefe im konkreten Fall nicht beurteilen konnten, wiesen wir darauf hin, dass die Briefe zu vernichten seien, sofern sich im Verlauf des Verfahrens herausstellt, dass sie nicht relevant sind.

In organisatorischer Hinsicht zeigte sich, dass die Stellung der Stabsstelle nicht unproblematisch ist und zu Interessenkollisionen führen kann. Die Stabsstelle fungiert als Geschäftsstelle der Kommission. Gleichzeitig ist sie auch Stabsstelle der Gesamtleitung der Ausbildungsstätte. In Fällen, in denen die Gesamtleitung Partei des Schlichtungsverfahrens ist, führt dies dazu, dass die Unabhängigkeit der Kommission gefährdet ist. Wir empfahlen deshalb, eine eigenständige Geschäftsstelle der Kommission einzurichten.

Der Datenschutzbeauftragte kann in Konfliktfällen meist nur Teilaspekte (Datenbearbeitungen, Behandlung von Auskunfts- und anderen Begehren) beurteilen. In solchen Fällen ist eine korrekte Behandlung von Auskunftsbegehren jedoch zentral und vertrauensbildend. Unsere Vermittlung führte im konkreten Fall insofern zum Erfolg, als schliesslich wenigstens das Auskunftsrecht gewährleistet wurde.

Auskunftsrecht und Geheimhaltungsvorschriften stellen wichtige datenschutzrechtliche Rahmenbedingungen dar, die auch bei personalrechtlichen Konflikten strikte zu beachten sind.

Optische Überwachung breitet sich aus

Mit einem Grundlagenbericht, Empfehlungen und Checklisten wurde auf den zunehmenden Einsatz der Videoüberwachung reagiert.

Der Datenschutzbeauftragte befasste sich im Berichtsjahr mehrfach mit dem Thema Videoüberwachung. Die allgemeine Überwachung von Personen mittels Videogeräten breitet sich immer mehr aus. Die technologischen Möglichkeiten der Videoüberwachung sind heute noch nicht ausgeschöpft und das Potenzial für Eingriffe in die Privatheit ist wachsend.

Eine Videoüberwachung beinhaltet in den meisten Fällen einen Eingriff in das Recht auf Privatheit der betroffenen Personen. Deshalb sind die öffentlichen Organe an die rechtsstaatlichen Voraussetzungen, wie sie für einen Eingriff in Grundrechte in der Verfassung definiert sind, gebunden. In einem Bericht zur Videoüberwachung durch öffentliche Organe stellen wir die Grundlagen dar (siehe www.datenschutz.ch). Jede Überwachung mittels Videogeräten hat auf einer ausreichenden rechtlichen Grundlage zu basieren. Für die Einschränkung des Grundrechts auf Privatheit bestehen klare rechtsstaatliche Voraussetzungen. Die Massnahme muss verhältnismässig sein und im öffentlichen Interesse liegen. Der Einsatz erfolgt heute jedoch mehrheitlich, ohne dass die Fragen nach der Eignung und der Erforderlichkeit dieser Massnahmen klar beantwortet sind. Deshalb wurde der Bericht mit Empfehlungen und Checkliste ergänzt. Sie ermöglichen die Evaluierung, ob der Einsatz einer Videoüberwachung sinnvoll ist, und geben im Weiteren konkrete Hinweise für die Gestaltung rechtlicher Rahmenbedingungen und betrieblicher Abläufe. Eine Videoüberwachung kann zu unterschiedlichen Zwecken eingerichtet werden. Es lassen sich drei Kategorien unterscheiden (observierende, dissuasive und invasive Videoüberwachung, welche im erwähnten Bericht dargestellt werden). Empfehlungen und Checkliste hingegen beziehen sich ausschliesslich auf die dissuasive Überwachung, mit der primär versucht wird, präventiv bestimmte öffentliche Räume zu beobachten. Sie wird zunehmend eingesetzt auf öffentlichen Plätzen, in Bahnhofsgebäuden oder in Sportanlagen, dient der inneren Sicherheit und richtet sich auf eine Vielzahl von unbestimmten Personen, die sich im überwachten Raum bewegen. Sie ist auf die Erkennbarkeit der Personen ausgerichtet. Damit handelt es sich um einen Eingriff in die persönliche Freiheit. Mittels technischer Zusätze wie der Erkennung von Verhaltensmustern und Verhaltensabweichungen oder der Gesichtserkennung erlaubt diese Form der Überwachung immer weiter gehende Eingriffe und mit der Digitalisierung und Aufzeichnung auch eine faktisch beliebige Weiterbearbeitung. Unter Umständen lassen sich sogar Bewegungs- und Persönlichkeitsprofile erstellen.

