Nummer 9

Tätigkeitsbericht 2003

dsb
datenschutzbeauftragter
kanton zürich

Nummer 9
Tätigkeitsbericht 2003

Der Datenschutzbeauftragte erstattet dem Regierungsrat jährlich oder nach Bedarf einen Bericht über seine Tätigkeit (§ 23 Datenschutzgesetz). Der vorliegende Tätigkeitsbericht 2003 Nr. 9 deckt den Zeitraum vom 1. Januar 2003 bis 31. Dezember 2003 ab.

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

Zürich, Juni 2004

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

Inhaltsverzeichnis

Der Wert der Privatheit

Die Privatheit der Bürgerinnen und Bürger erscheint immer gefährdeter. Während die Entwicklung der Technologie und die abnehmende Transparenz bisher die treibenden Faktoren waren, wird nun auch die notwendige Unterstützung für die Umsetzung des Datenschutzes in der Verwaltung reduziert.

Das Gesetz gibt dem Datenschutzbeauftragten die Aufgaben vor. Im Vordergrund stehen die Beratung, die Kontrolle und die Information der verantwortlichen Organe und der Bürgerinnen und Bürger. § 23 des Datenschutzgesetzes lautet wie folgt:

«Die Aufsichtsstelle
a) überwacht die Anwendung der Vorschriften über den Datenschutz;
b) berät in Zusammenarbeit mit den Fachstellen der Verwaltung die verantwortlichen Organe in Fragen des Datenschutzes und der Datensicherung;
c) erteilt den betroffenen Personen Auskunft über ihre Rechte;
d) vermittelt zwischen betroffenen Personen und verantwortlichen Organen;
e) orientiert die verantwortlichen Organe über wesentliche Anliegen des Datenschutzes.
Sie erstattet dem Wahlorgan jährlich oder nach Bedarf Bericht.
Diese Berichte werden veröffentlicht.»

Die bisherigen Tätigkeitsberichte geben Auskunft über die Schwerpunkte der Aktivitäten des Datenschutzbeauftragten. Seit der Einführung der Datenschutzgesetzgebung 1995 hat die Arbeitsbelastung ständig zugenommen. Während anfänglich die Beratung in vielen Einzelfällen im Vordergrund stand, sind es heute komplexe Fälle, die einen hohen Beratungsbedarf aufweisen. Gleichzeitig hat die Informatisierung der Verwaltung zu einem Ansteigen des Volumens der Datenbearbeitungen geführt. Erst im Jahre 2000 konnte mit einer regelmässigen Kontrolltätigkeit eine weitere gesetzliche Aufgabe, die bisher auf Einzelfälle bei einem konkreten Anlass beschränkt war, aufgenommen werden.

Minimale Ressourcen

Die Ressourcen, die dem Datenschutzbeauftragten für die Erfüllung seiner Aufgaben zur Verfügung stehen, sind minimal. Dies bedeutet, dass in der Beratungstätigkeit Antwortfristen von 3–4 Monaten die Regel sind und dass sich die Kontrolltätigkeit pro Jahr auf 8 von zirka 300 zu kontrollierende Stellen beschränken muss.

Auch im letzten Tätigkeitsbericht 2002 stellten wir fest, dass die Risiken für das informationelle Selbstbestimmungsrecht der Bürgerinnen und Bürger laufend steigen: Einerseits ist vielfach mit dem Fehlen angemessener Rechtsgrundlagen bei sensiblen Datenbearbeitungen keine Transparenz für die betroffenen Personen ge-

geben. Andererseits werden mit neuen Informationstechnologien neue Risikosituationen geschaffen, ohne dass die entsprechenden Sicherheitsmassnahmen getroffen werden. Der Datenschutzbeauftragte hat dafür zu sorgen, dass die verantwortlichen Stellen die datenschutzrechtlichen Rahmenbedingungen einhalten und dass die persönliche Freiheit der Bürgerinnen und Bürger respektiert wird.

Recht auf Privatheit

Die persönliche Freiheit ist eine wichtige Grundlage für unsere liberale Rechts- und Gesellschaftsordnung. Bereits in der Europäischen Menschenrechtskonvention (EMRK) wird das Recht auf Privatheit der Bürgerinnen und Bürger verankert. Die Bundesverfassung statuiert das Recht auf Datenschutz in den Art. 10 Abs. 2 und Art. 13 Abs. 2, welche die Garantie der persönlichen Freiheit und den Schutz vor Missbrauch von Daten enthalten. Das Datenschutzgesetz beinhaltet demnach eine Konkretisierung der verfassungsmässigen Rechte, indem Rahmenbedingungen für die Datenbearbeitungen formuliert werden. Damit gehört die Datenschutzgesetzgebung zu einem Grundpfeiler der liberalen Rechtsordnung.

Einschneidendes Sanierungsprogramm

Es ist klar, dass, wenn der Staat sparen muss, alle staatlichen Aufgaben überprüft werden müssen. Das Sanierungsprogramm 04 des Regierungsrates hat deshalb auch beim Datenschutzbeauftragten angesetzt. Dabei wird nicht auf die spezifische Situation des Datenschutzes Rücksicht genommen. Insbesondere wurde nicht berücksichtigt, dass die Stelle erst seit 1995 im Aufbau begriffen ist und bisher nie eine aufgabenadäquate Ressourcensituation geschaffen werden konnte.

Seit 1995 nimmt die Geschäftslast kontinuierlich zu. Zurzeit verfügt der Datenschutzbeauftragte über 5,2 Stellen und ein Globalbudget von 1,4 Mio. Franken. Das bedeutet, dass im Verhältnis zu den Informatikgesamtausgaben der kantonalen Verwaltung (das heisst ohne die Gemeinden, für die der Datenschutzbeauftragte auch zuständig ist) 0,6 Prozent für die Aufgabenerfüllung des Datenschutzbeauftragten ausgegeben werden. 2003 betrugen diese Informatikausgaben 196,7 Mio. Franken, was einer Verdoppelung seit 1996 entspricht.

Das Sanierungsprogramm 04 verlangt vom Datenschutzbeauftragten den Abbau von 0,5 Stellen und eine Einsparung von 0,18 Mio. Franken. Neben dem Stellenabbau entspricht dies 13,85 Prozent der finanziellen Ressourcen und liegt damit weit über dem Durchschnitt, den das Sanierungsprogramm den einzelnen Amtsstellen auferlegt. Vergleichsweise hat der Bereich Informatik 10 Mio. Franken einzusparen, was gerade 5,08 Prozent dieses Budgets entspricht.

Leistungsabbau beim Datenschutz

Diese verordneten Einsparungen haben einen Leistungsabbau beim Datenschutzbeauftragten zur Folge. Unmittelbar ist mit längeren Antwortzeiten bei der Beratung der Verwaltungsstellen und der Bürgerinnen und Bürger zu rechnen und die Mitwirkung bei wichtigen Vorhaben und Projekten der Verwaltung ist nur noch sehr partiell möglich. In Bezug auf die Kontrolltätigkeit ist festzuhalten, dass die schon bisher stark reduzierte Aufgabenerfüllung gerade im Informatiksicherheitsbereich die Risikosituation für die betroffenen Personen nicht vermindern hilft. Da insbesondere auch die Informationstätigkeit eingeschränkt wird, kann weniger präventiv mittels Seminaren und weiteren Aus- und Weiterbildungsmassnahmen auf die Umsetzung der Datenschutzgesetzgebung Einfluss genommen werden.

Der Abbau der Leistungen beim Datenschutzbeauftragten untergräbt auch die E-Government-Bemühungen. Eine wichtige Voraussetzung für die Akzeptanz dieser (interaktiven) Lösungen durch die Bürgerinnen und Bürger ist das Vertrauen und damit die Frage des Datenschutzes und der Sicherheit. Mit dem Leistungsabbau im Bereich Datenschutz wird das Misstrauen der Bürgerinnen und Bürger gegenüber den Datenbearbeitungen der Verwaltung nicht weiter behoben. Repräsentative Umfragen bestätigen immer wieder, dass die Bürgerinnen und Bürger dem Schutz ihrer Daten einen hohen Stellenwert einräumen. Nur wenn man das Vertrauen der Bevölkerung gewinnen kann, werden sich die hohen Investitionen in E-Government auch lohnen.

In einer Zeit, wo die Informations- und Kommunikationstechnologie immer mehr zu einem bestimmenden Faktor in unserer Gesellschaft wird und unbestritten ist, dass mit dieser Entwicklung auch die Risiken für den Schutz und die Sicherheit der Personendaten zunehmend sind, setzt der Abbau beim Datenschutz für die Bürgerinnen und Bürger ein widersprüchliches Zeichen. Nur wenn der Staat seine Verpflichtung im Bereich des Schutzes der Privatsphäre der Bürgerinnen und Bürger glaubhaft wahrnimmt, wird es gelingen, Vertrauen in staatliche Datenbearbeitungen und insbesondere auch Verständnis für Eingriffe in die Privatheit zu schaffen.

Angemessene Ressourcen?

Der Wert des Privaten in unserer Gesellschaft wird zwar nicht gemessen am Geld, das man bereit ist, für den Datenschutz auszugeben, doch spiegelt sich eine Wertschätzung des Privaten im staatlichen Umfeld insbesondere in den Bemühungen der Verwaltung für die Sicherstellung des Datenschutzes wider.

Trotz Sanierungsprogramm 04 ist deshalb zu fragen, ob genügend Ressourcen für den Datenschutz zur Verfügung gestellt werden. Genügend in diesem Zusammenhang meint angemessen, angemessen im Verhältnis zu den Risiken, die die Datenbearbeitungen für die betroffenen Personen beinhalten. Dabei ist festzustellen, dass die Verwaltung zunehmend komplexere Vorhaben im Bereich der Datenbearbeitungen umsetzt, die regelmässig auch immer höhere Anforderungen bezüglich der Gewährleistung des Datenschutzes und der Sicherheit stellen. Aus diesem Grunde müsste die Fragestellung lauten: Welche Risiken in Bezug auf den Datenschutz und die Sicherheit der Daten sind wir bereit zu tragen? Soll die Privatsphäre der Bürgerinnen und Bürger in der informatisierten Verwaltung gewährleistet werden, so kommt man nicht darum herum, dem Datenschutz den notwendigen Stellenwert und die angemessenen Ressourcen zur Verfügung zu stellen. Mit dem Sanierungsprogramm 04 wurde hier ein falsches Zeichen gesetzt.

Es ist deshalb zu hoffen, dass dies in der absehbaren Zukunft wieder korrigiert wird und die Frage näher diskutiert wird, wie das Vertrauen der Bürgerinnen und Bürger in die staatlichen Datenbearbeitungen gestärkt werden kann. Dabei wird man um die Frage der angemessenen Ressourcen für den Datenschutzbeauftragten nicht herumkommen.

Meilensteine im Jahre 2003

Trotz dieser für den Datenschutz getrübten Aussicht auf die unmittelbare Zukunft, konnten im Berichtsjahr einige markante Meilensteine gesetzt werden. Auf der gesetzgeberischen Ebene ist der Entwurf für ein Gesetz über die Information und den Datenschutz (IDG) in die Vernehmlassung gegeben worden (S. 34 ff.). Dieser Entwurf verzahnt in einem modernen Ansatz die Materien des Informationszugangs

und des Datenschutzes auf konsequente Art und Weise. Damit wird die Basis gelegt für einen modernen, wirkungsorientierten Datenschutz für die Bedürfnisse der informatisierten Verwaltung, die sich sowohl einem zunehmenden Informationsbedürfnis der Gesellschaft als auch einem intensiveren Schutzbedarf der Bürgerinnen und Bürger für ihre Privatsphäre gegenübersieht.

Im Hinblick auf die vermehrte Wirkungsorientierung hat der Datenschutzbeauftragte ein Qualitätsmanagementsystem eingeführt, das nach der allgemein bekannten Norm ISO 9001:2000 zertifiziert werden konnte (S. 32 ff.). Damit wurden die Voraussetzungen geschaffen, um einen modernen Datenschutz auch leistungs- und kundenorientiert umsetzen zu können.

Ein wichtiger Schritt in Bezug auf die Videoüberwachung im öffentlichen Verkehr konnte mit dem Zürcher Verkehrsverbund (ZVV) gemacht werden (S. 10 f.). Die erarbeiteten Richtlinien für Pilotprojekte können auch für ähnliche Problemstellungen in Bezug auf Videoüberwachungen in anderen Bereichen Anwendung finden.

Schwergewichtig geben die Datenbekanntgaben respektive der Datenaustausch zwischen verschiedenen Verwaltungsstellen immer wieder zu Fragen Anlass (S. 12; S. 15 f.; S. 16 f.; S. 19 f.; S. 23 f.; S. 24 f.). Besonders heikel sind solche Datenbekanntgaben, wenn es um den Verdacht auf strafbare Handlungen geht. Je nach Umfeld, in dem sich solche Informationen befinden (Polizei, Schule etc.), respektive nach dem Empfänger dieser Information (Arbeitgeber, andere Verwaltungsstelle, Eltern etc.) sind unterschiedliche Interessenabwägungen vorzunehmen. Eine regelmässige Datenbekanntgabe darf nur erfolgen, wenn hierfür eine ausreichende gesetzliche Grundlage besteht. Im Einzelfall ist zu prüfen, ob die Voraussetzungen der Amtshilfe gegeben sind. Die zahlreichen Fälle, die im letzten Jahr zur Beurteilung vorlagen, ermöglichen eine weitere Konkretisierung der Praxis in diesem Bereich.

Des Weiteren gehört die Informationssicherheit immer wieder zu den Kernthemen. Das Projekt Soprano, das die Einführung einer einheitlichen Sicherheitsinfrastruktur auf der Basis einer Public Key Infrastructure (PKI) vorsieht, konnte erfolgreich abgeschlossen und der Verwaltung zur operativen Umsetzung übergeben werden (S. 36). Allgemein hat sich hingegen gezeigt, dass in punkto Informationssicherheit noch ein grosser Handlungsbedarf besteht (S. 27 f.; S. 30 f.). Aus diesem Grunde legt der Datenschutzbeauftragte grossen Wert auf eine lösungsorientierte Sicherheitsberatung. Die Beratungsstelle für Informationssicherheit (BIS) ist auf grosses Interesse bei der Verwaltung gestossen. Nach einer Aufbauphase im vergangenen Jahr kann heute die Nachfrage nicht mehr befriedigt werden, da die notwendigen Ressourcen fehlen. Ebenso soll mit einer regelmässigen Kontrolltätigkeit, den Datenschutzreviews, in ähnlicher Weise auf die Sicherheit eingewirkt werden. Aus diesem Grunde wurde auch ein neues Instrument entwickelt, das eine Kontrolle noch effizienter machen soll. Auch hier ist festzustellen, dass mit den bestehende Ressourcen nur sehr wenig erreicht werden kann.

Erfreulich ist zu vermelden, dass in zahlreichen Projekten, die wir seit einigen Jahren bereits begleiten, Fortschritte in Bezug auf die Berücksichtigung der datenschutzrechtlichen Anliegen erzielt werden konnten (S. 37 ff.). Insbesondere sollen hier die notwendigen rechtlichen Grundlagen geschaffen werden, die eine transparente Datenbearbeitung ermöglichen.

Rahmenbedingungen und Richtlinien

Das Datenschutzgesetz setzt die Rahmenbedingungen, die in der Praxis oftmals mit Richtlinien zu konkretisieren sind.

KANTON

1. Videoüberwachung im öffentlichen Verkehr

Verbindliche Richtlinien bei Pilotprojekten des ZVV

Der Zürcher Verkehrsverbund (ZVV) plante die Durchführung von Videoüberwachungsmassnahmen in einzelnen Fahrzeugen von Verkehrsbetrieben, welche dem ZVV angehören. Die Massnahmen wurden mit der massiven Zunahme der Gewalt sowohl gegenüber Fahrgästen und Fahrpersonal als auch gegenüber Einrichtungen der Verkehrsbetriebe begründet, welche nebst immateriellen Schäden auch sehr hohe Kosten verursacht. Der ZVV beabsichtigte die Schaffung von einheitlichen Richtlinien für sämtliche für den ZVV tätigen Verkehrsbetriebe und ersuchte uns um Mitarbeit beim Erstellen von datenschutzkonformen Rahmenbedingungen zur Videoüberwachung. Parallel zur Erarbeitung der Richtlinien prüften wir auch das Pilotprojekt «Videoüberwachung in der Forchbahn».

In insgesamt vier Sitzungen mit Vertretern des ZVV, der Verkehrsbetriebe der Stadt Zürich (VBZ) sowie des Datenschutzbeauftragten der Stadt Zürich wurden Richtlinien für Pilotversuche zur Videoüberwachung im ZVV erarbeitet.

In Ermangelung einer entsprechenden Rechtsgrundlage war eine Videoüberwachung nur in Form von Pilotprojekten mit klarer zeitlicher und örtlicher Begrenzung und anschliessender Auswertung der Pilotprojekte möglich. Die Richtlinie regelt für alle Verkehrsunternehmen, die im Gebiet des ZVV tätig sind, Pilotprojekte für den Einsatz und Betrieb von fest installierten und mobilen Videoanlagen an öffentlich und allgemein zugänglichen Orten der Verkehrsunternehmen im ZVV wie Fahrzeugen, Haltestellen, Personenunterführungen, Parkplätzen und Verkaufsstellen. Die Pilotprojekte müssen Auskunft geben über die Auswirkung und Effizienz von Videoüberwachung, um zu einem späteren Zeitpunkt als Entscheidungsgrundlage für allfällige umfassendere Videoüberwachungen zu dienen. Der Umfang der Pilotprojekte ist so zu wählen, dass eine gut abgestützte Aussage über die Wirkung gemacht werden kann.

Videoüberwachungen in diesem Rahmen dürfen nur zur Sicherung von Beweisen zur Überführung der Täterschaft bei Straftaten eingesetzt werden. Als relevante Straftaten gelten Gewaltdelikte, Tätlichkeiten, Drohungen gegenüber Personal und Fahrgästen und Handlungen gegen die sexuelle Integrität gegenüber Personal und Fahrgästen sowie wiederholte, nicht geringfügige Sachbeschädigungen. Ein Pilotversuch mit Videoüberwachung ist nur zulässig, wenn eventuelle andere Methoden mit ähnlichem Aufwand, aber mit weniger Eingriffen in die persönliche Freiheit nicht zum Erfolg führten. Im Weiteren sind die Anlagen bewilligungspflichtig. Die Bewilligung wird für zwei Jahre Betriebszeit erteilt und kann jeweils um zwei Jahre verlängert werden. Die Bewilligung wird nicht erneuert, wenn die Anlage zur Erreichung der Sicherheitsziele nicht mehr notwendig ist. Die Unternehmung, welche die Videoanlage betreibt, erstellt einen jährlichen Bericht, der Auskunft gibt über den Sicherheitsgewinn im Bereich der Anlage.

Videokameras werden so positioniert, dass nur die für das verfolgte Ziel notwendige Zone in ihrem Aufnahmefeld erscheint. Aufgezeichnet wird in geschlossenen, vor dem Zugriff Dritter geschützten Systemen. Aufgezeichnete Daten werden spätestens nach 24 Stunden auf den Speichermedien gelöscht. Der Zeitabschnitt, in dem aufgezeichnet wird, hängt von der Sicherheitslage ab und ist auf die Dauer der Bedrohung zu begrenzen. Die Bilder werden ausschliesslich von berechtigten Personen ausgewertet. Die berechtigten Personen sind schriftlich festgelegt. Deren Anzahl wird so klein wie möglich gehalten. Die Aufzeichnungen dürfen keinesfalls zur Kontrolle von Arbeitstätigkeit, Arbeitszeit oder Arbeitsleistung von Mitarbeitenden verwendet werden. Die Videobilder dürfen nur anlassbezogen aufgeschaltet werden. Eine Videoüberwachung ohne Anlass ist mangels entsprechender Rechtsgrundlage unzulässig. Ist ein voraussichtlich strafrechtlich relevantes Ereignis dokumentiert, wird unverzüglich Strafanzeige eingereicht und bei Antragsdelikten ein Strafantrag erhoben. Ist ein solches Ereignis anhand von Bildaufnahmen dokumentiert und

Strafanzeige erstattet worden, dürfen die Aufnahmen zur Auffindung der mutmasslichen Täterschaft ausschliesslich an die zuständigen Untersuchungsbehörden, die Polizei und die Bahnpolizei für den internen Gebrauch weitergegeben werden. Gespeicherte Daten von Ereignissen werden bei der Unternehmung, welche die Videoanlage betreibt, nur so lange aufbewahrt, wie es für das Verfahren nötig ist.

Videoüberwachungen müssen für die Kunden des ZVV erkennbar an zentraler Stelle gekennzeichnet sein. Dazu sind ausschliesslich die offiziellen Piktogramme des ZVV in Kombination mit der Telefonnummer des ZVV-Contact als Auskunftsstelle für Fragen im Zusammenhang mit der Videoüberwachung an geeigneter Stelle angebracht. Die verantwortliche Unternehmung muss bei Anfrage jedermann Auskunft geben über die Art der Aufzeichnung und der Datenspeicherung und -auswertung.

Für jede Videoüberwachungsanlage sind zudem die Betriebsrichtlinien in einem Reglement festgehalten: Art der Videoüberwachung wie Art und Ort der Kameras, Art der Online-Beobachtung, Alarmierungsmöglichkeiten der Fahrgäste und Art der Speicherung; Betriebszeiten der Anlage; für die Anlage, die Auswertung der Daten, die Weitergabe von Daten und Bildern und die Einhaltung der Richtlinie verantwortliche Personen.

Mit den Richtlinien wurde ein detailliertes, praxisbezogenes Instrument für die Durchführung von Pilotprojekten im Bereich der Videoüberwachung geschaffen. Durch die seit Beginn des Projekts offene und enge Zusammenarbeit mit dem Datenschutzbeauftragten gelang eine datenschutzkonforme Ausgestaltung der Richtlinien, welche den Bedürfnissen der jeweiligen Verkehrsbetriebe, des ZVV sowie der betroffenen Personen Rechnung trägt.

