10 JAHRE DATENSCHUTZ IM KANTON ZÜRICH

Nummer 10

Tätigkeitsbericht 2004

dsb
datenschutzbeauftragter kanton zürich

10 JAHRE DATENSCHUTZ IM KANTON ZÜRICH

Am 1. Januar 1995 ist das Datenschutzgesetz des Kantons Zürich in Kraft getreten. Die Einführung dieser Gesetzgebung bei den öffentlichen Organen im Kanton Zürich wird durch die Tätigkeitsberichte des Datenschutzbeauftragten dokumentiert.

Die Tätigkeitsberichte 1–10 sind als Publikation beim Datenschutzbeauftragten oder als pdf-Dokument auf dessen Website **www.datenschutz.ch** als Download zu finden. Am 17. März 2005 fand aus Anlass des zehnjährigen Bestehens des Datenschutzgesetzes eine Veranstaltung statt, die einen Rückblick und einen Ausblick in Bezug auf den Datenschutz beinhaltete. Die Referate dieser Veranstaltung werden publiziert.

Nummer 10
Tätigkeitsbericht 2004

Der Datenschutzbeauftragte erstattet dem Regierungsrat jährlich oder nach Bedarf einen Bericht über seine Tätigkeit (§ 23 Datenschutzgesetz). Der vorliegende Tätigkeitsbericht 2004 Nr. 10 deckt den Zeitraum vom 1. Januar 2004 bis 31. Dezember 2004 ab.

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

Zürich, Juni 2005

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

Zunehmende Herausforderungen

Das Grundrecht der Bürgerinnen und Bürger auf den Schutz ihrer Privatheit hat sich mit der Datenschutzgesetzgebung etabliert. Die Herausforderungen für die Umsetzung des Datenschutzes zehn Jahre nach der Einführung des Datenschutzgesetzes im Kanton Zürich haben auf Grund der rasanten technologischen und gesellschaftlichen Entwicklung indessen weiter zugenommen.

Wer vor zehn Jahren meinte, mit der Einführung des Datenschutzgesetzes seien nun die Anliegen des Schutzes der Privatheit der Bürgerinnen und Bürger erfüllt, sah sich getäuscht. Nicht nur zeigte sich, dass die Umsetzung des Gesetzes im täglichen Verwaltungsablauf alles andere als eine Selbstverständlichkeit war, sondern auch, dass eine technologische Entwicklung die Verwaltung erfasste, die ganz neue Möglichkeiten der Datenbearbeitungen zuliess. Dazu kommt eine gesellschaftliche Haltung, die die Rolle der Grundrechte der liberalen Gesellschafts- und Rechtsordnung immer mehr in den Hintergrund drängt.

Umsetzung des Datenschutzes

Die Gewährleistung des Grundrechtes auf Datenschutz bedeutet, dass die Verwaltung ihre Abläufe den neuen gesetzlichen Anforderungen anzupassen hat. Bei jeglicher Bearbeitung von Personendaten hat die Frage in den Mittelpunkt zu rücken, wie den Anliegen des Persönlichkeitsschutzes der Bürgerinnen und Bürger zu begegnen ist. Damit decken sich die Anliegen des Datenschutzes mit den Zielsetzungen des «New Public Management» (NPM), das eine breite Verwaltungsreform einleitete. Der Bürger und die Bürgerin rückten in das Zentrum des Verwaltungshandelns. Um dies zu erreichen, mussten Prozesse geändert oder neue geschaffen werden. Soweit dies konsequent auch bei den Datenbearbeitungen umgesetzt wurde, konnten auch die Anliegen des Datenschutzes verwirklicht werden.

Doch vielfach griffen diese Projekte zu kurz, waren und sind einzig technologiegesteuert, so dass der Datenschutz auf der Strecke blieb oder bleibt. In den letzten Jahren zeigte sich indessen, dass eine konsequente Ausrichtung des Verwaltungshandelns auf die Bedürfnisse der Bürgerinnen und Bürger auch ohne weiteres die Respektierung der datenschutzrechtlichen Rahmenbedingungen ermöglichte. Das Spannungsfeld, in dem sich viele Verwaltungsstellen bei der Umsetzung des Datenschutzes vermeintlich befinden, wäre deshalb mit einer konsequenteren Besinnung auf die Zielrichtung des Handelns vermeidbar.

Vielfach werden diese Überlegungen auch durch die Sparmassnahmen auf allen Ebenen überlagert. Gerade hier wirkt sich eine konsequente Umsetzung des Datenschutzes als komplementär aus. Würden nämlich einerseits die Datenflüsse transparent gestaltet, indem entsprechende Rechtsgrundlagen geschaffen würden, und andererseits die Datenbearbeitungen auf die geeigneten und erforderlichen Daten reduziert, liessen sich heute viel effizientere und zielgerichtetere Datenbearbeitungssysteme aufbauen, und dies mit weit weniger Kosten. Doch leider hat eine Technologiegläubigkeit überhand genommen, die schon allein den Einsatz neuer Technologien als Erfolg bezeichnet. Die Ernüchterung, die sich heute beim E-Government auf Grund mangelnder nutzbringender Ergebnisse einstellt, ist symptomatisch. Dass der Datenschutz aber auch noch (mit)schuldig an dieser Tatsache sein soll, zeigt, wie wenig der Nutzen für die Bürgerinnen und Bürger bei diesen Entwicklungen im Vordergrund stand.

Die Umsetzung des Datenschutzes verbleibt damit auch nach zehn Jahren eine zentrale Aufgabe für viele Verwaltungsstellen. Dabei haben es die Stellen viel einfacher, die die Herausforderungen im Sinne eines bürgerorientierten Verwaltungshandelns offen angehen, als diejenigen, die den Schutz der Privatheit der Bürgerinnen und Bürger als lästige Zusatzaufgabe deklarieren.

Technologische Entwicklung

In den letzten zehn Jahren hat die Informationstechnologie die Gesellschaft und damit auch die Verwaltung in einem Ausmass geprägt, das nicht voraussehbar war. Die Möglichkeiten der Informationstechnologien haben den Umgang mit Daten radikal verändert und damit auch den Schutz und die Sicherheit von Daten ins Zentrum gerückt. Die Vernetzung auf der einen Seite und die die Schaffung von Datenverarbeitungssystemen mit unbegrenzten Möglichkeiten der Datenspeicherung und der Datenverwendung auf der anderen Seite haben die Risiken für die betroffenen Personen in Bezug auf den Schutz ihrer Privatheit potenziell erhöht. Der korrekte Umgang mit elektronischen Daten – die Einhaltung der datenschutzrechtlichen Prinzipien – und die Sicherheit der Daten als ein Teilbereich des Datenschutzes gehörten damit zur zentralen Aufgabe in jedem Informatikprojekt. Dabei genügte es nicht mehr, im Pflichtenheft zu erwähnen, die (datenschutz)rechtlichen Vorschriften seien einzuhalten. Vielmehr verlangte die neu ermöglichte intensivere Nutzung von Personendaten nach einem individuellen Datenschutzkonzept für jedes Projekt.

Auch hier zeigte sich, dass die Verwaltungsstellen unterschiedlich auf diese Herausforderungen vorbereitet waren. Soweit den datenschutzrechtlichen Vorgaben in den Projekten von Anfang an der notwendige Stellenwert eingeräumt wurde, konnte auch den neuen Risiken der Informationstechnologie angemessen begegnet werden. Hingegen sind bis heute Grossprojekte ohne die Umsetzung der datenschutzrechtlichen Rahmenbedingungen in Betrieb genommen worden, was angesichts der zu erwartenden weiteren technologi-

schen Entwicklungen für die Bürgerinnen und Bürger zu zunehmenden Risiken führt. So fehlen einerseits klare Rechtsgrundlagen für einzelne Datenbearbeitungen und andererseits Datenschutz- und Sicherheitskonzepte in der Umsetzung. Nur wenn es gelingt, heute diese angemessenen Rahmenbedingungen zu schaffen, wird es auch möglich sein, den neuen Herausforderungen der Technologie, die sich am Horizont bereits abzeichnen (Stichwort: «Ubiquitous Computing»), angemessen zu begegnen.

Gesellschaftliche Entwicklung

Das Verwaltungshandeln ist nicht losgelöst von der gesellschaftlichen und politischen Entwicklung zu betrachten. Dabei hat sich in den letzten Jahren gezeigt, dass sich die Grundrechte – und damit auch das Grundrecht auf Datenschutz – wieder vermehrt ihren Platz in der gesellschaftlichen Diskussion erkämpfen müssen. Einseitige Interessenabwägungen, die nur Kostenargumenten oder Sicherheitsforderungen ihr Gewicht zumessen, stellen längerfristig die Grundrechte in Frage. Gerade die Missachtung des Wertes der Privatheit hat einen verheerenden Charakter. Der Verlust der Privatheit ist ein irreversibler Prozess; Privatheit lässt sich nicht wiederherstellen. Was hingegen eine liberale Gesellschafts- und Rechtsordnung ohne Privatheit bedeutet, hat George Orwell bereits in seinem Buch «1984» vorweggenommen.

Die Achtung der Grundrechte im Rahmen der Umsetzung des Datenschutzes gehört damit auch zu einer vornehmen Pflicht der Verwaltungsstellen. Ihr nachzukommen zeugt von einem angemessenen und bürgerorientierten Verwaltungshandeln.

Rolle des Datenschutzbeauftragten

Im Spannungsfeld zwischen den Anliegen der Bürgerinnen und Bürger sowie der Umsetzung des Datenschutzgesetzes durch die Verwaltung hat der Datenschutzbeauftragte auf Grund der ihm vom Gesetz zugewiesenen Aufgaben für eine wirksame Umsetzung des Datenschutzes zu sorgen. Der Gesetzgeber hat ihm eine unabhängige Rolle zugewiesen, die es ihm ermöglicht, sowohl Beratungs- als auch Kontrollaufgaben wahrzunehmen. Dabei kann er nur Empfehlungen abgeben. Der Gesetzgeber hat sich allerdings nicht zu den Ressourcen für den Datenschutzbeauftragten geäussert, weshalb die Zuteilung der Ressourcen der Verwaltung überlassen ist, die aber «Partei» in diesem Spannungsfeld ist. Weniger als 0,5 % der jährlichen Informatikausgaben von kommunaler und kantonaler Verwaltung beträgt das Budget für den Datenschutzbeauftragten. Deshalb war es für den Datenschutzbeauftragten von Anfang an notwendig, Prioritäten zu setzen und andere wichtige Datenschutzanliegen zu vernachlässigen. Während damit in zahlreichen Bereichen, wo auch der Wille der Verwaltungsstellen für eine angemessene Umsetzung des Datenschutzes vorhanden war, positive Resultate erzielt wurden, konnten in anderen Bereichen, die sehr sensible Daten bearbeiten, bei dieser Ausgangs-

lage nur wenige Ziele des Datenschutzes erreicht werden. Insbesondere gelang es aber trotzdem, durch gezielte Sensibilisierungsmassnahmen auf die Anliegen des Datenschutzes hinzuweisen und bei zahlreichen grossen Projekten Verbesserungen im Sinne des Schutzes der Grundrechte der betroffenen Personen zu erzielen. Ebenso bemühte sich der Datenschutzbeauftragte, allen Anfragen von Bürgerinnen und Bürgern, die sich zunehmend Sorgen über die Bearbeitung ihrer Daten machen, angemessen entgegenzukommen. Einerseits konnten Rechtsauskünfte erteilt werden, oder der Datenschutzbeauftragte schaltete sich vermittelnd zwischen datenbearbeitender Stelle und betroffener Person ein. Andererseits konnten Verwaltungsstellen, die sich mit ihren Anliegen direkt an den Datenschutzbeauftragten wandten, mit Stellungnahmen und Handlungsanleitungen bedient werden. Damit lässt sich insgesamt eine positive Bilanz für die Arbeit des Datenschutzbeauftragten ziehen, was auch durch die Kundenumfrage im Rahmen der Überprüfung der Indikatoren des KEF und des Qualitätsmanagements bestätigt wurde.

Grundlage für Weiterentwicklung

Zehn Jahre Datenschutz im Kanton Zürich haben die Erfahrungen geliefert und zeigen auf, wie die Verwaltung künftig mit den Herausforderungen der Informations- und Kommunikationsgesellschaft umgehen sollte. Die Spannungsfelder und Schwierigkeiten bei der Umsetzung des Datenschutzgesetzes sind ein Hinweis, dass zwar die Zielsetzung des Datenschutzgesetzes und die Prinzipien des Datenschutzes klar formuliert sind, dass hingegen für die Umsetzung in einer sich dynamisch entwickelnden Informations- und Kommunikationsgesellschaft keine angemessenen Instrumente zur Verfügung stehen. Dies hat einerseits damit zu tun, dass die Konzeption des Datenschutzes noch auf der Grundlage einer zentralisierten Grossrechnertechnologie aufgebaut wurde und andererseits noch wenige Erfahrungen bestanden in Bezug auf die Instrumente für die Umsetzung des Datenschutzes.

Die Einführung des Öffentlichkeitsprinzips im Kanton Zürich hat die günstige Ausgangslage geschaffen, auch die Umsetzung des Datenschutzes nochmals zu klären. Richtig verstanden sind nämlich der Zugang zu Informationen und der Nichtzugang oder Schutz von Informationen die Kehrseite derselben Medaille. Die gesamtheitliche Betrachtung der Informationsverarbeitung von der Entstehung einer Information bis zu deren Archivierung, wie dies im Entwurf für ein Informations- und Datenschutzgesetz (IDG) im Kanton Zürich vorgesehen ist, ermöglicht es, nicht nur in den einzelnen Schritten der Informationsverarbeitung die Anliegen des Datenschutzes jeweilen angemessen zu integrieren, sondern auch den Datenschutz in Bezug auf eine Wirkungsorientierung bei seiner Umsetzung anzupassen.

Die aktuellen Herausforderungen für den Datenschutz sind damit auch eine Chance, den Datenschutz für die moderne Verwaltung in der Informations- und Kommunikationsgesellschaft fit zu machen.

Informatiksicherheit ist Teil des Datenschutzes

Die Entwicklung der Informations- und Kommunikationstechnologie prägte den Datenschutz in den letzten zehn Jahren. Ohne eine konsequente Umsetzung der Sicherheitsanliegen in der Informatik ist auch kein effektiver Datenschutz möglich. Der Datenschutzbeauftragte berät deshalb in allen Belangen der Informatiksicherheit sowie des technischen Datenschutzes.

Dass die technologische Entwicklung bei der Umsetzung des Datenschutzes eine wichtige Rolle spielen würde, zeigte sich bereits bei der Inkraftsetzung des Datenschutzgesetzes im Jahre 1995. 1995 gilt als der Beginn des Online-Zeitalters. Mit Windows 95 begann der Siegeszug des Personal Computers (PC) und dessen Vernetzung bis ins Wohnzimmer. Erstmals tauchten so genannte Makroviren auf, welche durch die Vernetzung bereits eine grosse Verbreitung fanden.

In einer von uns aufgelegten Studie von Prof. Dr. Ueli Maurer, ETH Zürich, «Sicherheit in Datennetzen» (publiziert in «Fakten» 1/1996), haben wir bereits Risiken und Lösungsmöglichkeiten vor allem in Bezug auf die Vertraulichkeit, Integrität und Authentizität von Personendaten aufgezeigt. In einer differenzierten Stellungnahme bezüglich der Internetanbindung an das kantonale Netzwerk wiesen wir auf das Fehlen einer kantonsweiten Informationssicherheitsstrategie hin.