Vor Anordnung einer Videoüberwachungsmassnahme muss das zuständige öffentliche Organ prüfen, ob eine Videoüberwachung im konkreten Fall die einzig sinnvolle Lösung ist.

Nach Evaluierung des zu lösenden Problems sind verschiedene Problemlösungsmöglichkeiten aufzuzeigen, welche als «passive Massnahmen» möglichst nicht in die Privatsphäre von betroffenen Personen eingreifen und das Grundrecht auf Schutz der Privatsphäre am wenigsten tangieren. Statt einer Videoüberwachung sind bauliche Massnahmen (Umbau von unübersichtlichen Plätzen und Durchgängen, Absperrung an unübersichtlichen Stellen, optische Gestaltung mit vermehrter Übersicht, stärkere Beleuchtung dunkler Orte oder Bewegungsmelder an kritischen Orten), personelle Massnahmen (Einrichtung eines Sicherheitsdienstes, Einsatz von Polizeipatrouillen) oder soziale Massnahmen (Einrichtung eines Treffpunktwagens, Errichtung einer öffentlichen Telefonzelle oder einer Notrufsäule, Belebung des öffentlichen Raumes durch Café oder Kiosk, sozialpädagogische Einrichtungen wie Trouble-shooting oder Gassenarbeit) sowie die Kombination verschiedener Massnahmen denkbar. Sämtliche Problemlösungsmöglichkeiten sind gegeneinander abzuwägen. Erweisen sich alle «passiven Massnahmen» als nicht tauglich oder als nicht durchführbar, kann in einem zweiten Schritt als «aktive Massnahme» eine Videoüberwachung in Betracht gezogen werden.

Erweist sich die Videoüberwachungsmassnahme im konkreten Fall als geeignete und erforderliche Massnahme, ist eine Rechtsgrundlage zu schaffen, welche folgenden Anforderungen zu genügen hat:

Inhaltlich:

- Ziel und Zweck der Massnahme müssen klar festgelegt sein.
- Der Zweck sowie das zu erreichende Ziel sind in der gesetzlichen Grundlage genau zu umschreiben.

Formell ist festzulegen:

- Wer überwacht (verantwortliche Stelle)
- Was überwacht wird (Örtlichkeiten)
- Wann überwacht wird (Zeiten)
- Zu welchem Zweck überwacht wird (Ziel)
- Wie überwacht wird (technische Möglichkeiten/Beobachtung oder Aufzeichnung)
- Wie die Auswertung des Bildmaterials erfolgt (Auswertung)
- Durch wen die Auswertung erfolgt (Verantwortung für Auswertung)
- Dauer der Aufbewahrung des Bildmaterials (Aufbewahrung)
- Wo das Auskunftsrecht betroffener Personen geltend gemacht werden kann (Auskunftsrecht)
- Falls die Videoüberwachung durch eine andere als die verantwortliche Stelle durchgeführt wird, ist eine entsprechende Datenschutzvereinbarung nötig.

Verhältnismässigkeit:

Der zeitliche sowie der örtliche Umfang der Videoüberwachung müssen definiert sein. Eine Überwachung soll nicht jederzeit, sondern nur dann stattfinden, wenn mit der Begehung von schweren Straftaten zu rechnen ist.