2. Berufsausübungsverbot für Rechtsanwälte

Publikation im Anwaltsregister im Internet

Das Obergericht publiziert das kantonale Anwaltsregister im Internet. Das Register steht als mehrseitiges Textdokument zur Verfügung; einleitend enthält es den Vermerk: «Wo ein einschlägiger Vermerk fehlt, besteht kein Berufsausübungsverbot.» Ein Rechtsanwalt schloss daraus, dass bei bestehendem Berufsausübungsverbot ein Vermerk angebracht wird, und bezweifelte die Zulässigkeit der Publikation solcher Vermerke im Internet, insbesondere da wegen Such- und Archivierungsfunktionen im Internet die Gefahr bestehe, dass solche temporären Berufsausübungsverbote noch lange Zeit später publik seien. Das Obergericht sah demgegenüber keinen Unterschied zwischen einer schriftlichen oder telefonischen Anfrage oder einer Konsultation des Internets und erkundigte sich nach unserer Rechtsauffassung.

Art. 10 Abs. 2 des schweizerischen Anwaltsgesetzes statuiert einen Anspruch auf Auskunft darüber, ob eine Anwältin oder ein Anwalt im Anwaltsregister eingetragen ist und ob gegen ihn/sie ein Berufsausübungsverbot besteht. Damit liegt eine gesetzliche Grundlage für die Datenbekanntgabe vor. Nach der Intention des Gesetzgebers geht es bei dieser Teil-Öffentlichkeit des Registers darum, dass sich jede Person vergewissern kann, ob ein Anwalt bzw. eine Anwältin, den/die sie konsultiert, zur Berufsausübung befähigt (und zugelassen) ist. Nicht erlaubt ist die Auskunft über ein früheres Berufsausübungsverbot, das im Zeitpunkt der Anfrage nicht mehr wirksam ist. Der Gesetzgeber bezeichnete es ausserdem als zulässig, eine Liste der im Register eingetragenen Anwälte und Anwältinnen zu publizieren. Hingegen scheint es nicht verhältnismässig, Berufsausübungsverbote im Internet zu publizieren. Die Wirkung einer solchen Publikation ist insbesondere auch im Lichte der «Archivierungsfunktion» des Internets zu betrachten. Es liegt ausserhalb des Einflussbereichs des Obergerichts und der betroffenen Personen, eine einmal erfolgte Publikation mittels Berichtigung, Nachführung o.Ä. «rückgängig» zu machen. Im Gegensatz zu einer gedruckten Publikation besteht die Problematik im Internet gerade darin, dass mittels Suchfunktionen ein erleichterter und jederzeitiger Zugang zu solchen Informationen möglich ist. Bei Drucksachen ist diese Möglichkeit naturgemäss mit einem grösseren Aufwand verbunden, womit auch die Gefährdung der Persönlichkeitsrechte abnimmt.

Unter diesen Gesichtspunkten erachteten wir es als zulässig, eine Liste der im Register eingetragenen Anwälte und Anwältinnen zu publizieren, wobei auch die Publikation im Internet möglich ist. Wir empfahlen dem Obergericht, periodisch eine aktualisierte Liste der zugelassenen Anwälte und Anwältinnen, bei denen kein Berufsausübungsverbot besteht, zu publizieren.

Von Aufsichtsbehörden verhängte Berufsausübungsverbote bei bewilligungs- bzw. registrierungspflichtigen Berufen sind nicht im Internet zu publizieren. Werden gestützt auf Rechtsgrundlagen Berufsregister im Internet veröffentlicht, sind jeweils nur die Angaben der aktuell zugelassenen Personen zu verbreiten, und die Registereinträge sind mit einem aktuellen Datum oder dem Datum der letzten Nachführung zu versehen.

3. Amtsblatt im Internet

Einschränkung der Publikationsdauer

Ein Bürger wandte sich mit folgendem Begehren an uns: Ein Bekannter und er besassen zusammen eine Liegenschaft, die vor mehreren Jahren zwangsversteigert worden war. Diese Zwangsversteigerung wurde damals ordnungsgemäss im Amtsblatt publiziert. Diese Publikation befand sich aber immer noch online auf dem Internet. Da die betroffene Person selbständiger Geschäftsmann war, schädigte diese Publikation ihren Ruf, zumal die damalige Zwangsversteigerung auf Grund der Zahlungsunfähigkeit des Miteigentümers erfolgt war. Er fragte uns an, ob es rechtmässig sei, wenn die Tatsache der Versteigerung immer noch im Internet im Amtsblatt publiziert sei.

Für die öffentliche Bekanntmachung der Steigerung liegen die entsprechenden gesetzlichen Grundlagen vor. Die Form der Publikation wird damit jedoch noch nicht genau definiert. In der Regel erfolgen die gesetzlich vorgesehenen Publikationen durch (meist einmalige) Mitteilung im Amtsblatt. Seit dem Jahr 1998 ist das Amtsblatt des Kantons Zürich auch online im Internet abrufbar. Die Möglichkeiten des Internets führen dazu, dass einmal erfolgte Einträge weltweit und praktisch unbeschränkt abrufbar sind. Mittels Suchkriterien können alle Einträge zu einem bestimmten Namen sehr einfach gefunden werden.

Im Falle einer Steigerungsanzeige gibt es keinen überzeugenden Grund, weshalb die Anzeige auch noch Monate und Jahre nach der Publikation und dem Abschluss des Verfahrens im Archiv abrufbar sein muss. Die Publikationsdauer ist somit unverhältnismässig und stellt einen Eingriff in die Privatsphäre dar. Wir empfahlen der betroffenen Person bei der Staatskanzlei als verantwortlichem Organ für das Online-Amtsblatt zu verlangen, dass der Eintrag aus dem Archiv entfernt werde.

Da die unbeschränkte Zugänglichkeit des Kantonalen Amtsblattes im Internet (insbesondere des Archivs) immer wieder zu Fragen aus datenschutzrechtlicher Sicht Anlass gab, erarbeiteten wir allgemeine Empfehlungen zu diesem Thema. Eine Durchsicht der verschiedenen Publikationen ergab erhebliche Unterschiede, was die Angabe von Details zu persönlichen (auch teilweise sensiblen) Daten betraf. Insbesondere bei publizierten Gerichtsurteilen und Publikationen im Vormundschaftsbereich wurden, je nach Auftraggeber, entweder nur die Namen genannt oder z.B. die gesamten Personalien zum Teil auch noch von Familienmitgliedern sowie weitere Angaben zur Sache. Alle diese Angaben waren über sämtliche seit 1999 erschienenen Ausgaben online mittels Suchfunktionen sehr einfach abrufbar. Diese uneingeschränkte Publikation erschien grundsätzlich unverhältnismässig. Wir erarbeiteten eine Tabelle mit Datenkategorien, wo wir je nach Sensibilität der Daten Vorschläge machten, was publiziert werden darf. Ferner empfahlen wir auch je nach Datenkategorie unterschiedliche Verweilfristen im Internet, nach deren Ablauf die Daten gelöscht werden sollten.

Die Staatskanzlei prüfte unsere Vorschläge, kam aber zum Schluss, dass unsere Vorschläge aus technischen Gründen nicht umsetzbar seien. Darauf einigten wir uns auf eine pragmatische Lösung: Der Inserateteil wird neu nur noch 3 Monate lang publiziert. Der Textteil soll weiterhin unbefristet zur Verfügung stehen, jedoch im Einzelfall auf Grund eines Sperrgesuchs (§ 11 DSG) der betroffenen Person eingeschränkt werden.

Mit der Beschränkung der Publikation des Inserateteils des Amtsblattes im Internet auf 3 Monate und eines Sperrrechts für Personendaten im Textteil wurde eine verhältnismässige Lösung für die Publikation des Amtsblatts im Internet gefunden.

4. Recht zur Einsicht in Untersuchungsunterlagen

Auskunftsrecht auch bei GPK

Die Geschäftsprüfungskommission (GPK) trat mit der Frage an uns heran, ob einer Person, die in ein GPK-Verfahren involviert war, ein Auskunftsrecht nach § 17 DSG zustünde.

Die Kompetenzen der GPK sind in § 49b Kantonsratsgesetz geregelt. Danach ist die GPK insbesondere zuständig für die Prüfung und Überwachung der staatlichen Verwaltung sowie für die ihr zugewiesenen Beschwerden. Das Verfahren der GPK kann demnach als eine Art Aufsichtsverfahren qualifiziert werden. Es handelt sich jedoch um ein Verfahren eigener Art.

Grundsätzlich ist das Datenschutzgesetz nicht anwendbar auf die hängigen Verwaltungsrechtspflegeverfahren, wo die Regeln des Verwaltungsrechtspflegegesetzes Geltung haben. Hingegen ist es anwendbar im erstinstanzlichen, nicht streitigen Verwaltungsverfahren, das in der Regel mit einer Verfügung erledigt wird. Es stellte sich nun die Frage, was für die Aufsichtsverfahren bei der GPK gilt, denn es liegt weder ein eigentliches Parteiverfahren vor, noch handelt es sich um ein streitiges Verfahren. Im Aufsichtsverfahren steht ferner kein formelles Rechtsmittel zur Verfügung. Wir schlossen daraus, dass das Datenschutzgesetz auf die Verfahren der GPK anwendbar ist. Das gilt zur Wahrung der Rechte der betroffenen Person, insbesondere des Aus-

kunftsrechts. Das Verwaltungsrechtspflegegesetz ist demgegenüber nur analog anwendbar, da die GPK keine Verwaltungsbehörde und somit nicht der Exekutive angegliedert ist.

Das Auskunftsrecht gemäss Datenschutzgesetz besteht bei allen nicht hängigen Verwaltungsverfahren.

5. Mehr Transparenz notwendig

Stellungnahmen in Vernehmlassungsverfahren

In mehreren Vernehmlassungen nahmen wir Stellung zu datenschutzrelevanten Fragen.

Das Bundesgesetz über Massnahmen gegen Rassismus, Hooliganismus und Gewaltpropaganda sieht u.a. die Änderung des Bundesgesetzes zur Wahrung der inneren und äusseren Sicherheit (BWIS) vor. Darin sollen Rechtsgrundlagen für ein elektronisches Informationssystem geschaffen werden, in welches Daten über Personen fliessen, die sich im Zusammenhang mit Publikumsveranstaltungen, namentlich mit Sportveranstaltungen, gewalttätig verhalten haben. Da die Bestimmung die Bearbeitung besonders schützenswerter Personendaten impliziert, wiesen wir auf die Ungenauigkeit gewisser Formulierungen hin. Es fehlte eine Bestimmung im Sinne des Zweckbindungsgebots, die den zugriffsberechtigten Stellen wie beispielsweise den kantonalen Polizeibehörden verbot, die Daten für andere Zwecke zu verwenden. Das Gesetz sieht ebenfalls vor, den Organisatoren von Publikumsveranstaltungen diese Daten weiterzugeben. Wir wiesen darauf hin, dass die Veranstalter durch geeignete Auflagen, Vereinbarungen oder auf andere Weise diesbezüglich zu verpflichten seien. Im Rahmen der Vernehmlassung zum Konzept eines kantonalen Gewaltschutzgesetzes brachten wir verschiedene Vorschläge ein. Das Gewaltschutzgesetz sieht diverse Informationsflüsse vor. So plant das Konzept beispielsweise einen proaktiven Beratungsansatz: Spezialisierte Opferberatungsstellen werden von der Polizei oder der Strafuntersuchungsbehörde automatisch benachrichtigt, wenn eine Person Opfer von häuslicher Gewalt geworden ist. Da es sich bei diesen Informationen um besonders schützenswerte Personendaten handelt, wiesen wir darauf hin, dass klare, formellgesetzliche Grundlagen zu schaffen seien. Diese müssen festhalten, wer welche Daten zu welchem Zweck bearbeitet und wem sie wofür weitergegeben werden dürfen.

Ohne von den zuständigen Stellen eingeladen worden zu sein, nahmen wir zum Vernehmlassungsentwurf zum kantonalen Kinder- und Jugendgesetz Stellung. Dieser enthielt Bestimmungen über eine zentrale Datenbank. Aus der Gesetzesbestimmung selber ergab sich nicht, dass es sich dabei um eine Datenbank handelte, welche sensible Personendaten verwaltete, nämlich diejenigen der Leistungsbezüger im Sinne des geplanten Gesetzes. Wir wiesen darauf hin, dass die entsprechenden Bestimmungen zu präzisieren seien. Insbesondere müsse festgehalten werden, wer welche Daten zu welchem Zweck bearbeite und wem wofür diese Daten weitergegeben würden. Ferner müssen für den Aufbau von gemeinsam genutzten zentralen Datenbeständen Regelungen über die Verantwortung und die Zugriffe getroffen werden.

In der Vernehmlassung zum Bundesgesetz über die Harmonisierung der Einwohnerregister und anderer amtlicher Personenregister hielten wir fest, dass die Einführung eines Eidgenössischen Personenidentifikators (EPID) hohe Risiken für die Privatsphäre der Bürgerinnen und Bürger beinhalte.

Die Einführung eines EPID, der auch zu administrativen Zwecken verwendet werden kann und damit die Möglichkeit eröffnen würde, eine beliebige Anzahl von Datensammlungen (eidgenössisch, kantonal oder kommunal) miteinander zu verknüpfen, ist – auch mit entsprechenden einschränkenden Rahmenbedingungen – daher abzulehnen. Der Persönlichkeitsschutz, wie er in der Bundesverfassung (BV) garantiert wird, wird unter solchen Umständen untergraben. In diesem Zusammenhang wiesen wir auf Art. 35 Abs. 2 BV hin, wonach alle Träger staatlicher Aufgaben zur Verwirklichung der Grundrechte verpflichtet werden. Die Würde des Menschen verträgt sich nicht mit dem System des «durchnummerierten Bürgers». Sie darf nicht zu Gunsten von rein statistischen Zielen und Zwecken angetastet werden. Ein EPID mit den vorstehenden Zielsetzungen könnte gegebenenfalls nur nach ausführlicher politischer Debatte in der Bevölkerung eingeführt werden. Diese ausführliche politische Diskussion kann nicht im Rahmen einer Vernehmlassung stattfinden. Die Einführung eines EPID ist in jedem Falle – und nach erfolgter Grundsatzdebatte – für jeden einzelnen Geschäftsprozess in den fachspezifischen Gesetzen zu begründen und die entsprechenden zulässigen – auch datenschutzrechtlichen – Nutzungen sind umfassend und präzis zu regeln.

Allerdings wäre aus Sicht des Datenschutzes nichts gegen die Einführung einer «individuellen Statistik-Nummer» einzuwenden, die beim Bundesamt für Statistik geführt und gepflegt wird, damit die statistischen Zielsetzungen sicherer und einfacher erreicht werden können.

Insbesondere für die Bearbeitung von sensiblen Personendaten sind klare gesetzliche Grundlagen notwendig, aus denen hervorgeht, welche Daten wie bearbeitet werden.

GEMEINDEN

6. Verlustscheine aus bevorschussten Alimenten

Voraussetzungen für die Abtretung der Forderung an private Inkassobüros

Zahlreiche Gemeinden haben Verlustscheine aus bevorschussten Alimenten. Eine Gemeinde fragte uns an, ob es möglich wäre, diese Verlustscheine an private Inkassobüros zu verkaufen, um so wenigstens zu einem Teil des bevorschussten Geldes zu kommen.

Wir machten die Gemeinde darauf aufmerksam, dass nicht alle öffentlichrechtlichen Forderungen abtretbar sind (Bundesgerichtsentscheid 111 Ib 150) und wir die Frage nur aus datenschutzrechtlicher Sicht abklären konnten.

Die Einschaltung eines privaten Inkassobüros zur Eintreibung staatlicher Forderungen stellt eine Datenbekanntgabe an Dritte dar. Eine Datenbearbeitung im Auftrag gemäss § 13 Datenschutzgesetz liegt nicht vor, weil die eingeschalteten Inkassostellen im Regelfall nicht als blosse Beauftragte der Gläubigerseite und damit nicht weisungsgebunden agieren.

Bei den bekannt zu gebenden Daten handelt es sich teilweise um besonders schützenswerte Personendaten. Es wird ersichtlich, dass der Schuldner oder die Schuldnerin den Unterhaltsverpflichtungen nicht nachzukommen vermag, geschieden ist, so und so viele Kinder hat, erfolglos betrieben wurde usw. Das Datenschutzgesetz verlangt eine klare gesetzliche Grundlage für die Bekanntgabe von besonders schützenswerten Daten. Eine solche ist nicht ersichtlich.

Eine andere Legitimationsgrundlage für eine Datenbekanntgabe wäre die Einwilligung des Schuldners oder der Schuldnerin. Die Annahme einer stillschweigenden Einwilligung, wenn der Schuldner oder die Schuldnerin innerhalb einer bestimmten Frist nach Ankündigung der geplanten Forderungsübergabe nicht reagiert, ist jedoch problematisch. Eine ausdrückliche, schriftliche Einwilligung ist vorzuziehen. Die betroffenen Personen dürfen auch nicht vor die Wahl gestellt werden zu zahlen oder in eine Übergabe der Forderung an eine private Inkassostelle einzuwilligen.

Besteht eine gesetzliche Grundlage oder eine gültige Einwilligung, ist weiter zu prüfen, ob im vorliegenden Fall sich allenfalls die Frage nach schützenswerten Interessen betroffener Personen stellt.

Ferner ist sicherzustellen, dass die private Inkassostelle das Zweckbindungsgebot beachtet und die Daten nur für die Eintreibung der Forderung benutzt. Eine Einspeisung in eine Datenbank über Zahlungsfähigkeit und -willigkeit der Schuldnerinnen und Schuldner oder eine Weitergabe an andere private Inkassoinstitute wäre unzulässig. Empfehlenswert ist jedenfalls die Überbindung von Auflagen durch Vertrag, indem beispielsweise Konventionalstrafen bei Datenmissbrauch angedroht werden.

Für den Verkauf von Verlustscheinen ist eine klare gesetzliche Regelung notwendig. Eine andere Möglichkeit wäre die ausdrückliche Einwilligung des Schuldners. Mittels vertraglicher Auflagen ist sicherzustellen, dass das Inkassobüro die Daten nicht zu einem anderen Zweck als der Eintreibung der Forderung gebraucht.

7. Aktenaufbewahrung bei unterschiedlichen Gesuchserledigungen

Dokumentationspflicht und Nachvollziehbarkeit gewährleisten

Verschiedentlich wurden wir von Verwaltungsstellen angefragt, ob im Fall von Gesuchsabweisungen oder bei Rückzügen von Anträgen die bereits eingereichten Unterlagen an die betroffenen Gesuchstellenden zurückzugeben, zu vernichten oder aufzubewahren seien.

In der Regel reichen Gesuchstellende auf Grund der in der Gesetzgebung, beispielsweise im Bereich der Zusatzleistungen oder auch der Sozialhilfe, statuierten Mitwirkungspflicht die notwendigen Unterlagen zur Berechnung des Anspruchs ein. Gestützt darauf erfolgt der Beschluss der Sozialbehörde. Wird das Gesuch abgelehnt, liegt es für den Gesuchstellenden nahe, von der Sozialbehörde die Rückgabe der eingereichten Unterlagen sowie die Löschung der bei ihr vorhandenen Daten zu verlangen.

Die Gesetzgebung im Bereich der Zusatzleistungen in Bund, Kanton und Gemeinde äussert sich nicht zur Frage, in welchen Fällen eingereichte Unterlagen nach Beschlussfassung durch die Sozialbehörde zu vernichten oder zurückzugeben sind. Somit ist davon auszugehen, dass grundsätzlich die üblichen Aufbewahrungsvorschriften zur Anwendung gelangen.

Die Sozialbehörde benötigt zur Abklärung des Anspruchs gewisse Unterlagen, auf welche sie ihren späteren Beschluss abstützt. Der Gesuchstellende seinerseits ist zur Mitwirkung bei der Abklärung des Anspruchs verpflichtet. Auf Grund der Dokumentationspflicht der öffentlichen Organe, deren Verantwortlichkeiten gegenüber den Aufsichtsbehörden sowie angesichts des Grundsatzes der Transparenz, welche die Nachvollziehbarkeit des Ent-

scheids gewährleisten, sind die für die Beschlussfassung geeigneten und erforderlichen Unterlagen auch bei einem abschlägigen Bescheid weiterhin aufzubewahren. Nach Ablauf der ordentlichen Aufbewahrungsfrist sind sie zu archivieren oder zu vernichten.

Je nach Verfahrensart sind folgende Unterscheidungen zu treffen: Bei voller oder teilweiser Gutheissung des Gesuchs liegt ein Sachentscheid vor. Es sind alle zur Durchführung des Rechtsverhältnisses relevanten Unterlagen während der gesetzlichen oder festgelegten Aufbewahrungsdauer aufzubewahren. Auch bei Ablehnung des Gesuchs wird ein Sachentscheid getroffen. Es sind alle für die Prüfung des Gesuchs und den Ablehnungsentscheid massgeblichen Unterlagen während der gesetzlichen oder festgelegten Aufbewahrungsdauer aufzubewahren.

Bei den Verfahrensentscheiden ist wie folgt zu unterscheiden: Bei Rückzug des Gesuchs sind das Gesuch, die Mitteilung des Rückzugs sowie Korrespondenzen und allfällige Aktennotizen zu Besprechungen während der gesetzlichen oder festgelegten Aufbewahrungsdauer aufzubewahren. Bei Nichteintreten auf das Gesuch sind alle für die Prüfung des Gesuchs und den Nichteintretensentscheid massgeblichen Unterlagen während der gesetzlichen oder festgelegten Aufbewahrungsdauer aufzubewahren. Bei Überweisung des Falles sind das Gesuch sowie das Überweisungsschreiben oder der Überweisungsbeschluss aufzubewahren. Die übrigen Unterlagen werden überwiesen, es werden keine Kopien zurückbehalten.

Auf Grund der Dokumentationspflicht der Verwaltung, der Transparenz der behördlichen Tätigkeit und Willensbildung sowie der Nachvollziehbarkeit eines Entscheids sind die notwendigen und geeigneten Unterlagen aufzubewahren. Bei Verfahrensentscheiden sind im Allgemeinen weniger Unterlagen aufzubewahren, da sie keine materiellen Auswirkungen haben. Bei Sachentscheiden sind jedoch sämtliche für den Entscheid relevanten Unterlagen aufzubewahren.

