Nr. 2

Tätigkeits-Bericht

Datenschutzbeauftragter des Kantons Zürich

1996

Tätigkeitsbericht

Nr. 2
1996

Der Datenschutzbeauftragte erstattet dem Regierungsrat jährlich oder nach Bedarf einen Bericht über seine Tätigkeit (§ 23 Datenschutzgesetz). Der vorliegende Tätigkeitsbericht Nr. 2 deckt den Zeitraum vom 1. Januar 1996 bis 31. Dezember 1996 ab.

Zürich, Februar 1997

Der Datenschutzbeauftragte
des Kantons Zürich
Dr. iur. Bruno Baeriswyl

Inhaltsverzeichnis

V. Datensicherheit

VI. Information

VII. Entwicklungen

Die Wirkung des Datenschutzgesetzes

Die Verwirklichung der datenschutzrechtlichen Grundanliegen erfordert von allen Verwaltungsstellen entsprechende Bemühungen. 1996 mussten diesbezüglich unterschiedliche Erfahrungen gemacht werden.

Mit der Einführung des Datenschutzgesetzes (DSG) gehen berechtigte Erwartungen der Bürgerinnen und Bürger einher: Das Grundrecht der persönlichen Freiheit, das den Schutz der Privatsphäre beinhaltet, soll beim Bearbeiten von Daten durch die Verwaltung gewährleistet werden. Wie das Datenschutzgesetz in der Praxis angewendet wird, ist deshalb für dessen Wirkung bezüglich der Grundrechte der betroffenen Personen entscheidend. In vielen Bereichen ist die Verwaltung mit der Umsetzung weitergekommen. Einige Feststellungen 1996 zeigen, dass es nicht ausreicht, nur den guten Willen in bezug auf den Datenschutz zu zeigen, sondern dass es auch darum geht, entsprechend zu handeln.

Von der Kenntnisnahme zur Umsetzung

Vielfach offen, manchmal auch versteckt, enthalten Antworten an den Datenschutzbeauftragten Bemerkungen wie «Das haben wir schon immer so gemacht, und es hat sich noch nie jemand beschwert» oder «Das ist ja nur eine Person, die sich beschwert». Meistens enden solche Stellungnahmen mit der Bestätigung, dass man selbstverständlich den Datenschutz «strikte einhalte». Der Wert solcher Deklarationen ist durch die Anfangsbemerkungen stark relativiert. Wir stellen fest, dass von der Kenntnisnahme der datenschutzrechtlichen Bestimmungen bis zu deren Umsetzung im eigenen Bereich offensichtlich noch grosse Hindernisse zu überwinden sind. Neben einer solchen Abwehrhaltung war teilweise eine Unkenntnis zu spüren, und die betroffenen Personen wurden bei datenschutzrechtlichen Anliegen von der Verwaltung abgewiesen.

Anwalt und Vermittler

Diese Situation führte dazu, dass der Datenschutzbeauftragte immer mehr als Anwalt und Vermittler der betroffenen Personen aufzutreten hatte. Diese Ombudsfunktion, die als Kernbestand zu den Aufgaben des Datenschutzbeauftragten gehört, ermöglichte es, in vielen Fällen vermittelnd tätig zu werden. Allerdings ist nicht zu verhehlen, dass teilweise versucht wurde, dem Datenschutzbeauftragten vorerst den Sachverhalt nicht offen darzulegen. Wir machten deshalb vermehrt von unserem Recht Gebrauch, uns Datenbearbeitungen vorführen zu lassen.

Mehr oder weniger Datenschutz?

Nachdem wir Verwaltungsstellen darauf aufmerksam machen mussten, dass das Datenschutzgesetz auch für ihren Bereich gelte, stellten wir fest, dass immer noch versucht wurde, je nach Situation den Datenschutz mehr oder weniger umzusetzen. Wir mussten

diesen Stellen mitteilen, dass das Datenschutzgesetz einzuhalten ist wie jedes andere Gesetz auch.
In sensiblen Bereichen der Datenbearbeitung ist bei den Mitarbeiterinnen und Mitarbeitern vielfach eine hohe Sensibilisierung für die Anliegen des Datenschutzes vorhanden. Vereinzelt stand dieser auf der Stufe der Leitung wiederum Skepsis gegenüber: Die Stärkung der Rechte der Bürgerinnen und Bürger, die im Auskunftsrecht einen Kernpunkt hat, wird als unangenehme Transparenz empfunden. Es wurde versucht, das Auskunftsrecht zu verweigern oder einzuschränken. Diese Grundhaltung erregte bei den betroffenen Person zu recht Misstrauen, und viele Anfragen gelangten an uns, weil diese Personen den Eindruck hatten, es werde ihnen keine vollständige Auskunft erteilt.

Verletzung von Datenschutzvorschriften

Es ist nicht akzeptabel, wenn grobe Verletzungen von Datenschutzvorschriften den betroffenen Personen gegenüber mit verharmlosenden Erklärungen gerechtfertigt werden: «Leider sind solche Versehen nicht völlig auszuschliessen, sind die Ärzte in juristischen Fragen, wie diejenigen der Zulässigkeit der Auskunftserteilung, doch naturgemäss nicht so versiert wie in ihrem eigentlichen Fachgebiet». Im konkreten Fall ging es immerhin um eine strafbare Verletzung des Amts- sowie des Arztgeheimnisses! Es wurde auch versucht, sich aus der Verantwortung des Datenbearbeiters zu stehlen. Einem Patienten, der sich wunderte, warum in seiner Krankengeschichte eine Kopie des Obduktionsberichtes seines Vaters lag, wurde sowohl vom betroffenen Spital wie auch von seinem Arzt die ausweichende Antwort gegeben, man wisse nicht mehr, wie dieser Bericht in die Krankengeschichte gelangt sei, man glaube aber mit seiner mündlichen Einwilligung gehandelt zu haben. Der Patient wunderte sich über eine solche Argumentation, hatte er doch erst bei der Einsicht in seine Krankengeschichte erfahren, dass dieser Bericht beigezogen worden war.

Bürgerorientierte Verwaltung

In der wirkungsorientierten Verwaltungsführung, die stark auf die automatisierte Datenverarbeitung setzt, ist das Datenschutzgesetz ein Katalysator. Seine Zielsetzungen decken sich mit den Anliegen der bürgerorientierten Verwaltung. Es verlangt die Transparenz der Datenbearbeitungen. Die Antwort auf die Gretchenfrage, wie hast du's mit dem Datenschutz, ist denn meistens auch die Antwort auf die Frage, wie bürgerorientiert ist diese Verwaltungsstelle. Je besser organisiert, je näher an den Bedürfnissen der Bürgerinnen und Bürger, desto weniger hat eine Verwaltungsstelle Mühe mit der Umsetzung des Datenschutzgesetzes. Dies zeigte sich bereits bei der Erstellung der Register der Datensammlungen, die bei solchen Verwaltungsstellen am wenigsten Schwierigkeiten bereitete.

Schwerpunkte der Tätigkeit

1996 war geprägt durch eine starke Zunahme der Geschäftslast in allen Bereichen. Auf diesem Hintergrund lassen sich einige Schwerpunkte hervorheben.

Sensible Umfragen

Umfragen beinhalten nicht nur die Involvierung einer grossen Anzahl Personen, sondern bedeuten auch immer eine hohe Konzentration von Daten. Für das Vertrauen der betroffenen Personen in solche Umfragen ist es deshalb notwendig, dass die Datenerhebungen mit einer klaren Zweckbindung erfolgen und die Daten nur anonymisiert bearbeitet werden. In einer grossangelegten Umfrage der Erziehungsdirektion mussten wir feststellen, dass dies nicht gewährleistet war (siehe S. 10). Erst auf unsere Intervention hin wurden die entsprechenden datenschutzrechtlichen Rahmenbedingungen erfüllt.
Im weiteren war auch das Prinzip der Verhältnismässigkeit der Datenbearbeitungen immer wieder in Erinnerung zu rufen. Jede Datenbearbeitung und -bekanntgabe darf nur diejenigen Daten umfassen, die für den jeweiligen Zweck geeignet und erforderlich sind. Auch wenn Rechtsgrundlagen in Form von Mitteilungsrechten und -pflichten bestehen, ist im Einzelfall abzuwägen, ob die bekanntzugebenden Daten geeignet sind, den anvisierten Zweck zu erreichen. Die Praxis, solche Mitteilungsrechte dahingehend auszulegen, es sei einfach immer alles mitzuteilen, führt dazu, dass

Die Kosten des Datenschutzes

Die kantonale Verwaltung gibt jährlich zwischen 100 und 150 Millionen Franken für ihre Informatiksysteme und -anwendungen aus. Mit rund 360 Stellen werden diese automatisierten Datenbearbeitungen betreut. Vergleicht man daneben die Ausgaben für Datenschutz und Datensicherheit, so muss man feststellen, dass sich da ein Fahrzeug auf der (Daten)autobahn befindet, dessen Geschwindigkeit oder Computerleistung ausreicht, um Satelliten in die Erdumlaufbahn zu dirigieren, dieses Fahrzeug aber nicht einmal mit Bremsen und Sicherheitsgurten, geschweige denn mit Airbag oder ABS ausgerüstet ist. Das Risiko dabei tragen nicht nur die Insassen, nämlich die Bürgerinnen und Bürger, deren Personendaten damit bearbeitet werden, sondern auch die Besitzer dieses Fahrzeuges, die unter diesen Umständen früher oder später mit einem Crash rechnen müssen. Es wird ihnen kaum gelingen, sich bei diesem Zustand des Fahrzeuges aus der Verantwortung zu ziehen.
Es ist deshalb vordringlich, dass nicht nur in die Geschwindigkeit investiert wird, sondern dass von den vorhandenen Mitteln ein angemessener Teil für die Sicherheit verwendet wird. Die Kosten für Datenschutz und Datensicherheit sind keine Zusatzkosten, sondern sie sind bedingt und notwendig durch den Einsatz moderner Informationstechnologie.
Für die Beratung in Fragen des Datenschutzes und der Datensicherheit, die Kontrolle, die Vermittlung zwischen betroffenen Personen und Verwaltung sowie die Information über die Anliegen des Datenschutzes verfügt der Datenschutzbeauftragte über zwei Stellen und ein Budget von 0,4 Mio. Franken. Diese Zahlen stehen in keinem Verhältnis zu den oben erwähnten.
Will die Verwaltung ihre gesetzliche Verantwortung im Bereich des Datenschutzes und der Datensicherheit wahrnehmen, muss sie auch in diesem Bereich die angemessenen Ressourcen einsetzen. Die Datenschutzpanne und der damit verbundene Vertrauensverlust bei den Bürgerinnen und Bürgern werden ein Mehrfaches an Kosten verursachen.

die Privatsphäre der betroffenen Personen oftmals in unzulässiger Weise beeinträchtigt wird (siehe S. 12).