Eine Überwachung soll auch nicht flächendeckend sein. Die Kameras müssen so platziert werden, dass nur die für den verfolgten Zweck absolut notwendigen Bilder in ihrem Aufnahmefeld erscheinen.

Verhältnismässig muss die Videoüberwachung auch im Hinblick auf eine geplante Aufzeichnung des Bildmaterials sein. Kann der Zweck mittels reiner Videobeobachtung ohne Aufzeichnung gewährleistet werden, ist diese Art der Überwachung vorzuziehen.

Erweist sich eine Aufzeichnung als notwendig, muss die Aufbewahrungszeit des Bildmaterials möglichst kurz sein. In der Regel ist das Bildmaterial innert 24 Stunden zu löschen oder zu überschreiben.

Eine Speicherung über die bekannt gemachte Aufbewahrungszeit hinaus ist im Falle der Einleitung eines Strafverfahrens möglich. Eine allfällige Weitergabe des Bildmaterials ist bei der Erfüllung eines Straftatbestandes und nur an die Strafverfolgungsbehörden möglich.

Beim Betrieb von Videoüberwachungsmassnahmen ist Folgendes zu beachten:

- Es ist durch gut sichtbare Hinweistafeln auf die Videoüberwachung hinzuweisen. Es ist mitzuteilen, ob eine Beobachtung oder eine Aufzeichnung erfolgt. Die für die Videoüberwachung verantwortliche Stelle muss die Bekanntmachung unterzeichnen.
- Die Kamera muss gut sichtbar aufgestellt werden.
- Mit dem Einsatz von so genannten «Privacy Filters» können Gesichter verschlüsselt werden, bis eine Aufnahme für eine allfällige Identifizierung benötigt wird.
- Nur berechtigte Personen dürfen Zutritt zu den Räumen haben, in denen das Bildmaterial gesichtet wird.
- Das Bildmaterial ist vor jeglicher unbefugten Verwendung zu schützen. Gespeichertes Bildmaterial muss an einem sicheren Ort aufbewahrt werden.
- Das Bildmaterial darf nur zum ursprünglich angegebenen Zweck verwendet werden. Wird die Verhinderung schwerer Verbrechen bezweckt, darf es nicht zur Feststellung unmoralischen, jedoch nicht strafbaren Verhaltens verwendet werden. Wird eine Beobachtung bekannt gemacht, darf nicht im Nachhinein eine Aufzeichnung erfolgen.
- Aufgezeichnetes Bildmaterial ist innert der festgelegten Zeit automatisch zu löschen.
- Es dürfen keine Kopien hergestellt werden.
- Eine weitere Aufbewahrung ist nur im Zusammenhang mit einem Vorfall im Rahmen der Beweissicherung möglich. Das Bildmaterial ist als Beweismittel gesichert aufzubewahren.
- Eine Weitergabe an die Strafuntersuchungsbehörden ist nur im Rahmen der Einleitung eines Strafverfahrens möglich und hat unverzüglich zu erfolgen.
- Die verantwortliche Stelle muss gewährleisten, dass das mit der Videoüberwachung betraute Personal für seine Aufgabe genügend geschult wird.
- Es muss periodisch überprüft werden, ob der Einsatz einer Videoüberwachungsmassnahme weiterhin erforderlich ist und die Rahmenbedingungen eingehalten werden.

Wie bereits im Tätigkeitsbericht Nr. 7 (2001), S. 10, ausgeführt, plante die Flughafenpolizei im Rahmen eines Pilotbetriebs die Einführung eines optischen Überwachungssystems mit einer systematischen Gesichtserkennung («Face Recognition»). Wir verfassten eine Stellungnahme, in der wir auf die bestehenden datenschutzrechtlichen und sicherheitstechnischen Mängel des Projekts hinwiesen.

Vor der geplanten Inbetriebnahme im Spätsommer stiess das System in den Medien auf ein breites Interesse. Der Datenschutzbeauftragte nahm mehrfach zum geplanten Pilotbetrieb Stellung.