1996 hat eine kantonale Arbeitsgruppe, in der wir wesentlich mitwirkten, ein Konzept erarbeitet, welches Richtlinien bezüglich der Sicherheit von Informatiksystemen und -anwendungen in der kantonalen Verwaltung regeln sollte. Dieses sieht vor, dass Daten, Informationen und Programme, die mit Informatiksystemen bearbeitet werden, in drei Sicherheitsstufen (S1–S3) zu klassifizieren sind. Für die Klassifizierung der Daten sowie für die Realisierung der notwendigen Massnahmen ist die einzelne Direktion verantwortlich. Bei der Erarbeitung des Konzeptes zeigte sich, dass die datenschutzrechtliche Anforderung eine gute Basis für eine generelle Sicherheitsstrategie der Verwaltung bilden konnte. Basierend auf diesem Konzept hatte der Regierungsrat einen Auftrag für eine verwaltungsweite Informationssicherheitspolitik erteilt.

Sicherheits-Check

1997 wurden erstmals weltweit Implementierungsfehler einzelner Betriebssysteme systematisch ausgenutzt. Mit dieser neuen Art von Angriffen (z.B. Ping of Death oder WinNuke) wurde es möglich, sowohl aus dem internen Netz wie

auch von einem beliebigen Punkt des Internets einen beliebigen Rechner lahm zu legen (Denial of Service oder kurz DoS-Attacke) oder eine bekannt gewordene Schwachstelle (Vulnerability) auszunutzen. Wegen dieser neuen Gefahren hat der Datenschutzbeauftragte in Zusammenarbeit mit der Finanzkontrolle ausgewählte Netzwerkkomponenten einem Sicherheits-Check unterzogen. Es wurden mit einem bewusst limitierten finanziellen, personellen und zeitlichen Aufwand Systeme mit sensiblen Daten überprüft, um Risiken und Schwachstellen aufzudecken und geeignete Massnahmen aufzulisten.

Richtlinien für die Sicherheit

Basierend auf dem erarbeiteten Sicherheitskonzept setzt die Informatiksicherheitsverordnung (ISV) vom 17. Dezember 1997 Richtlinien für die Umsetzung von Datensicherheitsmassnahmen in der kantonalen Verwaltung. Sie ist auch für Gemeinden verbindlich, sofern sie mit der kantonalen Verwaltung Daten austauschen. Basierend auf der Einteilung in die jeweilige Schutzstufe haben die Amtsstellen einen Plan vorzulegen, der aufzeigt, mit welchen organisatorischen und technischen Massnahmen die Schutzziele pro Sicherheitsstufe erreicht werden sollen. Der Datenschutzbeauftragte unterstützt die Verwaltung bei der Umsetzung der neuen Richtlinien. Ein wesentlicher Punkt der ISV ist die Verpflichtung der Direktionen und Amtsstellen, die Umsetzung und Einhaltung der Sicherheitsmassnahmen regelmässig durch unabhängige Stellen überprüfen zu lassen.

Die Informatiksicherheitsverordnung ISV gab für die bestehenden Informatiksysteme eine Umsetzungsfrist bis zum 31. März 2000 vor. Eine Arbeitsgruppe, der auch der Datenschutzbeauftragte angehörte, übernahm die Aufgabe, den Amtsstellen die notwendigen Hilfsmittel zur Verfügung zu stellen, um eine rasche und effiziente Umsetzung der notwendigen Sicherheitsmassnahmen zu gewährleisten.

In Ergänzung zur ISV hat der Regierungsrat die Richtlinien und Anforderungen an die papiergebundenen Informationen für verbindlich erklärt. Mit diesen Richtlinien liegen weitere praxisbezogene Handlungsanweisungen vor, um die Verwaltungsstellen bei der Umsetzung der Informationssicherheit zu unterstützen.

Der Datenschutzbeauftragte war mitverantwortlich für einen Antrag zur Schaffung von Grundlagen für den Einsatz von digitalen Signaturen in der kantonalen Verwaltung. In einem ersten Schritt sollte in einem Pilotprojekt (Soprano) der Einsatz von digitalen Signaturen in der Verwaltung geprüft werden. Die Erfahrungen aus diesem Pilotprojekt sollten in die Formulierung einer verwaltungsweiten Sicherheitspolitik einfliessen.

Konkrete Sicherheitsprojekte

Der Datenschutzbeauftragte hat mit der Teilnahme am Pilotprojekt Digitale Signatur (Soprano) notwendige Erfahrungen beim Einsatz einer Public-Key-

Infrastruktur gesammelt. Die technische Funktionalität wurde für alle Testfälle unter den Teilnehmern wie auch zwischen den Teilpiloten erfolgreich bewiesen.

Im Anschluss an den früheren Sicherheits-Check von 1997 wurden erneut Teilbereiche der Informatik einer Sicherheitsüberprüfung unterzogen. Trotz der steigenden Anzahl von Gefährdungen war das Resultat äquivalent zum früheren Test. Wir gaben generelle Empfehlungen ab und wiesen einzelne direkt betroffene Amtsstellen darauf hin, wie die wichtigsten Grundschutzmassnahmen in der Informatiksicherheit angemessen zu realisieren seien.

Erstmals stellten wir den Benutzenden des Internets auf unserem Web-Angebot einen so genannten Browser-Test zur Verfügung, der es ermöglichte, die Sicherheit des eigenen PC beim Anschluss an das Internet zu überprüfen. Zudem stellte der Datenschutzbeauftragte Checklisten für das Erstellen von Richtlinien und Weisungen in Bezug auf sichere Informatikarbeitsplätze zur Verfügung. Parallel dazu machten wir mit der Aktion «Sicher ist sicher…» auf die Risiken und Gefahren aufmerksam und leisteten so einen Beitrag zur Verbesserung der Sicherheit des PC-Arbeitsplatzes innerhalb der kantonalen Verwaltung.

Neue Virenattacken

Nachdem der Jahrtausendwechsel praktisch ohne die vorhergesagten Komplikationen überstanden worden war, war der Bedarf an Sicherheit bei den meisten Informatikanwendenden bzw. -betreibenden einstweilen gedeckt. Ein als Liebesbrief getarnter Virus namens «Loveletter» überschwemmte Anfang 2000 ohne Vorwarnung das Internet, so dass nach Schätzungen von Experten weltweit etwa 45 Millionen Computer infiziert wurden.

Angesichts des zunehmenden Gefährdungspotenzials wird die IT-Sicherheit immer bedeutender. Nachdem grundsätzlich die Notwendigkeit einer verlässlichen Sicherheitsinfrastruktur für die Kommunikation im Internet anerkannt worden war, erfolgte die Neupositionierung des Projektes Soprano als Teil des wif!-Programmes und als sicherheitstechnische Grundlage der E-Government-Initiative des Kantons Zürich. Beim Datenschutzbeauftragten kamen Themen wie die «Umleitung von E-Mails», der «externe Zugriff auf Server zu Servicezwecken (RAS)» und selbstverständlich die «Virenbekämpfung» in der IT-Sicherheitsberatung zum Tragen.

Keine Sicherheitsorganisation

Die Datenschutzreviews zeigen immer wieder auf, dass in der Praxis die Sicherheitsmassnahmen der ISV unterschiedlich umgesetzt werden. Einer der Gründe ist das Fehlen einer verwaltungsübergreifenden IT-Sicherheitsorganisation. Ein Antrag an das Strategiegremium (KOSIF) zur Ausarbeitung einer Informatiksicherheitsstrategie wurde mit dem Hinweis abgelehnt, dass diese Zielsetzung auch mit mehr Datenschutzreviews und zusätzlichen Sensibilisie-

rungsmassnahmen zu erreichen sei. Die dafür benötigten Ressourcen wurden jedoch nicht freigegeben.

Beratungsstelle für Informatiksicherheit (BIS)

Durch den Schutz von Informationen und Daten wird eine der wichtigsten Ressourcen der Verwaltungsstellen und öffentlicher Institutionen gesichert. Um deren wachsende Bedürfnisse im Bereich der Informations- und Informatiksicherheit abdecken zu können, hat der Datenschutzbeauftragte die Beratungsstelle für Informatiksicherheit (BIS) aufgebaut. Diese bietet umfassende, praxisorientierte Beratungsleistungen zu allen Themen der Informationssicherheit und des technischen Datenschutzes. Sie fördert das Bewusstsein über die Zusammenhänge von Informatiksicherheit und Datenschutz. Die Beratungsstelle für Informatiksicherheit begleitet schrittweise in allen Phasen eines Projektzyklus, berät in allen Belangen der Informations- und Informatiksicherheit, evaluiert, bewertet und implementiert Sicherheitslösungen und führt Schulungen durch.

Sicherheitsüberprüfungen bei zahlreichen Amtsstellen innerhalb der kantonalen Verwaltung zeigen immer noch einen grossen Handlungsbedarf in Bezug auf einen angemessenen Sicherheitsstandard auf. Einige der erkannten Schwachstellen verletzen nach wie vor die einfachsten Grundsätze der Informatiksicherheit. Dass die zahlreichen Bedrohungen so glimpflich für die Verwaltung abgelaufen sind, war reiner Zufall. Um zukünftigen Angriffen gewachsen zu sein, wurde eine direktionsübergreifend zusammengesetzte Notfallorganisation (IT Security Task Force) als Sofortmassnahme gebildet, welche für die Bewältigung von IT-Sicherheitsattacken zuständig ist. Um Risikosituationen souverän meistern zu können, hat sich die IT Security Task Force als Übergangslösung etabliert, bis eine neue, verwaltungsübergreifende IT-Sicherheitsstrategie diese Aufgabe neu regelt.

Kontrolle der Datenbearbeitungen

Durch den Aufbau eines konsequenten Kontrollkonzepts, der Datenschutzreview, stellt der Datenschutzbeauftragte eine kontinuierliche Überprüfung der Datenbearbeitungen sicher. Der Bedarf an Kontrollen kann indessen nicht im gewünschten Mass befriedigt werden.

Der Datenschutzbeauftragte überwacht die Anwendung der Vorschriften über den Datenschutz (§ 23 litera a Datenschutzgesetz [DSG]). Er kann ungeachtet allfälliger Geheimhaltungspflichten bei öffentlichen Organen oder beauftragten Dritten schriftlich oder mündlich Auskünfte über das Bearbeiten von Personendaten einholen, Einsicht in Unterlagen und Akten nehmen und sich Bearbeitungen vorführen lassen, soweit es für seine Tätigkeit notwendig ist (§ 24 DSG). Gemäss § 11 Absatz 2 Datenschutzverordnung (DSV) sind die verantwortlichen Organe verpflichtet, an der Feststellung des Sachverhaltes mitzuwirken. Diese umfassenden Auskunfts- und Einsichtsbefugnisse des Datenschutzbeauftragten werden durch eine entsprechende Schweigepflicht abgesichert. So sind der Datenschutzbeauftragte und seine Mitarbeitenden hinsichtlich Personendaten, die sie bei ihrer Tätigkeit zur Kenntnis nehmen, zur gleichen Verschwiegenheit verpflichtet wie das bearbeitende Organ (§ 25 Absatz 1 DSG).

Die Datenschutzreview ist das Mittel des Datenschutzbeauftragten, um die Kontrolle der Datenbearbeitungen zu planen und in den Amtsstellen, Kliniken und Spitälern, Schulen sowie Gemeinden anschliessend durchzuführen.

Studien, Überprüfungen und Konzepte

Die Studie «Sicherheit in Datennetzen» von Prof. Dr. Ueli Maurer, ETH Zürich (publiziert in «Fakten» 1/1996), soll den verantwortlichen Organen ermöglichen, ihre Verantwortung im Bereich Datensicherheit wahrzunehmen. Sie liefert die Grundlagen für Entscheidungsträger und Informatikverantwortliche, um im konkreten Einzelfall die angemessenen, dem Stand der Technik entsprechenden Datensicherheitsmassnahmen treffen zu können. Die im Kapitel 3, «Klassifikation von Bedrohungen und grobe Risikobewertung» («Fakten» 1/1996, S. 15 ff.), aufgeführten Überlegungen sind in die konzeptionellen Arbeiten zur Datenschutzreview eingeflossen. Das Konzept wurde 1997 zusammen mit anderen Datenschutzbeauftragten und externen Fachleuten erstellt und umfasste die Planung und Durchführung von rechtlichen, organisatorischen und technischen Kontrollen. Technische Angriffe von aussen und

innen durch einen spezialisierten Dienstleistenden wurden in den Jahren 1997 mit dem Sicherheits-Check ausgewählter Netzwerkkomponenten (Tätigkeitsbericht Nr. 3 [1997], S. 34 ff.) und 1999 mit der Überprüfung ausgewählter Sicherheitskomponenten (Tätigkeitsbericht Nr. 5 [1999], S. 30) durchgeführt. Diese Prüfungen hatten mit verhältnismässig geringem Aufwand gute Resultate erbracht, die anhand von Beispielen aus der Praxis zu einer Bewusstseinsbildung für die entsprechenden Risiken in der Verwaltung geführt haben. Speziell in den Bereichen unsichere Modemzugänge, Verwendung von E-Mail mit vertraulichen Daten und unbefriedigende Passwortqualität sind inzwischen eine umfassende Sensibilisierung und merkliche Verbesserungen erreicht worden.

Ein wesentlicher Punkt der Informatiksicherheitsverordnung vom 17. Dezember 1997 (ISV) ist die Verpflichtung der Direktionen und Amtsstellen, die Umsetzung und Einhaltung der Sicherheitsmassnahmen regelmässig durch unabhängige Stellen überprüfen zu lassen. Als Hilfsmittel zur Umsetzung wurde die Intranet-Applikation «Leitfaden zur Umsetzung der ISV» geschaffen. Allerdings wird in den Stellen der ISV oft nicht der entsprechende Stellenwert beigemessen (siehe auch unsere Auswertung in «Statistik 2: Umsetzungsstand Informatiksicherheitsverordnung» in Tätigkeitsbericht Nr. 9 [2003], S. 30 f.).

Regelmässige Durchführung der Datenschutzreview

Die Datenschutzreview überprüft im Detail rechtliche, organisatorische und technische Aspekte auf Grund von eingereichten Unterlagen und Angaben aus dem Review-Tool. Eine «Prüfung vor Ort» verifiziert die von der Stelle eingereichte Dokumentation und klärt offene Punke ab. Ein Schlussbericht schlägt der Amtsstelle, dem Spital, der Klinik oder der Gemeinde angepasste Handlungsempfehlungen zur Erhöhung oder Beibehaltung des getroffenen Massnahmenniveaus für Datenschutz und Informatiksicherheit vor. Der gesamte Prozess soll zudem für einen wirksamen Datenschutz und angemessene Massnahmen für Informatiksicherheit sensibilisieren.

Die Fokussierung auf die wichtigsten Themen wie Verträge mit Outsourcing-Partnern, Umsetzung der Informatiksicherheitsverordnung, Weisungen an Benützende und Betreibende, Verantwortlichkeiten, Passwortverwendung und Zugriffsdefinitionen in den Jahren 2000–2004 hat klare Defizite in den geprüften Stellen aufgezeigt. Die Resultate wurden laufend in unseren Tätigkeitsberichten publiziert.

Schwachstellen

Die durch den Datenschutzbeauftragten bemängelten Schwachstellen haben oft folgende Ursachen:

- Unklare Abgrenzung zu Dienstleistenden und Outsourcing-Firmen führen zu Lücken im Schutzniveau, da die Umsetzung von IT-Sicherheitsmassnahmen weder geplant noch kontrolliert wird (obwohl die Allgemeinen

Geschäftsbedingungen über die Geheimhaltung, den Datenschutz und die Daten- und Informationssicherheit bei der Erbringung von Informatikdienstleistungen (AGB Sicherheit) in den Verträgen die entsprechende Verantwortung klar zuweisen.

- In den Stellen oder bei den externen Partnern fehlt Fachwissen bezüglich IT-Sicherheit, in wenigen Fällen sogar das Bewusstsein für die Notwendigkeit entsprechender Massnahmen zum Schutz der Systeme und Anwendungen.