8. Meldungen ans Steueramt

Datenweitergabe durch die Berechnungsstelle für Zusatzleistungen

Die Berechnungsstelle für Zusatzleistungen einer Gemeinde fragte uns an, ob sie dem Steueramt melden dürfe, wenn sie feststelle, dass ein Antragsteller bei der Berechnungsstelle ein anderes Vermögen deklariere als gegenüber dem Steueramt. Dieselbe Frage stellt sich, wenn die Berechnungsstelle erfährt, dass der Antragsteller eine BVG-Auszahlung erhält, gleichzeitig aber noch Steuerschulden hat.

Das kantonale Sozialamt nahm hierzu ebenfalls Stellung, und wir konnten gemeinsam Folgendes festhalten:

In Bezug auf die Ergänzungsleistungen zur Alters-, Hinterlassenen- und Invalidenversicherung richtet sich die Datenbekanntgabe ans Steueramt nach Art. 13 ELG (Bundesgesetz über die Ergänzungsleistungen zur Alters-, Hinterlassenen- und Invalidenversicherung) in Verbindung mit Art. 50a Abs. 1 lit. e Ziff. 5 AHVG (Bundesgesetz über die Alters- und Hinterlassenenversicherung). Danach dürfen Organe, die mit der Durchführung, Kontrolle oder Beaufsichtigung der Durchführung des ELG betraut sind, Daten nur im Einzelfall und auf schriftlich begründetes Gesuch hin an Steuerbehörden bekannt geben. Da die Strafverfolgung aber in die Kompetenz der Kantone fällt, dürfen diese bestimmen, wann ein kantonales oder kommunales Organ einen begründeten Verdacht auf einen Straftatbestand an die zuständige Stelle meldet. Demnach muss die Berechnungsstelle für Zusatzleistungen den Steuerbehörden von sich aus mitteilen, wenn nach Wahrnehmungen in ihrer amtlichen Tätigkeit die Wahrscheinlichkeit einer unvollständigen Besteuerung besteht (§ 121 Abs. 1 Steuergesetz, § 21 Strafprozessordnung). Dies ist insbesondere dann der Fall, wenn der Gesuchsteller gegenüber der Berechnungsstelle ein höheres Einkommen oder Vermögen deklariert als gegenüber dem Steueramt.

Hingegen darf dem Steueramt nicht jeder steuerlich relevante Vorgang von sich aus gemeldet werden. Dafür findet sich erstens keine gesetzliche Grundlage und zweitens würde dies dem Prinzip der Selbstdeklaration in der Steuergesetzgebung widersprechen (vgl. Tätigkeitsbericht Nr. 8 [2002], S. 18 f.). Dazu ein Beispiel: Die Berechnungsstelle darf dem Steueramt nicht melden, wenn es von einer Erbschaft des Gesuchstellers erfährt. Die Meldepflicht entsteht erst, wenn die Berechnungsstelle feststellt, dass der Gesuchsteller die Erbschaft gegenüber dem Steueramt nicht deklariert hat.

Dasselbe gilt für BVG-Auszahlungen. Auch hier ist – immer vorbehältlich § 21 StPO – keine gesetzliche Grundlage ersichtlich, welche die Bekanntgabe von BVG-Auszahlungen ans Steueramt vorsieht, wenn der Gesuchsteller noch Steuerschulden hat.

Tatsachen, die bei der Anspruchsabklärung von Ergänzungsleistungen oder Beihilfen festgestellt werden und bei denen sich die Frage stellt, ob sie dem Steueramt gemeldet werden dürfen, sollten gleich behandelt werden, weil die entsprechenden Ansprüche oft im gleichen Verfahren abgeklärt werden. Das heisst, dass die obigen Ausführungen auch für Tatsachen gelten, die im Rahmen der Anspruchsabklärun-

gen für kantonale Beihilfen festgestellt wurden.

In jedem Fall ist aber zu prüfen, ob überwiegende öffentliche Interessen der Meldung an das Steueramt entgegenstehen. 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. Keine Rolle spielen Geheimhaltungspflichten, da diese in § 121 Abs. 1 Steuergesetz und in Art. 50a Abs. 1 Bundesgesetz über die Alters- und Hinterlassenenversicherung explizit ausgenommen werden.

Nur wenn die Berechnungsstelle feststellt, dass der Gesuchsteller gegenüber dem Steueramt nicht dieselben Angaben macht wie gegenüber der Berechnungsstelle für Zusatzleistungen und deshalb wahrscheinlich unvollständig veranlagt wird, darf sie diese Information ans Steueramt weiterleiten. Auf Grund des Selbstdeklarationsprinzips in der Steuergesetzgebung darf sie nicht jeden steuerlich relevanten Vorgang von sich aus melden. Erfährt die Berechnungsstelle von einer BVG-Auszahlung an den Gesuchsteller, darf sie dies dem Steueramt erst melden, wenn jener diese nicht selber deklariert hat.

9. Erhebung von Steuerdaten durch das Sozialamt

Beizug der Steuerdaten des Konkubinatspartners möglich

Eine Privatperson fragte uns an, ob das Sozialamt bei der Abklärung des Sozialhilfeanspruchs des Konkubinatspartners auf ihre Steuerdaten zugreifen dürfe, ohne ihr Einverständnis zu erlangen oder sie zumindest davon zu unterrichten.

Gemäss § 7 Abs. 1 DSG sind Personendaten in der Regel bei der betroffenen Person zu beschaffen. In gleicher Weise verlangt auch § 27 Abs. 1 der Verordnung zum Sozialhilfegesetz, dass die Abklärung der Verhältnisse in erster Linie durch Befragung des Hilfesuchenden und Prüfung seiner Unterlagen erfolgt. Der Hilfesuchende ist auf Grund der Mitwirkungspflicht gemäss § 18 Abs. 1 Sozialhilfegesetz sowie § 28 der Verordnung zum Sozialhilfegesetz unter Hinweis sowohl auf die Pflicht zur wahrheitsgemässen Auskunft wie auch auf die Folgen falscher Auskunft zur Zusammenarbeit mit den Sozialhilfebehörden verpflichtet.

Gibt die betroffene Person die für die Berechnung des Sozialhilfeanspruchs notwendigen Steuerdaten des Konkubinatspartners trotz Aufforderung durch das Sozialamt nicht bekannt, kann die Sozialbehörde in einem nächsten Schritt im Rahmen der Amtshilfe beim Steueramt die für die Abklärung des Sozialhilfeanspruchs erforderlichen Informationen beschaffen. Es empfiehlt sich aber, die betroffene Person und gegebenenfalls auch den Konkubinatspartner nach dem Grundsatz der Transparenz über dieses Vorgehen zu informieren.

Weiter stellte sich die Frage, ob eine nachträgliche automatische Überprüfung der Steuerzahlen in sämtlichen Sozialhilfefällen gerechtfertigt sei.

Das Bearbeiten von Personendaten muss für die Erfüllung der Aufgaben geeignet und erforderlich sein (§ 4 Abs. 3 DSG). Eine nachträgliche automatische Überprüfung der Steuerzahlen in sämtlichen Sozialhilfefällen ist nicht erforderlich und deshalb unverhältnismässig, da nicht davon auszugehen ist, dass sämtliche Angaben von Hilfesuchenden entweder falsch oder unvollständig sind. Ergeben sich in einzelnen Fällen Hinweise darauf, dass die eingereichten Unterlagen nicht korrekt oder trotz Abmahnung des Hilfesuchenden unvollständig sind, kann eine Überprüfung der Steuerzahlen beim Steueramt im Rahmen der Amtshilfe im Einzelfall erfolgen, wenn die entsprechenden Voraussetzungen erfüllt sind.

Im Rahmen eines mehrstufigen verhältnismässigen Vorgehens kann die Sozialbehörde nach vorangegangener Information auf die Steuerdaten des Konkubinatspartners zugreifen, da diese Angaben zur Berechnung des Anspruchs auf Sozialhilfe benötigt werden und bei Verletzung der Mitwirkungspflicht des Gesuchstellenden nicht anders beschafft werden können.

10. Vormundschaftsberichte ins Ausland

Umfang der bekannt zu gebenden Informationen

Von einer Vormundschaftsbehörde wurden wir angefragt, welche Angaben im Falle der Überweisung eines Falles infolge Wegzuges der betroffenen Personen einem ausländischen Staat bekannt gegeben werden dürfte.

Vorerst musste geklärt werden, ob die Datenschutzgesetzgebungen des ausländischen Staates und der Schweiz gleichwertig waren. Dies war der Fall. Andernfalls wäre eine Weitergabe von Daten nicht erlaubt.

Das Bearbeiten von Personendaten muss für die Erfüllung der Aufgaben geeignet und erforderlich sein. Somit ist im Einzelfall abzuklären, welche Unterlagen für die künftige Behandlung des Falles geeignet und erforderlich sind. Von vornherein nicht darunter fallen Unterlagen über abgeschlossene Massnahmen. Je älter die Unterlagen sind, desto weniger sind sie für die künftige Behandlung des Falles von Wichtigkeit.

Im von der abgebenden Behörde zu verfassenden Schlussbericht zur Überweisung werden diejenigen Massnahmen aufgelistet, welche noch nicht abgeschlossen und deshalb weiterzuführen sind. Dazu werden eingehendere Informationen bekannt gegeben. Zudem steht es der Behörde, an welche der Fall überwiesen wird, frei, bei Bedarf bei der überweisenden Behörde weitere Unterlagen anzufordern.

Ein gleichwertiges Datenschutzniveau vorausgesetzt, gibt die überweisende Behörde nur Akten weiter, welche für die weitere Bearbeitung des Falles von Wichtigkeit sind. Es ist eine Auswahl aus den bestehenden Unterlagen zu treffen und ein Schlussbericht zu verfassen.

11. Registrierte Partnerschaften

Datenbekanntgaben aus dem Einwohnerregister

Vom Verband Zürcher Einwohnerkontrollen wurden wir angefragt, ob die Einführung der registrierten Partnerschaften per 1. Juli 2003 Auswirkungen auf die Datenbekanntgaben der Einwohnerkontrollen habe.

Die Verordnung über die Registrierung gleichgeschlechtlicher Paare verpflichtet die Einwohnerkontrolle der Wohngemeinde in § 7 bei registrierten Partnerinnen und Partnern zur Anmerkung folgender Angaben:

a) das Bestehen einer Partnerschaft,
b) welches Zivilstandsamt die Registrierung vorgenommen hat,
c) das Datum der Registrierung,
d) Name, Vorname und Geburtsdatum der Partnerin oder des Partners.

Diese Angaben werden benötigt, damit die Einwohnerkontrolle der Meldepflicht von § 13 der Verordnung über die Registrierung gleichgeschlechtlicher Paare vom 21. Mai 2003 nachkommen kann. Laut § 4 Abs. 1 des Gesetzes über die Registrierung gleichgeschlechtlicher Paare werden die für Ehepaare gültigen Bestimmungen des Steuergesetzes und des Gesetzes über die Erbschafts- und Schenkungssteuer sowie des Sozialhilfegesetzes sinngemäss auf registrierte Partnerschaften angewandt. Für die Erbschafts- und Schenkungssteuer sowie die Handänderungssteuer gelten Partnerinnen und Partner als verheiratet. Für die Staats- und Gemeindesteuern werden die Partnerinnen und Partner getrennt besteuert (§ 17 Abs. 1 und 2 der Verordnung über die Registrierung gleichgeschlechtlicher Paare). Bei der Rechtsanwendung gelten Personen, für die eine registrierte Partnerschaft besteht, als Angehörige und als Lebenspartner (§ 16 der Verordnung).

Die Wirkungen der registrierten Partnerschaft erstrecken sich somit auf das Erbschaftssteuerwesen sowie auf die Sozialhilfe. Der bundesrechtliche Zivilstand hingegen erfährt keine Änderung. Es erfolgt keine Eintragung der registrierten Partnerschaft im Familienregister. Die Auskunft in § 9 Abs. 2 Datenschutzgesetz bezieht sich auf den bundesrechtlichen Zivilstand, welcher unverändert bleibt. Somit kann gestützt auf diese Bestimmung keine Auskunft über das Bestehen einer registrierten Partnerschaft erteilt werden.

Auskünfte der Einwohnerkontrollen an private Personen oder Organisationen sind jedoch möglich entweder mit dem Einverständnis der beiden Partnerinnen oder Partner (gemäss § 8 Abs. 1 lit. c DSG) oder aber gestützt auf § 9 Abs. 4 DSG bei Vorliegen eines besonders schützenswerten Interesses.

Auskünfte an andere öffentliche Organe wie Steuer- und Sozialhilfebehörden sind gestützt auf § 8 Abs. 1 lit. a DSG im Rahmen der Amtshilfe im Einzelfall und auf Gesuch hin möglich. Es erfolgt somit bei deren Errichtung keine automatische Meldung der registrierten Partnerschaft von der Einwohnerkontrolle an diese Behörden.

Die Einwohnerkontrolle führt die Tatsache der registrierten Partnerschaft in ihrem Register. Da jedoch der bundesrechtliche Zivilstand keine Änderung erfährt, ist eine Mitteilung über das Vorliegen einer registrierten Partnerschaft an Private nur mit dem Einverständnis der betroffenen Personen möglich. Im Bedarfsfall erfolgt im Rahmen der Amtshilfe eine Mitteilung an das Steueramt oder an das Sozialamt.

12. Fremdpersonen in Asylunterkünften

Keine Fotos von «Fremdschläfern»

Asylunterkünfte beherbergen oft unfreiwillig so genannte «Fremdschläfer». Dabei handelt es sich um Personen, die nicht in der jeweiligen Asylunterkunft untergebracht sind, sich aber trotzdem dort aufhalten. Wird eine solche Person erwischt, erhält sie ein dreimonatiges Hausverbot. Bei wiederholtem Verstoss wird Strafanzeige wegen Hausfriedensbruch eingereicht.

Da es sich dabei um Personen ausländischer Herkunft handelt, die für Mitteleuropäer nicht leicht voneinander zu unterscheiden sind, wurden wir angefragt, ob die Fremdschläfer fotografiert werden dürfen. Ferner stellte sich die Frage, ob diese Fotos im Bedarfsfall der Polizei weitergegeben werden dürfen.

Fotografien, auf denen eine Person erkennbar ist, sind Personendaten. Ermöglicht das Bild Rückschlüsse auf Rasse oder Religion der abgebildeten Person, handelt es sich um besonders schützenswerte Daten, bei deren Bearbeitung eine erhöhte Gefahr einer Per-

sönlichkeitsverletzung besteht. Bei Asylanten sind unter Umständen auf Grund ihres Aussehens Rückschlüsse auf ihre Rasse oder Religion möglich. Die Bearbeitung besonders schützenswerter Personendaten erfordert eine klare gesetzliche Grundlage. Da eine solche nicht existiert, ist das Fotografieren von «Fremdschläfern» nicht zulässig. Auch unter dem Aspekt der Verhältnismässigkeit (§ 4 Abs. 3 DSG) erscheint diese Massnahme weder geeignet noch erforderlich: Eine Fotografie garantiert nicht, dass die Personen nicht verwechselt werden. Ferner gibt es andere Vorkehrungen, um nur den berechtigten Personen Einlass in die Asylunterkünfte zu gewähren. In Betracht zu ziehen sind Zugangskontrollen durch spezielle Drehtüren, die nur mit Badge bedient werden können, Eingangskontrolleure oder dergleichen.

Da solche Fotografien nicht erlaubt sind, erübrigte sich auch die Frage der Weitergabe an die Polizei.

Um «Fremdschläfer» in Asylunterkünften fotografieren zu können, müsste eine klare gesetzliche Grundlage geschaffen werden. Asylbewerber, die keinen Zugang zur entsprechenden Asylunterkunft haben, können mittels geeigneter Zugangskontrollen abgewiesen werden.

FORSCHUNG UND STATISTIK

13. Evaluationsverfahren mit sensiblen Daten

Klare Rahmenbedingungen notwendig

Die Universität Zürich evaluiert in regelmässigen Abständen die Qualität der Arbeit in Forschung, Lehre und Dienstleistung (Evaluationsreglement der Universität Zürich). Da die Qualität massgebend von den beteiligten Personen abhängt, ist ein grosser Teil der erhobenen Daten personenbezogen und enthält teilweise besonders schützenswerte Personendaten. Ein Evaluationsverfahren umfasst eine Selbstevaluation der ausgewählten Einheit sowie eine Fremdevaluation durch Experten. Aus diesen Evaluationen werden Berichte erstellt, welche an verschiedene Stellen in Vernehmlassung gehen. Obwohl in diversen Erlassen rechtliche Grundlagen für das Evaluationsverfahren zu finden sind, sind sie wenig detailliert und klar. Die Universität Zürich bat uns um eine rechtliche Beurteilung und um konkrete Empfehlungen für die datenschutzkonforme Durchführung dieses Verfahrens:

Im Rahmen des Evaluationsverfahrens kann es nicht darum gehen, eine neue oder erweiterte Form der Mitarbeiterbeurteilung vorzunehmen. Die Themen sind daher auf das massgebliche, arbeitsspezifische Umfeld zu beschränken. Auf Ausführungen zu persönlichen Merkmalen und charakterlichen Eigenschaften betroffener Personen ist zu verzichten.

Gemäss datenschutzrechtlichen Grundsätzen ist bereits bei der Datenerhebung der Umfang auf das Notwendige zu beschränken. Die Erhebung soll in der Regel bei den Betroffenen erfolgen, evtl. aus allgemein zugänglichen Datenbanken (insbesondere betreffend Publikationen). Wir empfahlen, das Fragegeraster auf die notwendigen arbeitsbezogenen Daten zu beschränken. Die Selbstevaluation sollte Hinweise über die Verwendungszwecke der Daten und den Adressatenkreis für die Vernehmlassung beinhalten sowie über die Möglichkeit für die Betroffenen, Fragen nicht zu beantworten. Bei Fremderhebungen müssen die befragenden Experten über Auswahl und Umfang der Datenerhebung instruiert werden. Ferner muss für die Betroffenen die Möglichkeit bestehen, zu den durch Dritte erhobenen Daten Stellung zu nehmen.

Bei den Vernehmlassungen handelt es sich um den wohl heikelsten Bereich im gesamten Verfahren. Unproblematisch ist die Vernehmlassung nur dort, wo die Daten bereits in anonymisierter Form vorliegen, was nicht häufig der Fall sein dürfte. Viel häufiger werden sensible Personendaten und Persönlichkeitsprofile im Sinne der Transparenz einem breiten Kreis zur Vernehmlassung und Stellungnahme unterbreitet. Mittels Einverständniserklärungen können die Betroffenen in die Bekanntgabe der Daten anlässlich der Vernehmlassungen einwilligen. Diese Einwilligung muss freiwillig erfolgen und unter Kenntnis der konkreten Situation bzw. der Verwendung der Berichte, zu denen die Zustimmung erteilt wird. Der Zweck der Vernehmlassungsrunden muss klar kommuniziert werden (Verifizieren von Daten, Stellung nehmen, Meinung zum Ergebnis abgeben). Wo sensible Personendaten vorhanden sind, ist es absolut unerlässlich, den Personenkreis sorgfältig auszuwählen und möglichst klein zu halten. Die Berichte sollen nur auszugsweise an bestimmte Adressatenkreise verteilt und als vertraulich bezeichnet werden. Für die Berichte sind angemessene organisatorische und technische Massnahmen für die Sicherheit zu treffen. Bei der Auswertung und Zusammenfassung

der diversen Berichte gilt es, sich auf das Wesentliche zu beschränken. Alle Angaben müssen dem Zweck dienen, der mit dem Schlussbericht verfolgt wird. Da die Berichte weitgehend durch Dritte erstellt werden (unabhängige Gutachter) müssen diese bei der Auftragserteilung betreffend Datenschutz sensibilisiert werden.

Im gesamten Verfahren werden Daten bearbeitet, die vertraulich sind. Aus rechtlicher Sicht können das Amtsgeheimnis, besondere Berufsgeheimnisse sowie die Strafbestimmung von § 26 Datenschutzgesetz massgebend sein. Auf die Massnahmen zur Wahrung der Vertraulichkeit ist in geeigneter Weise aufmerksam zu machen und deren Einhaltung nach Möglichkeit zu kontrollieren.

Betroffene können Auskunft verlangen, welche Daten über sie bearbeitet werden. Sie haben demzufolge das Recht, die sie betreffenden Berichte einzusehen. Einschränkungen sind nur möglich, wenn gesetzliche Bestimmungen, überwiegende öffentliche Interessen oder überwiegende schützenswerte Interessen Dritter dies verlangen.

Gemäss Zweckbindungsgebot sind die evaluierten Daten und daraus entstandenen Berichte in erster Linie für Massnahmen und Entscheide, welche sich aus dem Evaluationsverfahren ergeben, zu verwenden. Die Organe, welche den Bericht erhalten, sind in § 16 des Evaluationsreglementes abschliessend aufgezählt.

Allfällige weitere Verwendungszwecke sind im heutigen Reglement nicht vorgesehen. Bearbeitungen für nicht personenbezogene Zwecke, z.B. für Planungen, sind möglich. Diese Zwecke müssten aber in einem Reglement der Evaluationsstelle definiert werden.

Aufzubewahren sind nur jene Personendaten, welche für den weiteren Verwendungszweck geeignet und erforderlich sind (für endgültig anonymisierte Daten bestehen keine Einschränkungen aus datenschutzrechtlichen Gesichtspunkten). Der Schlussbericht hat zwar keine eigenständige rechtliche Wirkung, ist jedoch die Grundlage für Entscheide und Massnahmen. Eine Neubeurteilung ist nach 6 Jahren vorgesehen. Eine Aufbewahrungsdauer für die massgeblichen Berichte von 10 Jahren erscheint deshalb als angemessen. Die Primärdaten aus den Erhebungen sind zu Beweiszwecken nur so lange aufzubewahren, als gegen einzelne Berichte Rechtsmittel ergriffen werden können.