Eine dringliche Anfrage aus dem Kantonsrat vom 8. Juli 2002 bezüglich gesetzlicher Grundlagen, Zwecks, Nutzen sowie Kosten des biometrischen

Gesichtserkennungssystems beantwortete der Regierungsrat am 24. Juli 2002. Er führte aus, dass die gesetzlichen Grundlagen, welche im in Revision befindlichen Bundesgesetz über die Ausländerinnen und Ausländer (AuG) geschaffen werden sollen, die Möglichkeit vorsehen, die Ankunft von Flugzeugpassagieren mit technischen Erkennungsverfahren zu überwachen.

Bis dahin befinde sich das Projekt in einer von September 2002 bis März 2003 befristeten Pilotphase und werde zunächst ausschliesslich bei vorgelagerten Grenzkontrollen eingesetzt. Bezweckt werde damit die Erprobung der technischen Eignung und der Einsetzbarkeit des Systems. Die Ausgestaltung dieser ersten Testphase sei daher genügend konkret. Die zweite Testphase sowie die definitive Einführung des Systems würden schliesslich auf einer vorgängig zu schaffenden Rechtsgrundlage beruhen.

Beim Face-Recognition-System der Flughafenpolizei sind die Fragen der Zweckbindung und der gesetzlichen Grundlagen von zentraler Bedeutung. Das System bezweckt, die illegal eingereisten Flugpassagiere, die über keine Dokumente mehr verfügen, an ihren Herkunftsort zurücksenden zu können. Technisch ist es jedoch ohne Weiteres möglich, die einmal erfassten, digitalisierten Aufnahmen auch zu anderen Zwecken zu verwenden, beispielsweise mit Fahndungsdatenbanken abzugleichen. Deshalb sind klare rechtliche Rahmenbedingungen zu formulieren, welche die Ziele und Aufgaben eines solchen Systems umschreiben, und es ist technisch zu verhindern, dass die Daten zu anderen Zwecken verwendet werden können.

Für die optische Überwachung fehlt oftmals eine klare gesetzliche Grundlage. Zudem erweisen sich viele Vorhaben als unverhältnismässig. Grundlagenbericht sowie Empfehlungen und Checkliste umschreiben die rechtlichen Rahmenbedingungen und geben konkrete Handlungsanleitungen für öffentliche Organe.

Rahmenbedingungen geben Leitplanken

Verschiedene Projekte entwickeln sich positiv unter Beachtung der Rahmenbedingungen.

1. Informations- und Datenschutzgesetz

Wirkungsorientierter Umgang mit Informationen und Personendaten

Im März 2002 hatte der Regierungsrat das Konzept für ein neues Informations- und Datenschutzgesetz verabschiedet (siehe Tätigkeitsbericht Nr. 7 [2001], S. 31ff.). Das Gesetz soll einerseits das neu einzuführende Öffentlichkeitsprinzip im Kanton Zürich regeln, andererseits das bestehende Datenschutzgesetz integrieren und modernisieren. Eine Arbeitsgruppe begann mit der Umsetzung des regierungsrätlichen Konzepts. Auf Grund der hohen Komplexität der Materie wurden zwei Experten beigezogen. Die Experten lieferten themenbezogene Konzeptionspapiere, welche verschiedene gesetzgeberische Varianten und deren Konsequenzen aufzeigten, einzelne Rechtsvergleiche anstellten und erste Formulierungsvorschläge lieferten. In einer Kerngruppe wurden diese Papiere in einzelne Paragrafen umgesetzt, die jeweils abschnittsweise in der Arbeitsgruppe diskutiert und gegebenenfalls angepasst wurden. Der Gesetzesentwurf soll bis Mitte 2003 vorbereitet sein, so dass in der zweiten Hälfte 2003 eine Vernehmlassung stattfinden kann.