- Die Umsetzung der ISV ist in den meisten Fällen nicht erfolgt, da eine Formulierung der Zielsetzungen im Bereich IT-Sicherheit und aus ihnen abgeleitete Massnahmenpläne als zu grosser Aufwand oder teilweise bei Themen wie einer IT-Sicherheitsstrategie als Sache der übergeordneten Organisationseinheit wie zum Beispiel der zuständigen Direktion eingestuft wird.

- Die Prozesse für Implementation und Betrieb von IT-Komponenten sind nicht formalisiert und sinnvoll dokumentiert, oft verlassen sich die Stellen stark auf ihre externen Partner.

- Eine zentrale Unterstützung in den Bereichen IT-Sicherheitsstrategie und IT-Sicherheitsorganisation zur Entlastung der Stellen bezüglich Aufwand und Sachkenntnis ist noch nicht umgesetzt. Sie wurde für die gesamte kantonale Verwaltung von den zuständigen Gremien abgelehnt (Tätigkeitsbericht Nr. 7 [2001], S. 28). Die Informatiksicherheitsverordnung ist als Grundlage zwar vorhanden, aber bis jetzt nicht den veränderten Gegebenheiten in der kantonalen Verwaltung angepasst worden.

Grundschutzmassnahmen getroffen

Positiv aufzuführen ist, dass in den meisten Stellen der Virenschutz auf Client und Server aktuell nachgeführt ist. Mit Hilfe von Managementkonsolen für die Virenschutzpakete können die meisten verantwortlichen Administratoren in mittleren und grösseren Umgebungen die aktuellen Versionen und deren Einsatzzeitpunkt überprüfen. Eine Zugriffsmatrix mit definierten Gruppen als Ansatz zu einem umfassenden Zugriffskonzept ist praktisch überall vorhanden. Der Einsatz einer Softwareverteilung im Sinne von überwachten Betriebsprozessen zur Korrektur von Betriebssystemen und Applikationen («Patch»-Management) beginnt sich auszubreiten und unterstützt damit nachhaltig formalisierte und kontrollierte Prozesse im täglichen IT-Betrieb.

Verbesserung der Datenschutzreview

Das Vorgehen sowie die Durchführung der Datenschutzreview wurden laufend verbessert und den vor allem technischen Anforderungen angepasst. Die Zertifizierung des Datenschutzbeauftragten nach ISO 9001 schliesst die Pla-

nung und Durchführung der Datenschutzreview in den kontinuierlichen Verbesserungsprozess des Datenschutzbeauftragten ein.

Die Zusammenarbeit mit der Finanzkontrolle als weiterer Prüfstelle für IT-Sicherheit im Kanton Zürich ist institutionalisiert und hat sich gut bewährt. Alle beteiligten Stellen profitieren vom erweiterten Umfang der Prüfung und vom reduzierten personellen Aufwand.

Mit der Aufschaltung des Internetangebots Review-Tool ist die Selbstbeurteilung zusammen mit den neu eingebauten Massnahmenempfehlungen und Umsetzungshilfen für alle kantonalen Stellen und die Gemeinden möglich.

Die Datenschutzreview und das Review-Tool sind die geeigneten Mittel für eine konsequente Kontrolle. Eine flächendeckende Überprüfung und eine Wiederholung in vernünftigen Abständen sind indessen erst mit angemessenen Ressourcen möglich.

Schutz vor Überwachung

Besondere Aufmerksamkeit muss der technologischen Entwicklung insofern zukommen, als jede Benutzung von Kommunikationsmitteln Datenspuren hinterlässt. Diese dürfen nicht zur Überwachung verwendet oder zur Erstellung von Persönlichkeitsprofilen verwertet werden.

Als Überwachung wird das gezielte Beobachten und Auswerten von Personen, Objekten oder Abläufen bezeichnet. Der Begriff wird vielseitig verwendet und ist weder positiv noch negativ besetzt. Überwachung kann legal oder rechtswidrig sein. Datenschutzrechtlich relevant ist eine Überwachung nur, wenn dabei Personendaten bearbeitet werden.

Neue Technologien

Schrift, Sprache und Bilder werden zunehmend digitalisiert, gespeichert und verbreitet. Funk- und Ortungstechnologie werden breit eingesetzt. Mit dem Einsatz von RFID-Chips ist es möglich, Daten berührungslos und ohne aktives Zutun auszutauschen. Datenverarbeitungssysteme werden immer kleiner und leistungsfähiger. Ein steigender Anteil unserer Kommunikation wird mittels elektronischer Hilfsmittel bewältigt. Die reine Empfangsmöglichkeit von Information wird häufig durch Interaktionsmöglichkeiten für die Benutzenden ergänzt. Ein steigender Anteil der elektronischen Geräte ist zudem in der Lage, Informationen nicht nur zu empfangen, sondern auch zu senden. So findet auf technischer Ebene gelegentlich auch bei reinem Informationsempfang durch den Benutzenden eine Interaktion statt. Auch Geräte ohne Übermittlungsmöglichkeit speichern gelegentlich Randdaten zur Benutzung. Die Vernetzung vereinfacht die Verknüpfung und Nutzung, aber auch eine oft damit zusammenhängende Änderung des ursprünglichen Bearbeitungszweckes von Daten.

Datenspuren

Die Benutzung elektronischer Hilfsmittel zur Kommunikation und Interaktion ermöglicht die Aufzeichnung derselben sowie von entsprechenden Randdaten. Dabei ist festzuhalten, dass gewisse Aufzeichnungen aus verschiedenen Gründen unabdingbar sind. Die Technik zum Erfassen, Speichern und Verarbeiten von Personendaten einschliesslich elektronischer Hilfsmittel zur Überwachung ist Allgemeingut geworden.

Elektronische Überwachungsmassnahmen

Elektronische Überwachungsmassnahmen zur Erhöhung der Sicherheit liegen im Trend. Durch präventive Überwachung einer Vielzahl von Personen sollen einerseits Straftaten und militärische und politische Bedrohungen frühzeitig erkannt, verunmöglicht oder mindestens in ihrer Zahl oder Auswirkung vermindert werden. Andererseits sollen durch Aufzeichnungen Beteiligte vereinfacht eruiert und die Begehung bewiesen werden können. Die mit jeder Überwachung verbundenen Eingriffe in die Persönlichkeitsrechte der Betroffenen werden jedoch immer seltener gegen die durch die Ergreifung einer Massnahme erhofften Vorteile ernsthaft abgewogen. Ob die vermehrte Überwachung mittels elektronischer Hilfsmittel tatsächlich zu mehr Sicherheit führen oder nur eine Verlagerung der Kriminalität und Bedrohungslage mit sich bringen wird, wird sich noch zeigen müssen.

Der Datenschutzbeauftragte «überwacht» die Anwendung der Vorschriften über den Datenschutz durch öffentliche Organe des Kantons und der Gemeinden (§ 23 lit. a DSG). Wir befassten uns im Laufe der vergangenen Dekade mit verschiedenen konkreten Anwendungsfällen.

Dabei lassen sich drei Phasen, welche die skizzierte technische und gesellschaftliche Entwicklung nochmals aufzeigen, ausmachen: Zwischen 1995 und 1998 standen Randdaten von Telefongesprächen im Vordergrund. Mit der Verbreitung von Computern und dem Internet richtete sich das Augenmerk dann auf die entsprechenden Datenspuren. In den Jahren 2001 bis 2003 wurde schliesslich die optische Überwachung thematisiert.

Randdaten von Telefongesprächen

Die Umstellung von analogen zu digitalen Telefongeräten im Festnetz und die Einführung des GSM-Mobiltelefonnetzes ermöglichen den Benutzenden, einen Teil der Randdaten der Gespräche zu nutzen. So ist die Rufnummer des Anrufenden – sofern von diesem nicht unterdrückt – ersichtlich; via Online-ETV (elektronisches Teilnehmerverzeichnis) oder in telefoninternen Verzeichnissen kann sie mit Zusatzangaben verknüpft werden. Anruflisten gehören zum Standard. In verwaltungseigenen digitalen Telefonzentralen können die Randdaten von Gesprächen aufgezeichnet und ausgewertet werden. Solche Randdaten unterstehen dem strafrechtlich geschützten Fernmeldegeheimnis nicht; es gelten die Datenschutzgesetze sowie die Vorschriften zum Schutz von Arbeitnehmenden.

Unter dem Titel «Datenaufzeichnungen in Telefonanlagen – Absicherung durch technische und organisatorische Massnahmen» befassten wir uns bereits im ersten Tätigkeitsbericht 1995 mit dem Protokollieren von Verbindungsdaten. In den folgenden drei Jahren wurde die Problematik weiter beleuchtet.

Datenspuren beim Internet

Der Versorgungsgrad der Bevölkerung in der Schweiz mit Computern betrug 1997 knapp 40 %. Damals nutzten rund 7 % der Bevölkerung das Internet regelmässig. Sieben Jahre später lag der Versorgungsgrad mit Computern bei rund drei Vierteln, wobei zwei Drittel der Bevölkerung über einen privaten Internetzugang verfügten.

Im Tätigkeitsbericht 1997 sowie in «Fakten» 1/1998 und 2/2000 gingen wir auf die Problematik von Datenspuren beim Einsatz von Computern und beim Gebrauch des Internets ein. Auf Grund dieser Vorarbeiten konnte der Regierungsrat per 1. Januar 2004 die Verordnung über die Nutzung von Internet und E-Mail erlassen. Diese regelt die Nutzung und die Verhinderung des Missbrauchs von Internet und E-Mail mit kantonalen Informatikmitteln durch die Mitarbeitenden des Kantons und seiner unselbständigen Anstalten. Zwischen dem Bedürfnis nach Kontrolle und dem Schutz der Mitarbeitenden wurde eine angemessene Lösung gefunden.

Optische Überwachung

In immer grösserer Zahl werden professionelle optische Überwachungsanlagen eingesetzt; via Internet fernsteuerbare Videokameras mit Bewegungsmelder, aber auch Mobiltelefone mit eingebauter Videokamera ermöglichen auch Privatpersonen Überwachungen und entsprechende Aufzeichnungen. Wir befassten uns mit Videoüberwachungen durch öffentliche Organe und erarbeiteten einen Grundlagenbericht sowie Empfehlungen und Checklisten für den Einsatz von Videoüberwachungen durch öffentliche Organe. Einen besonderen Schwerpunkt bildete die Mitwirkung bei Erarbeitung der «Richtlinien Pilotversuche Videoüberwachung» des Zürcher Verkehrsverbundes ZVV.

Datenschutzfreundliche Technikgestaltung

Da die verschiedenen Datenbearbeitungen (Telefonranddaten, Datenspuren in EDV-Systemen, optische Überwachung) nicht alternativ, sondern kumulativ vorgenommen werden, kommen die in einer späteren Phase bearbeiteten Daten zu denjenigen früherer Phasen hinzu. So steigt die Gesamtmenge der bearbeiteten Personendaten kontinuierlich an. Die Möglichkeiten, Daten miteinander zu verknüpfen und auch Persönlichkeitsprofile zu erstellen, werden damit stetig erweitert; die Gefahr, dass Daten zu einem anderen als dem ursprünglich bestimmten Zweck verwendet werden, steigt. Für betroffene Personen ist immer weniger ersichtlich, welche Daten von wem über sie bearbeitet werden. Dies trifft nicht nur für die von öffentlichen Organen bearbeiteten Daten zu, sondern gilt – es wurde aufgezeigt, dass die entsprechende Technik Allgemeingut geworden ist – in besonderem Masse auch für Bearbeitung von Personendaten durch Private.

Es ist davon auszugehen, dass sich die technischen Errungenschaften in rasantem Tempo weiterentwickeln werden. Neue technologische Entwicklungen dürfen jedoch einem angemessenen Grundrechtsschutz nicht zuwiderlaufen, weshalb datenschutzrechtliche Anliegen im Sinne einer datenschutzfreundlichen Technikgestaltung bereits im Stadium der Entwicklung einfliessen müssen.

Umfassende Beratungen und Stellungnahmen

In verschiedenen Einzelfällen wurden Fragen des Datenschutzes und der Sicherheit in kantonalen und kommunalen Verwaltungen bearbeitet.

KANTON

1. Geltungsbereich des Datenschutzgesetzes

Selbständige öffentliche Anstalt

Die Elektrizitätswerke des Kantons Zürich (EKZ) haben den Datenschutzbeauftragten ersucht, zu verschiedenen Fragen im Zusammenhang mit der Anwendung von Datenschutzvorschriften durch die EKZ Stellung zu nehmen.

Die EKZ sind als öffentliches Organ des Kantons Zürich zu betrachten; das Datenschutzgesetz des Kantons Zürich sowie die Datenschutzverordnung gelten auch für die EKZ. Sie unterstehen auch der Aufsicht des kantonalen Datenschutzbeauftragten. Soweit die EKZ als öffentliches Organ des Kantons Zürich handeln und der Aufsicht des Datenschutzbeauftragten des Kantons Zürich unterstehen, besteht kein Raum für die Anwendung des Bundesgesetzes über den Datenschutz und die Zuständigkeit des Eidgenössischen Datenschutzbeauftragten.

Bei einer Liberalisierung des Strommarktes und einer Änderung der Rahmenbedingungen der EKZ ist eine Neubeurteilung vorzunehmen. Sollten die EKZ in einem abgegrenzten Geschäftsfeld im freien Wettbewerb rein privatrechtlich handeln, zu denken ist hier an Stromkäufe auf dem freien Markt gemäss § 6 Abs. 1 EKZ-Gesetz, käme insoweit das Bundesgesetz über den Datenschutz zur Anwendung.

Die Informatiksicherheitsverordnung des Kantons Zürich gilt für die EKZ als selbständige öffentlichrechtliche Anstalt des Kantons Zürich nicht. Die EKZ unterstehen aber dem kantonalen Gesetz über die Auslagerung von Informatikdienstleistungen. Die Allgemeinen Geschäftsbedingungen über die Geheimhaltung, den Datenschutz und die Daten- und Informationssicherheit bei der Erbringung von Informatikdienstleistungen (AGB Sicherheit) stellen Hilfestellungen bei der Konkretisierung der gesetzlichen Anforderungen dar. Es ist Sache der öffentlichen Organe, für die Umsetzung der gesetzlichen Bestimmungen in Verträgen mit Dritten besorgt zu sein. In diesem Sinne können die AGB Sicherheit auch sinngemäss in den Verträgen mit Dritten integriert werden.

Die Einwohnerkontrollen der zürcherischen Gemeinden sind berechtigt, die EKZ über den Zu- oder Wegzug von mündigen Personen zu orientieren, wobei sich die Angaben zur Person auf das Notwendige (Name, Vorname, Adresse) zu beschränken haben; eine von einer Person im Sinne von § 11 DSG errichtete Datensperre ist in diesem Zusammenhang nicht zu beachten. Darüber hinaus sind öffentliche Organe berechtigt, den EKZ im Einzelfall Personendaten bekannt zu geben, soweit diese Daten zur Erfüllung der öffentlichen Aufgaben der EKZ notwendig sind. Die EKZ dürfen Personendaten – seien es selbst erhobene oder von anderen öffentlichen Organen erhaltene – nur zu dem Zweck bearbeiten, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich ist oder gesetzlich vorgesehen ist.

Soweit eine selbständige öffentliche Anstalt nicht am wirtschaftlichen Wettbewerb teilnimmt, gelten für sie die kantonalen datenschutzrechtlichen Bestimmungen.

2. Personensuche bei gelöschten Firmen

Verletzung des Persönlichkeitsschutzes

Eine Person war bei einer Aktiengesellschaft angestellt und im Handelsregister mit der Einzelprokura eingetragen. Das Unternehmen ging Konkurs und der Anstellungsvertrag wurde vom Konkursamt gekündigt. Obwohl die Aktiengesellschaft gelöscht war, erschien die Person immer noch bei der Personenabfrage im Internet.