Bekanntgabe von sensiblen Daten

Die Bekanntgabe von sensiblen Daten bedeutet immer einen schweren Eingriff in die Privatsphäre der betroffenen Personen. Eine Bekanntgabe verlangt deshalb qualifizierte rechtliche Voraussetzungen. In zahlreichen Gutachten nahmen wir zu solchen Datenbearbeitungen Stellung. Die Neustrukturierung der Arbeitsvermittlung war Anlass, die Frage abzuklären, inwieweit Daten, die einem Spezialgeheimnis unterliegen, an andere Amtsstellen weitergegeben werden dürfen (siehe S. 24). Auch das Führen von Bussenkontrollen auf kommunaler Ebene beinhaltet das Bearbeiten von sensiblen Daten. Eine Rechtsgrundlage für eine persönliche Strafkontrolle besteht dabei nicht (siehe S. 25).
Das Einbürgerungsverfahren wie auch die Datenbearbeitungen durch die Jugend- und Familienberatungsstellen berühren sensible Bereiche der Privatsphäre. Das Prinzip der Verhältnismässigkeit ist deshalb im Einbürgerungsverfahren strikte zu beachten (siehe S.26), und Datenbekanntgaben aus dem Bereich der Jugend- und Familienberatung, beispielsweise an Gerichte, dürfen nur erfolgen, wenn die Voraussetzungen der Amtshilfe klar gegeben sind (siehe S. 26).

Mangelnde Datensicherheit

Die Einstellung gegenüber den Fragen der Datensicherheit ist teilweise von einer beängstigenden Ignoranz geprägt. Unbedenklich werden immer leistungsfähigere EDV-Systeme angeschafft, die dem Benutzer immer mehr Möglichkeiten bieten und selbstverständlich verwaltungsintern und -extern vernetzt sind. Vielfach fehlt es dabei an elementarsten Sicherheitsanforderungen: Die Benutzerinnen und Benutzer werden in bezug auf die Datensicherheit nicht geschult, es bestehen keine Richtlinien im Umgang mit dem PC, den Passwörtern oder Disketten. Selbst bei umfangreichen Datenbearbeitungen mit sensiblen Personendaten sind Datensicherheitskonzepte die Ausnahme. Wir haben deshalb die Bemühungen um die Erstellung von Richtlinien für die Sicherheit von Informatiksystemen und -anwendungen in der kantonalen Verwaltung aktiv unterstützt (siehe S. 34). Des weiteren haben wir mit dem Symposium für Datenschutz und Informationssicherheit stark auf die Bedeutung der Datensicherheit für eine datenschutzkonforme

Bearbeitung von Personendaten hingewiesen (siehe S. 38). Nicht zuletzt werden wir aufgrund eines neu erarbeiteten Konzeptes die Überwachung und Kontrolle der Datenbearbeitungen intensivieren, um damit die verantwortlichen Stellen für eine angemessene Berücksichtigung der Datensicherheitsmassnahmen zu gewinnen (siehe S. 34).

Information und Sensibilisierung

Wir führten im vergangenen Jahr unsere Anstrengungen in bezug auf die Sensibilisierung der Verwaltungsstellen für die Anliegen des Datenschutzes weiter. Publikationen, Veranstaltungen, Seminare und Referate sind durchwegs auf ein sehr grosses und positives Echo gestossen. Das Bedürfnis nach einschlägigen Informationen ist hoch. Mit diesen Mitteln versuchen wir deshalb, möglichst viele Verwaltungsstellen anzusprechen.

Entwicklungen

In verschiedenen Bereichen, die wir im letztjährigen Tätigkeitsbericht aufgegriffen hatten, gab es zwischenzeitlich Entwicklungen (siehe S. 40). Es ist dabei erfreulich zu sehen, dass Anliegen des Datenschutzes bei Gesetzesrevisionen aufgegriffen werden (Revision des Steuergesetzes, Revision des Strassenverkehrsgesetzes). Auf der anderen Seite wird auch ersichtlich, wie lange es dauern kann, bis datenschutzrechtliche Grundanliegen berücksichtigt werden (Gesundheitswesen). Auf der einen Seite ist dabei positiv zu vermerken, dass gewisse Konkretisierungen in bezug auf die praktische Umsetzung datenschutzrechtlicher Bestimmungen vorgenommen wurden, auf der anderen Seite müssen wir feststellen, dass dies nicht mit der notwendigen Konsequenz erfolgt und Grundfragen in anderen Bereichen bis jetzt nicht angegangen worden sind (Vollzug des Krankenversicherungsgesetzes).

Ausblick

Die Ereignisse im vergangenen Jahr unterstrichen nicht nur die Wichtigkeit der Rolle des Datenschutzbeauftragten als Anwalt und Vermittler, sondern auch seine Bedeutung für die Beratung der Verwaltungen in allen Fragen des Datenschutzes und der Datensicherheit. Dass es dabei nicht ohne Kontrollen durch den Datenschutzbeauftragten geht, ist aufgrund der Komplexität der Materie und des benötigten Fachwissens selbstverständlich. Die bürgerorientierte Verwaltung ist in allen Bereichen mit Fragen des Datenschutzes konfrontiert. Es sollte deshalb eine selbstverständliche Aufgabe dieser Verwaltung sein, die Privatsphäre ihrer Bürgerinnen und Bürger zu schützen. Datenschutz und Datensicherheit müssen integrierter Bestandteil in der wirkungsorientierten Verwaltung sein.

Gute Ansätze

Sehr viele Verwaltungsstellen sind sich dieser Ausgangslage bewusst und versuchen, den Datenschutz angemessen und wirkungsvoll anzuwenden. Sie nehmen die Beratungen des Datenschutzbeauftragten zu generellen Fragen oder im Einzelfall in Anspruch. Unsere Feststellungen und Empfehlungen führten in der überwiegenden Zahl der Fälle zu positiven Reaktionen. Auch viele Gemeinden haben bereits die Vorkehrungen getroffen, um den Datenschutz umsetzen zu können, haben Datenschutzreglemente überarbeitet und Datenschutzberater oder -beauftragte bestellt (siehe S. 31). Diese positiven Ansätze sind die Grundlage, um verwaltungsweit effiziente und praxisbezogene Lösungen für die Verwirklichung der Anliegen des Datenschutzgesetzes zu finden. In vielen Bereichen, die 1996 den Datenschutzbeauftragten beschäftigten, sind Entwicklungen in diesem Sinne zu verspüren.

Handlungsbedarf auf verschiedenen Ebenen

Sowohl im Einzelfall als auch auf gesetzgeberischer Stufe wurde aufgrund konkreter Vorkommnisse ein datenschutzrechtlicher Handlungsbedarf aufgezeigt.

1. Evaluation der Schulqualität

Untersuchungsanordnung erfüllte Datenschutzanforderungen nicht

Eine breit angelegte Umfrage der Erziehungsdirektion sollte die Beurteilung der Oberstufe durch die Eltern sowie Schülerinnen und Schüler ermitteln wie auch Aufschluss geben über das in der Schule vermittelte Wissen. Zur Durchführung und Auswertung dieser Untersuchung war eine Privatfirma beauftragt worden. Zahlreiche Anfragen veranlassten uns, diese Umfrage einer datenschutzrechtlichen Prüfung zu unterziehen und uns die Datenbearbeitung bei der involvierten Beratungsfirma vorführen zu lassen.

Obwohl die Erziehungsdirektion in den Begleitschreiben versicherte, die Daten würden anonymisiert und die Fragebogen nachher vernichtet, stellte sich heraus, dass die vorliegenden Ergebnisse dennoch nach Personen auswertbar blieben. Der Fragebogen war so aufgebaut, dass auch nach einer Anonymisierung der Daten mittels der vorgesehenen EDV-Auswertung die betroffenen Lehrpersonen eruierbar waren und die Daten auch bezüglich der Zufriedenheit mit der einzelnen Lehrperson ausgewertet werden konnten. Die Befürchtungen, die uns gegenüber geäussert wurden, dass die erhobenen Daten missbraucht und insbesondere zweckentfremdet zu Leistungsbeurteilungen des Lehrpersonals benützt werden könnten, waren nicht auszuschliessen.