Unabhängig davon diskutierte der Verfassungsrat im Rahmen der Totalrevision der Kantonsverfassung Bestimmungen zum Schutz der Privatsphäre und zum Recht auf Informationszugang. Der Entwurf der neuen Verfassung statuiert ein ausdrückliches Recht auf Datenschutz sowie auf Zugang zu Informationen.

Das Informations- und Datenschutzgesetz bietet die Möglichkeit, den Zugang zu und den Schutz von Informationen einheitlich zu regeln und dabei den Lebenszyklus der Information (von der Erhebung bis zur Archivierung) modern und wirkungsorientiert zu gestalten. Dabei kann den Ansprüchen nach Transparenz der Verwaltung wie nach dem Schutz der Privatsphäre und den Geheimhaltungsinteressen des Staates gleichermassen Rechnung getragen werden.

2. Volkszählung 2000

Überwachung der Registerharmonisierung in den Gemeinden

Die Volkszählung 2000 wird als Übergangsvolkszählung bezeichnet. Mit den erhobenen Daten sollen die bestehenden Register so optimiert werden, dass sie in Zukunft weitgehend für statistische Zwecke eingesetzt werden können, insbesondere soll die Volkszählung 2010 vor allem registergestützt durchgeführt werden können. Ausnahmsweise dürfen die Gemeinden die aus der Volkszählung hervorgegangenen Angaben in einem klar umschriebenen Rahmen für die Nachführung bzw. Harmonisierung ihrer Register verwenden (Art. 4 Absatz 2 Volkszählungsgesetz). Zudem können die Daten des Gebäudefragebogens zum Aufbau des Gebäude- und Wohnungsregisters verwendet werden.

Dem Datenschutzbeauftragten ist die Überwachung der Harmonisierung der Einwohnerregister mit Blick auf die datenschutzrechtlichen Bestimmungen übertragen worden. Die Gemeinden wurden im November 2001 mittels eines Merkblatts über die gesetzlichen Grundlagen informiert. Zudem wurde im Detail auf die besonders zu beachtenden Punkte aus der Sicht des Datenschutzes aufmerksam gemacht. Zusätzlich erhielten sie ein Formular, mit dem der Abschluss der Datenbearbeitungen zur Harmonisierung der Register und die Vernichtung der entsprechenden Datensammlungen gegenüber dem Datenschutzbeauftragten bestätigt werden musste (Art. 30 Absatz 5 Volkszählungsverordnung).

Die Zusammenarbeit mit Gemeinden und EDV-Firmen war problemlos. Verzögerungen und Schwierigkeiten ergaben sich jedoch durch die Etappierung der Datenlieferungen durch das Bundesamt für Statistik. Weiter waren die Zuständigkeiten der beteiligten Stellen (Bundesamt für Statistik, Kantonales Statistisches Amt, Datenschutzbeauftragter, EDV-Dienstleister) häufig nicht klar. Bei den zuständigen Personen in den Gemeinden führte dies teilweise zu Unsicherheiten.

Der Rücklauf der Formulare war sehr gut. Ende 2002 haben ca. 75% der Gemeinden die Arbeiten im Zusammenhang mit der Registerharmonisierung

für ihren Bereich abgeschlossen und die Vernichtung der entsprechenden Unterlagen bestätigt. Bei zahlreichen Gemeinden, die mit externen EDV-Dienstleistern zusammenarbeiten, sind jedoch bei den externen Firmen die Arbeiten noch im Gang. Ebenso sind bei etwa 20% der Gemeinden, welche alle Arbeiten intern erledigen, die Arbeiten noch nicht vollständig abgeschlossen. Nur wenige Gemeinden haben sich nicht gemeldet und müssen nochmals kontaktiert werden. In einigen wenigen Fällen sind wegen Unklarheiten noch Rückfragen erforderlich.

Die Arbeiten im Zusammenhang mit der Registerharmonisierung aus der Volkszählung 2000 sollten im Jahr 2003 abgeschlossen werden können, und somit sollten alle diesbezüglichen personenbezogenen Daten auf Gemeindestufe vernichtet sein.