Diese Angaben schränkten die Kreditwürdigkeit der betroffenen Person ein, da ständig ein Zusammenhang zum Konkurs hergestellt wurde. Hinzu kam, dass die betroffene Person weder am Unternehmen beteiligt noch in der Geschäftsleitung oder im Verwaltungsrat tätig gewesen war.

Das Handelsregister ist öffentlich. Eine Personensuche entspricht nicht dem gesetzlichen Zweck des Handelsregisters. Wenn aus Sicht des Datenschutzes nicht ersichtlich ist, warum im Handelsregister

die Suche nach Personen möglich sein muss, so ist erst recht keine Begründung ersichtlich, warum auch gelöschte Personeneinträge per Personensuche abrufbar bleiben müssen.

Muss aus Beweisgründen diese Information noch zugänglich sein, kann hierfür die Firmensuche respektive die Bestellung eines Handelsregisterauszugs in Anspruch genommen werden.

Wir baten das Handelsregisteramt und die Direktion der Justiz und des Innern um eine Stellungnahme. Das Handelsregisteramt wies darauf hin, dass eine Löschung nicht eine definitive sein müsse, da eine Gesellschaft jederzeit (auch nach dem Konkursverfahren) zum Zwecke der Fortführung wieder eingetragen werden könne, wenn z.B. der Gläubiger glaubhaft mache, dass die Gesellschaft noch oder wieder über Aktiven verfüge, bzw. Prozesse anhängig gemacht werden. Ferner diene gerade die Personensuche auch der Verringerung der Wirtschaftskriminalität, indem Verknüpfungen über die verschiedenen Gesellschaften offenbar würden. Dies gelte auch bei gelöschten Gesellschaften. Vom Handelsregister würde eine schützende Wirkung ausgehen, wenn ersichtlich werde, dass eine Person immer wieder in einer konkursiten Gesellschaft sei bzw. gewesen sei. Ansonsten hätte niemand etwas zu befürchten. Nach Ansicht des Handelsregisteramtes würde das Verheimlichen den Sinn des Handelsregisters pervertieren. Man müsste die Publizität von gelöschten Firmen überhaupt verbieten, denn eine Differenzierung zwischen den verschiedenen Rechtsformen (Einzelfirmen/AG) wäre unzulässig. Bei den Rechtsformen fände man nämlich den Inhaber (auch einer gelöschten Firma) ohne die Personensuche, weil der Name von Gesetzes wegen Bestandteil des Firmennamens sei. Die Personensuche diene demzufolge dem vom Handelsregister angestrebten Gläubigerschutz. Die Argumentation, dass niemand etwas befürchten müsse, wenn er nichts zu verheimlichen habe, greift zu kurz: Es kann nicht sein, dass eine im Verhältnis zu den tatsächlichen Wirtschaftskriminellen grosse Anzahl Personen, die nichts zu verheimlichen hat, trotzdem unter den Folgen dieser Abrufbarkeit leidet. In dem betreffenden Fall hatte die betroffene Person nichts zu verbergen. Trotzdem wurde ständig ein Zusammenhang zwischen der Kreditwürdigkeit dieser Person und dem Konkurs des Unternehmens, wo sie angestellt gewesen war, hergestellt. Das wirtschaftliche Fortkommen dieser Person war gefährdet. Das private Interesse einer grossen Anzahl von unbescholtenen Bürgern am Schutz ihrer Privatsphäre wiegt in diesem Fall schwerer als das Interesse des Staates, in relativ wenigen Fällen die Möglichkeit zu haben, Wirtschaftskriminalität vermindern zu können.

Insofern dies überhaupt eine Zielsetzung des Handelsregisters gemäss den einschlägigen Bundesgesetzen sein soll, darf sie die berechtigten Anliegen des Persönlichkeitsschutzes nicht ignorieren. Wenn das Handelsregisteramt diesbezüglich anderer Meinung ist und die Personensuche zum Zwecke der Verminderung von Wirtschaftskriminalität anbieten will, muss jedoch wenigstens der Grundsatz der Verhältnismässigkeit (§ 4 Abs. 3 DSG) eingehalten werden. Wenn es sich beim abgefragten, gelöschten Personeneintrag um eine Person handelt, welche weder am Unternehmen beteiligt noch in der Geschäftsleitung oder im Verwaltungsrat eines Unternehmens tätig war, ist nicht ersichtlich, wie die Abfragemöglichkeit Wirtschaftskriminalität vermindern soll.

Auch Einträge in öffentlichen Registern wie dem Handelsregister haben sich an das Prinzip der Verhältnismässigkeit zu halten. Dies gilt insbesondere auch bei der Abrufbarkeit von Daten über das Internet.

3. Sektorielle Personenidentifikatoren

Fehlende verfassungsrechtliche Grundlage

Das Bundesgesetz über die Harmonisierung der Einwohnerregister sah ursprünglich die Schaffung eines einheitlichen eidgenössischen Personenidentifikators vor. Dieser Vorschlag wurde in der Vernehmlassung abgelehnt und auch die Vereinigung der Schweizerischen Datenschutzbeauftragten hat sich dagegen ausgesprochen (Resolution vom 9. April 2003 «Der Bürger im E-Government darf nicht zur Nummer werden»).

In der Folge entstand der Vorschlag, anstelle eines einheitlichen Personenidentifikators ein Modell mit sektoriellen Personenidentifikatoren zu schaffen. Der Datenschutzbeauftragte nahm zum Bundesgesetz über die sektoriellen Personenidentifikatoren im Rahmen des Vernehmlassungsverfahrens kantonsinterne Stellung.

Das Grundrecht auf Datenschutz verlangt, dass mit eidgenössischen Personenidentifikatoren Schutzmassnahmen getroffen werden, welche die mit dem Gesetzesentwurf entstehenden Risiken für die Persönlichkeitsrechte durch die erleichterten Abgleichsmöglichkeiten einschränken. Der vorgesehene eidgenössische Personenidentifikator mit Sektoraufteilungen enthält die verlangten Schutzmassnahmen jedoch nicht. Dem Bund fehlt für seine Einführung zudem die erforderliche verfassungsrechtliche Grundlage.

Der Datenschutzbeauftragte gelangte zum Schluss, dass auch das Modell der sektoriellen Personenidentifikatoren weiterhin die Schaffung von Personenidentifikatoren zu administrativen Zwecken vorsieht. Insofern besteht kein Unterschied zum bereits früher abgelehnten einheitlichen Personenidentifikator. Der Datenschutzbe-

auftragte begrüsst jedoch ausdrücklich weiterhin die Schaffung eines Personenidentifikators zu rein statistischen Zwecken, welche im Hinblick auf die Volkszählung 2010 eine zulässige Lösung darstellt.

Der vorgesehene eidgenössische Personenidentifikator mit Sektoraufteilungen enthält die vom Grundrecht auf Datenschutz verlangten Schutzmassnahmen für die Persönlichkeitsrechte der betroffenen Personen nicht.

4. Kundendaten im Konkursverfahren

Verschiedene Formen der Verwertung

Der Konkursrichter verhängte über eine Tanzschule den Konkurs. Der Nachmieter der Liegenschaft, in welcher sich die Tanzschule befunden hatte, gelangte mit der Bitte an den Konkursrichter, diesem den Kundenstamm der Tanzschule zu überlassen. Das Konkursamt fragte uns an, unter welchen Bedingungen der Kundenstamm im Rahmen der konkursamtlichen Versteigerung verwertet werden könne.

Wir verwiesen auf ein Gutachten der Datenschutzbeauftragten des Kantons Basel-Landschaft vom 27. Juni 2000. Darin wird ausgeführt, dass eine Verwertung von Aktiven aus der Konkursmasse zu den Aufgaben des Konkursamts gehört, weshalb auch die konkursamtliche Verwertung von Kundendateien dazugehören kann. Die Bekanntgabe von Kundendaten aus einer Konkursmasse erscheint somit zulässig.

Bei der Verhältnismässigkeit ist sodann ausschlaggebend, wie stark das ursprüngliche Vertragsverhältnis von einem besonderen Vertrauensverhältnis geprägt war. Je grösser dieses war, desto eher ist eine Datenbekanntgabe einzuschränken. Bei einem unqualifizierten Vertragsverhältnis wie beispielsweise zwischen einem Versandhaus und seiner Kundschaft ist eine Bekanntgabe der Kundendaten (Namen und Adressen) auch ohne Zustimmung der Kundschaft durch die Aufgabenerfüllung des Konkursamtes möglich. Zum gleichen Ergebnis gelangten wir beim Kundenstamm einer Tanzschule.

Bei einem qualifizierten Vertragsverhältnis wird grundsätzlich die Zustimmung der betroffenen Personen benötigt. Zwischen dem konkursiten Unternehmen und seiner Kundschaft bestand ein von einem besonderen Vertrauen abhängiges Vertragsverhältnis. Die betroffene Person muss demnach grundsätzlich nicht damit rechnen, dass jemand anders, zu dem sie kein Vertrauen hat oder kein Vertrauen haben muss, ihre Daten erfährt, weshalb ihre Zustimmung zur Datenbekanntgabe erforderlich ist. Bei der Form der Zustimmung ist sodann weiter zu differenzieren, welche Daten bekannt zu geben sind.

Bei wenig heiklen Daten genügt eine Anzeige mit einer angemessenen Widerspruchsfrist. Dies ist beispielsweise bei der Bekanntgabe der Bankbeziehung bei der Übernahme einer Bank im Rahmen einer Fusion der Fall. Bei heiklen Daten ist jedoch eine ausdrückliche vorgängige Zustimmung erforderlich. Dies gilt für die Bekanntgabe von Gesundheitsdaten und selbstverständlich in sämtlichen Fällen, welche von speziellen Geheimnissen betroffen sind (Patientengeheimnis, Anwaltsgeheimnis, Amtsgeheimnis).

Das Konkursamt darf im Rahmen seiner Aufgabenerfüllung Kundendateien verwerten. Je nach der Qualifikation des ursprünglichen Kundenverhältnisses sind unterschiedliche Formen der Verwertung zu beachten.

5. Austausch von Steuerdaten

Fehlende gesetzliche Grundlagen für Datendrehscheibe

Im Rahmen der Datendrehscheibe GeKaGe (Gebäudedaten für Kanton und Gemeinden) befassten wir uns mit einer weiteren Problematik, welche die Einspeisung und den Transport von Personendaten betraf.

Das System GeKaGe wurde ursprünglich für den Austausch von Informationen über Gebäude aufgebaut. Durch definierte Schnittstellen sollen Gebäudedaten über dieses Transportsystem effizient ausgetauscht werden können. Mittlerweile sind aber die Funktionalitäten der Plattform GeKaGe erweitert worden. Einerseits soll die Plattform neuerdings für den Datenaustausch zwischen Gemeindesteuerämtern und kantonalem Steueramt verwendet werden. Andererseits soll die Abteilung Direkte Bundessteuer des kantonalen Steueramtes Personendaten in den Datenmarkt GeKaGe einspeisen. Dabei handelt es sich um Name, Vorname, AHV-Nummer, Handelsregisternummer, Zivilstand, Geburts- bzw. Todesdatum, Staatszugehörigkeit, Heimatort, Beruf, Art der Steuerpflicht, Strassen- und Hausnummer, weitere Angaben zu Adresse und Wohnort und Telefonnummer. Im Datenmarkt GeKaGe werden diese Daten mit den Liegenschafts- und Gebäudedaten verknüpft.

Personenbezogene Daten dürfen zu einem Zweck bearbeitet werden, der für die betroffenen Personen transparent ist, indem er gesetzlich vorgesehen wird. Dieses Zweckbindungsgebot wird durchbrochen, wenn Daten ohne Rechtsgrundlage in einer Datendrehscheibe zur Verfügung gestellt und oder mit andern Daten kombiniert werden. Diese Kombination führt zu einer andern «Eingriffsqualität» bezüglich Privatsphäre. Ferner wird durch die Lieferung der Personendaten das Steuergeheimnis tangiert.

Bereits vor längerer Zeit haben wir festgehalten (siehe Tätigkeitsbericht Nr. 7 [2001], S. 36), dass für die Datenbearbeitungen im System GeKaGe Rechtsgrundlagen fehlen. Der Regierungsrat hat im Januar 2001 die Baudirektion beauftragt, Rechtsgrundlagen für die leistungsfähigen Informationssysteme im Bereich der Raumdaten auszuarbeiten. Ein diesbezüglicher Entwurf liegt bis heute nicht vor.

Aus dieser rechtsstaatlichen Sicht ist das System GeKaGe nicht ausreichend. Wir empfahlen dem Steueramt deshalb, auf die Verwendung des GeKaGe-Systems zu verzichten bzw. insbesondere keine Daten in GeKaGe einzuspeisen. Für die Vernetzung der Steuerämter von Kanton und Gemeinden empfahlen wir, in der Steuergesetzgebung transparente Rechtsgrundlagen mit einer klaren Zweckbestimmung für den Datenaustausch zu schaffen.

In der Folge wurde vom kantonalen Steueramt und vom Amt für Raumordnung und Vermessung ein Rechtsgutachten in Auftrag gegeben.

Der Gutachter kam zum Schluss, dass Personendaten, die allgemein zugänglich und offenkundig sind, nicht unter das Steuergeheimnis fallen. Dabei handelt es sich beispielsweise um die Tatsache, ob eine Person steuerpflichtig ist. Diese Tatsache ergibt sich aus der steuergesetzlichen Regelung der Steuerpflicht. Die diesbezüglichen wesentlichen Voraussetzungen wie Wohnsitz oder Aufenthalt im Kanton ergeben sich aus Telefonbüchern, tatsächlichen Beobachtungen oder – bei juristischen Personen – aus dem Handelsregisterauszug. Anders ist die Sachlage allerdings bei Personen, welche nicht im Telefonbuch auffindbar sind oder bei der Einwohnerkontrolle eine Datensperre errichtet haben. In solchen Fällen kann man nicht mehr von offenkundigen Tatsachen sprechen. Die Datensperre wirkt aber nicht gegenüber staatlichen Behörden, wenn diese über eine Rechtsgrundlage für die Datenbeschaffung verfügen. Die weiteren Angaben wie Geschlecht, Zivilstand, Geburts- oder Todesdatum, Ledigenname, Staatszugehörigkeit, Heimatort oder Beruf sind aber keinesfalls allgemein zugänglich und fallen demzufolge unter das Steuergeheimnis. Daraus folgt, dass die Datenbekanntgabe in den Datenmarkt GeKaGe eines Gesetzes im formellen Sinne bedarf. In diesem muss geregelt werden, wer welche Daten zu welchem Zweck abrufen darf.

Art. 39a Steuerharmonisierungsgesetz regelt die Datenweitergabe unter den Steuerbehörden. Auf Grund dieser Bestimmung ist gegen den Datentransport zwischen kantonalen und kommunalen Steuerbehörden mittels GeKaGe nichts einzuwenden.

Das Gutachten klärte auch die Frage, ob der Betrieb GeKaGe auf Grund seines verfassungswidrigen Zustandes eingestellt werden muss, bis eine Gesetzesgrundlage in Kraft ist. Das Gutachten verweist aber diesbezüglich auf einen bislang unveröffentlichten Bundesgerichtsentscheid vom 26. Mai 2003 (2P.225/2002), in welchem das Gericht festhält, dass verfassungswidrige Zustände bestehen bleiben dürften, wenn der Gesetzgeber aktiv darum bemüht sei, den bestehenden Zustand zu verbessern und eine verfassungskonforme Lösung auszuarbeiten.

Diesen Schlussfolgerungen des Gutachtens konnten wir uns weitgehend anschliessen. Das Einspeisen von Personendaten in den Datenmarkt GeKaGe seitens der Steuerämter bedarf einer klaren gesetzlichen Grundlage, welche noch geschaffen werden muss. Ebenso ist für den Gesamtbetrieb von GeKaGe eine entsprechende Rechtsgrundlage zu schaffen.