Aus der Untersuchungsanordnung erschien es uns nicht zwingend, dass auf den Fragebogen die Namen von Lehrerinnen und Lehrern respektive von Schülerinnen und Schülern erfasst werden. Diese Angaben waren für die wissenschaftliche Auswertung weder geeignet noch erforderlich (Prinzip der Verhältnismässigkeit, § 4 Abs. 3 DSG). Um gewisse Aussagen bestimmten Klassen zuzuordnen, wäre es möglich gewesen, die Fragebogen entsprechend zu codieren und nach deren Verteilung/Adressierung den Schlüssel zu vernichten.

Mit den solcherart anonymisierten Fragebogen hätten sich Datensicherheitsmassnahmen bei der Auswertung erübrigt (§ 12 Abs. 1 lit. a DSG).

Da die Daten auch nach der Anonymisierung in einer Form vorlagen, die Rückschlüsse auf betroffene Personen zuliessen, war das Prinzip der Zweckbindung der erhobenen Daten nicht gewährleistet (§ 4 Abs. 4 DSG). Des weiteren bestand keine vertragliche Vereinbarung mit der beauftragten Firma bezüglich des Datenschutzes (§ 13 DSG).

Es drängten sich daher verschiedene Massnahmen auf, deren Umsetzung wir der Erziehungsdirektion empfahlen.

Die Erziehungsdirektion verpflichtete darauf die beauftragte Firma vertraglich zur Beachtung der datenschutzrechtlichen Erfordernisse (ausschliesslich zweckgebundenes Bearbeiten der erhobenen Daten, keine Weitergabe dieser Daten nach aussen, Unterstellung unter die amtliche Schweigepflicht sowie Beachtung der Datensicherheit). Des weiteren war sicherzustellen, dass die Privatfirma die Unterlagen nach Beendigung der Untersuchung nicht der Erziehungsdirektion herausgab und damit eine zweckwidrige Verwendung möglich machte. Vertraglich verzichtete die Erziehungsdirektion daher auf die Herausgabe der erhobenen Datenbestände und beauftragte die Privatfirma, sämtliche Unterlagen nach Abschluss der Auswertungen sachgerecht und irreversibel zu vernichten.

Obwohl die Umfrage ohne Konsultation des Datenschutzbeauftragten lanciert worden war, wurde dank unseren Interventionen der Datenschutz sichergestellt. Danach konnte der Regierungsrat in Beantwortung einer Interpellation im Kantonsrat (Umfrage an der Sekundarstufe I; KR-Nr. 214/1996, 28. August 1996) bestätigen, dass bei dieser Umfrage die Bestimmungen des Datenschutzgesetzes eingehalten werden.

2. Datenschutzrechtliche Fragen beim Erkennungsdienst

Revisionsbedürftigkeit der einschlägigen Verordnung

Im Sommer 1994 war ein 17jähriger Jugendlicher im Zusammenhang mit einer von einer Jugendbande begangenen Sachbeschädigung festgenommen und anschliessend von der Polizei erkennungsdienstlich behandelt worden. Mangels Strafantrages hatte der Sachverhalt jedoch nicht näher ermittelt werden können. Folgerichtig hatte die Jugendanwaltschaft den Fall eingestellt, mit dem ausdrücklichen Hinweis, dass die Beteiligung der einzelnen Jugendlichen unterschiedlich gewesen sei. Zwei Jahre später war ein Mann, der Opfer eines Raubes geworden war, von der Polizei zur Durchsicht der einschlägigen Fotokartei aufgeboten worden. Dieser Mann hatte auf einem der vorgelegten Fotos zwar nicht den Räuber, jedoch den oben erwähnten Jugendlichen erkannt, der in der Zwischenzeit als Sportler ziemlich bekannt geworden war. Er hatte eine grosse Story gewittert und sich an die Medien gewandt, die an dem Fall selbstverständlich sehr interessiert gewesen waren; erst im letzten Moment hatte eine grossangelegte Berichterstattung in einem bekannten Boulevardblatt verhindert werden können. Der Rechtsvertreter des betroffenen Jugendlichen informierte uns über diesen Sachverhalt zur Prüfung weitergehender Massnahmen. Wir klärten ab, inwieweit die «Verordnung über die erkennungsdienstliche Behandlung von Personen» vom 22. Dezember 1960 noch den Erfordernissen des Datenschutzes entspricht. Dabei stellten wir einleitend fest, dass ein erkennungsdienstliches Verfahren aufgrund seiner Bedeutung und praktischen Ausgestaltung bis zum Eingreifen der zuständigen Bezirksanwaltschaft noch kein hängiges Verfahren gemäss § 3 lit.b DSG darstellt, weshalb das Datenschutzgesetz uneingeschränkt zur Anwendung gelangt.
Bei den aufgrund einer erkennungsdienstlichen Behandlung gewonnenen Daten handelt es sich zwar lediglich um allgemein wahrnehmbare Äusserlichkeiten einer betroffenen Person wie Grösse, Postur, Haarfarbe oder Fingerabdruck. Jedoch sind sie erhoben worden im Hinblick auf ein strafrechtliches Verfahren, weshalb sie gemäss § 2 lit. d Ziff. 4 DSG besonders schützenswert sind. An ihre Bearbeitung ist, gestützt auf § 5 DSG, ein strenger Massstab anzulegen. Somit genügt es nicht, wenn die wenigen und knappen Bestimmungen der Verordnung lediglich in polizeiinternen Merkblättern oder Dienstanordnungen konkretisiert werden. Um die nötige Transparenz, auch für die betroffenen Personen, zu ermöglichen, ist vielmehr eine klare gesetzliche Regelung zu verlangen. Im einzelnen ist bei der bestehenden Verordnung zu beanstanden, dass sie nicht präzise festlegt, unter welchen Voraussetzungen erkennungsdienstliche Unterlagen aufzubewahren sind; klar zu differenzieren wäre nach den unterschiedlichen Abschlussarten wie Freispruch, Einstellung oder Verurteilung. Geregelt ist auch nicht, unter welchen Umständen respektive zu welchen Zwecken das anlässlich einer konkreten Untersuchung erstellte erkennungsdienstliche Material weiterverwendet werden kann. Dieser Mangel ist gravierend, weil eine betroffene Person beispielsweise durch die Publikation von Fahndungsfotos schwerste Beeinträchtigungen in ihrer Persönlichkeit erleiden kann. Schliesslich muss auch die Aufbewahrung von erkennungsdienstlichen Unterlagen zeitlich limitiert werden. Dabei müssen die Fristen zur Schwere der verfolgten Tat in einem sinnvollen Verhältnis stehen; es geht nicht an, die polizeilich gesammelten Daten darüber hinaus aufzubewahren mit Hinweis auf eine auch später noch mögliche oder nützliche Verwertbarkeit. Schliesslich empfahlen wir, dass die Rechte der erkennungsdienstlich behandelten Personen in der entsprechenden Verordnung ausdrücklich verankert werden.

Die Polizeidirektion hat einen Handlungsbedarf in bezug auf diese Bestimmungen der Verordnung anerkannt und entsprechende Korrekturen in Aussicht gestellt. Diesbezügliche Gespräche mit Vertretern von Kantons- und Stadtpolizei Zürich haben stattgefunden.

3. Mitteilungen von Untersuchungshandlungen gegenüber Lehrpersonal

Prinzip der Verhältnismässigkeit nicht beachtet

Verschiedentlich wurden wir angefragt, wann in einem polizeilichen Ermittlungsverfahren oder in einer laufenden Strafuntersuchung gegenüber einer Lehrerin oder einem Lehrer der Sachverhalt der Erziehungsdirektion als deren Arbeitgeber gemeldet werden könne oder müsse. Solche Mitteilungen sind sehr sensibel, da es sich einerseits um besonders schützenswerte Daten handelt, andererseits lediglich ein Verdacht vorliegt, weshalb eine Beteiligung oder eine Schuld der fraglichen Lehrperson am zu ermittelnden Delikt noch keineswegs feststeht.
Während im polizeilichen Ermittlungsverfahren das Datenschutzgesetz unmittelbar anwendbar ist, ist es in hängigen Verfahren der Strafrechtspflege ausgeschlossen (§ 3 Abs. 2 lit b DSG). Die Grundsätze des Persönlichkeitsschutzes, die sich aus dem verfassungsmässigen Recht der persönlichen Freiheit herleiten, sind indessen in beiden Verfahren gleich zu beachten. Im Strafverfahren regeln die Weisungen für die Untersuchungsführung der Staatsanwaltschaft, unter welchen Voraussetzungen bereits die Eröffnung einer Strafuntersuchung an Dritte mitzuteilen ist. Die Weisungen halten fest, dass bei Untersuchungen gegen beamtete Personen dem Arbeitgeber diejenigen Sachverhalte zu melden sind, welche die berufliche Weiterverwendung in Frage stellen. In allen anderen Fällen ist erst der Abschluss des Verfahrens durch Strafbefehl oder Einstellung zu melden, ausser bei auch disziplinarrechtlich nicht relevanten Sachverhalten.
Ein gesonderter Abschnitt regelt den Fall von in Strafuntersuchung gezogenem Lehrpersonal. Ausdrücklich wird auf § 9 des Unterrichtsgesetzes und § 8 des Lehrerbildungsgesetzes hingewiesen, welche die Möglichkeit einer Einstellung im Dienst während der Dauer einer hängigen Strafuntersuchung vorsehen. Da aber die Sonderbestimmungen bezüglich Lehrpersonal nur die allgemeinen Grundsätze der Weisungen konkretisieren, sind während der laufenden Untersuchung auch hinsichtlich Lehrpersonal ausschliesslich solche Delikte zu melden, die sich auf die Lehrertätigkeit auswirken (also beispielsweise Verdacht auf Kindsmisshandlung oder -missbrauch, nicht jedoch Geschwindigkeitsübertretungen oder ähnliches).
Wir stellten fest, dass die Weisungen in der Praxis undifferenziert angewendet werden, indem alle Untersuchungseröffnungen mitgeteilt werden. Wir haben gegenüber den zuständigen Stellen mehrfach klar zum Ausdruck gebracht, dass damit das Prinzip der Verhältnismässigkeit verletzt wird, das besagt, dass nur Daten, die geeignet und erforderlich sind, bearbeitet werden dürfen.
Eine Überarbeitung der Weisungen wurde in Aussicht gestellt.