Evaluationsverfahren beinhalten in den meisten Fällen den Umgang mit sensiblen Personendaten. Aus diesem Grund empfiehlt es sich, klare Rahmenbedingungen zu schaffen.

PERSONALBEREICH

14. Mitteilungen der Polizei an den Arbeitgeber

Vorgehen bei Verdacht auf strafbare Handlungen

Von einer betroffenen Person wurden wir angefragt, ob die Mitteilung des Verdachts auf strafbare Handlungen von der Polizei an die Kantonale Verwaltung als Arbeitgeberin zulässig gewesen sei.

Bei der Mitteilung des Verdachts auf strafbares Verhalten handelt es sich um besonders schützenswerte Personendaten, weshalb an die gesetzliche Grundlage qualifizierte Voraussetzungen zu stellen sind. Es muss eine klare gesetzliche Grundlage im Polizei- oder im Personalrecht die Mitteilung des Verdachts erlauben.

Gemäss § 49 Personalgesetz haben sich die Angestellten rechtmässig zu verhalten, die Rechte und Pflichten des Volkes zu achten, die ihnen übertragenen Aufgaben persönlich, sorgfältig, gewissenhaft und wirtschaftlich auszuführen und die Interessen des Kantons in guten Treuen zu wahren. Das ausserdienstliche Verhalten von Arbeitnehmern im öffentlichen Dienst ist grundsätzlich nicht Gegenstand der Treuepflicht. Für den Staatsangestellten wie für jeden anderen Bürger gilt das gleiche Grundrecht der persönlichen Freiheit. Ist eine bestimmte Verhaltensweise vom Gesetz erlaubt, ist sie es auch für Staatsangestellte.

Zu prüfen blieb, ob bei Beginn der Ermittlung die Interessen des Kantons als Arbeitgeber verletzt wurden, indem die Glaubwürdigkeit der Justizorgane durch das zur Last gelegte Verhalten in Frage gestellt wurde und sich somit gestützt auf das öffentliche Interesse eine Mitteilung an den Arbeitgeber aufdrängte, welcher seinerseits im Rahmen des Dienstverhältnisses entsprechende

Massnahmen ergreifen musste. Wir gelangten zum Schluss, dass die Frage, ob der gewichtige Vorwurf der Verletzung der Glaubwürdigkeit der Justizorgane zu Recht bestand, sich im Anfangsstadium der Ermittlung, vor Einleitung der Strafuntersuchung, noch nicht mit genügender Sicherheit beurteilen liess. Angesichts der in Frage stehenden schützenswerten Interessen der betroffenen Person sowie der Unschuldsvermutung war die Mitteilung gestützt auf die nicht näher spezifizierte Begründung des öffentlichen Interesses gemäss § 49 Personalgesetz nicht zulässig.

Ein Verdacht ist keine feststellbare Tatsache. Er wird im Laufe der polizeilichen Ermittlung erhärtet und führt gegebenenfalls zur Eröffnung einer Strafuntersuchung. Der Zweck der polizeilichen Ermittlung ist die Überprüfung des noch unsicheren Wahrheitsgehalts des Anfangsverdachts. Bei der Mitteilung des Verdachts im Anfangsstadium der Ermittlung ist deshalb aus Gründen der nicht gesicherten Richtigkeit des Inhalts grosse Sorgfalt an den Tag zu legen. Die sich gegenüberstehenden Interessen sind umsichtig gegeneinander abzuwägen, da die Gefahr einer Persönlichkeitsverletzung mit entsprechenden nicht wieder gutzumachenden Folgen gross ist. Im Lauf der Strafuntersuchung zeigte sich, dass die Anschuldigungen falsch waren. Der bestehende Anfangsverdacht liess sich nicht erhärten. Das Strafverfahren wurde eingestellt. Wir gelangten zum Schluss, dass im Zeitpunkt der Mitteilung kein rechtsgenügender Verdacht für die Einleitung des Strafverfahrens bestanden hatte. Die Polizei hätte im Rahmen der Ermittlung die Erhärtung des Verdachts abwarten müssen, bevor sie die Mitteilung machte.

Dieses Beispiel zeigt, dass eine Mitteilung nur erfolgen darf, wenn sie für die Erfüllung der Aufgaben geeignet und erforderlich ist. Der Verdacht auf eine Straftat muss die Berufsausübung schwer beeinträchtigen oder verunmöglichen und das Verhalten der verdächtigten Person ihre berufliche Tätigkeit grundsätzlich in Frage stellen. Dieser Zusammenhang ist bei einer Lehrperson, welche dem Verdacht der Ausbeutung von Schülerinnen und Schülern ausgesetzt ist, evident. Die Tätigkeit der im zu beurteilenden Fall betroffenen Person war jedoch trotz des Verdachts nicht von vornherein nicht mehr ausführbar. Zudem erfolgte die in Frage stehende strafbare Handlung ausserhalb der beruflichen Tätigkeit, es bestand mit dieser kein Zusammenhang. Da keine Anhaltspunkte darauf hinwiesen, dass Personen gefährdet waren, zu welchen im Rahmen der beruflichen Tätigkeit Kontakte bestanden, war die Mitteilung zur Aufgabenerfüllung weder geeignet noch erforderlich. Es hätte genügt, zu einem späteren Zeitpunkt eine entsprechende Mitteilung zu machen unter der Voraussetzung, dass sich der Verdacht erhärtet hätte.

Für künftige Fälle empfahlen wir die Schaffung von klaren gesetzlichen Grundlagen und entsprechenden Richtlinien im Polizei- oder im Personalrecht, welche in der Praxis ein einheitliches, den Anforderungen der Legalität und der Verhältnismässigkeit genügendes Vorgehen ermöglichen. Als Beispiel verwiesen wir dazu auf die Regelung in § 5 der revidierten Lehrerpersonalverordnung.

Durch die Schaffung von klaren gesetzlichen Grundlagen und entsprechenden Richtlinien im Polizei- oder im Personalrecht, welche in der Praxis ein einheitliches, den Anforderungen der Legalität und der Verhältnismässigkeit genügendes Vorgehen ermöglichen, kann Transparenz geschaffen werden.

15. Aktenherausgabe im Ombudsverfahren

Ermessensspielraum im Rahmen des Verhältnismässigkeitsprinzips

Eine Mitarbeiterin des Kantons wandte sich an den Ombudsmann, weil sie sich gegen ihre Entlassung wehren wollte. Der Ombudsmann forderte darauf vom betreffenden Verwaltungsbetrieb die Personalakten der entlassenen Mitarbeiterin, des Vorgesetzten sowie eines weiteren Angestellten an.

Gemäss § 89 Abs. 1 des Verwaltungsrechtspflegegesetzes prüft der Ombudsmann des Kantons Zürich, ob die Behörden nach Recht und Billigkeit verfahren. Damit darf er alle Formen des Handelns oder Nichthandelns von Verwaltungsbehörden überprüfen. Der Ombudsmann wird auf Beschwerde hin oder von sich aus tätig und klärt den Sachverhalt von Amtes wegen ab. Die Behörden, mit denen sich der Ombudsmann in einem bestimmten Fall befasst, trifft eine Mitwirkungspflicht: Sie sind dem Ombudsmann gegenüber zur Auskunft und zur Vorlage der Akten verpflichtet. Weil der Ombudsmann sämtliche Formen des Handelns oder Nichthandelns der Verwaltungsbehörden auf Recht und Billigkeit überprüfen kann, liegt es in seinem Ermessen, zu entscheiden, welche Akten er für seine Abklärungen benötigt. Damit liegt eine ausreichende Rechtsgrundlage für eine Datenbekanntgabe an den Ombudsmann vor.

Im konkreten Fall wurde der Ombudsmann auf Grund der Beschwerde einer betroffenen Person tätig. Seine Abklärungen bezogen sich auf das Anstellungsverhältnis dieser Person. Es erscheint grundsätzlich angemessen, die Personaldossiers der von diesem Arbeitsverhältnis betroffenen Personen zu verlangen (Angestellte, Vorgesetzte). Allenfalls stellt sich die Frage, ob die Herausgabe einzelner

Unterlagen auf Grund des Prinzips der Verhältnismässigkeit zu verweigern wäre (Arztzeugnisse etc.). Personalakten über weitere dort angestellte Personen können dem Ombudsmann herausgegeben werden, wenn dieser über den konkreten Beschwerdefall hinaus Ermittlungen tätigt. Ebenso ist hier das Prinzip der Verhältnismässigkeit zu beachten.

Auf Grund dieser Rechtslage obliegt es dem Ombudsmann, seine Begehren um Aktenherausgabe gegenüber der Verwaltungsstelle in einem gewissen Grade zu spezifizieren, damit – beiderseits – nach dem Prinzip der Verhältnismässigkeit die Unterlagen herausgegeben werden können.

Da der Ombudsmann über eine umfassende Kognitionsbefugnis verfügt, liegt es weitgehend in seinem Ermessen, zu entscheiden, welche Akten er für seine Abklärungen benötigt. Zu beachten ist das Prinzip der Verhältnismässigkeit.

INDIVIDUALRECHTE

16. Umgang mit dem Auskunftsrecht

Klare Regelung gegeben

Ein Vater wurde von seiner von ihm getrennt lebenden Ehefrau beschuldigt, die gemeinsame Tochter sexuell missbraucht zu haben. Die Mutter wandte sich mit ihrem Verdacht an eine Opferberatungsstelle. Der Vater bestritt die Vorwürfe und wünschte Einsicht in die Akten. Mit Hinweis auf die Geheimhaltungspflicht der Opferberatungsstellen wurde ihm diese aber verweigert, worauf er sich zwecks Beratung und Vermittlung an uns wandte.

Jede Person, die sich ausgewiesen hat, kann vom verantwortlichen Organ Auskunft verlangen, welche Daten über sie in dessen Datensammlungen bearbeitet werden (§ 17 Datenschutzgesetz).

Die Auskunft darf aufgeschoben, eingeschränkt oder verweigert werden, wenn eine gesetzliche Bestimmung, überwiegende öffentliche Interessen oder überwiegende schützenswerte Interessen Dritter dies verlangen (§ 18 Abs. 1 Datenschutzgesetz).

Art. 4 Opferhilfegesetz lautet: «Personen, die für eine Beratungsstelle arbeiten, haben über ihre Wahrnehmungen gegenüber Behörden und Privaten zu schweigen.

Die Schweigepflicht gilt auch nach Beendigung der Mitarbeit für die Beratungsstelle.

Die Schweigepflicht entfällt, wenn die betroffene Person damit einverstanden ist.

Wer die Schweigepflicht verletzt, wird mit Gefängnis oder mit Busse bestraft.»

Das Opferhilfegesetz enthält eine klare gesetzliche Geheimhaltungspflicht, welche zur Verweigerung des Auskunftsrechts führt.

Einem Insassen einer Strafanstalt wurde zwar Einsicht in die ihn betreffenden Daten gegeben, jedoch verweigerte man ihm die Kopien dieser Datenbestände.

Das Auskunftsrecht umfasst auch die Abgabe von Kopien derjenigen Unterlagen, in welche Einsicht gegeben wird. Der Anspruch ergibt sich gestützt auf § 10 Abs. 2 Datenschutzverordnung in Verbindung mit § 17 Datenschutzgesetz.

Dem Auskunftsrecht kann eine gesetzliche Geheimhaltungspflicht entgegenstehen. Wird aber die Auskunft erteilt, besteht kein Grund, nicht auch Kopien abzugeben.

Der Umgang mit dem Auskunftsrecht ist in der Datenschutzgesetzgebung klar geregelt.

GESUNDHEIT UND SOZIALVERSICHERUNG

17. Pflegebedarfsabklärungssysteme

Verbesserungen dank Datenschutzkonzepten

Nachdem im Kanton Zürich Pflegebedarfsabklärungssysteme evaluiert worden waren, die unverhältnismässige Datenbearbeitungen beinhalteten, empfahlen wir den Leistungserbringern (Kranken- und Pflegeheime), von der Einführung eines neuen Systems abzusehen, bis die datenschutzrechtlichen Fragestellungen gelöst seien (siehe Tätigkeitsbericht Nr. 8 [2002], S. 13 f.). In der Folge fand eine Aussprache unter Beteiligung der Koordinationskonferenz Leistungserbringer Pflege (KLP), des Verbands Zürcher Krankenhäuser (VZK), der Gesundheitsdirektion, von Vertretern von Heimen, der Spitex-Organisation, der Systemanbieterinnen (Q-Sys AG mit dem System «RAI/RUG» und Curaviva mit dem System «BESA») sowie des Datenschutzbeauftragten statt. Es zeigte sich, dass die Leistungserbringer (Heime) mangels spezifischen Fachwissens Schwierigkeiten in der Umsetzung der komplexen rechtlichen und technischen Fragen im Zusammenhang mit diesen Systemen haben; sie wünschten deshalb, dass diese Fragestellungen direkt zwischen den Systemanbietenden und uns geklärt würden. Daraufhin empfahlen wir den Systemanbietenden die Abfassung eines Datenschutzkonzepts.

Ein Datenschutzkonzept soll die Datenbearbeitungen im Einzelnen beschreiben und verbindlich festlegen. Das Ziel ist, die Bearbeitung so auszugestalten, dass die einzelnen Bearbeitungsschritte (Erfassung, Verwendung, Bekanntgabe etc.) hinsichtlich Zweck, Rechtsgrundlagen, Verhältnismässigkeit, Integrität, Sicherheit und Verantwortung mit dem Datenschutzgesetz in Einklang stehen. Bezüglich Sicherheit hat sich eine Systemanbieterin insbesondere um Sicherheitsfragen auf der Ebene Applikation bzw. der Client-Server-Architektur zu kümmern. Es sind dem Gefährdungspotenzial entsprechend angemessene Massnahmen zu treffen (z.B. Verschlüsselung). Die Abfassung eines Datenschutzkonzepts ist ein erster Schritt in Richtung eines umfassenden Datenschutz-Managementsystems.

Beide Systemanbietenden reichten uns Datenschutzkonzepte sowie die Systemdokumentation zur Begutachtung ein. Grundsätzlich erachteten wir die Konzepte bzw. den Ablauf der einzelnen Datenbearbeitungen als geeignet, eine verhältnismässige Bewohnerbeurteilung durchzuführen. Einzelne Verbesserungsmassnahmen sind noch zu treffen. Teilweise bestanden noch erhebliche Mängel bezüglich Umfang der erfassten Daten (Frage der Verhältnismässigkeit) und bezüglich Anonymisierung für die Qualitätssicherung und das Benchmarking. Weiter wurden recht umfangreiche «Merkblätter» verfasst, welche für die einzelnen Personen, die mit dem System umgehen müssen, wertvolle Informationen enthalten. Auch die dazugehörige Information der Bewohnerinnen und Bewohner ist transparent und praktikabel.

Wir informierten beide Systemanbieterinnen über die noch bestehenden Mängel und die zu treffenden Verbesserungsmassnahmen. Auch wiesen wir darauf hin, dass es sich bei unserer Begutachtung lediglich um eine summarische Prüfung der Dokumente im Hinblick auf das Konzept der Datenbearbeitungen handle. Eine detaillierte Systemprüfung oder gar Zertifizierung war mangels Ressourcen bzw. Rechtsgrundlagen nicht möglich. Die weitere Umsetzung unserer Empfehlungen obliegt den Systemanbieterinnen sowie den verantwortlichen Organen.

Mit einem Datenschutzkonzept kann ein verantwortliches Organ oder eine Anbieterin eines Systems sicherstellen, dass Datenbearbeitungen den Anforderungen des Datenschutzgesetzes genügen. Die Abfassung eines solchen Konzepts ist insbesondere in Bereichen mit sensiblen Daten oder mit komplexen Systemen oder Abläufen zu empfehlen.

18. Auskünfte von Haus- und Kinderärzten an Schulärzte

Beschränkte Bekanntgabemöglichkeit

Seit Beginn des Schuljahres 2003/2004 haben Eltern die Möglichkeit, die schulärztliche Untersuchung statt durch den Schularzt durch den Haus- oder Kinderarzt vornehmen zu lassen. Das Volksschulamt fragte uns an, welche Angaben der Haus- oder Kinderarzt in diesem Fall dem Schularzt nach erfolgter Untersuchung zu machen habe.

Die Gemeinden sorgen für ärztliche Überwachung der Gesundheit der Lehrer, Kinder und Jugendlichen in allen Schulen und Anstalten ihres Gebietes (§ 56 Gesundheitsgesetz).

Die Gemeinden lassen alle Schüler vor Beginn des ersten Schuljahres und in der Oberstufe schulärztlich untersuchen. Sie können eine zusätzliche Untersuchung in der Mittelstufe vorsehen. Die Untersuchungen umfassen Grösse, Gewicht, Seh- und Hörvermögen sowie die Kontrolle des Impfzustandes (§ 43a Volksschulverordnung). Die Eltern werden über Umfang und Zeitpunkt sowie die Ergebnisse der Untersuchungen informiert. Untersuchungen, die über

den Umfang gemäss § 43a Abs. 2 hinausgehen, sind nur mit Zustimmung der Eltern zulässig. Die Eltern können die Untersuchung durch einen Arzt ihrer Wahl durchführen lassen (§ 43b Volksschulverordnung).

Die Bekanntgabe der vom Haus- oder Kinderarzt gemäss § 43a Abs. 2 Volksschulverordnung erhobenen Gesundheitsdaten der Kinder muss sich auf eine klare gesetzliche Grundlage stützen. Da keine solche gesetzliche Grundlage vorhanden ist, schlugen wir dem Volksschulamt folgenden Ablauf vor: Der Haus- oder Kinderarzt bestätigt dem Schularzt lediglich, dass er den Untersuch gemäss § 43a Abs. 2 Volksschulverordnung durchgeführt und allfällig nötige schulrelevante Massnahmen ergriffen hat.

Das Volksschulamt bevorzugte ein anderes Vorgehen: Der Haus- oder Kinderarzt füllt wie der Schularzt die ärztliche Schülerkarte mit den entsprechenden gesundheitlichen Angaben aus und schickt die Karte verschlossen an den Schularzt. Dieser hat ein Einsichtsrecht, weil er gemäss § 56 Gesundheitsgesetz für die ärztliche Überwachung der Gesundheit der Kinder zuständig ist und dieser Pflicht nur nachkommen kann, wenn es ihm möglich ist, zu kontrollieren, ob die Hausärzte die gesetzlich vorgeschriebenen Untersuchungen korrekt ausführen.

Wir vertraten den Standpunkt, dass in diesem Fall eine entsprechende klare gesetzliche Grundlage nötig sei, weshalb die Volksschulverordnung entsprechend für die Bekanntgabe der in § 43a Abs. 2 der Verordnung erwähnten Gesundheitsdaten vom Haus- oder Kinderarzt an den Schularzt zu ergänzen sei.

In der Folge entschied sich das Volksschulamt für unseren Vorschlag, welcher ohne Ergänzung der bestehenden gesetzlichen Grundlagen umgesetzt werden kann.

Führt der Hausarzt anstelle des Schularztes die schulärztliche Untersuchung durch, gibt er dem Schularzt lediglich bekannt, dass er die Untersuchung durchgeführt und die notwendigen schulrelevanten Massnahmen ergriffen hat.

BILDUNG

19. Verdacht auf sexuelle Handlungen

Berichtigung und Mitteilung bei Freispruch

Vor einigen Jahren wurde eine Lehrperson an einer Mittelschule wegen Verdachts auf sexuelle Handlungen mit Schülerinnen vom Dienst suspendiert und in der Folge von der Bildungsdirektion entlassen. Die Suspendierung wurde den betroffenen Eltern damals durch das Rektorat brieflich mitgeteilt.

In der Folge wurde die Lehrperson mit Urteil des Obergerichts strafrechtlich freigesprochen und das Verhalten der Bildungsdirektion mit Urteil des Verwaltungsgerichts als teilweise unverhältnismässig bezeichnet.

Die Lehrperson verlangte darauf vom Rektorat die Adressen derjenigen Eltern, welche damals über die erfolgte Suspendierung informiert worden waren, damit sie diesen den Ausgang des Verfahrens mitteilen könne. Das Rektorat fragte uns an, ob die Adressen herausgegeben werden müssten.

Wer ein schützenswertes Interesse hat, kann vom verantwortlichen Organ verlangen, dass es Daten berichtigt oder vernichtet. Zudem kann er verlangen, dass das verantwortliche Organ den Entscheid oder die Berichtigung Dritten mitteilt oder veröffentlicht (§ 19 Abs. 2 lit. a und b Datenschutzgesetz).

Die Lehrkraft hat nach erfolgtem Freispruch von den strafrechtlichen Tatbeständen Anspruch auf Berichtigung sowie auf Mitteilung der Berichtigung. Dieser Berichtigungsanspruch beinhaltet jedoch nicht die Herausgabe der Adressen der Eltern der Schülerinnen und Schüler, welche die Lehrkraft im Zeitpunkt der Suspendierung unterrichtete. Da die Lehrkraft ein berechtigtes Interesse an der Berichtigung sowie der entsprechenden Mitteilung hat, muss

die Mittelschule von sich aus diejenigen Eltern, welche damals über die erfolgte Suspendierung informiert worden waren, in ihrem Namen über den rechtskräftigen Freispruch der Lehrkraft informieren. Damit wird den berechtigten Interessen sowohl der Eltern, der Schülerinnen und Schüler als auch der Lehrkraft entsprochen.

Die Lehrperson wollte auch ihre Kolleginnen und Kollegen an der Mittelschule über den Ausgang des Strafverfahrens, welches mit der Anzeige einer Arbeitskollegin seinen Anfang genommen hatte, informieren. Dazu wünschte sie Angaben darüber, welche Informationen sie ihren Kolleginnen und Kollegen an einer internen Veranstaltung bekannt geben dürfe.

Wir empfahlen der Lehrkraft folgendes Vorgehen, das die Persönlichkeitsrechte der beteiligten Personen beachtet: Sämtliche Angaben über Drittpersonen können die Persönlichkeitsrechte dieser Personen verletzen und haben deshalb zu unterbleiben. Die Angaben zum Verfahrensablauf haben ohne Angaben zu den einzelnen Personen zu erfolgen. Es dürfen somit keine Angaben über diejenigen Personen gemacht werden, welche Anzeige erstatteten oder im Laufe der Untersuchung in das Verfahren miteinbezogen wurden, sei es als Auskunftspersonen, Zeugen oder Geschädigte. Wir machten darauf aufmerksam, dass es der betroffenen Lehrperson jedoch freisteht, verfahrensrelevante Angaben über ihre eigene Person zu machen. Weiter dürfen keine Angaben über diejenigen Personen erfolgen, welche die Untersuchung führten oder sonst daran beteiligt waren.