Für den Betrieb einer Datendrehscheibe, welche hohe Risiken für die Persönlichkeitsrechte der betroffenen Personen aufweist, sind entsprechende Rechtsgrundlagen notwendig.

6. Erhebung von Steuerdaten von Drittpersonen

Amtshilfe durch die Stipendienbehörde

Wir hatten zu beurteilen, ob die Abteilung Stipendien für die Berechnung des Stipendienanspruchs Auskunft über die Steuerdaten der Eltern des Gesuchstellenden erhalten darf. Die Eltern widersetzten sich dem Begehren. Sie machten geltend, eine Datensperre errichtet zu haben.

§ 19 Bildungsgesetz lautet: «Die für das Bildungswesen zuständige Direktion entscheidet über die Ausrichtung und Rückforderung von Ausbildungsbeiträgen. Die Verwaltungs- und Rechtspflegebehörden des Kantons und der Gemeinden haben der zuständigen Behörde die zur Prüfung der Beitragsgesuche erforderlichen Auskünfte unentgeltlich zu erteilen.»

Die Stipendienbehörde kann somit unter gewissen Umständen direkt bei den Steuerbehörden um Auskunft über die Steuerzahlen von Eltern von Gesuchstellenden ersuchen. Dies unter der Voraussetzung, dass die Auskunft für die Aufgabenerfüllung nötig ist und nicht anders beschafft werden kann. In diesem Fall der Amtshilfe ist das Einverständnis der betroffenen Personen nicht nötig.

Wir empfahlen der Abteilung Stipendien ein schrittweises Vorgehen, wobei vorerst der Gesuchstellende zur Mitwirkung verpflichtet wird. Führt dies zu keinem Ergebnis, werden die Eltern angeschrieben und um Auskunft gebeten. Dabei wird ihnen erläutert, dass im Wei-

gerungsfall als letzter Schritt die Amtshilfe in Anspruch genommen werden kann und die zur Stipendienberechnung benötigten Steuerzahlen direkt beim Steueramt erfragt werden. Wird dieses schrittweise Vorgehen eingehalten, welches den Anforderungen an die Verhältnismässigkeit des Verwaltungshandelns entspricht, ist eine amtshilfeweise Bekanntgabe durch das Steueramt zulässig.

Gemäss § 11 Abs. 1 Datenschutzgesetz (DSG) kann die betroffene Person die Bekanntgabe ihrer Daten sperren lassen. Die Möglichkeit der Datensperre beschränkt sich jedoch auf die Bekanntgabe von Daten an private Personen oder Organisationen. Die Bekanntgabe von Steuerdaten durch das Steueramt an die Stipendienbehörde richtet sich nach § 8 Abs. 1 DSG, wonach öffentliche Organe Personendaten bekannt geben dürfen, wenn die Daten für den Empfänger im Einzelfall zur Erfüllung seiner öffentlichen Aufgaben notwendig sind. Dabei ist im Rahmen der Amtshilfe einzig zu prüfen, ob die Stipendienbehörde die vom Steueramt verlangten Angaben zur Erfüllung ihrer gesetzlichen Aufgaben im konkreten Fall tatsächlich benötigt oder ob diese Angaben nicht auf einem anderen Weg, namentlich durch Nachfragen bei der betroffenen Person, beschafft werden können. Somit ist eine allfällige Datensperre gemäss § 11 Abs. 1 DSG bei einer Auskunfterteilung des Steueramts an die Stipendienbehörde nicht zu beachten.

Die Stipendienbehörde kann zur Berechnung des Stipendienanspruchs Auskunft über die Steuerdaten der Eltern des Gesuchstellenden erhalten, wenn dies zur Aufgabenerfüllung unabdingbar ist. Eine Auskunft ist im Rahmen der Amtshilfe als letztes Mittel zulässig.

7. Fahren ohne gültigen Fahrausweis

Erarbeitung von Datenschutzrichtlinien

Der Zürcher Verkehrsverbund ZVV bat uns um datenschutzrechtliche Beratung beim Projekt «Fahren ohne gültigen Fahrausweis». Neu sollen die Personalien jedes Schwarzfahrers – auch bei sofortiger Barzahlung – erhoben werden. Je öfter eine Person ohne gültigen Fahrausweis innerhalb einer bestimmten Zeitspanne angehalten wird, desto höher fällt der entsprechende Zuschlag aus. Die strafrechtliche Verfolgung bleibt vorbehalten. Alle Schwarzfahrer sollten dadurch gleich behandelt werden.

Hintergrund waren hohe Einnahmeverluste durch Schwarzfahrer und sinkende Zahlungsmoral.

Wir kamen zum Schluss, dass die gesetzlichen Grundlagen im Transportgesetz für eine Registrierung genügten, und berieten den ZVV betreffend Umsetzung der datenschutzrechtlichen Grundsätze. Der ZVV setzte die Empfehlungen entsprechend um.

Die Registrierung von allen Schwarzfahrern ist auf Grund des Transportgesetzes rechtmässig. Die datenschutzrechtlichen Rahmenbedingungen sind zu beachten.

8. Verfahren zur Adoption

Datenerhebung im Gesuchsdossier

Eine Privatperson ersuchte uns um Überprüfung des Gesuchsdossiers der Zentralbehörde Adoption, welches nebst der Anmeldung einen Antrag auf Bewilligung zur Aufnahme eines Kindes zwecks Adoption sowie mehrere Beilagen (Personalien, Beweggründe für Adoption, Arztzeugnis etc.) enthält. Einerseits wurden wir gebeten abzuklären, wer zu welchem Zweck das einzureichende Dossier erhält. Andererseits wurde im Rahmen des beizulegenden Arztzeugnisses bemängelt, es fehle diesbezüglich an der gesetzlich erforderlichen Entbindung des Arztes vom Arztgeheimnis.

Den Unterlagen war zu entnehmen, dass das gesamte Dossier bei der Zentralbehörde Adoption des Amtes Jugend und Berufsberatung des Kantons Zürich einzureichen sei. Nicht klar ersichtlich war jedoch, wie das Verfahren innerhalb der Zentralbehörde Adoption weiter verläuft, welche Personen zum Dossier Zugang haben, wer am Entscheid beteiligt ist und was mit dem Gesuchsdossier bis zum Abschluss des Verfahrens beziehungsweise danach geschieht.

Das datenschutzrechtliche Prinzip der Zweckbindung bedeutet, dass die eingereichten Unterlagen nur zur Beurteilung des Adoptionsgesuchs verwendet werden dürfen. Soweit Personendaten systematisch, namentlich mit Fragebogen, erhoben werden, sind Rechtsgrundlage und Zweck der Bearbeitung anzugeben. Im Rahmen der Transparenz sollten im Gesuchsdossier nähere Angaben zu diesem Punkt gemacht werden, da solche auf den einzureichenden Fragebögen fehlen.

Künftige Adoptiveltern werden verpflichtet, ein ärztliches Zeugnis durch einen von ihnen bestimmten Arzt ausstellen zu lassen. Indem die Gesuchstel-

lenden das Arztzeugnis dem Dossier beilegen, willigen diese als berechtigte Personen in die Offenbarung des Arztgeheimnisses gemäss Art. 321 Abs. 2 des Strafgesetzbuches ein. Die Rechtfertigung der Offenbarung des Geheimnisses liegt im vorliegenden Fall also nicht in der Entbindung des Arztes vom Arztgeheimnis durch die Gesundheitsdirektion, sondern in der Einwilligung durch die Betroffenen selbst.

Bezüglich Verhältnismässigkeit hat die Durchsicht des umfangreichen Gesuchsdossiers ergeben, dass die gestellten Fragen für die Erfüllung der Aufgaben der Zentralbehörde Adoption insgesamt als geeignet und erforderlich erscheinen.

Bei der Bearbeitung von Daten mittels Gesuchsformularen ist darauf zu achten, dass Rechtsgrundlagen und Zweck der Datenerhebung für die betroffene Person transparent sind.

GEMEINDEN

9. Protokolle von Zweckverbänden
Weitergabe an Trägergemeinden

Ein Zweckverband fragte uns an, ob die Protokolle der Heimkommission, falls sie Personendaten enthielten, an die Trägergemeinden des Zweckverbands verschickt werden dürften.

Die Zweckverbandsstatuten regeln die Frage des Versands der Protokolle der Heimkommission nicht. Ausschlaggebend ist die Verhältnismässigkeit. Es ist zu beurteilen, ob die Personendaten, welche in den Protokollen der Heimkommission enthalten sind, von den Verbandsgemeinden zu deren Aufgabenerfüllung benötigt werden. Dazu ist die Kenntnis der Aufgabenteilung zwischen Verbandsgemeinden und Zweckverband sowie der entsprechenden Verantwortlichkeiten nötig.

Werden die Protokolle den Verbandsgemeinden sodann zugestellt, ist der Zugang auf diejenigen Mitarbeitenden der Verbandsgemeinden zu beschränken, welche die Informationen zur Aufgabenerfüllung benötigen. Das Protokoll ist demnach zum Beispiel durch den Gesundheitsvorstand oder den Gesundheitssekretär aufzubewahren oder durch denjenigen Gemeinderat, welcher das Thema Alters- und Pflegeheim betreut. Die Protokolle dürfen selbstverständlich nicht sämtlichen Mitarbeitenden der Gemeindekanzlei zur Einsicht freistehen.

Zu erwähnen bleibt, dass ein Mitglied des jeweiligen Gemeinderates in seiner Funktion als Mitglied der Heimkommission auf jeden Fall Anspruch auf ein Protokoll hat. Fallen die Funktionen der Mitgliedschaft in der Heimkommission mit denjenigen des Ressortvorstands für den Bereich der Alters- und Pflegeheime in der betreffenden Gemeinde zusammen, erübrigt sich eine Zustellung des Protokolls an die Gemeinde.

Protokolle von Heimkommissionen werden den Trägergemeinden des Zweckverbands zur Verfügung gestellt, falls diese die Angaben für die Aufgabenerfüllung der Verbandsgemeinden tatsächlich benötigen. Der Zugang zu den Protokollen ist in den Verbandsgemeinden zu beschränken.

10. Lohndaten für Heimkommission
Keine generelle Offenlegung

Ein Zweckverband fragte uns an, ob den Mitgliedern der Heimkommission die Löhne der Mitarbeitenden offen gelegt werden dürften.

In den Zweckverbandsstatuten fehlt eine entsprechende Regelung. Festgelegt ist, aus wie vielen Mitgliedern sich die Heimkommission zusammensetzt, wie viele aus jeder Verbandsgemeinde stammen, dass je eines der Verbandsgemeinde-Mitglieder dem jeweiligen Gemeinderat angehören muss, meist auch, dass die Heim-Kommission den Stellenplan genehmigt und ein Besoldungsregulativ erlässt. Fest steht ebenfalls, dass die Heimleitung das Personal einstellt.

Entscheidend ist, ob neben dem Präsidenten der Heimkommission und der Ressortleitung Personal die übrigen Heimkommissionsmitglieder die Lohndaten sämtlicher Mitarbeitenden zu ihrer Aufgabenerfüllung benötigen. Das scheint meist nicht zuzutreffen, ausser die einzelnen Heimkommissionsmitglieder sind die Vorgesetzten von entsprechenden Abteilungen des Alters- und Pflegeheims und haben in dieser Funktion Einsicht in die entsprechenden Mitarbeiterdossiers. Ist dies nicht der Fall, ist eine Bekanntgabe unverhältnismässig, da die Lohndaten zur Aufgabenerfüllung der übrigen Mitglie-

der der Heimkommission weder geeignet noch erforderlich sind.

Lohndaten von Mitarbeitenden eines Alters- und Pflegeheims sind nur den Vorgesetzten sowie denjenigen Mitgliedern der Heimkommission zugänglich, welche diese zur Aufgabenerfüllung unbedingt benötigen.

11. Aufsichtstätigkeit

Aufsichtsbeschwerden gegen einzelne Gemeinden

Im Berichtsjahr hatte der Datenschutzbeauftragte erstmals Aufsichtsbeschwerden gegen zwei Gemeinden zu beurteilen. Es ging um die Beratungstätigkeit der kommunalen Datenaufsichtsstellen in zwei konkreten Fällen. Auf Grund des vorgelegten Sachverhaltes und dessen Beurteilung durch die kommunalen Aufsichtsstellen waren keine Anhaltspunkte für eine nicht korrekte Bearbeitung der Eingaben der betroffenen Personen festzustellen. Beide Beschwerden wurden demnach abgewiesen.

Der kantonale Datenschutzbeauftragte trägt auch die Oberaufsicht über kommunale Datenschutzstellen und behandelt diesbezügliche Aufsichtsbeschwerden.

12. Keine Registrierung von Auskunftsgesuchen

Datenbearbeitung der Einwohnerkontrolle

Eine Privatperson erkundigte sich, ob die Einwohnerkontrolle registrieren müsse, wer über welche Person Auskünfte verlangt und worauf sich die Anfrage bezieht. Zudem wollte sie wissen, ob – vorausgesetzt, die Anfragen werden registriert – ein Anspruch auf Auskunftserteilung bestehe.

Eine generelle Registrierung von anfragenden Personen und entsprechenden Gesuchen erfordert eine gesetzliche Grundlage. Eine solche ist nicht vorhanden. Daraus folgt, dass die Einwohnerkontrolle weder registrieren darf, wer ein Auskunftsgesuch gemäss § 9 DSG gestellt hat, noch, worüber Auskunft verlangt wurde. Folglich kann auch keine Auskunft darüber erteilt werden, wer welche Informationen verlangt hat.

Auch bei einer Sperrung der Bekanntgabe von Daten an private Personen und Organisationen muss die Einwohnerkontrolle grundsätzlich weder registrieren, wer ein Auskunftsgesuch gestellt hat, noch, worüber Auskunft verlangt wurde.

Einzig bei der Durchbrechung der Datensperre (§ 11 Abs. 2 DSG) hat sie unter Umständen zur Gewährung des rechtlichen Gehörs bekannt zu geben, wer welche Auskunft verlangt hat.

Die Einwohnerkontrolle darf weder registrieren, wer ein Auskunftsgesuch gestellt hat, noch, worüber Auskunft verlangt wurde. Eine Ausnahme ist einzig bei der Durchbrechung der Datensperre im Rahmen der Gewährung des rechtlichen Gehörs möglich.

FORSCHUNG UND STATISTIK

13. Forschungsprojekt über Jugendliche

Fragen der Einwilligung

Das Forschungsprojekt «Jugendliche aus dem Balkan – eine Herausforderung für die Zürcher Jugendhilfe?» des Schweizerischen Nationalfonds sah vor, Jugendliche mit Herkunft aus dem Westbalkan mündlich zu ihren Erfahrungen mit der Zürcher Jugendhilfe zu befragen. Der Zugang zu den Jugendlichen sollte über einzelne Bezirks- und Jugendsekretariate und Jugendanwaltschaften geschaffen werden. Da die Jugendlichen noch nicht 18 Jahre alt waren, stellte sich die Frage nach der Notwendigkeit der Einwilligung der Erziehungsberechtigten.

Zum einen fragte sich, ob die Jugendanwaltschaften, die Bezirks- und Jugendsekretariate die Adressen der Jugendlichen an die Forschungsstelle weitergeben dürfen, ohne das Einverständnis der Jugendlichen oder der Erziehungsberechtigten einzuholen.

Die Bearbeitung von Personendaten zu Forschungszwecken erfolgt gestützt auf § 12 DSG unter wesentlich erleichterten Voraussetzungen, da die Anonymisierung der Daten sowie die Publikation der Ergebnisse ohne Rückschlüsse auf die betroffenen Personen durch die forschende Stelle vorgängig mittels verbindlicher Vereinbarung garantiert werden müssen.