4. Umgang mit Krankengeschichten

Herausgabeanspruch und Einsichtsrechte

In verschiedenen Fällen wurden wir von betroffenen Personen bezüglich des Einsichtsrechts in ihre Krankengeschichte und in bezug auf deren Herausgabe konsultiert.
Ein Patient, dessen Klinikaufenthalt über 10 Jahre zurücklag, verlangte bei der Klinikdirektion die Herausgabe seiner Krankengeschichte. Dies wurde ihm aus prinzipiellen Gründen verweigert, nachdem die Klinikdirektion mit der Gesundheitsdirektion Rücksprache genommen hatte. In der Begründung wurde festgehalten, dass aufgrund von § 13 der Patientenrechtverordnung (PatRV) das Eigentum der Krankengeschichte beim Krankenhaus liege und dass diese während mindestens zehn Jahren aufbewahrt bleibe. Über die weitere Aufbewahrung entscheide der Chefarzt gemäss § 13 Abs. 2 PatRV, allenfalls könne die Klinik die Vernichtung anordnen, da die zehnjährige Aufbewahrungsdauer

abgelaufen sei. Ein Herausgabeanspruch wurde grundsätzlich abgelehnt. Die Klinik entschied sich für die weitere Aufbewahrung der Krankengeschichte.
In unseren Schreiben an die Klinik und die Gesundheitsdirektion wiesen wir darauf hin, dass die Bestimmung von § 13 Abs. 2 PatRV als reine Kompetenznorm zu betrachten sei und für die weitere Aufbewahrung der Krankengeschichte eine gesetzliche Grundlage oder die Einwilligung der betroffenen Person notwendig sei. Im übrigen war darauf hinzuweisen, dass ein Herausgabeanspruch für die Krankengeschichte im privatrechtlichen Bereich bereits aufgrund der auftragsrechtlichen Bestimmungen (Art. 400 OR) gegeben ist. Des weiteren hat das Bundesgericht für diesen Bereich festgehalten, dass das Eigentum an der Krankengeschichte beim Patienten liege (BGE 119 II 222ff.). Eine unterschiedliche Behandlung im öffentlich-rechtlichen Bereich müsste aus einem überwiegenden öffentlichen Interesse gegeben sein. Unsere Stellungnahme führte dazu, dass die Klinikleitung auf die weitere Aufbewahrung der Krankengeschichte verzichtete und diese in Anwesenheit der betroffenen Person vernichtete. Auf die grundlegenden Fragen wurde nicht eingetreten (siehe auch S. 40).
Beim Einsichtsrecht in die eigene Krankengeschichte stellte sich vor allem die Frage, wieweit Informationen von Dritten dem Gesuchsteller gegenüber abgedeckt werden können. § 14 Abs. 2 lit. a PatRV besagt, dass keine Einsicht in Angaben von nicht zum Krankenhaus gehörenden Drittpersonen gewährt werde. Diese Bestimmung widerspricht § 17 DSG und ist deshalb rechtswidrig. Das Bundesgericht hat in einem Entscheid (BGE 122 I 153 ff.) diese Rechtsauffassung bestätigt.
Grundsätzlich ist einer gesuchstellenden Person eine vollständige Auskunft zu erteilen, wobei im konkreten Einzelfall eine Interessenabwägung, insbesondere mit schützenswerten Interessen Dritter, stattzufinden hat (§ 18 DSG). Jede Einschränkung des Einsichtsrechts ist dabei zu begründen (§ 20 DSG). Im zitierten Bundesgerichtsentscheid, der eine zürcherische Klinik betraf, wurde zwar die Auslegung von § 14 Abs. 2 lit. a PatRV im konkreten Fall als nicht willkürlich bezeichnet; es wurde indessen ausdrücklich darauf hingewiesen, dass das kantonale Datenschutzgesetz zum damaligen Zeitpunkt noch nicht anwendbar war.
Die Gesundheitsdirektion hat in einem Kreisschreiben zur PatRV diesen Bundesgerichtsentscheid diesbezüglich nicht berücksichtigt (siehe S. 40).

---

5. Umfrage über Spitalzufriedenheit
Ausdrückliche Zustimmung notwendig

Das Kantonsspital Winterthur plante, die Erfahrungen von spitalentlassenen Patientinnen und Patienten wissenschaftlich auszuwerten, um künftig vermehrt auf deren Wünsche einzugehen sowie die Betreuungsqualität zu sichern und zu optimieren. Einer privaten Firma sollten für entsprechende Interviews Namen, Alter, Telefonnummer, Versicherungsklasse und behandelnde Klinik einer grossen Anzahl von ehemaligen Patientinnen und Patienten zugestellt werden, wobei die Teilnehmenden nach Zufallsprinzip auszuwählen waren. Die Direktion des Spitals entwarf in der Folge einen Brief, worin die betroffenen Personen um ihr Einverständnis für eine entsprechende Weiterleitung ihrer Daten angefragt wurden; ein Stillschweigen wurde dabei als Zustimmung gedeutet, währenddem eine Absage innert weniger Tage mitzuteilen gewesen wäre. Dieser Briefentwurf wurde uns zur Stellungnahme unterbreitet.
Bei Daten von Patientinnen und Patienten handelt es sich um den Gesundheitsbereich betreffende und somit besonders schützenswerte Personendaten, deren Bearbeitung strikten Anforderungen genügen muss (§ 5 i.V. mit § 2 lit. d DSG): Entweder ist eine klare gesetzliche Grundlage vorhanden, oder eine gesetzlich klar umschrie-

bene Aufgabe lässt die Daten unentbehrlich erscheinen. Falls weder die eine noch die andere Voraussetzung erfüllt ist, darf die Datenbearbeitung nur gestützt auf eine Einwilligung der betroffenen Personen erfolgen.
Im vorliegenden Sachverhalt stand die Zustimmung der betroffenen Personen im Vordergrund (Art. 321 Abs. 2 StGB). Bei solchen Fällen ist mit Vorteil eine ausdrückliche Zustimmungserklärung einzuholen; zumindest aber ist ein klarer und gut sichtbarer Hinweis erforderlich, dass die geplante Datenbearbeitung auf absolut freiwilliger Basis durchgeführt wird, weshalb die Zustimmung ohne weiteres verweigert werden kann. Ausserdem muss bei einer systematischen Befragung der austretenden Patientinnen und Patienten gemäss § 7 Abs. 2 DSG sowohl die Rechtsgrundlage wie auch der Zweck der Bearbeitung bekanntgegeben werden. Schliesslich rieten wir dem anfragenden Spital, gegenüber der privaten Firma mittels Vereinbarung aufgrund von § 13 DSG für die Beachtung des Datenschutzes zu sorgen.

6. Volkszählung 2000 / Vollautomatisches Strafregister

Mitberichte im Vernehmlassungsverfahren

In zahlreichen Vernehmlassungsverfahren wurden wir zu Mitberichten eingeladen. Aus datenschutzrechtlicher Sicht haben wir zu den Gesetzesänderungen in bezug auf die Volkszählung 2000 und das vollautomatisierte Strafregister Vorbehalte anbringen müssen.
Die vorgesehene Teilrevision des Volkszählungsgesetzes und des Bundesstatistikgesetzes in bezug auf die Volkszählung 2000 beinhaltet einen übermässigen Eingriff in die Grundrechte der betroffenen Personen, da sie das Zweckbindungsgebot und das Statistikgeheimnis umgeht. Die Revision sieht vor, dass die für statistische Zwecke erhobenen Daten zur Nachführung von administrativen Registern der Verwaltung herangezogen werden. Zwar wird hierfür mit der neuen Gesetzesbestimmung die formelle gesetzliche Grundlage geschaffen, materiell beinhaltet diese Bestimmung aber eine Abkehr vom datenschutzrechtlichen Grundprinzip der Zweckbindung erhobener Daten. Der Datenschutz erfährt dadurch in diesem Bereich eine wesentliche Einschränkung. Die Bürgerinnen und Bürger haben Anspruch darauf, dass zum Zweck der Statistik erhobene Personendaten, zu deren Bekanntgabe sie nach bisherigem Recht unter Strafdrohung und nach vorgesehenem neuen Recht unter Kostenfolgen angehalten werden, nicht zu Verwaltungszwecken bearbeitet werden. Das Vertrauen in die Statistik als Garantin einer nicht personenbezogenen Datenbearbeitung wird andernfalls missbraucht. Dies wird ebenfalls zur Folge haben, dass die Bereitschaft zur Mitwirkung an den statistischen Erhebungen und somit deren Qualität in Frage gestellt wird. Im übrigen sieht auch die Empfehlung des Europarates zum Schutze von Personendaten, die zu statistischen Zwecken erhoben und bearbeitet werden, eine klare Zweckbindung statistischer Daten vor. Die Verwendung von statistischen Daten zur Nachführung von Verwaltungsregistern bedeutet zudem eine Durchbrechung des Statistikgeheimnisses.