Hingegen dürfen die involvierten Behörden wie Polizei, Bezirksanwaltschaft und Gericht genannt und der Verlauf und der Ausgang des Verfahrens geschildert werden. Es kann beispielsweise gesagt werden, dass Anzeige erstattet wurde, jedoch nicht durch welche Person. Oder es kann der Verlauf der Untersuchung geschildert werden, jedoch ohne Nennung der an der Untersuchung beteiligten Personen. Oder es kann gesagt werden, dass die Bezirksanwaltschaft die Untersuchung in den Augen der betroffenen Lehrperson nicht fachgerecht geführt habe, jedoch nicht welche Person sie geführt habe.

Der Berichtigungsanspruch beinhaltet nicht die Herausgabe von Adressen von Eltern, welche vor Jahren über den Beginn einer Strafuntersuchung informiert wurden. Die betroffene Lehrperson hat lediglich Anspruch auf Berichtigung und Mitteilung, indem das ursprünglich informierende Rektorat die Eltern über den Ausgang des Verfahrens in Kenntnis setzt. Der Berichtigungsanspruch beinhaltet allgemeine Angaben zum Ablauf und zum Ausgang des Verfahrens ohne Bezug zu den dahinter stehenden Personen.

20. Fehlbare Jugendliche

Information an die Eltern und weitere Stellen

Eine Gemeindepolizei plante verstärkte Kontrollen von Jugendlichen, um die zunehmenden Nachtruhestörungen, Belästigungen und physische und verbale Gewalt in der Gemeinde einzudämmen. Eltern und die anderen Verwaltungsstellen sollten möglichst früh über das fehlbare Verhalten der Jugendlichen informiert werden. Damit sollten Lösungen gefunden werden, welche die besondere Situation der Jugendlichen berücksichtigten und schwerer wiegende Eingriffe verhinderten.

Die Erhebung der Daten bei polizeilichen Kontrollen und deren Weitergabe an Amtsstellen im Rahmen der polizeilichen Ermittlungsverfahren erfolgen im Rahmen der gesetzlichen Vorschriften.

Die Gemeindepolizei ging jedoch einen Schritt weiter, weil sie erwog, weitere Stellen zu benachrichtigen, was bei einem «normalen Verfahrensablauf» nicht der Fall ist.

Auch für diese Meldungen sind jedoch die datenschutzgesetzlichen Voraussetzungen zu erfüllen. Bei den bekannt zu gebenden Daten handelt es sich um besonders schützenswerte Personendaten, weil sie im Zusammenhang mit polizeilichem Handeln erhoben wurden. Für eine Bekanntgabe solcher Daten ist eine klare gesetzliche Grundlage oder die Einwilligung der betroffenen Person notwendig.

In einem anderen Fall ging es um eine ähnliche Fragestellung. Wir wurden angefragt, ob die Schule den Eltern mitteilen dürfe, wenn deren Kind in der Schule beim Kiffen oder alkoholisiert angetroffen werde.

Die Schülerinnen und Schüler haben auf die Schulgemeinschaft Rücksicht zu nehmen und die Anweisungen der Schule zu befolgen (§ 18 Mittelschulgesetz).

Laut § 22 Abs. 1 Mittelschulgesetz informieren die Schulen die Eltern oder andere Erziehungsberechtigte über wichtige Schulangelegenheiten sowie insbesondere über Leistung und Verhalten der Schülerinnen und Schüler.

Eltern mündiger Schülerinnen und Schüler werden auch ohne deren Zustimmung über wichtige Schulangelegenheiten informiert, sofern sie für den Unterhalt dieser Schülerinnen und Schüler aufkommen (§ 19 Mittelschulverordnung).

Eine Informationspflicht besteht demnach nur bei wichtigen Schulangelegenheiten oder strafbarem Verhalten. Ein allfälliger Alkoholkonsum oder -missbrauch muss sich bei unmündigen Schülerinnen und Schülern negativ auf

Leistung und Verhalten auswirken. Ein einmaliger Vorfall von geringer Tragweite genügt nicht.

Bei mündigen Schülerinnen und Schülern fällt als weitere Voraussetzung der Aspekt der Unterhaltspflicht der Eltern ins Gewicht. Eine wichtige Schulangelegenheit liegt demnach vor, wenn sich Leistung und Verhalten negativ auf die Unterhaltspflicht der Eltern auswirken, indem beispielsweise eine Nichtpromotion mit nachfolgender Repetition einer Klasse und den entsprechenden finanziellen Folgen für die Eltern in Aussicht steht.

Wichtige Schulangelegenheiten liegen zudem bei schwereren disziplinarischen Massnahmen vor, welche durch Konvent oder Schulleitung ausgesprochen werden und bis zur Androhung des Ausschlusses aus der Schule gehen können (Art. 29 Ziff. 7–9 der Schulordnung der Kantonsschulen) sowie selbstverständlich bei strafbarem Verhalten (Drogenhandel und -konsum, Erpressung, Nötigung).

Das fehlbare Verhalten Jugendlicher darf nicht ohne weiteres den Eltern oder anderen Verwaltungsstellen mitgeteilt werden. Will die Polizei solche Informationen weitergeben, benötigt sie die Einwilligung der Jugendlichen oder eine klare gesetzliche Grundlage. Die Schule hat gegenüber den Eltern Informationspflichten, aber auch -rechte.

21. Korrespondenz als Grundlage für Begutachtung

Verwendung einzig für den bei der Beschaffung vorgesehenen Zweck

Eine Bildungseinrichtung hat sich mit der Frage an uns gewandt, ob sie die von einer studierenden Person an verschiedene Stellen der Institution gerichtete Korrespondenz im Rahmen einer Administrativuntersuchung zur Begutachtung des psychischen Gesundheitszustandes dieser Person beiziehen dürfe.

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. Der Zweck der Briefe liegt in der Erledigung des Schriftverkehrs zwischen studierender Person und Verwaltung. Eine Verwendung zur Abklärung des psychischen Gesundheitszustandes stellt eine Zweckänderung dar. Da weder eine gesetzliche Grundlage besteht, welche diese Zweckänderung erlaubt, noch die Einwilligung der betroffenen Person vorliegt oder anzunehmen ist, ist eine Zweckänderung nur für nicht personenbezogene Zwecke möglich. Dies war nicht der Fall, da eine Administrativuntersuchung durchgeführt werden sollte.

Wir schlugen folgendes, den Vorgaben der Verhältnismässigkeit entsprechendes Vorgehen vor: Da die Einwilligung der betroffenen Person zur psychiatrischen Abklärung nicht erhältlich ist, kann diese in einem ersten Schritt im Rahmen der Administrativuntersuchung zur psychiatrischen Abklärung aufgefordert werden. Kommt sie der Aufforderung nicht nach, wird ihr unter Fristansetzung angedroht, als Untersuchungsmassnahme die erwähnte Korrespondenz zur Abklärung beizuziehen. Kommt die betroffene Person dieser Aufforderung nicht nach, kann androhungsgemäss verfahren werden. Diese Schritte werden im Rahmen der Administrativuntersuchung mit Zwischenverfügungen angeordnet. Die betroffene Person kann dagegen das jeweilige Rechtsmittel ergreifen.

Die Bearbeitung von Personendaten darf nur für den bei der Beschaffung vorgesehenen Zweck erfolgen, eine Zweckänderung ist nur bei Vorliegen einer entsprechenden gesetzlichen Grundlage, bei Einverständnis der betroffenen Person oder für einen nicht personenbezogenen Zweck möglich.

22. Musterblatt für Schülerüberweisungen

Einheitliches Formular für sämtliche Schulgemeinden

Bei der Überweisung von einzelnen Schülerinnen und Schülern in eine andere Schulstufe, in ein anderes Schulhaus oder in eine andere Schulgemeinde müssen Personendaten weitergegeben werden. Die Schulgemeinden gingen dabei uneinheitlich vor, weshalb wir immer wieder Anfragen erhielten, welche Daten zu erfassen und bekannt zu geben seien.

Das Volksschulamt erarbeitete mit der Vereinigung der Schulsekretärinnen und Schulsekretäre sowie dem Datenschutzbeauftragten ein einheitliches und für alle Schulgemeinden verbindliches Formular für den Übertritt in eine andere Schulstufe, in ein anderes Schulhaus oder in eine andere Schulgemeinde. Wir achteten dabei darauf, dass nur die für die Aufgabenerfüllung geeigneten und erforderlichen Personendaten erfasst würden. Es sind dies folgende Daten:

- Name und Vorname
- Geburtsdatum
- Heimatort
- Geschlecht
- Muttersprache
- Konfession

Bei der Konfession darf nur die Zugehörigkeit zu einer der drei im Kanton Zürich anerkannten Landeskirchen erfasst werden. Diese Konfessionszugehörigkeiten werden im Auftrag der

entsprechenden Kirchgemeinden erfragt. Die Erfassung anderer Religionszugehörigkeiten ist nicht gestattet, da die Religionszugehörigkeit für die Aufgabenerfüllung der Schule nicht relevant ist.

Weiter erhoben werden:

- Klasse
- bisherige Lehrperson
- Inhaber der elterlichen Sorge
- allfällige Tagesbetreuung
- Datum des Austritts aus der bisherigen Schule

Zudem werden Abklärungen von Stütz- und Fördermassnahmen, Dispensationen sowie eine allfällige auswärtige Schulung erfasst, dies jedoch während höchstens der letzten zwei Jahre und nur insofern sie noch aktuelle Unterrichtsrelevanz besitzen. Die Erziehungsberechtigten und die Schulpflege nehmen im Rahmen der Transparenz mittels Unterschrift vom Überweisungsblatt Kenntnis. Das Formular ist seit Beginn des Schuljahres 2003/2004 in Kraft.

Mit dem einheitlichen Musterblatt für die Überweisung von Schülerinnen und Schülern der Volksschule wurde ein für die Praxis brauchbares Instrument für die Schulgemeinden geschaffen. Es enthält die bei der Überweisung einer Schülerin oder eines Schülers geeigneten und erforderlichen Personendaten.

23. Schulische Standortgespräche
Durchführung und Protokollierung

Die Abteilung Bildungsplanung der Bildungsdirektion ersuchte uns um Prüfung zweier Formulare und Handreichungen zur Durchführung von schulischen Standortgesprächen. Eine Vereinheitlichung dieser Gespräche hat die interdisziplinäre diagnostische Einschätzung der Situation von Schülerinnen und Schülern der Kindergartenstufe, der Primarschulstufe und der Sekundarschulstufe I zum Zweck.

Erfasst werden sowohl beim Vorbereitungs- als auch beim Protokollformular die neun Bereiche Allgemeines Lernen, Mathematisches Lernen, Lesen und Schreiben, Kommunikation, Bewegung und Mobilität, Umgang mit Menschen, Umgang mit Anforderungen, Für sich selbst sorgen sowie Freizeit, Erholung und Gemeinschaft. Die beteiligten Personen, namentlich Eltern, Lehrpersonen und Mitarbeitende von sonderpädagogischen Diensten, legen zusammen Zielsetzungen, Massnahmen und Verantwortlichkeiten für das betroffene Kind fest und unterzeichnen zum Schluss das Protokoll.

Wir wiesen darauf hin, dass die schulischen Leistungen und das Sozialverhalten in der Schule erfasst werden könnten, jedoch keine Fragen zum Privatleben gestellt werden dürften, ausser sie seien unterrichtsrelevant. Ausserschulisches Verhalten ist von der Schule grundsätzlich nicht zu erfassen. Eine konstruktive Zusammenarbeit beruht auch in diesem Bereich auf Freiwilligkeit, weshalb im Formular auf die Freiwilligkeit der Angaben zum Privatbereich hinzuweisen ist. Neben der Nennung des Zwecks der Bearbeitung verlangten wir auf dem Formular eine klare Aussage, ob das Ausfüllen der Formulare freiwillig erfolge. Die Zweckbindung verlangt, dass die erhobenen Personendaten keinesfalls für andere Zwecke als zur schulischen Standortbestimmung verwendet werden dürfen. Zudem sind nur für die Aufgabenerfüllung geeignete und erforderliche Personendaten zu erheben. Da Fragenkataloge zum Datensammeln auf Vorrat und damit zu unnötigen Bearbeitungen von Personendaten anregen, verlangten wir zudem den Hinweis, nur die zur Lösung des aktuellen Problems erforderlichen Angaben zu machen und auf Angaben in nicht relevanten Bereichen zu verzichten. Zudem sind verifizierbare Angaben zu machen. Auf Werturteile ist zu verzichten. Weiter ist auf die Information von Eltern sowie Schülerinnen und Schülern betreffend Ziel und Vorgehen grossen Wert zu legen. Insbesondere haben Eltern und Jugendliche ein Recht zur Einsicht in die Unterlagen. Zudem war die Aufbewahrungsfrist, welche bis zum vollendeten 18. Altersjahr des betroffenen Kindes festgelegt wurde, zu lang. Die Unterlagen sind nur so lange aufzubewahren, bis die sich aus dem Standortgespräch ergebende Massnahme abgeschlossen ist, spätestens jedoch bis zwei Jahre nach Abschluss des Standortgesprächs. Danach sind sie zu vernichten. Die Bildungsdirektion nahm in der Folge die entsprechenden Ergänzungen vor.

Erweisen sich schulische Standortgespräche als nötig, wird von der Bildungsdirektion ein einheitliches Vorgehen gemäss Vorbereitungs- und Protokollformular, beide umschrieben in den Handreichungen, gewünscht. Sie berücksichtigen die datenschutzrechtlichen Grundsätze.

INFORMATIONSSICHERHEIT

24. Sicherheitsüberprüfung verschiedener Amtsstellen

Fehlen von IT-Sicherheitskonzepten

Die Beratungsstelle für Informatiksicherheit (BIS) des Datenschutzbeauftragten hat den Auftrag, die implementierten Sicherheitsvorkehrungen verschiedener Amtsstellen zu begutachten und, bei Bedarf, auf ein adäquates Niveau anzuheben.

Wir bewerteten die operationellen Risiken innerhalb der Stellen und testeten die Sicherheit aller relevanten Systeme innerhalb der jeweiligen Bereiche. Gefundene Schwachstellen wurden mit kontrollierten Attacken weiter überprüft.

Die durchgeführten Arbeiten wurden schriftlich festgehalten und die Resultate standen den Stellen nach Abschluss der IT-Sicherheitsanalyse zur Verfügung. Die als hoch priorisierten Massnahmen, insbesondere mit Fokus Organisation und Technik, wurden unmittelbar nach der Sicherheitsanalyse zusammen mit den Verantwortlichen der Stelle so weit als möglich ohne grosse Kostenfolge aktiv umgesetzt. Alle offen gebliebenen Arbeiten wurden auf einer Massnahmenliste zusammengefasst und zusammen mit der Stelle priorisiert und terminiert.

Das Sicherheitsniveau einzelner Amtsstellen konnte auf Grund der durchgeführten Tests als gut bewertet werden. Andere Amtsstellen jedoch konnten nur als ungenügend taxiert werden. Die getroffenen Massnahmen entsprachen nicht den rudimentärsten Grundsätzen der Informatiksicherheit. Aus diesem Grund waren wir der Meinung, dass die Infrastrukturen dieser Stellen zurzeit nur mit einem erheblichen Sicherheitsrisiko betrieben werden konnten. Wir rieten dringend von einer produktiven Nutzung der gefährdeten Infrastrukturen ab, solange die von uns aufgezeigten Mängel mit hoher und mittlerer Priorität nicht behoben worden sind.

Generell wurde festgestellt, dass ein explizites Sicherheitsmanagement bei keiner der von uns bewerteten Amtsstellen besteht. Dieser Umstand stellt ein grosses Risiko bezüglich Kontinuität und Sicherheit der Informatiksysteme der gesamten kantonalen Verwaltung dar.

Eine kontrollierte Attacke ist ein Instrument, um die Sicherheit der bereitgestellten Dienste zu verifizieren. Allerdings gibt sie nur Aufschluss über den aktuellen Stand der bestehenden Konfiguration der Einrichtungen. Um die angestrebten IT-Sicherheitsniveaus S1 – S3 der Informatiksicherheitsverordnung (ISV) zu erreichen, empfehlen wir, verwaltungsweit ein ganzheitliches IT-Sicherheitskonzept zu erarbeiten und einzuführen.

Der übergreifende Charakter dieses IT-Sicherheitsprozesses macht es notwendig, sicherheitsspezifische Rollen innerhalb der kantonalen Verwaltung festzulegen. Den Rollen sind die entsprechenden Aufgaben zuzuordnen, die wiederum von qualifizierten Mitarbeitenden ausgeführt werden. Nur so kann gewährleistet werden, dass alle wichtigen Aspekte der Informationssicherheit berücksichtigt und sämtliche anfallenden Aufgaben effizient und effektiv erledigt werden können.

Die Sicherheitsüberprüfungen bei zahlreichen Amtsstellen zeigen noch einen grossen Handlungsbedarf in Bezug auf einen angemessenen Sicherheitsstandard auf.

25. Sicherheitsüberprüfung einer Internetplattform

Gravierende Mängel festgestellt

Der Kanton Zürich beteiligt sich an einer Internetplattform, die wir einer routinemässigen Sicherheitsüberprüfung unterzogen. Dabei wurde eine schwerwiegende Sicherheitslücke entdeckt. Da diese Schwachstelle bereits die rudimentärsten Grundsätze der IT-Sicherheit verletzte, empfahlen wir den Betreibern, die Web-Plattform ganzheitlich auf Implementierungsfehler hin zu überprüfen und Mängel gegebenenfalls zu beheben.

Später überprüften wir die überarbeitete Webseite nochmals kurz. Die Überprüfung erfolgte über das Internet und konzentrierte sich vorwiegend auf die Applikationssicherheit. Die Webseite wurde mittels einfacher Werkzeuge kompromittiert und somit wurden keine eigentlichen Hackerangriffe (SSL Denial of Service, Authentification Denial of Service, Cookie Poisoning, Cross-Site Scripting usw.) gegen die Webseite durchgeführt. Bei der Überprüfung wurden Werkzeuge und Techniken verwendet, wie dies so genannte «Script Kiddies» anwenden würden. Ein «Script Kiddie» ist jemand, der Software benutzt um andere Computersysteme anzugreifen. Entscheidend hierbei ist, dass das «Script Kiddie» selbst keine Programmierfähigkeiten besitzt, sondern nur die Programme anderer nutzt.

Das Sicherheitsniveau der Applikation wurde auf Grund der durchgeführten Tests immer noch als ungenügend bewertet. Einige der Schwachstellen verletzten nach wie vor die einfachsten Grundsätze der Informatiksicherheit. Aus diesem Grund waren wir der Meinung, dass die geprüfte Webseite zurzeit mit einem erheblichen Sicherheitsrisiko betrieben werde. Wir rieten deshalb von einer produktiven Nutzung der getesteten Applikation ab, solange die von uns aufgezeigten Mängel mit hoher und mittlerer Priorität nicht behoben worden sind.

Da das System bereits konzeptionelle Mängel aufweist, empfahlen wir, als ganzheitliche Sicherheitslösung den Einsatz einer so genannten «Applica-

tion Security Gateway» in Betracht zu ziehen. Anschliessend sollte die Internetplattform durch Spezialisten ganzheitlich auf allfällige Implementierungsfehler hin überprüft werden.

Während dieser Prüfung haben wir systembedingte und operationelle Risiken ausser Betracht gelassen. Sollte ein ganzheitliches Sicherheitsmanagement bei den Betreibern der Webseite noch nicht erarbeitet und implementiert worden sein, empfahlen wir, ein solches zu schaffen und einzuführen. Nur so kann eine Kontinuität und Sicherheit auf Dauer garantiert werden. Um Ausfälle oder Sicherheitsverletzungen zu minimieren, ist es notwendig, die finanziellen und personellen Ressourcen zu überprüfen und gegebenenfalls bereitzustellen.

Eine kontrollierte Attacke ist das bestbekannte Instrument, um die Sicherheit der bereitgestellten Dienste zu verifizieren. Allerdings gibt sie nur Aufschluss über den aktuellen Stand der bestehenden Konfiguration der Einrichtungen. Die Durchführung von regelmässigen Sicherheitstests durch qualifizierte Spezialisten wird ausdrücklich empfohlen, um die laufenden Konfigurationsanpassungen der Systeme zu kontrollieren.

26. Bewältigung von IT-Sicherheitsattacken

Mitwirkung beim Aufbau einer IT Security Taskforce

Seit August 2003 hat die Anzahl der Virenattacken (Blaster, Sobig, My Doom usw.) auf Systeme der kantonalen Verwaltung massiv zugenommen. Die Perimeter-Sicherheit des kantonalen Netzwerkes (KZH-Netz bzw. neu LEUnet) hat erfolgreich alle eingehenden bösartigen Programme (Viren, Würmer, trojanische Pferde) abgefangen. Dennoch fand der Blaster-Wurm bzw. Sobig-Virus einen Weg, sich innerhalb der kantonalen Verwaltung auszubreiten, und dies, obwohl das Kantonsnetzwerk gegenüber dem Internet durch Firewalls geschützt ist. Es wird vermutet, dass die Viren durch verseuchte Notebooks eingeschleppt wurden. Dies einerseits, weil sich auf den betroffenen Systemen kein adäquater Virenschutz befand und andererseits keine Restriktionen zur Notebooknutzung vorhanden waren.