Somit können die angefragten Jugendanwaltschaften, Bezirks- und Jugendsekretariate die entsprechenden Adressen ohne vorgängige Einwilligung der betroffenen Jugendlichen oder deren Eltern bekannt geben.

Zum andern war zu prüfen, ob mit minderjährigen Personen mündliche Befragungen zu Forschungszwecken durchgeführt werden dürfen, ohne vorgängig das Einverständnis der Erzie-

hungsberechtigten einholen zu müssen.

Das informationelle Selbstbestimmungsrecht ist ein verfassungsmässiges Recht. Es gilt auch für Jugendliche unter 18 Jahren, soweit sie urteilsfähig sind. Diese können Rechte ausüben, die ihnen um ihrer Persönlichkeit willen zustehen (Art. 19 Abs. 2 Zivilgesetzbuch, ZGB). Bei Kindern und Jugendlichen ist von einer Urteilsfähigkeit für die Befragung zum erwähnten Forschungszweck ab ungefähr 14 Jahren auszugehen. Diese müssen sich als betroffene Personen selbstverständlich mit der Befragung einverstanden erklären. Das Forschungsprojekt ist ihnen altersentsprechend zu erklären. Dabei sind sie ausdrücklich darauf aufmerksam zu machen, dass eine Teilnahme freiwillig ist. Das Einverständnis der Erziehungsberechtigten ist in diesem Fall nicht notwendig. Eine entsprechende Information der Eltern im Rahmen der notwendigen Erklärungen an die Jugendlichen in Form eines Beiblattes erscheint jedoch zumindest sinnvoll.

Verwaltungsstellen dürfen zu Forschungszwecken Adressen von Kindern und Jugendlichen bekannt geben, ohne dass vorgängig das Einverständnis von Kindern, Jugendlichen oder Erziehungsberechtigten eingeholt werden muss. Eine Einwilligung der Erziehungsberechtigten bei der Befragung urteilsfähiger Jugendlicher ist nicht notwendig.

PERSONALBEREICH

14. Pilotprojekt Case Management
Unterstützung bei der Rehabilitation

Der Personaldienst der Direktion der Justiz und des Innern führt zwischen Juli 2004 und Ende 2005 das Pilotprojekt «Reha-Unterstützung» durch. Dabei geht es in erster Linie darum, erkrankte Mitarbeitende durch so genannte Case Manager im Genesungsprozess zu unterstützen sowie ihre Berufs- bzw. Arbeitsfähigkeit zu erhalten. Seitens des Kantons sollen dadurch Lohn- bzw. Rentenleistungen vermindert werden.
Aus datenschutzrechtlicher Sicht sind dabei die folgenden Rahmenbedingungen zu beachten:

Die im Case Management zu erhebenden Daten stellen besonders schützenswerte Personendaten im Sinne von § 2 lit. d DSG dar. Im geltenden Personalrecht gibt es keine rechtliche Grundlage, welche die Einsetzung eines Case Manager ermöglichen und die Mitarbeitenden zur Zusammenarbeit mit dem Case Manager verpflichten würde. Erkrankte Mitarbeitende können durch die zuständige Direktion in begründeten Fällen verpflichtet werden, sich einer vertrauensärztlichen Untersuchung durch einen vom Regierungsrat gewählten und von der Beamtenversicherungskasse im Einzelfall bestimmten Vertrauensarzt zu unterziehen. Dieser erstellt ein Gutachten, dessen Ergebnisse der Direktion mitgeteilt werden. In keinem Fall sind Mitarbeitende verpflichtet, den Grund einer Erkrankung oder eine ärztliche Diagnose Vorgesetzten, der Direktion oder Dritten mitzuteilen.

Eine fehlende gesetzliche Grundlage für eine Datenbearbeitung kann im Einzelfall durch die Einwilligung der betroffenen Person ersetzt werden (§ 5 lit. c DSG). Von dieser Möglichkeit soll im Pilotversuch Gebrauch gemacht werden. Dabei ist sicherzustellen, dass betroffene Mitarbeitende ihren Entscheid in Kenntnis des Projektes und der Rechtslage unbeeinflusst fällen.

Informationen sind auch im Case Management grundsätzlich bei der betroffenen Person zu beschaffen (§ 7 Abs. 1 DSG). Der Einbezug weiterer Personen ist nur statthaft, soweit eine Einwilligungserklärung, allenfalls verbunden mit der Entbindung von der beruflichen Schweigepflicht, vorliegt; zu kontaktierende Dritte sind namentlich zu bezeichnen.

Die vorgesehene Regelung – Vertrag der Direktion mit einer juristischen Person, welche den Case Manager bestimmt; dieser wiederum kann Dritte beauftragen – entbindet die Direktion der Justiz und des Innern nicht von ihren Aufgaben und ihrer Verantwortung gegenüber der betroffenen Person.

Bei der Abfassung der Verträge der Direktion mit den externen juristischen Personen sind die Checklisten für Outsourcing-Verträge des Datenschutzbeauftragten zu beachten. Gegenüber den im Einzelfall eingesetzten Case Managers ist ein Weisungsrecht der Direktion zu vereinbaren; nur so kann diesen das Amtsgeheimnis überbunden werden. Verträge mit Dritten sind der Genehmigung durch die Direktion zu unterstellen; die Beachtung der erwähnten Checklisten ist zu überprüfen.

Mitarbeitende betreffende Anordnungen (z.B. ärztliche Untersuchung, Kursteilnahme) sind durch die Direktion in Verfügungsform zu erlassen; die Case Managers können entsprechende Anträge stellen.

Die im Case Management erhobenen Daten sind Teil der Personalakten (§§ 21 f. VVO zum Personalgesetz). Es ist für eine entsprechende Aufbewahrung zu sorgen. Spätestens beim Abschluss eines Case Management sind sie ins Personaldossier zu integrieren, wobei sicherzustellen ist, dass die Akten nur

der betroffenen Person und einem allfällig später eingesetzten Vertrauensarzt offen stehen. Die Aufbewahrungsdauer ist zu regeln.

Die im Case Management erhobenen Daten dürfen nur zum vorgesehenen Zweck verwendet werden. Entsprechende Regelungen sind in die Verträge mit Dritten und in Pflichtenhefte der Beteiligten (Projektleitung, Berater, Steuerungsgruppe, Case Manager) aufzunehmen. Der Informationsfluss ist explizit zu regeln.

Es ist darauf zu achten, dass die im Case Management erhobenen und bearbeiteten Daten im Einzelfall geeignet und erforderlich sind, den vorgesehen Zweck zu erfüllen. Entsprechend sind die Verträge mit Dritten und die Pflichtenhefte der Beteiligten (Projektleitung, Berater, Steuerungsgruppe, Case Manager) auszugestalten.

Es ist darauf hinzuweisen, dass sich infolge der im Versuchsbetrieb vorgesehenen Doppelrollen einzelner Personen verschiedene Abgrenzungsschwierigkeiten ergeben dürften; eine Anpassung der Projektorganisation ist deshalb zu prüfen.

Die Abgabe der direktionsinternen Weisung sowie eine von der Direktion genehmigte Informationsschrift über das Case Management, dessen Funktionsweise und die Rollen der Beteiligten als Grundlage für den Teilnahmeentscheid sowie die von der Direktion erlassenen Anordnungen haben die Transparenz für die betroffene Person zu sichern.

Die Durchführung eines Versuchsbetriebes mit der «Case-Management-Methode» bedarf klarer Rahmenbedingungen und beruht auf freiwilliger Teilnahme. Für eine definitive Einführung ist das Personalgesetz zu ändern.

15. Datenerhebung im Personalbereich

Einholen von Auskünften

Von einer betroffenen Amtsstelle wurden wir auf einen Erhebungsbogen aufmerksam gemacht, welcher eine Polizeistation an Gemeinden verschickt, um Angaben über Aspiranten der Kantonspolizei zu erhalten. Der Erhebungs- oder Fragebogen zirkuliert in der Gemeinde von der Einwohnerkontrolle zur Vormundschaftsbehörde, zum Betreibungsamt und zum Steueramt. Dabei werden in diesen vier Sachbereichen Angaben zur betroffenen Personen verlangt.

Der Staat als Arbeitgeber darf Personendaten seiner Angestellten, die für das Arbeitsverhältnis notwendig und geeignet sind bearbeiten. Personendaten dürfen im Hinblick auf die Besetzung einer Stelle beschafft werden, soweit sie für die Beurteilung der Eignung, der Leistung und des Verhaltens für das Anstellungsverhältnis notwendig und geeignet sind. Sie sind nach Möglichkeit bei der betroffenen Person selbst zu beschaffen. Diese Daten sind bei Nichtanstellung zurückzugeben oder zu vernichten, wenn die betroffene Person der weiteren Aufbewahrung nicht zustimmt (§ 34 Personalgesetz).

Als Aspirantin und Aspirant für das Polizeikorps oder die Flughafen-Sicherheitspolizei kann aufgenommen werden, wer u.a. einen guten Leumund besitzt und die charakterlichen, geistigen und körperlichen Voraussetzungen für den Dienst im Polizeikorps oder in der Flughafen-Sicherheitspolizei erfüllt (§ 8 Kantonspolizeiverordnung).

Daraus folgt, dass die Kantonspolizei bei der Auswahl ihres künftigen Personals zusätzliche Erhebungen vornehmen darf.

Die Auskünfte müssen jedoch im Rahmen der Verhältnismässigkeit für die Abklärung von Eignung und Leumund einer Person notwendig und geeignet sein und müssen im Rahmen der Transparenz durch die betroffene Person selber oder mit deren Einverständnis eingeholt werden.

Der Bewerber oder die Bewerberin ist selber für die Einholung der entsprechenden Informationen besorgt. Sie holt bei der Gemeinde einen Betreibungsregisterauszug, ein Handlungsfähigkeitszeugnis sowie einen Meldeschein ein und gibt diesen zusammen mit den Bewerbungsunterlagen ab. Erweist es sich in einem weiteren Schritt als notwendig, Angaben zu überprüfen oder solche direkt bei einer Amtsstelle einzuholen, dürfen keine Fragebogen verschickt werden, welche bei verschiedenen Verwaltungsstellen zirkulieren. Jede Amtsstelle ist im Rahmen der Amtshilfe im Einzelfall gesondert anzufragen.

Auskünfte über geleistete oder nicht geleistete Steuerzahlungen sind unseres Erachtens nicht relevant für die Eignung als Aspirant bei der Kantonspolizei.

Im Rahmen der Leumundsabklärung sind folgende Auskünfte erlaubt:

- Bestehen vormundschaftlicher Massnahmen (Handlungsfähigkeitszeugnis)
- Vorliegen von Betreibungen (Betreibungsauszug)
- Einwohnerkontrollbescheinigung (Wohnsitzbestätigung)

Bei den Steuerausweisen sind höchstens Auskünfte über steuerbares Einkommen und Vermögen möglich, da diese auch gegenüber Privaten erteilt werden, sofern die betroffene Person keine Datensperre errichtet hat. Keinesfalls möglich und auch weder geeignet noch notwendig sind Angaben über bezahlte oder nicht bezahlte Steuern. Bestehen tatsächlich Steuerschulden, werden diese automatisch im Betreibungsregister ersichtlich.

Gewisse Verwaltungsstellen wie die Kantonspolizei dürfen bei der Auswahl ihres künftigen Personals zusätzliche Erhebungen vornehmen. Diese haben jedoch im Rahmen der Verhältnismässigkeit sowie der Transparenz primär bei der betroffenen Person selbst zu erfolgen.

INDIVIDUALRECHTE

16. Umfang des Auskunftsrechts
Herausgabe von Kopien

Im Rahmen von Standortbesprechungen füllen die Mitarbeiter einer Strafanstalt für jeden Insassen eine Checkliste aus. Ein Insasse der Strafanstalt wandte sich an uns, nachdem er die Anstaltsleitung um Einsicht und Kopie seiner Checkliste gebeten hatte. Während die Einsichtsnahme grundsätzlich gewährt wurde, wurden ihm jedoch die entsprechenden Kopien verweigert, mit der Begründung, die Checkliste sei ein internes Arbeitsinstrument.

Jede Person, die sich ausgewiesen hat, kann vom verantwortlichen Organ Auskunft verlangen, welche Daten über sie in dessen Datensammlungen bearbeitet werden (§17 DSG). Das Auskunftsrecht bezieht sich auf alle. Einzig persönliche Notizen fallen nicht darunter. Dieser Begriff ist jedoch eng auszulegen: Als persönliche Notizen gelten nur gerade Gedächtnisstützen wie beispielsweise die Notiz, man müsse jemanden zurückrufen, oder Agendaeinträge. Da sich die Checkliste nicht unter diesen Begriff subsumieren lässt, untersteht sie dem Auskunftsrecht. Die Tatsache, dass die Anstaltsleitung diese Liste als internes Arbeitsinstrument bezeichnet, vermag nichts daran zu ändern.

Das Auskunftsrecht umfasst jedoch nicht nur das Recht zur Einsicht, sondern auch die Abgabe von Kopien derjenigen Unterlagen, in welche Einsicht gegeben wird. Der Anspruch auf Kopie ergibt sich gestützt auf § 10 Abs. 2 Datenschutzverordnung in Verbindung mit § 17 DSG.

Das Auskunftsrecht umfasst auch die Abgabe von Kopien derjenigen Unterlagen, in welche Einsicht gewährt wird.

17. Kein Recht auf Löschung
Eintrag in Polizeidatenbank

Im Tätigkeitsbericht Nr. 8 [2002], S. 15 f. haben wir auf mangelhafte Lösch- und Korrekturmöglichkeiten für die von Einträgen in der polizeilichen Datenbank Polis betroffenen Personen hingewiesen.

Erneut gelangte eine Person an uns, gegen welche die Kantonspolizei Ermittlungen geführt und einen entsprechenden Registereintrag erstellt hatte. Die anschliessend gegen die betroffene Person durchgeführte Strafuntersuchung wurde mit einer Einstellungsverfügung abgeschlossen. Auf Gesuch hin ergänzte die Kantonspolizei den Registereintrag mit einem Vermerk über die Einstellungsverfügung, weigerte sich aber, den Eintrag in ihrer Datenbank zu löschen.

Der betroffenen Person konnten wir im Sinne einer Vermittlung nicht weiterhelfen. Wir teilten ihr mit, dass wir eine Vermittlung zwischen ihr und der Kantonspolizei als wenig Erfolg versprechend erachteten, und wiesen sie auf den verwaltungsrechtlichen Weg hin. Tatsächlich ist die Verordnung, welche die Rechte der betroffenen Personen in Bezug auf die Datenbank Polis regeln sollte, noch nicht in Kraft gesetzt worden. Ob den Minderheitsanträgen des Datenschutzbeauftragten in der entsprechenden Arbeitsgruppe gefolgt wird, ist deshalb offen.

Das Recht auf Löschung von Daten sollte grundsätzlich auch bei polizeilichen Datenbanken gewährleistet sein.

GESUNDHEIT UND SOZIALVERSICHERUNG

18. Diagnosecodes auf Spitalrechnungen

Unverhältnismässige Datenbekanntgabe

Tarmed ist ein Tarifsystem, welches die einheitliche Abwicklung der Leistungsvergütung zwischen Leistungserbringern und Kostenträgern im ambulanten Bereich regelt. Tarmed fordert eine systematische Diagnosebekanntgabe auf Arztrechnungen. Der Eidgenössische Datenschutzbeauftragte (EDSB) kommt in einem Bericht vom Juni 2004 dabei zum Schluss, dass eine systematische personenbezogene Datenbearbeitung im Rahmen der Leistungsabrechnung unverhältnismässig und somit rechtswidrig ist, wenn sie mit mehr als den tatsächlich erforderlichen Personendaten vorgenommen wird, da für die einzelnen, von den Versicherern wahrzunehmenden Aufgaben nicht immer der ganze personenbezogene Datensatz erforderlich ist und die Datenbearbeitung in dieser Form somit nicht verhältnismässig ist.