Im Rahmen von Massnahmen zur Verbesserung der Effizienz und der Rechtsstaatlichkeit in der Strafverfolgung sollen Rechtsgrundlagen für die Schaffung eines automatisierten Strafregisters («Vostra») geschaffen werden. Wir haben im Vernehmlassungsverfahren darauf hingewiesen, dass mit dem automatisierten Strafregister ein komplexes Informatiksystem aufgebaut wird, dessen notwendige, formell gesetzliche Grundlagen die Revision beinhalten. Hingegen sind ungenügende Anhaltspunkte vorhanden, wie die damit verbundenen hohen Gefährdungen für die Persönlichkeitsrechte der betroffenen Personen materiell

gelöst werden sollen. Insbesondere die Rechte der betroffenen Personen und die organisatorischen und technischen Massnahmen in bezug auf die Datensicherheit sind nicht konkretisiert. Des weiteren fehlen Angaben zu der Ausgestaltung der Zugriffsmöglichkeiten innerhalb des Kantons. Wir behielten uns deshalb die datenschutzrechtliche Überprüfung der kantonalen Regelung vor.

---

7. IV-Daten an die Fremdenpolizei
Keine Weitergabe ohne Einwilligung

Die Fremdenpolizei ersuchte die IV-Stelle (Invalidenversicherung) der Sozialversicherungsanstalt im Zusammenhang mit Gesuchen zur Verlängerung der Aufenthaltsbewilligung um Angaben über ausländische Staatsangehörige, insbesondere ob IV-Abklärungsmassnahmen oder berufliche Eingliederungsmassnahmen in der Schweiz gewährt würden, und gegebenenfalls um Zustellung einer Kopie der entsprechenden Verfügung.
Die Sozialversicherungsanstalt stellte sich – nach Rücksprache mit dem Bundesamt für Sozialversicherung – auf den Standpunkt, dass Auskünfte lediglich erteilt werden, wenn ein schriftliches, begründetes Gesuch der Fremdenpolizei im Einzelfall vorliegt, aus dem hervorgeht, dass die Auskünfte zum Zwecke der Verlängerung der Aufenthaltsbewilligung benötigt werden, und wenn die Auskünfte im Interesse der betroffenen Person sind und somit von einer mutmasslichen Einwilligung ausgegangen werden kann. In diesem Fall wird lediglich mitgeteilt, welche IV-Abklärungsmassnahmen oder Eingliederungsmassnahmen tatsächlich durchgeführt werden und wie lange sie voraussichtlich dauern. Die IV-Stelle legte uns ihre Rechtsauffassung zur Beurteilung vor. Wir konnten uns dieser grundsätzlich anschliessen. Gesetzliche Grundlagen in Form von Mitteilungsrechten oder -pflichten, die der Sozialversicherungsanstalt erlauben würden, der Fremdenpolizei die erwünschten Unterlagen weiterzugeben, bestehen keine.
Eine stillschweigende Einwilligung der betroffenen Person darf nur in klaren, d.h. für die betroffene Person günstigen Fällen angenommen werden. Daher stellte sich die Frage nach der Möglichkeit zur Amtshilfe im Einzelfall.
Gemäss dem Prinzip der Subsidiarität ist die Amtshilfe nur zulässig, wenn keine anderen Mittel zur Verfügung stehen, um eine gesetzliche Aufgabe zu erfüllen. Für die Fremdenpolizei besteht ohne weiteres die Möglichkeit, ihre Verwaltungsaufgabe zu erfüllen, indem sie sich direkt an die betroffene Person wendet, diese befragt, einen Nachweis verlangt oder eine ausdrückliche Einwilligung zur Rückfrage bei der Sozialversicherungsanstalt einholt. Die Amtshilfeleistung hat auch deshalb zu unterbleiben, weil ihr eine besondere gesetzliche Schweigepflicht aufgrund Art. 50 Abs. 1 AHVG und Art. 60 IVG entgegensteht. § 10 lit. b DSG sieht vor, dass öffentliche Organe die Datenbekanntgabe abzulehnen oder einzuschränken haben, wenn gesetzliche Geheimhaltungspflichten oder besondere Datenschutzvorschriften es verlangen. Eine Datenbekanntgabe der IV-Stelle an die Fremdenpolizei ist deshalb nur aufgrund einer Einwilligung der betroffenen Person gemäss § 8 Abs. 1 lit. b DSG möglich. Die Fremdenpolizei muss sich in diesen Fällen an die betroffene Person wenden.

8. Gebäudedaten als Personendaten

Fragen der Herausgabe an Dritte

Die Finanzdirektion forderte das Statistische Amt und die Gebäudeversicherung zu einem Datentransfer an eine private Firma im Zusammenhang mit einem Gutachten betreffend die Überarbeitung einer regierungsrätlichen Weisung über die Liegenschaftenbewertung und die Festsetzung der Eigenmietwerte auf. Wir wurden um eine Beurteilung aus datenschutzrechtlicher Sicht gebeten. Ebenfalls zur Stellungnahme wurde uns eine Vorstudie betreffend das Projekt über Gebäudedaten des GIS-DLZ (Geographisches Informations-System Dienstleistungszentrum) vorgelegt. In beiden Fällen waren die Fristen so kurz bemessen, dass wir in einer summarischen Antwort nur die allgemeinen Grundsätze darlegen konnten.

Verschiedene Amtsstellen im Kanton Zürich bearbeiten im Rahmen ihrer Aufgaben Daten über Grundstücke resp. Gebäude. Entgegen einer verbreiteten Meinung sind Gebäudedaten nicht einfach Sachdaten. Als Personendaten gelten gemäss § 2 lit. a DSG Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen. Sobald die Gebäudedaten ausreichen, um das Gebäude zu individualisieren, d.h. die Adresse oder die Katasternummer des Grundstückes festzustellen, sind – im Zusammenhang mit dem Grundsatz der Öffentlichkeit des Grundbuches nach Art. 970 ZGB – die jeweiligen Eigentümer bestimmbar. Dadurch ist der Personenbezug gegeben, und es handelt sich bei den Gebäudedaten um Personendaten.

Die Bekanntgabe von Personendaten durch öffentliche Organe ist an die Voraussetzungen von § 8 DSG gebunden.

Beim geplanten Datentransfer im Zusammenhang mit der Überarbeitung der Weisung waren diese Bedingungen nicht erfüllt. In Frage kam allerdings ein Bearbeiten im Auftrag gemäss § 13 DSG. Grundsätzlich kann das verantwortliche Organ einen Dritten – sei es ein anderes öffentliches Organ, sei es einen Privaten – mit einer Datenbearbeitung beauftragen. Dabei ist der Dritte an die Bestimmungen des DSG gebunden. Im vorliegenden Fall bestand insbesondere die Gefahr, dass das Zweckbindungsgebot nach § 4 Abs. 4 DSG verletzt werden könnte. Der privaten Firma hätten die gemäss § 35c Grundbuchverordnung nicht veröffentlichten Angaben über die Gegenleistung bei Handänderungen von kantonseigenen Grundstücken übermittelt werden sollen. Auch wenn die private Firma die datenschutzrechtlichen Vorschriften einzuhalten bereit gewesen wäre, war nicht sichergestellt, dass sie diese Kenntnisse nur zum vorgesehenen Zweck verwendet hätte. Den Mitarbeiterinnen und Mitarbeitern dieser Firma wären Informationen bekannt geworden, die sie im Rahmen ihrer übrigen Tätigkeit nicht einfach «vergessen» könnten. Damit hätte die Firma einen ungerechtfertigten Marktvorteil erlangt. Aus datenschutzrechtlicher Sicht handelt es sich dabei um eine Zweckentfremdung von Daten.

Aufgrund unserer diesbezüglichen Bedenken wurde der Gutachterauftrag neu formuliert, so dass nur noch aggregierte Daten, d.h. errechnete Durchschnittswerte, zur Verfügung zu stellen waren. Eine personen- oder objektbezogene Individualisierung liess sich nicht mehr herstellen, womit die Anforderungen des Datenschutzes erfüllt waren.

Das Projekt des GIS-DLZ sieht die Zusammenführung von Daten verschiedener öffentlicher Organe vor. Dabei sind drei Lösungsvarianten mit verschiedenen Integrationsstufen vorgesehen. In diesem Zusammenhang stellte sich die Frage nach der Rechtsgrundlage für die Datenbekanntgabe durch die involvierten Amtsstellen, die nur in Einzelfällen vorhanden sein dürfte. Je integrierter die Lösung aussehen würde, um so weniger vermögen die bestehenden Rechtsgrundlagen zu genügen. Wenn mehrere Organe dieselben Daten bearbeiten, stellt sich auch die Frage nach der Datenhoheit resp. der Verantwortung für die Datenbearbeitung. Wird eine gemeinsame Datensammlung betrieben, so ist ein hauptverantwortliches Organ zu bezeichnen (§ 6 Abs. 2 DSG).

Beim Projekt des GIS-DLZ standen weiter Aspekte der Datensicherheit

zur Diskussion. Personendaten sind gemäss § 4 Abs. 5 DSG durch angemessene organisatorische und technische Massnahmen gegen das unbefugte Bearbeiten zu schützen. Diese Massnahmen müssen dem Stand der Technik entsprechen (§ 1 Abs. 2 DSV). Sie haben sich insbesondere auf die in § 2 DSV aufgeführten Bereiche zu beziehen. Aus der Sicht der Datensicherheit wäre eine integrierte Lösung zu bevorzugen, da sich hier die Massnahmen leichter realisieren liessen. Bei der Wahl dieser Variante müssten aber die noch fehlenden Rechtsgrundlagen geschaffen werden.