Die Kontrolle der Harmonisierung der Einwohnerregister und der Vernichtung der Personendaten durch den Datenschutzbeauftragten erwies sich als nützliche und vertrauensbildende Massnahme gegenüber der Bevölkerung.

3. Neues Personalinformationssystem

PALAS löst bisherige Systeme ab

Das neue Personalinformationssystem PALAS hat am 1. Januar 2003 seine produktive Phase aufgenommen. Neben der Lohnadministration als zentrales Element sind zusätzlich dezentrale Personalsysteme für einzelne Bereiche vorgesehen. Da es sich bei den Personaldaten um sensible Daten handelt und zusätzlich die Problematik der dezentralen Bearbeitung dieser Daten hinzukam, haben wir dieses Projekt von Anfang an begleitet.

Das System bot selber keine integrierte Sicherheitslösung an, weshalb eine Sicherheitslösung zu finden war, die insbesondere die Anliegen der Authentizität, der Vertraulichkeit und der Integrität gewährleistet. Um keine proprietäre Lösung einsetzen zu müssen, sondern eine Lösung, die von den betroffenen Verwaltungsstellen auch für andere Zwecke verwendet werden kann, setzte man auf die im wif!-Projekt Soprano entwickelte Public-Key-Infrastruktur (PKI). Entsprechende Lösungsansätze wurden evaluiert und eine Implementierung ist vorgesehen mit dem Realisierungsprojekt Soprano.

Eine Berücksichtigung der Sicherheitsanforderungen von Anfang an ermöglicht die Entwicklung von Sicherheitslösungen, die allgemein genutzt werden können und nicht projektspezifisch aufgebaut werden müssen.

4. E-Government-Projekte

Sicherheitsaspekte im Vordergrund

Bei der Begleitung der E-Government-Projekte im Berichtszeitraum standen die sicherheitstechnischen Fragen im Vordergrund. Einerseits wurden entsprechende Konzepte ausgearbeitet, um die sicherheitsspezifischen Fragestellungen beim Intranet- und insbesondere beim Internet-Portal des Kantons Zürich konkretisieren zu können. Aus datenschutzrechtlicher Sicht wurden die «Privacy Policies» für beide Plattformen beurteilt. Andererseits wurden wir in einem spezifischen Projekt in eine Sicherheitsüberprüfung involviert, die zahlreiche Mängel zum Vorschein brachte. Insbesondere zeigte sich, dass das Fehlen eines kantonalen Informatiksicherheitskonzepts zu einem unverhältnismässigen Aufwand für die einzelnen Verwaltungsstellen führt. Ebenso können mit dem Einsatz einer einheitlichen Informatiksicherheitsinfrastruktur Investitions- und Projektkosten gespart werden.

Nach wie vor zeigt sich, dass die E-Government-Projekte aus datenschutzrechtlicher und sicherheitstechnischer Sicht sehr sensibel sind. Diese Situation dürfte mit der weiter angestrebten Interaktion mit den Bürgerinnen und Bürgern noch zunehmen.

Kontinuierliche Informationstätigkeit

Mit Informations- und Ausbildungsmassnahmen wird die Beachtung des Datenschutzes gefördert.

1. Symposium on Privacy and Security

Update und ein Blick auf die Entwicklungen

Am 30. und 31. Oktober 2002 veranstaltete die Stiftung für Datenschutz und Informationssicherheit zum siebten Mal das Symposium on Privacy and Security. Rund 550 Teilnehmende aus dem In- und Ausland fanden sich im Kongresshaus Zürich zu diesem Anlass ein. Wie im Vorjahr wurden neben Plenumsveranstaltungen verschiedene Tracks angeboten. Es bestand somit die Auswahl zwischen Vorträgen mit technologischem und betriebswirtschaftlichem und solchen mit organisatorischem und rechtlichem Schwerpunkt. Während am ersten Tage die «brennendsten Fragen der Privatheit und Informationssicherheit» behandelt wurden, wurde am zweiten Tag ein «Blick auf die Entwicklungen und Herausforderungen» geworfen.