Der Bericht des EDSB zeigt zahlreiche Problembereiche im Tarmed-Umfeld auf, die gesamthaft zu lösen sind. Im Kanton Zürich ging es darum, Elemente aufzuzeigen, die die Gefahr einer widerrechtlichen Datenbekanntgabe durch öffentlich-rechtliche Spitäler verringern. Wir verfassten ein Schreiben an die Gesundheitsdirektion, in welchem wir sie aufforderten, die nötigen Massnahmen zu treffen, bis die im Bericht des EDSB geforderten Rahmenbedingungen umgesetzt sind.

Die Gesundheitsdirektion blieb dabei bei der Regelung von 1997, bis eine gesamtschweizerische Lösung gefunden ist. Die Weisung aus dem Jahre (1997) (vgl. Tätigkeitsbericht Nr. 3 [1997], S. 20 f.) sieht vor, dass der 2-stellige ICD-10-Diagnosecode den Versicherern bekannt gegeben wird. Schon damals war diese Regelung nur im Sinne einer Übergangslösung gedacht, fand aber nie eine verbindliche Regelung auf gesamtschweizerischer Ebene. Als Übergangsregelung bleibt sie demnach weiterhin bestehen.

Mit der Bekanntgabe von Diagnosecodes an Versicherer erfolgt eine unverhältnismässige und daher rechtswidrige Datenbearbeitung. Eine gesamtschweizerische Lösung ist dringend notwendig.

19. Anspruchsabklärung bei der Sozialversicherung

Angaben im Rahmen der Mitwirkungspflicht

Eine Gemeindestelle für Zusatzleistungen verlangte zur Beurteilung des Anspruchs auf Zusatzleistungen und zur Abklärung der spezifischen Frage des Verzichts auf Einkünfte einen ausführlichen Arztbericht mit Angaben über den Grund der Arbeitsunfähigkeit /Angabe der Krankheit oder Behinderung, das Vorliegen einer vollen oder einer teilweisen Arbeitsunfähigkeit, den bisherigen gesundheitlichen Verlauf mit Auswirkung auf die Arbeitsunfähigkeit, den voraussichtlichen künftigen gesundheitlichen Verlauf mit Auswirkung auf die Arbeitsunfähigkeit sowie das Datum des Beginns des Bestehens einer teilweisen Arbeitsunfähigkeit.

Der Arztbericht, welcher der Gemeindestelle zur Verfügung stand, enthielt lediglich ein Kurzzeugnis und bestätigte ohne weitere Angaben eine seit Monaten bestehende gänzliche Arbeitsunfähigkeit. Die Gemeindestelle verlangte von der betroffenen Person genauere Angaben zur Beurteilung des Anspruchs, welche sie bei ihrem Arzt einzuholen hatte.

Die gesetzlichen Grundlagen für den Bereich der Ergänzungsleistungen finden sich im Gesetz über Ergänzungsleistungen (ELG), in der Verordnung (ELV) sowie in der Wegleitung über die Ergänzungsleistungen zur AHV und IV (WEL). Die für die Datenbekanntgabe im geschilderten Fall massgebenden Bestimmungen der WEL sehen vor, dass als Einnahmen grundsätzlich auch alle Einkünfte und Vermögenswerte anzurechnen sind, auf die verzichtet worden ist, und Einkünfte, auf die verzichtet worden ist, in gleicher Weise angerechnet werden wie Einkünfte, auf die nicht verzichtet worden ist.

Da der betroffenen Person eine Zusatzrente ausbezahlt wurde, galt sie als rentenberechtigt. Es war somit abzuklären, ob auf Einkünfte verzichtet wurde. Die Gemeindestelle führte eine Einkommensberechnung durch. Dabei musste sie prüfen, ob ein fiktives Erwerbseinkommen anzurechnen war. Das Kurzzeugnis genügte nicht, um die Arbeitsunfähigkeit und damit das fiktive Erwerbseinkommen detailliert zu berechnen.

Die Gemeindestelle war deshalb berechtigt, die näheren Umstände der Arbeitsunfähigkeit abzuklären. Die betroffene Person war dabei im Rahmen der im ganzen Sozialversicherungsrecht geltenden Mitwirkungspflicht verpflichtet, die notwendigen und geeigneten Angaben zur Abklärung des Leistungsanspruchs zu machen.

Die Sozialversicherungsorgane dürfen die geeigneten und erforderlichen Angaben zur Beurteilung des Leistungsanspruchs von den Versicherten erheben.

BILDUNG

20. Lehrpersonen ohne Unterrichtsberechtigung

Gesetzliche Grundlagen für interkantonale Liste

Immer wieder waren in den letzten Jahren Fälle bekannt geworden, in welchen einer Lehrperson die Unterrichtsberechtigung in einem Kanton entzogen worden war, eine Anstellung in einem anderen Kanton jedoch vorgenommen wurde oder die Lehrkraft mangels Kenntnis des Berechtigungsentzuges weiterbeschäftigt wurde. Die Schweizerischen Konferenz der kantonalen Erziehungsdirektoren (EDK) plante deshalb den Aufbau einer interkantonalen Datenbank mit dem Ziel, die weitere Beschäftigung oder die Neuanstellung von solchen Lehrkräften zu unterbinden.

Die erforderliche – und von den Datenschutzbeauftragten verlangte – gesetzliche Grundlage zur Führung einer Datenbank mit Angaben zu Lehrpersonen ohne Unterrichtsberechtigung wird gegenwärtig im Rahmen der Revision der interkantonalen Vereinbarung über die Anerkennung von Ausbildungsabschlüssen geschaffen. Im Kanton Zürich ist eine Änderung des entsprechenden Beitrittsgesetzes in Vorbereitung.

Mit diesem Vorgehen können im Nachhinein die notwendigen gesetzlichen Grundlagen geschaffen werden, welche die Rahmenbedingungen für die Registrierung einer Person in dieser Datenbank definieren.

Gesetzliche Grundlagen bedeuten Transparenz und Rechtssicherheit bei der Registrierung von Personen in einer Datenbank.

21. Daten an Schulgemeinden

Bekanntgabe durch Einwohnerkontrolle

Es ist zulässig, dass die Einwohnerkontrolle der zuständigen Schulgemeinde zum Zweck der Eröffnung einer eigenen Schülerdatenbank einmalig einen Datensatz der entsprechenden Personen zukommen lässt. Weitergegeben werden dürfen nur die für die Schule geeigneten und erforderlichen Daten der Schüler und Schülerinnen (Name, Vorname, Adresse, Geburtsdatum, gesetzlicher Vertreter, Nationalität).

Aus Sicht des Datenschutzgesetzes ist es gleichbedeutend, ob Daten ausgedruckt oder in elektronischer Form bekannt gegeben werden. In diesem Sinne steht einer elektronischen Weitergabe nichts entgegen.

Die Einwohnerkontrolle ist ebenfalls befugt, der Schulgemeinde die Daten (Name, Vorname, Adresse, Geburtsdatum, gesetzlicher Vertreter, Nationalität) von zu- und wegziehenden Schülern weiterzugeben. Dasselbe gilt für die Daten von Schülern, welche kurz vor dem Schuleintritt stehen.

Eine allfällige bei der Einwohnerkontrolle von den gesetzlichen Vertretern der Schüler errichtete Datensperre kann im vorliegenden Fall durchbrochen werden, da sie für die Datenweitergabe an ein anderes öffentliches Organ nicht gilt.

Für die Schulplanung ist es nicht erforderlich, dass noch nicht schulpflichtige Kinder namentlich bekannt sind. Es genügt die Bekanntgabe der Anzahl von Kindern, welche in einem bestimmten Jahr geboren sind, allenfalls aufgeschlüsselt nach bestimmten Dorfteilen.

Die Einwohnerkontrolle kann den Schulgemeinden die geeigneten und erforderlichen Angaben über Schülerinnen und Schüler bekannt geben.

22. Weitergabe von psychologischen Gutachten

Einwilligung notwendig

Eine Sozialhilfebehörde hatte ein Gutachten über einen Schüler erstellen lassen. Zweck war u.a. festzustellen, wer die Kosten für die Privatschule des Kindes tragen müsse. Das Gutachten enthielt nicht nur Informationen über die Persönlichkeitsstruktur des Kindes, sondern auch sensible Angaben zur Familie. Wenig später beauftragte die Schulpflege die Schulpsychologin mit der Erstellung eines schulpsychologischen Gutachtens über das Kind. Zweck war hier festzustellen, ob schulische Fördermassnahmen angezeigt wären. Im Rahmen dieses Auftrags erhielt die Schulpsychologin den Hinweis von der Schulpflege auf das bereits bestehende Gutachten der Sozialhilfebehörde und auf die Möglichkeit, mit dem dafür verantwortlichen Gutachter – ebenfalls ein Psychologe – zu sprechen. Die Schulpflege wies die Schulpsychologin ferner darauf hin, dass die Familie des Kindes der Schulpflege die Einsicht verweigert habe. Dies sei aber zu Unrecht geschehen, weil sie gestützt auf dieses Gutachten einem Gesuch der Familie um Kostenübernahme für die Privatschule entsprochen habe. Die Schulpsychologin telefonierte in der Folge mit dem Gutachter. Sie erklärte ihm den Grund ihrer Anfrage und fragte ihn nach seinem allgemeinen Eindruck von dem Kind und dessen schulischen Möglichkeiten. Die Äusserungen des Gutachters flossen in den schulpsychologischen Bericht an die Schulpflege ein. Daraus war ersichtlich, dass der Gutachter sich zu diversen Seiten der Persönlichkeit des Kindes geäussert hatte, u.a. zum schulabhängigen Wissen, zur Lernhaltung und zu den Interessen.

Die Mutter des Kindes wünschte eine Beurteilung der Frage, ob die Schulpflege die Schulpsychologin auf das

Gutachten und auf die Möglichkeit, mit dem Gutachter zu sprechen, habe hinweisen und ob der Gutachter seinerseits diese Auskunft habe geben dürfen.

Beim Gutachten des Psychologen handelte es sich um ein Persönlichkeitsprofil im Sinne von § 5 DSG: Die Bearbeitung von Persönlichkeitsprofilen bedarf klarer gesetzlicher Grundlagen oder der ausdrücklichen Einwilligung der betroffenen Person.

Die Einwilligung der Familie in eine Einsichtnahme durch die Schulpflege lag nicht vor.

Die Schulpflege machte geltend, die Einsicht in das Gutachten sei ihr zu Unrecht verweigert worden, hätte sie doch gestützt darauf über die Kostengutsprache für die Privatschule entscheiden müssen. Tatsächlich sieht das Gesetz über die Volksschule und die Vorschulstufe (VSG) in § 1 Abs. 2 vor, dass Schulbehörden, Lehrkräfte und Eltern zusammenarbeiten. Aus dieser Bestimmung kann eine gewisse Mitwirkungspflicht der Eltern abgeleitet werden. Dies hätte sich im vorliegenden Fall dahin gehend konkretisieren können, dass die Eltern der Schulpflegebehörde das Gutachten zugänglich machen, um die Entscheidfindung über die Kostenübernahme für die Privatschule zu ermöglichen. Die Schulpflege beantragte aber erst nach diesem Entscheid Einsicht in das Gutachten. Aus den uns vorliegenden Informationen erhellte sich also nicht, warum die Schulpflege nachträgliche Einsicht ins Gutachten begehrte. Eine Einsicht ins Gesamtgutachten wäre daher nicht erforderlich gewesen, da die Empfehlungen des Psychologen ausgereicht hätten.

Der Psychologe hatte das Gutachten im Auftrag der Sozialhilfebehörde einer anderen Gemeinde erstellt. Ohne anders lautende ausdrückliche Ermächtigung darf die beauftragte Stelle Personendaten nur für das auftraggebende Organ verwenden und nur diesem bekannt geben (§ 13 Abs. 2 DSG). Eine solche Ermächtigung lag nicht vor. Der Gutachter hätte demzufolge der Schulpsychologin keine Auskunft erteilen dürfen.

Soweit keine gesetzlichen Grundlagen bestehen, dürfen (schul)psychologische Gutachten nur mit der Eiwilligung der betroffenen Person (der Eltern) weitergegeben werden.

23. Datenschutz im Schulpsychologischen Dienst

Empfehlungen und Richtlinien überarbeitet

Die Vereinigten Schulpsychologinnen und Schulpsychologen im Kanton Zürich (VSKZ) überarbeiteten ihre Empfehlungen für den Datenschutz in Schulpsychologischen Diensten des Kantons Zürich aus dem Jahr 1996.

Die überarbeiteten Empfehlungen enthalten Anleitungen zum Umgang mit Personendaten. Zunächst werden die Grundsätze des Datenschutzes erläutert, sodann werden in gesonderten Abschnitten nähere Ausführungen und Empfehlungen zum Auskunftsrecht und zur Akteneinsicht der betroffenen Personen gemacht. Zudem wird auf das Amts- und das Berufsgeheimnis eingegangen sowie das Vorgehen bei gerichtlichen und vormundschaftlichen Verfahren erläutert. Der Anhang enthält in Form eines Flussdiagramms eine Anleitung zur Datenbekanntgabe. Zudem enthält er Vorlagen für ein Merkblatt für Eltern sowie ein Formular zur Entbindung von der Schweigepflicht durch Eltern oder Jugendliche sowie eine Vorlage für ein Formular zur Entbindung von der Schweigepflicht durch die vorgesetzte Behörde. Die überarbeiteten Empfehlungen decken die alltäglichen Fragestellungen in Schulpsychologischen Diensten in breitem Mass ab und bieten eine gute Arbeitshilfe in der Praxis. Sie erweisen sich auch im Beratungsalltag als nützliches Hilfsmittel.

Die Schulpsychologischen Dienste im Kanton Zürich verfügen über praxisnahe Empfehlungen für den Datenschutz.

INFORMATIONSSICHERHEIT

24. Sicherheitsinitiative
Konzept zur Erhöhung des Grundschutzes

Der Regierungsrat hat beschlossen, mit einer auf zwölf Monate befristeten Initiative den IT-Sicherheitsgrundschutz der kantonalen Verwaltung zu analysieren und gegebenenfalls mit entsprechenden Sofortmassnahmen zu verbessern. Dem Datenschutzbeauftragten wurde die Koordination übertragen mit dem Auftrag, dem Regierungsrat einen Schlussbericht vorzulegen.

Der Datenschutzbeauftragte hat ein Konzept erarbeitet, welches sich zum Ziel setzt, das Sicherheitsniveau aller Amtsstellen mit Massnahmen ohne grosse Kostenfolge deutlich anzuheben. Dabei werden die Anforderungen der Informatiksicherheitsverordnung (ISV) pragmatisch berücksichtigt.

Das Konzept sieht eine Beurteilung der Stärken und Schwächen der Informationssicherheit bei allen Direktionen und der Staatskanzlei vor. Dabei folgt eine Untersuchung aller Ämter mit eigenen Informatikeinheiten. Die Überprüfung wird in Form einer «GAP-Analyse» durchgeführt, wobei jeweils der Soll- und der Ist-Zustand festgehalten werden.