9. Datenschutz und Parlamentarische Untersuchungskommission

Anwendbarkeit des Datenschutzgesetzes

Eine Anfrage der Parlamentarischen Untersuchungskommission (PUK), welche die Vorkommnisse in der sogenannten «Wirteaffäre» untersucht, betraf die Frage nach den datenschutzrechtlichen Aspekten der Tätigkeit der PUK, insbesondere in bezug auf die Veröffentlichung des Berichts.
Nach Abschluss der Untersuchungen erstattet eine Parlamentarische Untersuchungskommission dem Kantonsrat einen schriftlichen Bericht (§ 34n des Kantonsratsgesetzes). Dieser Bericht wird regelmässig zuhanden der Medien und der Bevölkerung veröffentlicht.
Eine Prüfung des Geltungsbereiches des DSG ergab, dass dieses auf die PUK anwendbar ist. Für das Verfahren der PUK wird zwar verschiedentlich auf das Verwaltungsrechtspflegegesetz (VRG) sowie auf die Zivilprozessordnung (ZPO) verwiesen. Trotzdem ist dieses Verfahren nicht als hängiges Verfahren im Sinne von § 3 Abs. 2 lit. b DSG zu betrachten. Der Ausschluss der hängigen Verfahren der Zivil-, Verwaltungs- und Strafrechtspflege vom Geltungsbereich des Datenschutzgesetzes wurde geschaffen, weil die Rechtspflegegesetze in der Regel Bestimmungen über den Persönlichkeitsschutz der Verfahrensbeteiligten enthalten und deshalb ein Konflikt mit dem Datenschutzgesetz vermieden werden sollte. Partielle Verweise auf gewisse Bestimmungen in anderen Verfahrensrechten reichen daher nicht aus, um das DSG auszuschliessen, weil wesentliche Elemente eines Rechtspflegeverfahrens bei den Untersuchungen der PUK nicht erfüllt sind. Ein Ausschluss der PUK vom Geltungsbereich des DSG müsste deshalb ausdrücklich statuiert sein, wie dies beispielsweise im Kanton Bern oder im Bund geschehen ist.
Bei der Veröffentlichung von Personendaten im PUK-Bericht handelt es sich um eine Datenbekanntgabe im Sinne von § 8 DSG, für die eine gesetzliche Grundlage in § 34n des Kantonsratsgesetzes besteht. In bezug auf die Veröffentlichung von Personendaten sind jedoch die Prinzipien der Verhältnismässigkeit und der Zweckbindung zu beachten.
Ausgehend von den Aufgaben des Kantonsrates und dem konkreten Mandat der PUK sind all jene Daten geeignet und erforderlich, die dem Kantonsrat erlauben, seine Aufsichtsrechte wahrzunehmen, und wo es darum geht zu beurteilen, ob der Kantonsrat Massnahmen (z.B. Disziplinarverfahren oder Schadenersatzforderungen) zu treffen hat. Im wesentlichen sind damit Angaben über Amtspersonen gemeint, die der Aufsicht des Kantonsrates unterliegen resp. unterlagen. Anders verhält es sich bei Personen, die nicht der Aufsicht des Kantonsrates unterstehen wie beispielsweise Sachverständige oder Zeugen. Daten dieser Personen, soweit sie nicht für das Verständnis der Sachverhaltsdarstellung notwendig sind, können nur mit deren Einwilligung veröffentlicht werden.
Das Zweckbindungsgebot untersagt die Verwendung von Daten für Zwecke, die nicht bei der Beschaffung angegeben wurden, weder aus den Umständen ersichtlich noch gesetzlich festgelegt sind. Aufgrund ihrer Informationsrechte – die gesetzlich vorgesehen sind – kann die PUK auch Daten einsehen und verwenden, die von den

Verwaltungsstellen zu anderen Zielen beschafft und bearbeitet werden. Einschränkend wirken aber auch hier das Verhältnismässigkeitsprinzip sowie die Pflicht zur Interessenabwägung gemäss § 10 DSG. Vor der Veröffentlichung hat die PUK daher zu prüfen, ob Daten von Drittpersonen (z.B. Briefe, Dokumente), die als Personen in die Untersuchung nicht involviert sind, aufgrund offensichtlich schützenswerter Interessen von einer Veröffentlichung auszunehmen sind. Dabei ist vor allem abzuklären, inwieweit die Person mit der Bekanntgabe solcher Daten durch die PUK zu rechnen hatte oder eine Erwähnung in diesem Rahmen sie belasten könnte. Unproblematisch ist die Veröffentlichung, wenn diesbezügliche Daten anonymisiert werden oder wenn die Zustimmung der betroffenen Person für die Bekanntgabe eingeholt werden kann.

10. Einsichtsrechte bei Archiven

Datenschutzrechtliche Behandlung von archivierten Personendaten

Verschiedene Anfragen betrafen die Frage nach der Behandlung von archivierten Personendaten, insbesondere bei Gesuchen um Akteneinsicht durch Dritte. Zwei Organen erstatteten wir ein Gutachten betreffend die archiv- resp. datenschutzrechtliche Behandlung solcher Daten. In einem weiteren Fall ersuchte eine Anstalt um Beratung im Zusammenhang mit einem Einsichtsgesuch eines Dritten in die Akten eines ehemaligen Insassen.
Das kantonale Archivgesetz, das in der Volksabstimmung vom 24. September 1995 angenommen wurde, ist bisher noch nicht in Kraft gesetzt worden, weshalb die VO über das Staatsarchiv vom 10. April 1974 (ArchivVO) weiterhin Gültigkeit besitzt. Grundsätzlich ist das Datenschutzgesetz auf den Bereich der Archivierung anwendbar, da das Aufbewahren von Daten vom Datenschutzgesetz umfasst wird (§ 1 und § 2 lit. f DSG).
Das Prinzip der Verhältnismässigkeit bestimmt, dass Daten für die Erfüllung der Aufgaben geeignet und erforderlich sein müssen (§ 4 Abs. 3 DSG). Nicht mehr benötigte Personendaten sind deshalb zu vernichten (§ 14 Abs. 1 DSG). Das verantwortliche Organ hat für jede Datensammlung die Aufbewahrungsdauer festzulegen. Ausdrücklich behält das DSG die Bestimmungen der Archivierung vor (§ 14 Abs. 2 DSG). Daten sind demnach nicht zu vernichten, sofern sie archiviert werden.
Die ArchivVO sieht als Hauptzweck für die Aufbewahrung von Akten beim Staatsarchiv die Sicherstellung einer dauerhaften dokumentarischen Überlieferung vor. In § 4 des neuen Archivgesetzes wird dieser Zweck dahingehend präzisiert, dass damit rechtlichen, administrativen, kulturellen und wissenschaftlichen Zwecken gedient werden soll. Akten von langfristiger oder dauernder Bedeutung sind dem Staatsarchiv abzuliefern. § 8 des neuen Archivgesetzes statuiert eine Anbietungspflicht für die öffentlichen Organe gegenüber dem Staatsarchiv. Mit der Archivierung erfolgt demnach in bezug auf die ursprüngliche Datenbearbeitung eine Zweckänderung. Für diese Daten oder Akten sind nicht mehr die ursprünglich geltenden Rechtsgrundlagen massgebend, sondern diejenigen, welche die Archivierung regeln.
Gemäss § 6 ArchivVO sind Akten in der Regel frühestens nach zehn und spätestens nach 20 Jahren dem Staatsarchiv abzuliefern. § 7 ArchivVO regelt, dass diese Akten während 35 Jahren, vom Zeitpunkt ihrer Anlage an gerechnet, für private Benutzer nicht zugänglich sind. Das neue Archivgesetz verlängert diese Fristen bei Personendaten. Mit den Schutzfristen im Archivrecht wird eine Interessenabwägung in bezug auf die Einsichtsrechte vorweggenommen, indem Dritten generell erst nach Ablauf dieser Schutzfristen Einsicht gewährt wird. In Ausnahmefällen kann diese Einsicht früher gewährt

werden. Die Schutzfristen müssen auch gegenüber den abliefernden Stellen gelten, da sie nicht mehr aus eigenem Recht über die Daten verfügen können. Dieses Rückkoppelungsverbot ist als Konsequenz der Zweckänderung zwingend. Die ursprüngliche Verwaltungsstelle verliert ihre Verfügungsberechtigung, da sie die Grundsätze gemäss § 4 ff. DSG für die Bearbeitung dieser Daten nicht mehr erfüllt.
§ 1 lit. a ArchivVO ermächtigt das Staatsarchiv, diese Daten zu bearbeiten. Die Einsichtsrechte richten sich für private Personen wie auch Verwaltungsstellen nach den archivrechtlichen respektive datenschutzrechtlichen Bestimmungen. Nach Ablauf der erwähnten Schutzfristen stehen die Akten allgemein zur Verfügung. Allerdings ist auch dann § 10 DSG zu beachten. Die Einsicht kann eingeschränkt oder mit Auflagen verbunden werden, wenn wesentliche öffentliche oder offensichtlich schützenswerte Interessen einer betroffenen Person vorliegen (§ 10 lit. a DSG); des weiteren bei gesetzlichen Geheimhaltungspflichten oder besonderen Datenschutzvorschriften (§ 10 lit. b DSG). Grundsätzlich ist das Staatsarchiv für die Erteilung dieser Einsichtsrechte zuständig, wobei in bezug auf die Interessenabwägung die abliefernde Stelle (öffentliche Interessen) oder betroffene Personen (private Interessen) angehört werden können.
Bei Einsichtsgesuchen vor Ablauf der Schutzfrist stellt sich die Frage, wer über Ausnahmen bestimmt und nach welchen Kriterien diese bewilligt werden können. Grundsätzlich liegt die Verantwortung für die Bearbeitung der Personendaten bei demjenigen Organ, das die Daten zur Erfüllung seiner Aufgaben bearbeitet (§ 6 Abs. 1 DSG). Das Staatsarchiv ist demnach verantwortlich für die archivierten Akten. In bezug auf eine Ausnahmebewilligung hält § 7 ArchivVO allerdings systemwidrig fest, dass diese von der abliefernden Stelle zu erteilen ist. Nach welchen Kriterien solche Bewilligungen zu gewähren sind, wird in der ArchivVO nicht erwähnt. Das neue Archivgesetz ermöglicht Ausnahmen «aus wichtigen Gründen» (§ 10 Abs. 2; § 18 lit. a). Durch Auslegung ist deshalb zu bestimmen, in welchen Bereichen die wichtigen Gründe liegen müssen. Dabei ist wiederum von der Zweckbindung der im Archiv aufbewahrten Daten auszugehen. Eine Ausnahmebewilligung ist daher aufgrund rechtlicher, administrativer, kultureller oder wissenschaftlicher Zielsetzungen möglich. Das datenschutzrechtliche Zweckbindungsgebot verhindert eine andere Verwendung dieser Daten. Das Gesuch um eine Ausnahmebewilligung ist deshalb mit im Zweckbereich der Archivierung liegenden Interessen zu begründen. Der Entscheid hat die durch die Schutzfristen gewährleisteten Interessen (§ 10 DSG) abzuwägen. Nur wenn überwiegende Interessen beispielsweise wissenschaftlicher Art vorliegen, dürfen die Schutzfristen ausnahmsweise ganz, teilweise oder mit Auflagen durchbrochen werden.