Innerhalb der kantonalen Verwaltung existiert kein übergeordnetes Sicherheitsdispositiv. Wir wandten uns deshalb an alle Informatikverantwortliche (IV) der Direktionen sowie an die Interessengemeinschaft EDV der Gemeinden (IGEDV-ZH). Dadurch, dass innerhalb der Verwaltung keine zentrale Stelle existiert, welche für die Kommunikation und Koordination der einzelnen Massnahmen in solchen Fällen verantwortlich ist, konnte einerseits nicht mit Sicherheit nachvollzogen werden, ob alle verantwortlichen Stellen in der Verwaltung tatsächlich informiert wurden. Andererseits waren einzelne Informatikverantwortliche sich ihrer Verantwortung nicht bewusst oder weigerten sich, vorgeschlagene Massnahmen umzusetzen.

Das grundsätzliche Problem ist, dass die kantonale Verwaltung über keine direktionsübergreifende Informatik-Sicherheits-Strategie (Policy) verfügt. Genau eine solche wäre jedoch notwendig, um derartige Situationen souverän meistern zu können. Es ist davon auszugehen, dass in Zukunft vermehrt mit derartigen Angriffen auf die Informationssysteme gerechnet werden muss und dass diese nicht zwingend so glimpflich für die Verwaltung ablaufen müssen wie in den jüngsten Fällen.

Um zukünftigen Angriffen gewachsen zu sein, haben wir zusammen mit der Abteilung für Informatikplanung (AIP) eine direktionsübergreifend zusammengesetzte Task Force ins Leben gerufen, welche für die Bewältigung von IT-Sicherheitsattacken innerhalb des kantonalen Netzwerkes zuständig ist. Bei der IT-Security Taskforce handelt es sich um eine reine Notfallorganisation (eine «Feuerwehr»), welche nicht zuständig für die Umsetzung von IT-Sicherheitsmassnahmen in den Verwaltungsstellen ist. Die Verantwortung für die IT-Sicherheit obliegt nach wie vor der obersten Leitung der entsprechenden Organisationseinheit, wie dies in der ISV festgelegt ist.

Die IT Security Taskforce übernimmt folgende Aufgaben:

- Verbreiten von Information und Handlungsanweisungen an die verantwortlichen Stellen (Direktionen, Ämter usw.) bei aufkommender Gefahr oder eingetretenen Angriffen auf die Informationssysteme.
- Anordnen und Durchsetzen von spezifischen Massnahmen (im Extremfall kann das auch die Trennung vom Netzwerk bedeuten) zum ganzheitlichen Schutz des kantonalen Netzwerkes.
- Berichterstattung im Eskalationsfall an das KOSIF bzw. Kantonale IT-Team (KITT).
- Beobachtung und Analyse der globalen IT-Sicherheitslage.

Die Taskforce-Mitglieder setzen sich aus allen Bereichen der kantonalen Verwaltung (Direktionen, Behörden, Gemeinden, Rechtspflege sowie selbständige Unternehmen) zusammen, welche ihre eigene Organisationseinheit wie auch die zugeordneten internen und externen Stellen und Dienste vertreten. Die Mitglieder der Taskforce sind verantwortlich für die Weiterleitung der Informationen und getroffenen Entscheide innerhalb ihrer Organisationseinheit und der zugeordneten Einheiten.

Diese Notfallorganisation wurde als Übergangslösung bzw. Sofortmassnahme gebildet, bis eine neue, verwaltungsübergreifende IT-Sicherheitsstrategie diese Aufgabe neu regelt.

POLIZEI UND JUSTIZ

27. Verordnungsentwurf für Polis
Ergebnisse einer Arbeitsgruppe

Wir haben im letztjährigen Tätigkeitsbericht (vgl. Tätigkeitsbericht Nr. 8 [2002], S. 15) auf den bestehenden gesetzgeberischen Handlungsbedarf in Bezug auf das von der Kantonspolizei geführte Informatiksystem Polis hingewiesen. Dies auf Grund zahlreicher Beschwerden von Bürgerinnen und Bürgern betreffend ihre Registrierung in diesem System, insbesondere in Bezug auf die Löschung oder die Berichtigung von Daten.

In der Zwischenzeit wurde die eingesetzte Arbeitsgruppe, in welcher der Datenschutzbeauftragte ebenfalls vertreten war, aktiv und hat einen Verordnungsentwurf vorgelegt. Dieser Entwurf nimmt die anstehenden datenschutzrechtlichen Fragen auf. Er umschreibt Ziel und Zweck der Datenbank, die Datenkategorien wie auch die Datenbekanntgabemöglichkeiten sowie die Aufbewahrungsdauer der Daten. Im Entwurf ergibt sich eine grundsätzliche Differenz in Bezug auf die aus datenschutzrechtlicher Sicht wesentliche Frage der Löschung von Daten.

Wir sind der Auffassung, dass bei Freispruch, Einstellung des Verfahrens, Sistierung und Nichtanhandnahme des Strafverfahrens die entsprechenden Personendaten zu löschen oder zumindest die Zugriffsrechte auf diese Personendaten einzuschränken sind. Der Verordnungsentwurf sieht lediglich die Berichtigung vor, wobei die Varianten der Löschung und der Zugriffseinschränkung in den Vernehmlassungsentwurf aufgenommen wurden. Nach der Auswertung der Vernehmlassung soll die überarbeitete Verordnung dem Regierungsrat vorgelegt werden.

Mit dem Entwurf einer Verordnung zum Polizeisystem Polis wurden gesetzgeberische Arbeiten in Angriff genommen, die auch in das geplante Polizeigesetz einfliessen können.

28. Erkennungsdienstliche Behandlung von Personen
Warten auf die Verordnung

Bereits in unserem Tätigkeitsbericht Nr. 2 [1996], S. 11 haben wir auf den allgemein anerkannten Handlungsbedarf in Bezug auf die Verordnung über die erkennungsdienstliche Behandlung von Personen aufmerksam gemacht, letztmals im Tätigkeitsbericht Nr. 7 [2001], S. 11 f. Im letzten Jahr wurde uns nun ein überarbeiteter Verordnungsentwurf zur Stellungnahme unterbreitet. Zwar trägt er in weiten Teilen den datenschutzrechtlichen Anforderungen Rechnung. Leider wies er noch erhebliche Mängel auf.

Einer der Hauptpunkte, die Vernichtung des erkennungsdienstlichen Materials, der insbesondere zur Erarbeitung dieser Verordnung geführt und immer wieder zu Beschwerden Anlass gegeben hatte, wurde jedoch nicht angemessen gelöst. Die Verordnung sieht vor, dass bei Personen, die rechtskräftig freigesprochen wurden oder gegen die eine Strafuntersuchung definitiv und rechtskräftig eingestellt wurde, erkennungsdienstliches Material erst nach Ablauf der absoluten Verjährungsfrist der Straftat vernichtet wird.

Diese Bestimmung ist unverhältnismässig. Bei einem Freispruch hat die Vernichtung sofort zu erfolgen, bei der Einstellung des Verfahrens spätestens ein Jahr nach Eintritt der Rechtskraft.

Die weitere Aufbewahrung des erkennungsdienstlichen Materials lässt die betroffene Person unter einem dauernden Verdacht einer möglichen Straftat stehen und verletzt damit die Unschuldsvermutung. Der eigentliche Zweck der Datenbearbeitung wurde bereits erreicht, weshalb die weitere Aufbewahrung einer rechtswidrigen Datenbearbeitung auf Vorrat entspricht. Mit der Vernichtung des erkennungsdienstlichen Materials in diesen Fällen wird auch das Ermittlungsverfahren nicht behindert, da ja bei einer allfälligen Wiederaufnahme des Verfahrens (Revision) ein genügend konkreter Tatverdacht gegen die betroffene Person bestehen muss, der auch wiederum erlauben würde, eine erkennungsdienstliche Massnahme anzuordnen.

Generell wird die Vernichtungsfrist auf 20 Jahre nach Vollzug, Ablauf oder Einstellung festgelegt. Es gibt keine Abstufungen der Aufbewahrung in Bezug auf Verbrechen oder Vergehen oder bezüglich unbedingter Strafen oder bedingter Strafen oder einstweiliger Einstellungen des Strafverfahrens.

Dies ist ebenfalls unverhältnismässig. Es ist deshalb eine Abstufung vorzunehmen, die bei bedingten Strafen und bei der definitiven Einstellung des Verfahrens die Vernichtung bereits nach 5 Jahren vorsieht.

Die Verordnung befindet sich immer noch in der Überarbeitung. Es ist zu hoffen, dass sie entsprechend angepasst wird.

Nach wie vor besteht eine grosse Rechtsunsicherheit in Bezug auf die Behandlung von erkennungsdienstlichem Material, weshalb die Verabschiedung der entsprechenden Verordnung nicht mehr auf sich warten lassen sollte. Die datenschutzrechtlichen Aspekte sind zu berücksichtigen.

DATENSCHUTZREVIEW

29. Überarbeitung der Datenschutzreview

Neues Werkzeug zur Analyse

Der Datenschutzbeauftragte prüft systematisch mittels der Datenschutzreview die kantonale Verwaltung und die Gemeinden. Der Schwerpunkt der bisherigen Prüfungen lag nebst rechtlichen Fragen im organisatorischen und technischen Bereich bei den wichtigsten Grundschutzmassnahmen für IT-Sicherheit wie den Verantwortlichkeiten, dem Virenschutz, der Verwendung der Passwörter und dem Zugriffsschutz. Die Datenschutzreview wurde einer Überarbeitung unterzogen, wobei das Hauptgewicht auf ein für alle beteiligten Stellen verfügbares Werkzeug im Internet gelegt wurde (siehe Kasten). Dieses Tool ermöglicht es den Amtsstellen, den Direktionen und allen Gemeinden sowie selbstverständlich weiteren interessierten Kreisen auf Grund des von ihnen beantworteten Fragenkatalogs eine Grobanalyse ihrer getroffenen Massnahmen in den Bereichen Recht, Organisation und Technik mit einer ersten Bewertung grün, gelb oder rot zu erhalten. Vorschläge im Sinne von Massnahmenempfehlungen gehören ebenso zu dieser Internetapplikation wie eine ausführliche Hilfestellung über Inhalt und Verwendung. Die Benützenden werden nebst dem webbasierten Tool zusätzlich offline durch eine Papierversion (mit demselben Umfang an Fragen und manuellen Auswertungsmöglichkeiten) unterstützt. Der Datenschutzbeauftragte wird im Rahmen der Datenschutzreview als Vorbereitung seiner Prüfungstätigkeit von den geprüften Stellen eine Auswertung aus dem Tool einfordern. Dieser Schritt ermöglicht es, die Prüfungszeiten kurz zu halten, da auf Grund des Gesamtbilds und den im Einzelnen beantworteten Fragen aus dem Tool die wichtigsten Prüfungsgebiete zur Vor-Ort-Prüfung gezielt ausgewählt werden können.

Für die Umsetzung eines wirksamen Datenschutzes zusammen mit den organisatorischen und technischen Massnahmen im Bereich IT-Sicherheit sind die wichtigsten Schritte mittels des neuen Werkzeugs vorgegeben. Damit lassen sich rasch und wirksam die erforderlichen Massnahmen in den Bereichen Datenschutz und IT-Sicherheit planen und umsetzen.

Die Ampel weist den Weg

Bei der neuen Anwendung des Datenschutzbeauftragten im Internet werden die Anwendenden in sinnvollen und verständlichen Schritten durch die Thematik geführt. Zuerst wird ausgewählt, ob die Stelle mit mobilen Arbeitsplätzen ausgerüstet ist oder Outsourcing betreibt, damit der Fragenkatalog entsprechend zusammengestellt werden kann. Die allgemeinen Angaben zur Stelle und die Angabe der Sicherheitsstufe bilden die System- und Risikoanalyse der Informatiksicherheitsverordnung nach. Die Kontrollfragen werden in der Reihenfolge Recht, Organisation und Technik abgearbeitet. Antwortmöglichkeiten sind ja, nein, teilweise relevant, nicht relevant, wobei die Antwort «Nicht relevant» die Frage aus der Bewertung ausschliesst. Die Auswertung erfolgt auf Grund der Anzahl und der Gewichtung der Fragen. Die Ampel steht auf Grün, falls mindestens 80% der Fragen positiv beantwortet werden (auf gelb bei 50–79% ja, auf Rot bei weniger als 50% ja oder falls eine oder mehrere so genannte K.O.-Fragen nicht positiv beantwortet worden sind). Nach der Kurzbewertung dienen wahlweise verschiedene Ansichten eines Reports (mit Antworten im Detail, mit den zugehörigen Empfehlungen usw.) der Stelle als konkreter Vorschlag für einen Umsetzungsplan.

30. Regelmässige Datenschutzreviews

Handlungsbedarf in den meisten geprüften Stellen

Der Datenschutzbeauftragte hat wiederum bei ausgewählten Amtsstellen der kantonalen Verwaltung und den Gemeinden des Kantons Zürich Datenschutzreviews durchgeführt (siehe Tätigkeitsbericht Nr. 2 [1996], S. 34, Nr. 5 [1999], S. 32, Nr. 6 [2000], S. 32, Nr. 7 [2001], S. 29 und Nr. 8 [2002], S. 23). Mit diesem Vorgehen sind in einem möglichst kurzen Zeitrahmen die geprüften Stellen für ausgewählte Bereiche des Datenschutzes und der IT-Sicherheit zu sensibilisieren. Die Stellen sollen als Ergebnis der Prüfung auf Grund der Empfehlungen des Datenschutzbeauftragten ihre Datenbearbeitungen an die rechtlichen Rahmenbedingungen anpassen und Verbesserungen im organisatorischen und technischen Bereich vornehmen.

Da die inhaltliche Stossrichtung der Review seit dem Jahr 2000 nicht verändert wurde, kann nun ein Quervergleich der geprüften Stellen vorgelegt werden. Die bereits in den früheren Tätigkeitsberichten aufgeführten hauptsächlichen Empfehlungen sind auch mit den im Jahr 2003 vorgenommenen Prüfungen bestätigt worden.

Die Ergebnisse der bisherigen Prüfungen des Datenschutzbeauftragten der Jahre 2000 bis 2003 sind in den folgenden Statistiken 1 bis 4 zusammengefasst.

Statistik 1: Bewertung

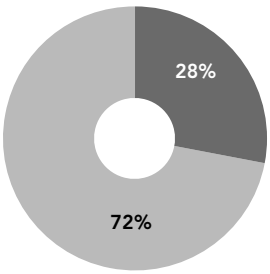
Als «Gut» wurden mehrheitlich grössere Amtsstellen und Gemeinden (ca. 10 000 Einwohner) taxiert. Es befinden sich jedoch auch mittlere Gemeinden (ca. 5000 Einwohner) mit seriös umgesetzten Massnahmen für Datenschutz und IT-Sicherheit in dieser Kategorie.

Statistik 2: Umsetzungsstand Informatiksicherheitsverordnung

Die Umsetzung der Informatiksicherheitsverordnung (ISV) ist nur teilweise erfolgt. Grob zwei Drittel aller Stellen müssen die Massnahmenpläne noch erstellen und genehmigen lassen.

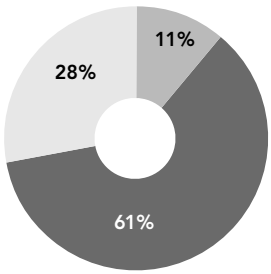
Ergebnisse der geprüften Stellen (Statistiken 1 bis 4)

Bewertung durch den Datenschutzbeauftragten



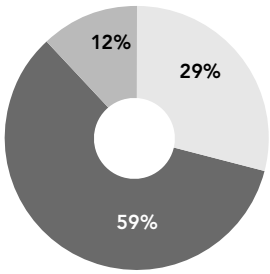
0%	sehr gut
28%	gut
72%	befriedigend

Umsetzungsstand Informatiksicherheitsverordnung (ISV)



11%	Massnahmenpläne in Ordnung
28%	Massnahmenpläne ergänzen
61%	Massnahmenpläne erstellen

Nachholbedarf im Vertragswesen



12%	Verträge in Ordnung
29%	alle Verträge nachführen
59%	teilw. Verträge nachführen

Empfehlungen an die geprüften Stellen in Prozent

Verantwortlichkeiten	Sensibilisierung der Mitarbeitenden planen und durchführen	94
Virenschutz	In einer (PC-)Weisung kommunizieren	94
ISV	Massnahmenpläne abnehmen	89
Verantwortlichkeiten	ISV-Umsetzungsverantwortung zuweisen	72
Passwörter	In einer (PC-)Weisung kommunizieren	72
Zugriffskonzept	Schriftliches Konzept erstellen	67
Passwörter	Anforderungen technisch umsetzen	61
Verantwortlichkeiten	Revision und Kontrolle bestimmen	50
Verantwortlichkeiten	Funktionsbeschreibung erstellen	39
Zugriffskonzept	Zugriffsregelung ausserhalb der Applikationen erstellen und in ein Konzept konsolidieren	39
Passwörter	Administration der Benützenden korrekt durchführen	33
Zugriffskonzept	Zugriffe via Modem, RAS etc. ersetzen	28
Verantwortlichkeiten	Umsetzungsverantwortung für Datenschutz zuweisen	17
Virenschutz	Auf Server nachführen	17
Virenschutz	Auf Clients nachführen	11

Statistik 3: Vertragswesen

Nur wenige Verträge im Informatikbereich (insbesondere Outsourcing) enthalten ausreichende Bestimmungen zu Datenschutz und Sicherheit.

Statistik 4: Wichtigste Empfehlungen

Die Sensibilisierung der Benützenden (inklusive die Kommunikation der Massnahmen und Verantwortlichkeiten im Bereich Virenschutz und Passwortverwendung) kommt bisher zu kurz. Zugriffskonzepte sind meistens nur ansatzweise vorhanden. Die technische Einrichtung von minimalen Anforderungen an die Passwörter auf den lokalen Servern ist nicht befriedigend und sollte auch im Hinblick auf eine meist nicht durchgeführte Härtung der Betriebssysteme dringend in Angriff genommen werden.

■ Die Datenschutzreview als Kontrollinstrument in den Bereichen Recht, Organisation und Technik zeigte wiederum einen teilweise grossen Handlungsbedarf in den geprüften Stellen. In diesen Bereichen sind vermehrte Anstrengungen notwendig.

Verträge mit externen Dienstleistern

Häufig beziehen Verwaltungsstellen und Gemeinden Informatikdienstleistungen bei externen Dritten. Ebenfalls verbreitet ist die Auslagerung von Rechenzentrumsdienstleistungen oder sogar ein vollständiges Outsourcing der gesamten Informatikdienstleistungen an verwaltungsinterne Informatikdienste oder an externe, meist private Dienstleister.

In all diesen Fällen muss eine datenschutzkonforme Bearbeitung von Personendaten sichergestellt werden, da beispielsweise bei Installationen, Software-Updates und insbesondere bei Auslagerungen das Personal des Informatikdienstleisters in der Regel auch Zugriff auf Personendaten hat. Dazu ist der Abschluss von schriftlichen Verträgen notwendig. In der Praxis erweisen sich die Vertragswerke oftmals als mangelhaft. Die Verträge haben den Zweck und den Umfang der Datenbearbeitungen durch die externen Partner bzw. deren Aufgaben klar und detailliert zu umschreiben. Bestimmungen über die Geheimhaltung, den Datenschutz und die Daten- und Informationssicherheit sind ebenfalls notwendig; die Verantwortlichkeiten auf beiden Seiten sind festzulegen, und die Anforderungen an die Sicherheit sind für beide Vertragsparteien durch eine Sicherheits-Policy verbindlich zu regeln. Der Kanton Zürich hat «Allgemeine Geschäftsbedingungen für die Sicherheit, den Datenschutz und die Daten- und Informationssicherheit» (AGB Sicherheit, September 2001) erlassen, die beim Bezug von Informatikdienstleistungen durch kantonale Organe zwingend dem Dienstleister zu überbinden sind. Dazu bestehen Checklisten für Outsourcing-Verträge. Der Datenschutzbeauftragte empfiehlt allen öffentlichen Organen, diese Hilfsmittel zu verwenden und die «AGB Sicherheit», insbesondere bei der vollständigen oder teilweisen Auslagerung von Informatikdienstleistungen, zu überbinden. Allzu oft nehmen die öffentlichen Organe Vertragstexte und Allgemeine Geschäftsbedingungen der Dienstleister ohne weiteres entgegen. Nebst unvorteilhaften Haftungswegbedingungsklauseln wird regelmässig auch die Verantwortung des Dienstleisters stark reduziert, und es fehlen die erwähnten Datenbearbeitungs- und Geheimhaltungsregelungen. Zu empfehlen ist deshalb, dass eine Vertrags-Policy festgelegt wird (welche Bedingungen werden akzeptiert) und eine Verantwortung für die Pflege der Verträge (einschliesslich periodischer Überprüfung und Nachführung) besteht.

Datenschutz mit Qualität

Das Qualitätsmanagementsystem des Datenschutzbeauftragten wurde nach der allgemein anerkannten Norm ISO 9001:2000 zertifiziert.

Das Projekt zum Aufbau des Qualitätsmanagementsystems konnte mit der Zertifizierung nach dem anerkannten und allgemein bekannten Standard ISO 9001:2000 erfolgreich abgeschlossen werden. Kern des Qualitätsmanagementsystems (QMS) ist die Definition von Dienstleistungsprozessen sowie die ablauforientierte Strukturierung der Organisation und der Tätigkeiten des Datenschutzbeauftragten. Der Aufbau des QMS des Datenschutzbeauftragten erfolgte im Rahmen des wif!-Querschnittprojekts Qualitätsmanagement.