Eröffnet wurde die Veranstaltung durch einen Vortrag von Augustinus Heinrich Graf Henckel von Donnersmarck. Er sprach über die ethische Dimension von Privatheit und Sicherheit. Die Teilnehmenden konnten in der Folge einen der beiden angebotenen Tracks wählen, wobei in den Pausen die Möglichkeit bestand, zwischen den Tracks hin- und herzuwechseln.

Das Spektrum der Vorträge und die angeregten Diskussionen zeigen deutlich den Bedarf an einer steten Auseinandersetzung mit den Themen Privatheit und Informationssicherheit. Diese Aufgabe nimmt das Symposium wahr und leistet damit einen aktiven Beitrag an die Aus- und Weiterbildung im Bereich des Datenschutzes und der Informationssicherheit.

2. Seminare, Referate und Tagungen

Kontinuierliche Aus- und Weiterbildung

Die bewährten Seminare im Rahmen der Aus- und Weiterbildung führten wir auch im Berichtsjahr weiter. Daneben hielten wir auf Anfrage verschiedene Referate und Seminare.

Der modulare Aufbau der Seminare und Referate ermöglichte eine zielgruppenorientierte und bedürfnisgerechte Ausgestaltung der jeweiligen Veranstaltungen. So führten wir Kurse durch für den Verband Zürcher Einwohnerkontrollen (VZE), für den Verein Zürcher Gemeindeschreiber und Verwaltungsfachleute (VZGV), für die Aus- und Weiterbildung von Gefängnismitarbeitenden und weitere Stellen.

Nach wie vor besteht ein grosses Bedürfnis nach spezifischer Aus- und Weiterbildung im Bereich Datenschutz und Informationssicherheit. Zur Vervollständigung und Erweiterung von Angeboten an neue Zielgruppen sind wir derzeit mit der Überarbeitung des Aus- und Weiterbildungskonzepts befasst.

Die Seminare, Referate und Tagungen sprechen ein breites Publikum an. Ein in Arbeit befindliches Aus- und Weiterbildungskonzept will eine zielgruppenorientierte und effiziente Vermittlung der datenschutzrechtlichen Belange unter Einbezug moderner Lernformen weiter verstärken.

3. Zeitschrift «digma»

Aktuelle und fundierte Informationen

Auch der zweite Jahrgang von «digma», der Zeitschrift für Datenrecht und Informationssicherheit, bot eine breite und fundierte Auswahl an Themen und Schwerpunkten an. Die Zeitschrift ist die führende Publikation in der Schweiz zu den Themen Datenschutz und Informationssicherheit. Folgende Themenschwerpunkte wurden im Berichtsjahr behandelt:

- «digma» 2002.1
  Surveillance
- «digma» 2002.2
  E-Health
- «digma» 2002.3
  Der Wert des Privaten
- «digma» 2002.4
  E-Government

Die einzelnen Artikel bieten vertiefte Abhandlungen innerhalb des Schwerpunktthemas. Dabei wird eine Brücke zwischen Recht und Technik geschla-

gen. Hinzu kommen Artikel zu Trends, Gesetzgebung, Rechtsprechung und Praxis.

Der Datenschutzbeauftragte konnte dabei auf verschiedenen Ebenen mitwirken. Wir konnten einzelne Themen und Arbeiten aus dem Alltag wissenschaftlich oder praxisorientiert auswerten und einem breiten Publikum zugänglich machen. Nebst der regelmässig erscheinenden Rechtsprechungsrubrik konnten wir Artikel zu Videoüberwachung, zur Passwortbewirtschaftung und zu Datenschutz in geografischen Informationssystemen einbringen.

Auch die Vereinigung der Schweizerischen Datenschutzbeauftragten publiziert regelmässig über ihre Aktivitäten.