Die Register der Datensammlungen

Das Erstellen der Register der Datensammlungen bedeutete für viele Verwaltungsstellen den ersten direkten Kontakt mit dem Datenschutzgesetz. Für die Bürgerinnen und Bürger schafft das Register die notwendige Transparenz der Datenbearbeitungen.

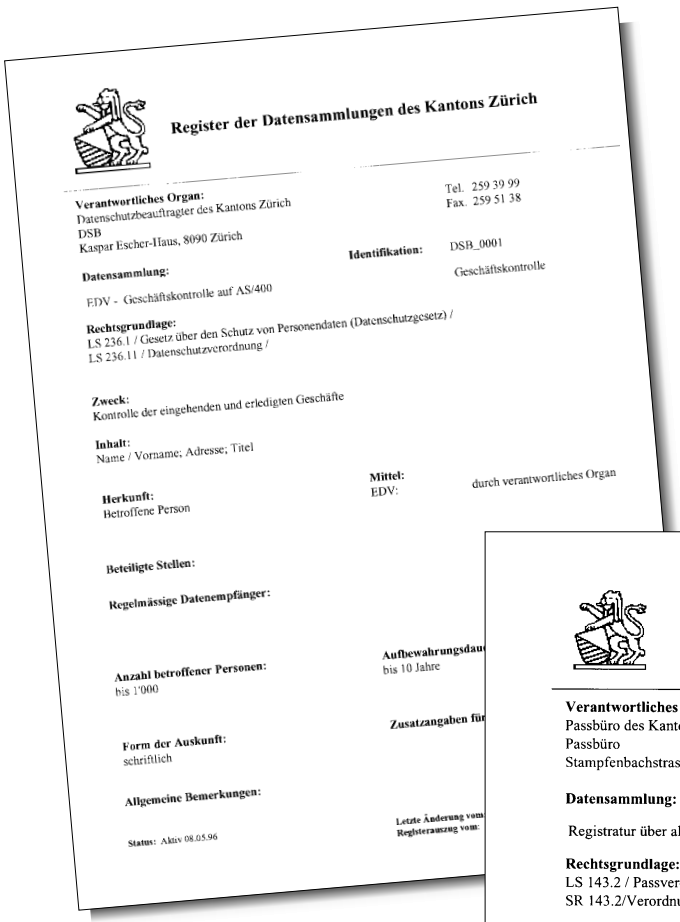
1. Zielsetzungen der Registrierung

Die Bedeutung von § 15 DSG

Jedes verantwortliche Organ, das Daten bearbeitet, hat ein öffentliches Register seiner Datensammlungen zu führen (§ 15 Abs. 1 DSG). Das Register schafft damit die gesetzlich vorgeschriebene Transparenz der Datenbearbeitungen der Verwaltung.
Es ist ein notwendiges Instrument jeder Verwaltungsstelle, die Personendaten bearbeitet, um ihre Verantwortung im Bereich des Datenschutzes und der Datensicherheit wahrnehmen zu können. Das Register gibt einen Überblick, welche Daten durch welche Stellen und mit welchen Mitteln bearbeitet werden. Es ist deshalb zugleich ein ausgezeichnetes Ordnungs- und Führungsinstrument für die Verwaltung, da es Handlungsbedarf und Handlungsmöglichkeiten aufzeigen kann. Es gibt Informationen über die Art und die Sensibilität von Daten, zeigt Datenflüsse auf und dient als Grundlage für die Planung und Überprüfung von Datensicherheitsmassnahmen.
Die Register der Datensammlungen ermöglichen es den betroffenen Personen, sich über das Bestehen von Datensammlungen zu informieren, um so zu erfahren, wo in der Verwaltung Personendaten über sie und zu welchem Zweck bearbeitet werden. Das Register dient somit auch der Wahrung der Rechte und Ansprüche der betroffenen Personen gemäss § 17 DSG (Auskunftsrecht) und § 19 DSG (Weitere Rechte). Für die Verwaltung wird damit ebenfalls eine effiziente Auskunftserteilung an Bürgerinnen und Bürger ermöglicht.
Der Inhalt des Registers ist durch die gesetzlichen Bestimmungen vorgegeben (§ 15 Abs. 2 DSG; § 8 Abs. 2 DSV). Über jede Datensammlung sind die folgenden Angaben zu registrieren:

- Rechtsgrundlage der Aufgabenerfüllung;
- Zweck der Bearbeitung;
- Mittel der Bearbeitung;
- Art der bearbeiteten Personendaten;
- Herkunft der Personendaten;
- Beteiligte Stellen an der Datensammlung;
- Regelmässige Datenempfänger;
- Anzahl der betroffenen Personen;
- Aufbewahrungsdauer der Daten.

Neben diesen gesetzlichen Angaben enthält das Register im weiteren die notwendigen administrativen Auskünfte zum verantwortlichen Organ (genaue Anschrift) und zur Wahrnehmung des Auskunftsrechts.
Gemäss § 15 Abs. 3 und 4 DSG in Verbindung mit § 8 Abs. 3–5 DSV sind gewisse Datensammlungen nicht zu registrieren oder die Registrierung ist nicht zu veröffentlichen.
Der Datenschutzbeauftragte hat die kantonalen und kommunalen Organe bei der Erstellung der Register der Datensammlungen unterstützt. Die Übergangsbestimmungen des DSG verlangen, dass die Register der Datensammlungen binnen zweier Jahre nach Inkrafttreten des DSG erstellt sind. Diese Frist lief für die kantonale Verwaltung am 31. Dezember 1996 ab, für die kommunalen Verwaltungen (politische Gemeinden, Schulgemeinden und Kirchgemeinden) hat der Regierungsrat auf begründetes Gesuch hin diese Frist bis zum 30. Juni 1997 erstreckt.



Register der Datensammlungen des Kantons Zürich

Verantwortliches Organ:
Datenschutzbeauftragter des Kantons Zürich
DSB
Kaspar Escher-Haus, 8090 Zürich
Tel. 259 39 99
Fax. 259 51 38

Datensammlung: EDV - Geschäftskontrolle auf AS/400
Identifikation: DSB_0001 Geschäftskontrolle

Rechtsgrundlage:
LS 236.1 / Gesetz über den Schutz von Personendaten (Datenschutzgesetz) /
LS 236.11 / Datenschutzverordnung /

Zweck:
Kontrolle der eingehenden und erledigten Geschäfte

Inhalt:
Name / Vorname; Adresse; Titel

Herkunft:
Betroffene Person

Mittel:
EDV: durch verantwortliches Organ

Beteiligte Stellen:

Regelmässige Datenempfänger:

Anzahl betroffener Personen:
bis 1'000

Aufbewahrungsdau
bis 10 Jahre

Form der Auskunft:
schriftlich

Zusatzangaben für

Allgemeine Bemerkungen:

Status: Aktiv 08.05.96

Letzte Änderung vom:
Registerauszug vom:

Register der Datensammlungen des Kantons Zürich

Verantwortliches Organ:
Passbüro des Kantons Zürich
Passbüro
Stampfenbachstrasse 17, 8090 Zürich
Tel. 259 20 34
Fax. 259 20 38

Datensammlung: Registratur über alle ausgestellten Pässe
Identifikation: SK_0001 Passdatensammlung

Rechtsgrundlage:
LS 143.2 / Passverordnung / § 12
SR 143.2/Verordnung über den Schweizerpass / Art. 17 Abs. 2 /

Zweck:
Sicherstellung eines geordneten Geschäftsablaufs im Passbüro

Inhalt:
Name / Vorname; Geschlecht; Zivilstand; Geburtsdatum / Alter; Adresse; Heimatort / Nationalität; Zivilrechtl. Handlungsfähigkeit; Strafrechtl. Verfahren/Sanktionen; - Passnummer; - Ausstellungs- und Ablaufdatum des Passes; - Personalien der Kinder bei Kindereinträgen
Strafrechtliche Verfahren/Sanktionen: Durch Untersuchungs- und Gerichtsbehörden verfügte Passsperren.