Leitbild als Grundlage des Qualitätsmanagements

Grundlage für die Umsetzung der gesetzlichen Aufgaben und für die Festlegung der Dienstleistungen des Datenschutzbeauftragten ist das Leitbild. Es enthält die übergeordneten Ziele und legt den Grundstein, wie diese erreicht und wie dabei den Anspruchsgruppen begegnet werden soll. Daraus ergeben sich die Qualitätsansprüche an die Dienstleistungen und an die Betriebs- und Führungskultur, die das QMS umsetzen soll:

- Qualität beim Datenschutzbeauftragten bedeutet, Leistungen anzubieten, die ihn zum kompetenten und glaubwürdigen Ansprechpartner für öffentliche Organe und Bürgerinnen und Bürger in allen Fragen des Datenschutzes und der Informationssicherheit machen. Er thematisiert die Chancen und Risiken der Informations- und Kommunikationsgesellschaft in Bezug auf den Datenschutz und die Sicherheit und übernimmt eine führende Rolle in dieser Diskussion. Er nimmt seine Aufsichtsrechte über die verantwortlichen Organe in einem Klima des Vertrauens wahr. Im Vordergrund steht dabei die Prävention von Datenschutzverletzungen – einerseits durch Sensibilisierung und Aufklärung der betroffenen Personen, andererseits durch Information, Beratung und Schulung der verantwortlichen Organe.
- In Bezug auf die Festlegung der Dienstleistungen und der entsprechenden Arbeitsabläufe bedeutet Qualität beim Datenschutzbeauftragten Effizienz und Effektivität. Kundenzufriedenheit ergibt sich dabei nicht nur durch kompetente Beratung, sondern auch durch das Angebot von Lösungen und Verbesserungsvorschlägen. Aber auch Offenheit und Vertrauen sowie Respekt für die gegenseitigen Interessen gehören dazu. Effizienz resultiert aus schonendem Umgang mit Ressourcen und speditiver Vorgehensweise. Effektiv ist die Dienstleistung des Datenschutzbeauftragten nur, wenn sie zum Schutz der Privatheit beiträgt. Durch das Qualitätsmanagement soll für alle Anspruchsgruppen die Art und Weise der Dienstleistungen transparent werden. Das Qualitätsmanagement soll das Bewusstsein für Qualität und die Dienstleistungsmentalität des Teams fördern, indem alle Mitarbeitenden in massgeblicher Weise in die laufende Verbesserung der Dienstleistungen miteinbezogen werden.

Der Aufbau des QMS bedingt alsdann die Analyse bereits bestehender Dienstleistungen in Bezug auf die geforderten Qualitäten. Sie werden überprüft, ob sie effektiv, effizient und kundenorientiert sind. Ist das nicht der Fall, muss die Dienstleistung verbessert werden. Die definierten Dienstleistungen werden in Arbeitsabläufen oder Prozessen durch Flussdiagramme dargestellt und dokumentiert. Das System sieht laufende Überprüfung und Qualitätssteigerung vor, indem die Ergebnisse der Leistungen anhand eines Messkonzepts gemessen und die Prozesse im Bedarfsfall verbessert werden.

Die Dienstleistungsprozesse

Auf Grund des Gesetzes und der Qualitätsziele im Leitbild wurden fünf Hauptdienstleistungen (Prozesse) definiert:

- Der Beratungsprozess umfasst die Beantwortung von Rechtsfragen, die Begleitung von Projekten, das Verfassen von Vernehmlassungen, die Beratung über Informatiksicherheit usw. Die Beratung erfolgt je nachdem mündlich oder schriftlich. Auch Besprechungen oder die Mitwirkung in Arbeitsgruppen gehören dazu. Die Beratung in Anspruch nehmen können öffentliche Organe und Privatpersonen.
- Die Information als weiterer Prozess hat einen hohen Stellenwert. Dabei geht es vor allem um die Sensibilisierung für die Anliegen des Datenschutzes und der Informationssicherheit. Sie ist deshalb so wichtig, weil sie

sehr effektiv in einem frühen Stadium die Art und Weise von Datenbearbeitungen beeinflussen kann. Aus- und Weiterbildung, Publikationen, Medienanlässe gehören dazu.

- Die Kontrolle der Einhaltung der Vorschriften über den Datenschutz kann in zwei Prozessen erfolgen: Der erste Prozess besteht in einer regelmässigen, anlassunabhängigen Kontrolle und erfolgt mittels der Datenschutzreview. Die Datenschutzreview ist eine rechtliche, organisatorische und technische Prüfung von Organisationseinheiten bezüglich ausgewählter Aspekte des Datenschutzes und der Informatiksicherheit. Der zweite Prozess umfasst anlassbezogene Kontrollen. Hier wird jeweils im Einzelfall festgelegt, auf welche Weise bei wem welche Datenbearbeitungen geprüft werden.
- Der Prozess der Vermittlung im Sinne einer Ombudsfunktion kommt zum Zuge, wenn sich verantwortliche Organe und betroffene Personen über Datenbearbeitungen nicht einigen können. Bei der Vermittlung ist wesentlich, dass beide Seiten über die Abklärungen des Datenschutzbeauftragten informiert sind.
- Der Prozess Berichten umfasst in erster Linie die Erstattung eines jährlichen Tätigkeitsberichts zu Händen des Regierungsrates. Der Tätigkeitsbericht wird veröffentlicht und anlässlich einer Medienkonferenz präsentiert.

Nutzen eines QMS

Der Aufbau eines QMS lohnt sich aus verschiedenen Gründen: Das QMS ist ein lernorientiertes Führungs- und Organisationsinstrument. Es stellt sicher, dass die Dienstleistungen mit den übergeordneten Zielen des Datenschutzes übereinstimmen. Die Strategie wird in den operativen Arbeitsabläufen ständig umgesetzt und kann anhand von Kontrollen auf ihre Zielgerichtetheit überprüft werden. Die Dienstleistungen und ihre Arbeitsabläufe werden überdacht, gestrafft und damit effizienter gestaltet. Priorisiert wird, was grosse Wirkung für den Schutz der Privatheit entfaltet. Fehlerquoten, Leerläufe und deren Kosten werden gesenkt. Die Dokumentation der Prozesse in Flussdiagrammen macht die Abläufe und ihre Abhängigkeiten untereinander sowie die Schnittstellen transparent. Gleichzeitig können so die Prozesse besser gesteuert werden. Aufgaben, Kompetenzen und Verantwortlichkeiten sind klar geregelt. Das System verpflichtet durch regelmässige Messungen zur kontinuierlichen Qualitätssteigerung. Mittels Kundenumfrage werden die Anspruchsgruppen befragt, ob sie mit den Leistungen des Datenschutzbeauftragten zufrieden sind und wo sie Verbesserungspotenzial sehen. Die international anerkannte Zertifizierung steigert die Glaubwürdigkeit und die Anerkennung des Datenschutzbeauftragten bei allen Anspruchsgruppen.

Datenschutz
mit Qualität

Öffentlichkeitsprinzip und moderner Datenschutz

Der Entwurf für ein Gesetz über die Information und den Datenschutz (IDG) verzahnt in einem modernen Ansatz die Materien des Informationszugangs und des Datenschutzes konsequent.

Auf Grund einer kantonsrätlichen Motion hatte der Regierungsrat die Direktion der Justiz und des Innern mit der Erarbeitung eines Gesetzesentwurfs zur Einführung des Öffentlichkeitsprinzips beauftragt. Das Gesetzeskonzept sah vor, das Öffentlichkeitsprinzip und den Datenschutz in einem einheitlichen Gesetz zu regeln und beide Materien aufeinander abzustimmen (siehe Tätigkeitsbericht Nr. 7 [2001], S. 31 ff.). Unter Mitwirkung von zwei Experten erarbeitete die Arbeitsgruppe, welche bereits das Konzept ausgearbeitet hatte, einen Gesetzesentwurf, der im Dezember 2003 durch den Regierungsrat zu Händen der Vernehmlassung verabschiedet wurde. Der Datenschutzbeauftragte wirkte an den Arbeiten intensiv mit. Entstanden ist ein kompakter Entwurf eines Gesetzes über die Information und den Datenschutz (IDG) mit nur wenig mehr Gesetzesparagrafen, als das Datenschutzgesetz bereits heute enthält. Der Entwurf leistet damit auch einen Beitrag an die Einschränkung der Gesetzesflut. Er wurde anlässlich einer Medienkonferenz der Öffentlichkeit vorgestellt und in die Vernehmlassung geschickt.

Der Entwurf des IDG enthält folgende Schwerpunkte:

- Ziel und Zweck des IDG ist, Grundsätze im Umgang der öffentlichen Organe mit Informationen zu regeln. Ausgegangen wird hier von einem umfassenden Informationsbegriff. Personendaten sind eine Teilmenge der Informationen. Zielsetzungen sind die Wahrung des Schutzes der Grundrechte beim Umgang mit Informationen, insbesondere der Schutz der Persönlichkeit, die Gewährleistung des Zugangs zu Informationen und die Förderung der Informationstätigkeit der öffentlichen Organe. Dabei sollen die Interessen am Zugang und allfällige Interessen an der Geheimhaltung von Informationen ausgeglichen werden.
- Das Gesetz gilt für sämtliche öffentlichen Organe. Ausnahmen sind vorgesehen für öffentliche Organe, die am wirtschaftlichen Wettbewerb teilnehmen und dabei nicht hoheitlich handeln, sowie für alle hängigen verwaltungsinternen und gerichtlichen Rechtspflegeverfahren.
- Als wichtigen Grundsatz statuiert der Entwurf, dass der Umgang mit Informationen so zu gestalten ist, dass jedes öffentliche Organ rasch, umfassend, sachgerecht und verständlich informieren kann. Damit findet die Informationsbearbeitung nicht mehr nur rein innenorientiert statt (Aufgabenerfüllung und Rechenschaftsablage gegenüber Aufsichtsorganen), sondern erhält auch eine Aussenorientierung im Sinne von Transparenz des staatlichen Handelns.
- Das DSG enthält heute Bestimmungen zur Datensicherheit und zählt in der Verordnung verschiedene Sicherheitsmassnahmen exemplarisch auf (z.B. Benutzerkontrollen, Datenträgerkontrollen, Eingabekontrollen etc.). Anstelle dieser nicht mehr zeitgemässen Regelung gibt das IDG verschiedene Schutzziele vor, nach denen sich die Massnahmen zu richten haben. Für die Massnahmen selbst wird hingegen einerseits auf das Verhältnismässigkeitsprinzip, andererseits auf technische Standards und «best practices» verwiesen. Damit kann besser auf die technologischen Entwicklungen reagiert werden.
- Beim Umgang mit Personendaten wurde Wert auf eine bessere Wirkungsorientierung gelegt. Zur Bearbeitung von Personendaten genügt in Zukunft eine klare gesetzliche Aufgabenumschreibung; zusätzliche Bestimmungen über das Bearbeiten von Personendaten zwecks Erfüllung dieser Aufgaben sind nicht notwendig. Eine Ausnahme besteht hingegen bei der Bearbeitung von besonderen (bisher «besonders schützenswerten») Personendaten. Hier ist eine hinreichend bestimmte Regelung in einem formellen Gesetz erforderlich.
- Auch für die Datenbeschaffung werden Verbesserungen geschaffen. Anstelle der Beschaffung bei der betroffenen Person tritt der Grundsatz, dass die Beschaffung für die betroffene Person erkennbar sein muss. Damit können öffentliche Organe Daten auch bei anderen öffentlichen Organen erheben, sofern dies transparent wird.
- Bereits bisher statuierte der Verhältnismässigkeitsgrundsatz, dass nur die notwendigen Daten bearbeitet werden

dürfen. Hinzu treten moderne Prinzipien wie Datenvermeidung und Datensparsamkeit sowie Anonymisierung, Pseudonymisierung und Verschlüsselung. Dabei geht es vor allem um die elektronischen Datenbearbeitungen durch Informatikmittel und -systeme. Solche Systeme sind nach diesen Prinzipien zu gestalten (datenschutzfreundliche Technikgestaltung).

- Ein Teil des Öffentlichkeitsprinzips ist die Informationstätigkeit der öffentlichen Organe. (Der andere Teil ist das Recht der Bevölkerung, individuell auf entsprechende Anfrage Zugang zu Informationen zu erhalten; siehe dazu unten.) Nach dem IDG sollen alle öffentlichen Organe über alle Tätigkeiten von allgemeinem Interesse von sich aus informieren. Insbesondere sind Informationen über Aufbau, Zuständigkeiten bzw. Aufgaben sowie über Ansprechpersonen zu publizieren. Der Gesetzesentwurf regelt hier, was bereits heute verbreitete Praxis darstellt.
- Gesondert geregelt wird die Bekanntgabe von Personendaten. Dabei werden die bisherigen Bestimmungen des Datenschutzgesetzes weitgehend übernommen. Neu ist, dass auch die Bekanntgabe besonderer Personendaten eine hinreichend bestimmte Regelung in einem formellen Gesetz erfordert. Ausserdem ist die Bekanntgabe auch zulässig, wenn diese zur Abwendung einer unmittelbaren Gefahr für Leib und Leben notwendig ist. Damit nimmt der Gesetzgeber die Interessenabwägung zwischen dem Rechtsgut Schutz von Leib und Leben und dem Rechtsgut Persönlichkeitsschutz vor.
- Mit dem Öffentlichkeitsprinzip entsteht neu ein Rechtsanspruch auf Zugang zu Informationen. Dieser Anspruch steht jedermann zu. Sofern ein erstinstanzliches Verfahren hängig ist, richtet sich der Anspruch nach den Verfahrensbestimmungen.
- Wie bisher besteht weiterhin das datenschutzrechtliche Recht auf Auskunft über die «eigenen» Personendaten.
- Die Bekanntgabe von Informationen bzw. Personendaten ist nicht unbeschränkt (Teil V). Den Interessen an einem Zugang zu bzw. einer Bekanntgabe von Informationen sind allfällige öffentliche oder private Interessen an der Geheimhaltung gegenüberzustellen. Sind diese Interessen höher zu gewichten, ist der Zugang einzuschränken bzw. zu verweigern. Dies gilt ebenso bei entgegenstehenden gesetzlichen Geheimhaltungsbestimmungen.
- Bei den Verfahrensvorschriften ist erwähnenswert, dass ein Zugangsgesuch abgelehnt werden kann, wenn bereits veröffentlichte, auf angemessene Weise zugängliche Informationen verlangt werden oder wenn durch das Gesuch ein unverhältnismässiger Aufwand verursacht würde, etwa weil Informationen zuerst in einer Weise ausgewertet werden müssten, wie es das öffentliche Organ für seine Aufgabenerfüllung selbst gar nicht benötigen würde.
- Betrifft das Gesuch Daten von Drittpersonen, sind diese durch Anhörung ins Verfahren einzubeziehen. Bei besonderen Personendaten ist gar eine ausdrückliche Zustimmung der betroffenen Person(en) erforderlich.
- Der Datenschutzbeauftragte erhält zusätzliche Aufgaben im Bereich des Öffentlichkeitsprinzips. So wird er zum Beauftragten für Informationszugang und Datenschutz. Er berät, kontrolliert, vermittelt und informiert zukünftig in Fragen des Datenschutzes und des Informationszugangs. Nicht zuständig ist er hingegen für die Informationstätigkeit und den Entscheid über die Zugangsgesuche. Hier bleiben die einzelnen öffentlichen Organe weiterhin verantwortlich.
- Zusätzliche Aufgaben des Beauftragten bestehen darin, die Entwicklungen im Bereich der Informations- und Kommunikationstechnologien zu beobachten und zu bewerten, die öffentlichen Organe im Bereich der Umsetzung der Informationssicherheitsmassnahmen zu unterstützen und die Einführung von Qualitätsstandards in der Informationsbearbeitung zu fördern.
- Das Amtsgeheimnis gilt nur noch insoweit, als überwiegende öffentliche oder private Interessen an der Geheimhaltung oder eine gesetzliche Geheimhaltungsbestimmung bestehen.

Umfassender Informationsbegriff

Der zürcherische Gesetzesentwurf setzt die bisherigen Entwicklungen im Bereich Öffentlichkeitsprinzip und Datenschutz in der Schweiz fort. Nachdem der Kanton Bern als Pionier und später verschiedene Westschweizer Kantone das Öffentlichkeitsprinzip durch Erlass eines Informationsgesetzes eingeführt hatten, schuf der Kanton Solothurn im Jahr 2001 ein Informations- und Datenschutzgesetz, das beide Materien – Öffentlichkeitsprinzip und Datenschutz – im gleichen Gesetz regelte. Dabei bilden die beiden Materien jeweils gesonderte Teile des Gesetzes, und es werden die Schnittstellen geregelt. Das Öffentlichkeitsgesetz des Bundes, welches noch in der parlamentarischen Beratung steht, enthält Verweisungen auf das Datenschutzgesetz; das Datenschutzgesetz regelt die Fälle der Öffentlichkeit von Personendaten. Der Entwurf des Kantons Zürich stellt eine Weiterentwicklung des Solothurner Modells dar, indem die beiden Materien nicht mehr gesondert geregelt sind, sondern konsequent ineinander verzahnt werden. Dabei wird von einem umfassenden Informationsbegriff ausgegangen. Wo eine besondere Behandlung der Personendaten gerechtfertigt ist, werden ergänzende Bestimmungen geschaffen.

Erfolgreicher Abschluss von Soprano

Das Projekt Soprano konnte im vergangenen Jahr erfolgreich abgeschlossen werden. Die operative Umsetzung liegt nun bei der Verwaltung.

Das Projekt Soprano hatte zum Ziel, die Voraussetzungen für die Einführung einer verwaltungsweiten Sicherheitsinfrastruktur auf der Basis einer Public-Key-Infrastruktur (PKI) zu schaffen. Wir haben in unseren Tätigkeitsberichten (vgl. Tätigkeitsbericht Nr. 7 [2001], S. 34 f., Tätigkeitsbericht Nr. 8 [2002], S. 20) regelmässig über das Projekt berichtet.

Die Schweizerische Informatikkonferenz (SIK) wie auch der Bund sahen ebenfalls in der zukunftsträchtigen Technologie der PKI die Möglichkeit eines sicheren, vertraulichen und verwaltungsübergreifenden Datenaustausches. Die SIK setzte sich in der Folge dafür ein, dass eine für alle Kantone verfügbare Infrastruktur aufgebaut wird. Der Bund war bereit, seine Infrastruktur für die Kantone zu öffnen und Zertifikate an die Kantone auszugeben. In gemeinsamen Gesprächen wurden die Voraussetzungen geklärt und eine Grobplanung verabschiedet.

Mit diesem Vorstoss der SIK und des Bundes veränderten sich die Voraussetzungen für das Projekt Soprano. Es stellte sich die Frage, ob es sinnvoll sei, im Kanton Zürich eine eigene Infrastruktur aufzubauen. Nach einer intensiven Evaluation entschied der Regierungsrat, sich in Bezug auf die Einführung einer einheitlichen Sicherheitsinfrastruktur dem gemeinsamen Projekt von Bund und SIK anzuschliessen und den Vergabeentscheid für eine eigene Infrastruktur zu widerrufen. Ausschlaggebend waren Argumente der Wirtschaftlichkeit, der Flexibilität, der Akzeptanz und die Möglichkeit des schrittweisen Ausbaus. Damit wurde ein Strategiewechsel vollzogen, der sich im Hinblick auf die Zusammenarbeit mit dem Bund und den Kantonen in zahlreichen gemeinsamen Anwendungen als sinnvoll erweisen kann. Der Bund wie der Kanton Zürich haben sich Wissen und Erfahrungen im Bereich der PKI aufgebaut, aus denen nun Synergien für die gemeinsame Zusammenarbeit entstehen können. Voraussetzung ist allerdings, dass der bisher eingeschlagene Weg konsequent umgesetzt wird und die Verwaltungsstellen, die einen Bedarf geltend machen, umgehend mit Zertifikaten versorgt werden. Mit den bisherigen Pilotprojekten und zahlreichen weiteren interessierten Stellen ist eine genügend grosse Nachfrage vorhanden, um das Projekt rasch voranzuführen.

Diese Entwicklung bedeutete für das Projekt Soprano, dass die geplante Pilotphase mit einer eigenen Infrastruktur überflüssig wurde, da mit der bestehenden Infrastruktur des Bundes direkt die operative Phase eingeleitet werden konnte. Deshalb wurde das Projekt Soprano abgeschlossen.

Die neue Verantwortung für die Umsetzung wurde der Direktion für Justiz und Inneres übertragen, die ihrerseits ihre eigene Infrastruktur ablösen muss und nun für die gesamte Verwaltung als Ansprechpartner in punkto PKI zur Verfügung steht. Sie hat auch die Aufgabe, die im Projekt Soprano vorgezeichneten Schritte in die Praxis umzusetzen.

Mit dem Projekt Soprano konnten erfolgreich die Grundlagen gelegt werden, um eine sichere Informatikinfrastruktur in der kantonalen Verwaltung und in den Gemeinden zu schaffen. Es liegt nun an den einzelnen Verwaltungsstellen, unter Führung der Direktion der Justiz und des Innern zusammen mit dem Bund, diese umzusetzen.

Sensible Datenbearbeitungen

In zahlreichen Projekten konnten Fortschritte in Bezug auf die Berücksichtigung datenschutzrechtlicher Anliegen erzielt werden.

1. Elektronisches Rechtsinformationssystem

Weiterhin offene Fragen

Das Rechtsinformationssystem (RIS) der Direktion der Justiz und des Innern benötigt klare Regelungen in Form eines Reglements sowie eine verhältnismässige Systemkonfiguration. Das Reglement wurde auf Grund unserer Stellungnahme nicht ausreichend nachgebessert (siehe Tätigkeitsbericht Nr. 8 [2002], S. 16 f.). Leider lässt es nach wie vor Transparenz vermissen. So ist insbesondere unklar, welche Daten zu welchem Zweck erfasst werden und was mit den erfassten Daten weiter geschieht. Weiter fehlt es an klaren Regelungen über die Zugriffsberechtigungen. Der überarbeitete Entwurf sah vor, dass die Amtsleitungen weitgehende Kompetenzen zur Einrichtung zusätzlicher Zugriffe – auch über ihren Bereich hinaus – innehaben. Wir wiesen darauf hin, dass in jedem Geschäftsfeld der Direktion – Strafverfolgung Erwachsene, Jugendstrafverfolgung, Strafvollzug sowie weitere wie Opferhilfe etc. – eine Rechtsgrundlage für das Führen einer Geschäftskontrolle besteht. Innerhalb der Geschäftsfelder ist denn auch das Führen eines gemeinsamen Personenstamms zulässig.

Gegenseitige Zugriffe über die jeweiligen Geschäftsfelder hinaus sind hingegen grundsätzlich nicht nötig, sondern sind erst zu ermöglichen, wenn im Einzelfall ein Datenaustausch notwendig wird. So soll beispielsweise die Opferhilfestelle auf die Strafverfolgungsdaten eines Täters erst zugreifen können, wenn ein Opfer ein Opferhilfegesuch bezüglich dieser Tat eingereicht hat.