Im Berichtsjahr ist überdies eine Verbindung von «digma» mit dem Symposium on Privacy and Security gelungen. Ein Teil der am Symposium gehaltenen Referate konnte in «digma» publiziert werden.

«digma» ist ein wichtiges Informationsmedium für alle Verantwortlichen in den Bereichen Management, Organisation, Recht und Technik. Es bietet aktuelle und fundierte Informationen zu Datenschutz und Informationssicherheit.

4. Zusammenarbeit der Datenschutzbeauftragten

Kommunale Datenschutzbeauftragte und DSB+CPD.CH

Auf kantonaler Ebene finden vierteljährlich Sitzungen der kommunalen Datenschutzbeauftragten statt, an denen auch der kantonale Datenschutzbeauftragte teilnimmt. Folgende Themen waren im Berichtsjahr aktuell: Datenbanken der Polizeiorgane, Datenschutz im Bereich der Landeskirchen, optische Überwachung, das geplante Informations- und Datenschutzgesetz, die Sozialhilfestatistik des Bundes sowie Einzelfragen aus dem Bereich der Einwohnerkontrollen sowie der Einbürgerung.

Auf nationaler Ebene nahm die Vereinigung der Schweizerischen Datenschutzbeauftragten (DSB+CPD.CH) in verschiedenen Vernehmlassungsverfahren Stellung zu Gesetzgebungsvorhaben. Zudem befassten sich die Mitglieder der Vereinigung in den Arbeitsgruppen Informationstechnologien, Gesundheit, Register und Innere Sicherheit mit aktuellen Problemstellungen.

Im November fand die 9. Schweizerische Konferenz der Datenschutzbeauftragten in Zug statt. Thema der Konferenz waren der vom Bund im Rahmen der Harmonisierung von Personenregistern geplante Eidgenössische Personenidentifikator, biometrische Verfahren zur Gesichtserkennung sowie Sicherheit und Privacy. Die Diskussion zwischen den Vertretern des Bundesamtes für Statistik, des Bundesamtes für Justiz und den Datenschutzbeauftragten zeigte das ernsthafte Risikopotenzial für die Privatsphäre bei der Einführung des Eidgenössischen Personenidentifikators auf. Der Vortrag über biometrische Verfahren gab Aufschluss über die grundsätzliche Problematik dieser Technologien.

Die Zusammenarbeit mit anderen Datenschutzbeauftragten ermöglicht eine vertiefte Betrachtung sowie ein gezieltes und koordiniertes Vorgehen bei aktuellen Themen und Fragestellungen im Bereich des Datenschutzes und der Informationssicherheit.

Datenschutzbeauftragter des Kantons Zürich
Postfach, 8090 Zürich
Tel.: 043 259 39 99
Fax: 043 259 51 38
E-Mail: datenschutz@dsb.zh.ch
Web: www.datenschutz.ch

Datenschutzbeauftragter
Dr. iur. Bruno Baeriswyl

Stellvertreter
lic. iur. Marco Fey

Juristisches Sekretariat
lic. iur. Barbara Mathis
lic. iur. Barbara Egli (bis 31.3.2003)
lic. iur. Adrian Obrecht (bis 31.5.2003)
lic. iur. Karin Schoch (ab 1.6.2003)

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

Beratungsstelle für Informationssicherheit (BIS)
Oliver Wyler, NDS IT S

Projektleitung/Koordinationsstelle Soprano
Hans-Peter Leibacher

Sekretariat
Martina Richard (ab 15.2.2003)

Tätigkeitsbericht Nr. 8 (2002)
ISSN 1422-5816

Konzeption und Produktion
Fabian Elsener Mediengestaltung, Zürich

Druck
KDMZ
Gedruckt auf Recyclingpapier

Bezug
Datenschutzbeauftragter des Kantons Zürich
Postfach, 8090 Zürich
Tel.: 043 259 39 99
Fax: 043 259 51 38
E-Mail: datenschutz@dsb.zh.ch
Web: www.datenschutz.ch