Beim Soll-Zustand wird von einem einheitlichen und verwaltungsweiten Grundschutz ausgegangen (ISV, BSI-Grundschutzhandbuch sowie nach dem britischen Standard BS 7799). Die Überprüfungen werden risikoorientiert und stichprobenweise durchgeführt und beinhalten die Bewertung der wichtigsten Systeme und Applikationen sowie der Organisation in Bezug auf Sicherheitslücken (logisch/physisch). Auf Grund der Ergebnisse der GAP-Analyse werden praxisorientierte Massnahmen (priorisiert zusammengefasst in Form eines Massnahmenkatalogs) erarbeitet. Die Sicherheitsinitiative unterstützt anschliessend ausgewählte Amtsstellen aktiv bei der Umsetzung der aus der Sicherheitsanalyse ersichtlichen Sofortmassnahmen. Eine prägnante und verständliche Berichterstattung mit einer Prioritätenliste für Massnahmen wird den Direktionen bzw. Amtsstellen nachhaltig einen Pfad zu mehr Sicherheit aufzeigen. Ferner wird damit die Sensibilisierung für IT-Sicherheit bei allen Verantwortlichen besser ausgebildet. Zeitgleich zu den Analysen ist eine Sensibilisierungskampagne für alle Mitarbeitenden der kantonalen Verwaltung in Form eines Intranet-basierten Trainings geplant.

Mit der Sicherheitsinitiative werden eine nachhaltige Verbesserung des Grundschutzes und eine Sensibilisierung für die Anliegen der Sicherheit angestrebt.

25. Sensibilisierung von Mitarbeitenden
Workshops für Verwaltungsstellen

Verschiedene Amtsstellen der kantonalen Verwaltung sowie zahlreiche Gemeindeverwaltungen hatten mit Unterstützung der Beratungsstelle für Informatiksicherheit des Datenschutzbeauftragten eine eigene IT-Nutzungsweisung erarbeitet und veröffentlicht. Diese ist, ergänzend zur E-Mail- und Internet-Verordnung des Kantons Zürich, für alle Mitarbeitenden der jeweiligen Institution verbindlich. Einzelne Stellen sind an uns herangetreten, um die Sensibilisierung bezüglich IT-Sicherheit ihrer Mitarbeitenden zu erhöhen.

Die Beratungsstelle für Informatiksicherheit hat zu diesem Zweck einen Workshop erarbeitet, an dem sich die Mitarbeitenden der Verwaltungseinheiten über die Gefahren und Risiken beim Umgang mit den aktuellen Technologien informieren konnten. Es wurde erklärt, wie durch richtiges Verhalten das Risiko einer Gefährdung sowohl privat wie auch geschäftlich wesentlich vermindert werden kann.

Das Echo der Workshops war durchwegs positiv. Nach Rückfrage bei den einzelnen Amtsstellen und Gemeinden wurde eine positive Veränderung des Verhaltens der jeweiligen Mitarbeitenden in puncto Sicherheit bestätigt. Es wurde beispielsweise während der Kaffeepause über sicherheitsrelevante Themen diskutiert, die zum Teil in der Tagespresse erschienen waren. Einzelne Teilnehmende haben sich sogar persönlich beim Workshopleiter bedankt, da sie durch die neuen Erkenntnisse im privaten Umfeld vor Schaden bewahrt wurden.

Mit verschiedenen Workshops konnten Mitarbeitende zahlreicher Verwaltungsstellen für die Anliegen der Sicherheit sensibilisiert werden.

26. IT-Sicherheitsberatungen
Regelmässige Prüfungen notwendig

Die Beratungsstelle für Informatiksicherheit des Datenschutzbeauftragten hatte mehrere Aufträge, die implementierten Sicherheitsvorkehrungen von Gemeindeverwaltungen, Amtsstellen sowie eines grossen Spitals zu verifizieren. Um dies zu überprüfen, testeten wir die Sicherheit aller relevanten Systeme innerhalb der Netzwerke. Des Weiteren galt es, auch die Schwachstellen zu eruieren, die unberechtigten Zugriff auf die Systeme ermöglichen würden. Dabei verwendeten wir dieselben Werkzeuge und Techniken, wie dies Hacker tun würden.

Während diesen Prüfungen haben wir festgestellt, dass in keiner der überprüften Institutionen ein übergeordnetes Sicherheitsmanagement existiert. Dieser Umstand stellt ein Risiko bezüglich Kontinuität und Sicherheit dar. So werden beispielsweise Anwendende nicht gezwungen, regelmässig ihre Passwörter zu ändern. Zudem wird eine adäquate Passwortqualität nicht von den Systemen gefordert. So ist es möglich, dass Passwörter von zum Teil administrativen Benutzerkonten bis zu sieben Jahre nicht geändert wurden. Nur auf den wenigsten der überprüften Systeme werden regelmässige Sicherheitsupdates eingespielt. Mit regelmässigen Software-Updates (Patches) werden Sicherheitslücken in der bestehenden Systemsoftware geschlossen. So wird verunmöglicht, dass das Betriebssystem des Computers infiziert bzw. dass Hacker bekannte Sicherheitslücken für ihre Zwecke missbrauchen können.

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 ist aber notwendig, um die laufenden Konfigurationsanpassungen der Systeme zu kontrollieren.

Mit zielgerichteten Beratungen und Überprüfungen einzelner Verwaltungsstellen konnte die Sicherheit teilweise markant verbessert werden.

DATENSCHUTZREVIEW

27. Regelmässige Kontrollen
Verbreitete Mängel beim Grundschutz

Die Hauptzielsetzungen der Datenschutzreview wurde im Jahr 2004 mit den Punkten «Sensibilisierung für Datenschutz und IT-Sicherheit» sowie «Empfehlungen zur Anpassung der rechtlichen Rahmenbedingungen und zu Verbesserungen im organisatorischen und technischen Bereich» nicht verändert. Die Prüfgebiete

- Umsetzung Informatiksicherheitsverordnung,
- Weisungen an Benützende und Betreibende,
- Regelung der Verantwortlichkeiten;
- Einsatz von Virenschutzprogrammen,
- Passwörter (Anforderungen der technischen Implementierung und Verwendung),
- Zugriffskonzept und
- Vertragswesen (insbesondere Verträge mit externen Dienstleistenden)

sind wie die Jahre zuvor gleich geblieben.

Eine Erweiterung wurde im Rahmen der Überarbeitung der Datenschutzreview für das Jahr 2005 vorgenommen.

Die Gemeinden und Amtsstellen haben mit wenigen Ausnahmen die Bewertung «befriedigend» erhalten. Wie schon in den Jahren zuvor festgestellt, werden die Massnahmen für Datenschutz und Informatiksicherheit bei den geprüften Amtsstellen mit unterschiedlicher Priorität behandelt.

Die letztes Jahr in unserem Tätigkeitsbericht Nr. 9 [2003], S. 31 bereits publizierte Liste der wichtigsten Empfehlungen ist im Grundsatz mit einer identischen Gewichtung immer noch gültig. Folgende Punkte sind bei allen geprüften Stellen im Jahr 2004 zentral:

- Massnahmenpläne gemäss Auftrag Informatiksicherheitsverordnung (ISV) erstellen oder überarbeiten und anschliessend durch die vorgesetzte Stelle abnehmen lassen;
- In den Funktionsbeschreibungen die Verantwortung für Revision und Kontrolle gemäss ISV zuweisen;
- Die Verantwortlichkeit der Benützenden für Virenschutz und die Verwendung von Passwörtern in einer Weisung detailliert kommunizieren;
- Ein schriftliches Zugriffskonzept (inklusive an die Organisation angepasste Rollendefinitionen) erstellen;
- Auswertungen der Zugriffe sinnvoll definieren, regelmässig auswerten und bei Bedarf Massnahmen treffen;
- Die «Allgemeinen Geschäftsbedingungen für die Sicherheit, den Datenschutz und die Daten- und Informationssicherheit» (AGB Sicherheit, September 2001) bei Bezug von Informatikdienstleistungen in die Verträge mit externen Dienstleistenden einbeziehen.

Die Notwendigkeit der Durchführung der Datenschutzreview ist auch im Jahr 2004 auf Grund der Resultate unbestritten. Folgende zwei Initiativen tragen zusätzlich zur Wirksamkeit der Kontrollmassnahmen des Datenschutzbeauftragten bei:

- Die Internetapplikation Review-Tool (siehe Seite 37) ergänzt die Anstrengungen für Sensibilisierung in den Bereichen Datenschutz und IT-Sicherheit. Durch die Selbstbeurteilungmöglichkeit erweitert das Tool den Umfang der berücksichtigten Stellen.
- Das Projekt «Sicherheitsinitiative» ermöglicht es, die Amtsstellen der Zentralverwaltung zu überprüfen und anschliessend das Niveau der IT-Sicherheit (siehe S. 35) festzustellen und mit Sofortmassnahmen stufengerecht anzuheben.

Die Datenschutzreview ist ein zentrales Instrument, um einzelne Datenschutz- und Sicherheitsmassnahmen überprüfen zu können.

28. Review-Tool im Internet
Möglichkeit der Selbstüberprüfung

Die neue Internetanwendung (zu finden unter https://review.datenschutz.ch) des Datenschutzbeauftragten (siehe Tätigkeitsbericht Nr. 9 [2003], S. 30) ist mittels einer Broschüre bei den Gemeinden und den kantonalen Stellen den Benützenden vorgestellt und von diesen gut aufgenommen worden.

In sieben Schritte führt die Überprüfung der eigenen Datenbearbeitungen durch das Review-Tool zu einem verbesserten Schutzniveau. Zentral zur Beurteilung der aktuellen Situation ist das vom Tool ausgewiesene Resultat in den Ampelfarben

- Rot (bedeutet «Massnahmen sind dringend einzuleiten»),
- Gelb («Verschiedene Massnahmen sind zusätzlich notwendig») und
- Grün («Getroffene Massnahmen weiterführen»).

Das Tool empfiehlt auf Grund der einzelnen Antworten abgestimmte Massnahmen, die in den Planungs- und Umsetzungsprozess auf einfache Weise übernommen werden können.

Um die Anwendung des Review-Tools zu erleichtern, sind ausführliche Hilfestellungen für die Selbsteinschätzung online abrufbar:

- eine generelle Hilfe zum Tool und zur Datenschutzreview (alle Themen als PDF-Datei downloadbar),
- FAQs mit den wichtigsten Hinweisen zur Datenschutzreview und zum Tool und
- pro Frage ein Hilfetext, oft verbunden mit Text- und Konzeptvorschlägen, als PDF-Datei zur weiteren Bearbeitung downloadbar.

Der Fragenkatalog sowie die dazugehörige Auswertungsmöglichkeit sind auch als netzwerkunabhängiges Werkzeug in Papierform beim Datenschutzbeauftragten erhältlich.

- Für die Umsetzung eines wirksamen Datenschutzes können die wichtigsten Massnahmen im rechtlichen, organisatorischen und technischen Bereich durch die Verantwortlichen auf einfache Weise systematisch beurteilt werden.

Das Online-Review-Tool ist eine Ergänzung der Datenschutzreview und ermöglicht allen Verwaltungsstellen eine Selbstüberprüfung.

Zugriffskonzept – neue Hilfestellung

Bei der Durchführung der Datenschutzreview wurde oft festgestellt, dass in den geprüften Amtsstellen und Gemeinden einzelne Massnahmen zum Zugriffsschutz mit einem mittleren bis sogar grossen Aufwand getroffen werden, jedoch eine Struktur respektive eine Übersicht der getroffenen Massnahmen in einem zusammenfassenden Konzept beinahe immer fehlt. Diese Massnahmen können in der Folge nicht an einheitliche Vorgaben angepasst werden, was meistens zu Lücken im Sicherheitsdispositiv führt.

Die neu vorliegende Hilfestellung zeigt in vier Abschnitten auf verschiedene Weise den Weg zu einem Zugriffs- respektive Berechtigungskonzepts auf.

Die Einführung formuliert den Bedarf und die zentralen Punkte beim Management der Zugriffe.

Auf Grund des inhaltlichen Rasters können die Lücken bei den Massnahmen und der zugehörigen Dokumentation schnell bestimmt werden.

Die wichtigsten Punkte in Form einer nummerierten Checkliste zeigen die Eckpfeiler des Konzepts auf.

Detaillierte Erläuterungen für die zu beschreibenden und umzusetzenden Anforderungen in den Bereichen Daten- und Programmzugriff können den durch die Hilfe zusammengestellten Massnahmentexten des IT-Grundschutzhandbuchs (Bundesamt für Sicherheit in der Informationstechnik, Bonn, Weblink www.bsi.de) entnommen werden.

Die Hilfestellung für ein Zugriffs- respektive Berechtigungskonzept ist als pdf-Datei im Internet-Angebot des Datenschutzbeauftragten als Download zu finden.

POLIZEI UND JUSTIZ

29. Biometrisches Gesichtserkennungssystem

Verordnung erlassen

Mit dem biometrischen Gesichtserkennungssystem FAREC können bei vorgelagerten Grenzkontrollen am Flughafen Zürich der illegalen Migration verdächtige Personen in Bewegung erfasst werden, nachdem sie einer Kontrollzone zugewiesen worden sind. Die aufgenommenen Bilder werden zusammen mit Personendaten und eingescannten Reisedokumenten erfasst. Bei einer späteren Kontrolle innerhalb der Aufbewahrungsfrist wird ein Bildvergleich vorgenommen.

Im Tätigkeitsbericht Nr. 9 [2003] S. 37 haben wir über die Aufnahme des ersten von der Kantonspolizei Zürich zwischen Mitte Februar 2002 und Mitte Juni 2003 durchgeführten Pilotversuches berichtet. Während des ganzen Jahres 2005 findet nun ein zweiter Pilotversuch statt. Der Regierungsrat hat eine entsprechende befristete Verordnung erlassen. In diese sind wesentliche Anliegen des Datenschutzes eingeflossen.

Eine formellgesetzliche Grundlage für die Überwachung von Flugpassagieren mittels technischer Erkennungsverfahren soll im neuen Bundesgesetz über die Ausländerinnen und Ausländer geschaffen werden.

Der Einsatz von Technologien, die Risiken für die Persönlichkeitsrechte der betroffenen Personen beinhalten, hat auf einer entsprechenden Rechtsgrundlage zu erfolgen.

30. Zustellung von Gerichtsurkunden

Verhältnismässige Angaben

Die Angaben auf Gerichtsurkunden geben immer wieder Anlass zu Beschwerden von betroffenen Personen. Gemäss § 3 Abs. 2 lit. a kommt das Datenschutzgesetz in Verfahren der Rechtspflege erst nach deren Rechtskraft zur Anwendung. Die Verwaltungskommission des Obergerichtes hat mit Kreisschreiben vom 30. September 1940 sowie mit Beschluss vom 27. August 1974 Richtlinien für die Zustellung von Gerichtsurkunden erlassen. Diese gelten auch für die Bezirksgerichte. In Zivil- und Strafsachen sind demnach auf dem Umschlag einer Gerichtsurkunde aufzuführen:

a) bei erledigten Geschäften die Adresse, die Geschäftsnummer, die Nummern der zurückgesandten Aktenstücke und das Erledigungsdatum,

b) bei laufenden Geschäften die Adresse, die Geschäftsnummer, das Datum des Beschlusses oder der Verfügung und allfällige Beilagen (z.B. Rekursschrift),

c) bei Vorladungen die Adresse, die Geschäftsnummer und das Verhandlungsdatum.

Die Parteibezeichnung und die Art des Geschäftes sind überall wegzulassen. Auch aus dem Aufdruck auf den Briefumschlägen und deren Beschriftung darf sich kein Hinweis auf den Inhalt der Sendung (z.B. Einzelrichter in Strafsachen oder dergleichen) ergeben. Unter Beachtung dieser Regelungen sind die Angaben als verhältnismässig zu bezeichnen.

Die Angaben auf Gerichtsurkunden haben sich auf die geeigneten und erforderlichen Daten zu beschränken.

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. Beda Harb

Juristisches Sekretariat
lic. iur. Barbara Mathis
lic. iur. Karin Schoch

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

Beratungsstelle für Informatiksicherheit (BIS)
Oliver Wyler, NDS FH Informatiksicherheit

Sekretariat
Martina Richard
Sara Puttin

Tätigkeitsbericht Nr. 10 (2004)
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

10 JAHRE DATENSCHUTZ IM KANTON ZÜRICH

www.datenschutz.ch