Technisch ist das System deshalb wie folgt zu gestalten:

- Die einzelnen Geschäftsfelder sind – auch hinsichtlich Personenstamm – voneinander zu trennen.
- Wenn in einem Geschäftsfeld ein neues Geschäft eröffnet werden soll, kann innerhalb des Personenstammes des Geschäftsfelds geprüft werden, ob diese Person bereits bekannt ist.
- Ein Zugriff auf Daten eines anderen Geschäftsfelds ist nur zu ermöglichen, wenn diese Daten für die zugreifende Stelle relevant sind und diesbezüglich formell ein Geschäft eröffnet wurde.
- Ebenfalls ungenügend geregelt waren die Löschfristen für die Daten. Ausserdem wiesen wir auf weitere Einzelheiten hin. Die Direktion der Justiz und des Innern machte daraufhin Vorschläge zur Regelung der Löschung bzw. der Aufbewahrungsdauer. Wir bemängelten dabei die vorgesehene Möglichkeit, weitgehende Ausnahmen von den vorgesehenen Regelungen zu treffen. Ein weiterer überarbeiteter Reglementsentwurf steht noch aus.

Das Rechtsinformationssystem ist technisch nach Geschäftsfeldern getrennt zu führen. Gegenseitige Zugriffe sind erst auf Anlass zu ermöglichen. Ausserdem ist ein detailliertes Reglement über die Datenbearbeitungen zu erlassen, das klare Rahmenbedingungen setzt und möglichst davon absieht, davon wiederum Ausnahmen zu ermöglichen.

2. Gesichtserkennung am Flughafen

Aufnahme des Pilotbetriebs

Im Projekt «Face Recognition» – dem automatisierten Gesichtserkennungssystem der Flughafenpolizei – wurde im Berichtsjahr der angekündigte Pilotbetrieb durchgeführt (siehe Tätigkeitsberichte Nr. 7 [2001], S. 10 und Nr. 8 [2002], S. 29 f.). Wir nahmen dies zum Anlass, uns das System vorführen und die Abläufe erläutern zu lassen. Zur Verfügung standen dazu verschiedene interne Systemunterlagen wie Besprechungsprotokolle mit dem Lieferanten und eine Art Betriebsweisung. Da keine Systemdokumentation existiert, führten wir keine eigentliche Prüfung des Systems durch. Die ersten Resultate des Pilotbetriebs veranlassten die Kantonspolizei, den Versuchsbetrieb zu verlängern.

Wir teilten der Direktion für Soziales und Sicherheit mit, dass für das System Rechtsgrundlagen zu schaffen seien, welche insbesondere eine klare Zweckumschreibung beinhalten müssten, und empfahlen, die Erarbeitung der gesetzlichen Grundlagen rasch anzugehen.

Gegen Ende des Berichtsjahres verlangten wir von der Flughafenpolizei ei-

nen Statusbericht über den Pilotbetrieb und die weiteren technischen und gesetzgeberischen Schritte. Wir erhielten eine Zusammenfassung der Auswertungen der ersten Phase des Pilotbetriebs. Ausserdem stellte die Flughafenpolizei die Aufnahme der zweiten Phase in Aussicht, bei der das System weiterhin im Rahmen der vorgelagerten Grenzkontrollen eingesetzt werden soll. Dabei sollen die der illegalen Migration verdächtigten Personen in einer vordefinierten Zone in Bewegung aufgezeichnet und die Bilder mit Kopien der Reisedokumente verknüpft werden. Technisch sollen mehrere Suchläufe im System ermöglicht und die Daten neu 60 statt 30 Tage aufbewahrt werden. Für diese Phase stellte die Flughafenpolizei spezifische Rechtsgrundlagen in Aussicht.

Wir erhielten mittlerweile einen Entwurf für eine Verordnung über den Versuchsbetrieb des biometrischen Gesichtserkennungssystems FAREC am Flughafen Zürich-Kloten zur Vernehmlassung.

Das Gesichtserkennungssystem der Flughafenpolizei erfordert eine gesetzliche Grundlage, welche klare Regelungen über den Zweck des Systems, die Art der bearbeiteten Daten, deren Verwendung, die Dauer der Aufbewahrung sowie – falls geplant – die Bekanntgabe an andere Stellen enthält. Ausserdem sind angemessene organisatorische und technische Sicherheitsmassnahmen zu treffen.

3. Bearbeitung von raumbezogenen Daten

Kontrolle und Gesetzesentwurf

Die Systeme zur Bearbeitung raumbezogener Daten – einerseits das Geografische Informationssystem (GIS), andererseits das System «Gebäudedaten für Kanton und Gemeinden» (GeKaGe) – wurden laufend weiter ausgebaut. GeKaGe wurde so angepasst, dass es den Vorgaben des Bundes für ein Gebäude- und Wohnungsregister (GWR) entspricht. Obwohl wir mehrfach den Erlass eines Gesetzes für die Bewirtschaftung raumbezogener Daten für die Systeme GIS und GeKaGe/GWR-ZH verlangt hatten, liess ein diesbezüglicher Entwurf weiter auf sich warten (siehe Tätigkeitsbericht Nr. 7 [2001], S. 36 f. mit weiteren Hinweisen). Dies veranlasste uns, beim Amt für Raumordnung und Vermessung eine Kontrolle bezüglich dieser Systeme durchzuführen.

Wir verlangten dazu eine umfassende Dokumentation der Systeme (Applikationsbeschreibungen, Beschreibungen der Datenkategorien und Bearbeitungsabläufe, Zugriffskonzepte etc.). Die Auswertung der Unterlagen erwies sich als ausserordentlich aufwändig, da die Dokumentation sehr umfangreich war und die Systeme komplex sind. Mittlerweile waren offenbar auch die Gesetzgebungsarbeiten wieder aufgenommen und vorangetrieben worden, so dass wir gegen Ende des Berichtsjahres einen Vorentwurf eines Geoinformationsgesetzes zu einer ersten Stellungnahme erhielten. Dieser neue Entwurf stellt gegenüber früheren Entwürfen einen Fortschritt dar, insbesondere da er sich nicht mehr nur auf die kantonalen Systeme GIS und GeKaGe/GWR-ZH beschränkt, sondern allgemeine Regelungen für die Bearbeitung von Geoinformationen aufstellt und damit auch den Gemeinden Grundlagen für deren Systeme liefert. In materieller Hinsicht brachten wir mit unserer Stellungnahme verschiedene Verbesserungsvorschläge ein. So ist unseres Erachtens das Verhältnis zu den einzelnen Sachgesetzgebungen noch zu wenig geklärt. Der Entwurf verweist allgemein auf die Bestimmungen der einzelnen Sachgesetze (z.B. Planungs- und Baugesetz, Natur- und Heimatschutzgesetz etc.), die gewisse Daten für «öffentlich» erklären. Es fehlt jedoch an Klarheit über die Tragweite dieser «Öffentlichkeit». Nötig sind auch Regelungen über allfällige Verknüpfungen von Daten und deren Zwecke. Festzuhalten war aber auch, dass auf der Grundlage dieses Entwurfs weitergearbeitet werden kann.

Unser Bericht zur Überprüfung der Systeme GIS und GeKaGe/GWR-ZH fiel zeitlich mit der Stellungnahme zum Gesetzesentwurf zusammen. Wir empfahlen dem Amt für Raumordnung und Vermessung, die Systeme vorderhand nicht weiter auszubauen, bis das Geoinformationsgesetz verabschiedet ist, und den Gesetzesentwurf im Sinne unserer diesbezüglichen Stellungnahme zu überarbeiten.

Auch auf schweizerischer Ebene gab es verschiedene Aktivitäten. Im Rahmen des Impulsprogramms «e-geo.ch» wurde ein Vorentwurf eines Geoinformationsgesetzes erarbeitet. Das Verhältnis dieses Entwurfes zum Datenschutzgesetz sowie zum Entwurf des kantonalen Geoinformationsgesetzes ist noch zu klären.

Die Schweizerische Organisation für Geo-Information (SOGI) verfasste einen Schlussbericht und ein Merkblatt «Datenschutz und Raumdaten». Allerdings enthält das Merkblatt verschiedene rechtlich nicht haltbare Aussagen. Die Vereinigung der Schweizerischen Datenschutzbeauftragten sah sich deshalb veranlasst, eine Stellungnahme dazu abzugeben. Ein weiterer Diskussions-

punkt im Berichtsjahr war die Frage des Austauschs von Steuerdaten über GeKaGe. Die Abteilung Direkte Bundessteuer des Steueramtes bedient GeKaGe mit Personendaten. Zudem sollen in Zukunft auch Datentransfers zwischen den Gemeindesteuerämtern und dem kantonalen Steueramt über GeKaGe stattfinden. Anlässlich einer Aussprache zwischen dem Steueramt, dem Amt für Raumordnung und Vermessung und dem Datenschutzbeauftragten hatten wir auf die generell ungelösten datenschutzrechtlichen Fragen bei GeKaGe hingewiesen. Fragwürdig schien insbesondere die Ausdehnung eines Systems, das dem Austausch von Gebäudedaten dient, auf weitere Zwecke wie den Austausch von Personendaten. Wir warfen auch die Frage auf, ob ein solches Vorgehen mit dem Steuergeheimnis vereinbar sei. Das Steueramt liess zu diesen Fragen ein Rechtsgutachten erarbeiten, welches insgesamt zum Schluss kam, dass gesetzliche Grundlagen für das geplante Vorhaben zu schaffen seien.

Das Geoinformationsgesetz ist weiterzubearbeiten und möglichst rasch dem Parlament vorzulegen. Es hat einen klaren Rahmen für die Bearbeitung von raumbezogenen Daten bzw. von Geoinformationen zu schaffen.

Information im Zentrum

Für die Umsetzung der datenschutzrechtlichen Anliegen ist die Information von zentraler Bedeutung.

1. www.datenschutz.ch

Aktuelle Beratung und Informationen

Das neue Informationskonzept des Datenschutzbeauftragten, das eine Konzentration der Informationsaktivitäten auf die Homepage und auf «digma» bedeutete (siehe Tätigkeitsbericht Nr. 6 [2000], S. 39 f.), hat sich bewährt (zu «digma» siehe S. 41). Dadurch kann das Informationsbedürfnis von Verwaltung und Bevölkerung mit wenig Ressourcen effizient und effektiv abgedeckt werden.

Die Homepage wird periodisch aktualisiert. Der Schwerpunkt liegt auf der Publikation von Beratungsfällen. Individuelle Beratungen, die grundsätzliche Fragen und Fälle betreffen oder von allgemeinem Interesse sind, werden als «Häufig gestellte Fragen» (FAQ) oder als Themen veröffentlicht. Der Nutzen ist bedeutend, entfallen doch zukünftige Anfragen zum gleichen Thema oder sie können mit minimalem Aufwand innert kürzester Zeit erledigt werden.

Ein zweiter Schwerpunkt ist das Angebot von Selbsthilfeinstrumenten. So konnten wir eine überarbeitete Version des Passwort-Checks aufschalten. Der Passwort-Check ist allseits beliebt; täglich testen mehrere Hundert Personen aus Verwaltung, Unternehmen und Bevölkerung die Qualität ihrer Passwörter. Einfach verständliche Anleitungen helfen den Benutzenden, sichere Passwörter zu bilden. Weitere Selbstschutzinstrumente stehen über eine Liste von Links zu anderen Angeboten indirekt zur Verfügung. Umzusetzen waren im Berichtsjahr auch die Harmonisierungsentscheide des Regierungsrates. Einerseits besteht die Anforderung, eine URL nach dem Muster <www.«Name Verwaltungseinheit».zh.ch> zu führen.

Dies ist bereits seit längerem dadurch erfüllt, dass unser Angebot auch unter *www.datenschutz.zh.ch* sowie *www.dsb.zh.ch* zu erreichen ist. Andererseits war die kantonale Kopfzeile einzubauen, die eine direkte Navigation zwischen allen Angeboten des Kantons ermöglicht.

Die Homepage ist weiterhin das zentrale Informationsmedium des Datenschutzbeauftragten. Interessierte Personen und Verwaltungsstellen können sich dank regelmässigen Aktualisierungen über praktische Fälle und neue Entwicklungen informieren.

2. Symposium on Privacy and Security

Identität und Anonymität in einer vernetzten Welt

Das zweitägige Symposium on Privacy and Security fand im Oktober 2003 statt und widmete sich dem Thema «Identität und Anonymität in einer vernetzten Welt».

E-Business und E-Government können ohne angemessenes Identitätsmanagement nicht funktionieren. Unternehmen wie Verwaltung stehen in einem Spannungsfeld zwischen – einerseits – der nötigen Qualität von Identifizierung und Authentifizierung, damit ihre Geschäftsinteressen geschützt sind (z.B. Informationssicherheit, kein Zugriff für Unberechtigte) und die rechtlichen Rahmenbedingungen eingehalten werden (z.B. Bekämpfung von Geldwäscherei). Andererseits besteht das berechtigte Bedürfnis, dass die Prozesse und damit die Kostenstruktur nicht zu sehr belastet werden und die Anwendungsfreundlichkeit nicht zu stark leidet.

Ein weiteres Spannungsfeld tut sich auf zwischen den Interessen der Betreiber eines Identitätsmanagementsystems und denjenigen der Betroffenen. Ihnen liegt daran, in den verschiedenen Kontexten und Rollen als berechtigte Personen Zugriff auf die Ressourcen zu erhalten, ihre Rechte und Pflichten wahrnehmen zu können, ohne die Kontrolle über ihre Identität(en) und die damit verbundenen Daten abgeben zu müssen, oder vielleicht wollen die Betroffenen sogar anonym bleiben.

Für Unternehmen und Verwaltung zentrale Themen sind die Bedeutung von Identitätsmanagement, aktuelle Forschungsprojekte und Unterschiede der einzelnen bereits in Gebrauch stehenden Konzepte, das Identitätsmanagement der Zukunft, die Kontrolle über die Identitäten und das Mass an Identität, das für die Gewährleistung der (Informations-)Sicherheit nötig ist.

Namhafte Referenten aus dem In- und Ausland referierten zu diesen Themen und stellten ihre Erfahrungen und Erkenntnisse aus der Praxis vor. Paneldiskussionen boten Gelegenheit zur kri-

tischen Hinterfragung der vorgestellten Thesen.

Das Symposium ist zum festen Bestandteil des Weiterbildungsangebotes des Datenschutzbeauftragten und zu einer willkommenen Plattform für den Erfahrungsaustausch im Bereich Datenschutz und Informationssicherheit avanciert. Namhafte Referenten aus dem In- und Ausland stellen hier ihre Themen vor und berichten von ihren Erfahrungen aus der Praxis.

3. Zeitschrift «digma»
Kontinuität mit Qualität

Im Berichtsjahr ging «digma» bereits in ihr drittes Jahr. Die Zeitschrift zeichnet sich durch Kontinuität und Qualität aus. Änderungen ergaben sich bei den Herausgebern und im Layout. Anstelle von Rolf Oppliger, der sich aus der Herausgeberschaft zurückgezogen hatte, konnte Michael Waidner gewonnen werden. Kleine Anpassungen im Layout führten zu einer konsequenteren Umsetzung des Gestaltungskonzepts.

Inhaltlich wurden folgende Schwerpunkte behandelt:

- «digma» 2003.1
  Return on Investment
- «digma» 2003.2
  10 Jahre Datenschutzgesetz
- «digma» 2003.3
  Identitätsmanagement
- «digma» 2003.4
  Versicherungen

Aus Anlass des 10-jährigen Bestehens des Datenschutzgesetzes des Bundes (Inkraftsetzung per 1. Juli 1993) setzten sich verschiedene Autoren in «digma» 2003.2 mit der Frage nach der Wirkung des Gesetzes und seinen Mängeln auseinander. Zentral waren Aspekte des Zusammenwirkens von Recht und Technik, die technische Umsetzung rechtlicher Anforderungen oder die Anpassung des rechtlichen Rahmens auf Grund technischer Entwicklungen.

Auch wir konnten verschiedene Beiträge aus unserem Beratungs- und Informationsalltag in «digma» publizieren: Checkliste zur Videoüberwachung, Qualitätsmanagementsystem des Datenschutzbeauftragten, «Schwarze Listen» von Versicherern sowie wichtige Gerichtsentscheide.

In «digma» erscheinen regelmässig Artikel zu wichtigen Schwerpunktthemen und aktuelle Beiträge. Durch die Mitwirkung des Datenschutzbeauftragten bei «digma» werden Artikel zu auch im Kanton Zürich aktuellen Themen publiziert, und es entsteht ein wertvoller Know-how-Transfer in allen wichtigen Fragen des Datenschutzes und der Informationssicherheit.

4. Aus- und Weiterbildung
Zahlreiche Seminare und Referate

Die Grundlagenseminare im Rahmen der kantonalen Aus- und Weiterbildung führten wir auch im Berichtsjahr wieder durch. Daneben hielten wir auf Anfrage weitere Seminare. So führten wir die bewährten Kurse für den Verband Zürcher Einwohnerkontrollen (VZE) sowie für den Verein Zürcher Gemeindeschreiber und Verwaltungsfachleute (VZGV), für die Aus- und Weiterbildung von Gefängnismitarbeitenden, für die römisch-katholische Zentralkommission, für ein Sprachtherapieheim, für Mitarbeitende eines Stellennetzes sowie der Abraxas durch. Zudem hielten wir auf Anfrage zahlreiche Referate.

Der Bedarf nach gezielter Aus- und Weiterbildung im Bereich des Datenschutzes und der Informationssicherheit konnte aber nicht abgedeckt werden. Die personellen Ressourcen des Datenschutzbeauftragten setzen hier eine Grenze. Deshalb sieht das neu erarbeitete Weiterbildungsangebot vor, allgemeine Aus- und Weiterbildung im Rahmen eines Internetangebotes zur Verfügung zu stellen und darauf aufbauend allgemeine Vertiefungsseminare und fachspezifische Seminare anzubieten.

Der Bedarf an Aus- und Weiterbildung im Bereich des Datenschutzes und der Informationssicherheit ist zunehmend und konnte nur teilweise abgedeckt werden.

5. Synergien durch Zusammenarbeit
Mitwirkung in Arbeitsgruppen der Datenschutzbeauftragten

Auf kantonaler Ebene fanden drei Sitzungen der kommunalen Datenschutzbeauftragten statt, an denen auch der kantonale Datenschutzbeauftragte teilnahm. Folgende Themen waren im Berichtsjahr aktuell: Informations- und Datenschutzgesetz, Videoüberwachung, Datenbanken der Polizeiorgane, Datenerfassung und -weitergabe durch Einwohnerkontrollen, Aufbewahrung von Unterlagen bei Abweisung und Rückzug des Gesuchs sowie Einzelfragen aus dem Bereich der Einwohnerkontrollen, der Zusatzleistungen, der schulärztlichen Dienste, der Zustellung von Stimmrechtsausweisen sowie der Einbürgerung. Die Zusammenarbeit mit den kommunalen Datenschutzbeauftragten ermöglicht einen regen Erfahrungsaustausch und ein koordiniertes Vorgehen bei Fragen grundsätzlicher Art.

Auf nationaler Ebene sind wir vertreten im Büro der Vereinigung der schweizerischen Datenschutzbeauf-

tragten (DSB+CPD.CH) sowie in weiteren Arbeitsgruppen. Die Vereinigung beschäftigt sich mit allen aktuellen Fragen des Datenschutzes, womit in der Zusammenarbeit wertvolle Synergien für die kantonale Arbeit gewonnen werden können.

Ebenso organisierte die Vereinigung die 10. Nationale Konferenz der Datenschutzbeauftragten, welche in Genf stattfand und sich hauptsächlich dem Thema Spam («unerwünschte E-Mail») widmete.

Mit der Zusammenarbeit unter den Datenschutzbeauftragten können Informationen ausgetauscht und gemeinsam Lösungen diskutiert werden.

6. Datenschutz in der Telekommunikation

Tagung der internationalen Arbeitsgruppe

Die Internationale Arbeitsgruppe Datenschutz in der Telekommunikation hat ihre Frühjahrstagung in Zürich durchgeführt. Die vom Berliner Beauftragten für Datenschutz und Informationsfreiheit geleitete Arbeitsgruppe setzt sich zusammen aus Vertreterinnen und Vertretern von Datenschutzbehörden aus allen Kontinenten. Die Arbeitsgruppe trifft sich regelmässig zweimal pro Jahr. Die Themen, mit denen sich die Arbeitsgruppe an ihrer Zürcher Sitzung auseinander setzte, umfassten die Entwicklungen im Bereich des Internet- und Telekommunikationsrechts in den einzelnen Ländern sowie Entwicklungen im Bereich des E-Government. Spezifische Themen waren das Internet und weitere den Datenschutz im Telekommunikationsbereich betreffende Sachverhalte. Die Arbeitsgruppe nimmt jeweils in Arbeitspapieren zu einzelnen Problembereichen Stellung. Diese Papiere werden veröffentlicht (www.datenschutz-berlin.de).

Die Arbeitsgruppe hat in Zürich ihr 33. Meeting abgehalten. Sie gehört zu den ersten international koordinierten Datenschutzgremien und arbeitet deshalb eng mit der Internationalen Konferenz der Datenschutzbeauftragten und der Europäischen Konferenz der Datenschutzbeauftragten zusammen. Damit wird ein kontinuierlicher Informationsaustausch sichergestellt.

Die Zusammenschlüsse der Datenschutzbeauftragten sind sehr wichtig, um über die für die tägliche Arbeit wichtigen Informationen verfügen zu können, gerade in einem Bereich, wo die Technologie vielfach die Geschwindigkeit angibt.

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

Datenschutzbeauftragter
Dr. iur. Bruno Baeriswyl

Stellvertreter
lic. iur. Marco Fey (bis 31.7.2004)

Juristisches Sekretariat
lic. iur. Beda Harb (ab 1.4.2004)
lic. iur. Barbara Mathis
lic. iur. Karin Schoch

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

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

Sekretariat
Martina Richard

Tätigkeitsbericht Nr. 9 (2003)
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
datenschutz@dsb.zh.ch
www.datenschutz.ch