Herkunft:
Betroffene Person; Eigene Erhebung; Von Dritten

Mittel:
EDV: durch verantwortliches Organ

Beteiligte Stellen:

Regelmässige Datenempfänger:

Anzahl betroffener Personen:
über 100'000

Aufbewahrungsdauer der Daten:
über 20 Jahre

Form der Auskunft:
schriftlich; mündlich (am Schalter / im Büro); Einsichtnahme

Zusatzangaben für Auskunftsbegehren:
Ausweisnummer; Kopie Personalausweis; Geburtsdatum; Angabe über Ereignis

Allgemeine Bemerkungen:

Status: Aktiv 25.06.96

Letzte Änderung vom: 25.06.96
Registerauszug vom: 28.02.97

Auszüge aus dem Register der Datensammlungen der kantonalen Verwaltung

2. Die Register der kantonalen Verwaltung

Automatische Zugriffsmöglichkeit

Die Register der kantonalen Verwaltung und der kantonalen öffentlichen Einrichtungen werden beim Datenschutzbeauftragten zu einem zentralen Register zusammengeführt (§ 16 DSG in Verbindung mit § 8 DSV). Um den administrativen Aufwand für die Erfassung der einzelnen Register und des Zentralregisters klein zu halten, erfolgte die Erfassung der Datensammlungen auf kantonaler Ebene EDV-gestützt.
Mit Weisung vom 17. Januar 1996 haben wir die betroffenen Direktionen und Verwaltungsstellen über das Vorgehen betreffend die Erstellung der Register informiert. Jede Direktion erhielt die notwendigen Informationen und konnte von einem entsprechenden Ausbildungsangebot des Datenschutzbeauftragten und einer ständigen Unterstützung profitieren. Innerhalb der Frist bis zum 31. Dezember 1996 konnten 420 registrierte Datensammlungen gezählt werden. Nicht alle Direktionen sind fristgerecht ihren gesetzlichen Verpflichtungen nachgekommen. Indessen haben alle säumigen Direktionen gegenüber dem Datenschutzbeauftragten erklärt, ihre Verpflichtungen bis Ende des ersten Quartals 1997 erfüllen zu wollen.
Die Direktionen, welche die Registrierung abgeschlossen haben, unterzeichneten eine Erklärung, dass sämtliche ihrer Datensammlungen registriert wurden und dass keine weiteren registrierungspflichtigen Datensammlungen bestehen. Diese Direktionen und Verwaltungsstellen verfügen nun über das gesetzliche Register der Datensammlungen, das von allen Personen, die es wünschen, eingesehen werden kann.
Diese Datensammlungen sind beim Datenschutzbeauftragten in einem zentralen Register zusammengefasst. Auch dieses Register ist öffentlich und kann jederzeit eingesehen werden. Es bietet dem Datenschutzbeauftragten die Grundlage, um im Einzelfall und generell die Rechtmässigkeit der Datenbearbeitungen überprüfen zu können. Diese allgemeine Aufgabe wird noch einige Zeit in Anspruch nehmen. Das zentrale Register wird durch den Datenschutzbeauftragten periodisch veröffentlicht. Eine geeignete Form der Publikation im Rahmen des Tätigkeitsberichts, die auch in sinnvoller Art und Weise die Veränderungen in den Registern berücksichtigt, wird zurzeit geprüft.

3. Die kommunalen Register

Aufbau mittels eines Musterregisters

Die Pflicht zur Registrierung der Datensammlungen trifft auch die politischen Gemeinden, die Schul- und die Kirchgemeinden. Um den zahlreichen politischen Gemeinden, die nicht über ein spezifisches datenschutzrechtliches Fachwissen verfügen, eine Hilfe bei der Erstellung der Register zu geben, fanden wir eine Möglichkeit der Zusammenarbeit mit dem Verband der Zürcherischen Gemeindeschreiber und Verwaltungsbeamten (VZGV), dem Gemeindepräsidentenverband (GPV) sowie der Firma Federas AG, die in diesem Bereich ihre Beratungsdienstleistungen anbot. Auf der Basis einer Mustersammlung und der diesbezüglichen kantonalen EDV-Anwendung erarbeitete die Federas im Auftrag des VZGV das Angebot eines Musterregisters für die politischen Gemeinden. In einer gemeinsamen Veranstaltung mit dem VZGV, GPV, der Direktion des Innern und dem Datenschutzbeauftragten konnten den Vertreterinnen und Vertretern der Gemeinden die Einzelheiten in bezug auf die Erstellung der Register der Datensammlungen erläutert werden. Um den Gemeinden die Umsetzung dieses Musterregisters auf ihre Verhältnisse zu ermöglichen, erstreckte der Regierungsrat die Frist zur Erstellung der Register bis zum 30. Juni 1997.

Ohne auf dieses Musterregister zu warten, haben einzelne Gemeinden eigenständig ihr Register der Datensammlungen erstellt und dem Datenschutzbeauftragten zur Begutachtung eingereicht. Diese Register entsprachen durchwegs den gesetzlichen Anforderungen. Die Schulgemeinden erarbeiten unter der Führung der Vereinigung Zürcherischer Schulsekretäre und -sekretärinnen (VZS) ebenfalls ein Musterregister. Im Rahmen der Arbeitsgruppe Datenschutz der Kirchen soll ebenfalls eine Mustersammlung für die Kirchgemeinden erstellt werden.

Das Auskunftsrecht

Jede Person kann von einer Verwaltungsstelle jederzeit Auskunft verlangen, welche Daten über sie bearbeitet werden (§ 17 DSG). Sie hat dazu ein schriftliches Gesuch an die entsprechende Verwaltungsstelle zu richten (§ 10 DSV). Das Register der Datensammlungen gibt die Anhaltspunkte, welche Daten von einer Amtsstelle bearbeitet werden. Das Register ist öffentlich und kann von allen Personen bei der jeweiligen Amtsstelle, dem Datenschutzbeauftragten oder auf kommunaler Ebene bei der Gemeinde eingesehen werden.
Das Auskunftsgesuch ist an die zuständige Verwaltungsstelle (Steueramt, Einwohnerkontrolle, Fürsorgebehörde usw.) zu richten; es wäre nicht ausreichend präzisiert, wenn beispielsweise der Adressat des Gesuches die «kantonale Verwaltung» wäre. Eine weitere Präzisierung wie Angaben über ein bestimmtes Ereignis oder ein ungefähres Datum oder eventuell eine Geschäftsnummer erleichtern die Auskunftserteilung.
Das Auskunftsgesuch ist nicht von einem Interessennachweis abhängig, ausser die Auskunft würde zu einem unverhältnismässigen Verwaltungsaufwand führen (§ 18 Abs. 2 DSG). Die Auskunft erstreckt sich über alle Daten, die bei der bestimmten Amtsstelle über die gesuchstellende Person vorhanden sind. Des weiteren gibt die Amtsstelle die Rechtsgrundlage und den Zweck des Bearbeitens an sowie die an der Datensammlung beteiligten Stellen und die regelmässigen Datenempfänger (§ 10 DSV).
Die Auskunft wird in der Regel schriftlich erteilt, zum Beispiel in Form von Kopien. Sie kann auf Verlangen auch mündlich oder durch Einsichtnahme erfolgen.
Wenn überwiegende öffentliche Interessen oder überwiegende schützenswerte Interessen Dritter dies verlangen, kann die Auskunft aufgeschoben, eingeschränkt oder verweigert werden (§ 18 DSG). Jede Einschränkung der Auskunft ist durch die Verwaltungsstelle zu begründen (§ 20 DSG).
Das Auskunftsrecht gehört zu den sogenannt höchstpersönlichen Rechten und kann von jeder urteilsfähigen Person, auch wenn sie nicht mündig ist, wahrgenommen werden. Als Kernelement des Datenschutzgesetzes ist das Auskunftsrecht nicht Selbstzweck, indem es lediglich der Information oder sogar der Neugier der betroffenen Person dienen soll. Vielmehr ist es die Grundlage, damit jede Person die sie betreffenden Datenbearbeitungen überprüfen und allenfalls ihre weiteren Persönlichkeitsrechte wahrnehmen kann. Wer ein schützenswertes Interesse hat, kann vom verantwortlichen Organ verlangen, dass widerrechtliche Datenbearbeitungen unterlassen oder Daten berichtigt oder vernichtet werden (§ 19 DSG).
Bei schwerwiegenden Verletzungen der Persönlichkeitsrechte durch widerrechtliche Datenbearbeitungen können auch weitergehende Ansprüche auf Schadenersatz oder Genugtuung entstehen.
In sensiblen Bereichen der Datenbearbeitungen, wie beispielsweise im Personalbereich oder im Gesundheitswesen, nehmen bereits heute viele Personen ihr Auskunftsrecht wahr.

Grundsätzliche Fragen auf kommunaler Stufe

Sensible Datenbearbeitungen in unterschiedlichen Bereichen waren Anlass zu grundsätzlichen Stellungnahmen, wobei die Bedeutung des Prinzips der Verhältnismässigkeit zu unterstreichen war.

1. Arbeitslosenversicherung und Arbeitsvermittlung

Anforderungen an die Bekanntgabe von Personendaten

Ein Regionales Arbeitsvermittlungszentrum (RAV) bat uns um Beratung in verschiedenen Fragen des Datenaustauschs. Dabei war zu prüfen, unter welchen Voraussetzungen im konkreten Fall Daten über (arbeitslosen-)versicherte Personen, insbesondere an die Gemeinden, weitergegeben werden dürfen.

Durch die Neuorganisation im Arbeitslosenversicherungsbereich sind die Gemeinden nicht mehr unmittelbar mit Aufgaben beim Vollzug der Arbeitslosenversicherung und Arbeitsvermittlung betraut. Diese Aufgaben werden neu von Regionalen Arbeitsvermittlungszentren erfüllt.

Die Weitergabe von Daten durch Regionale Arbeitsvermittlungszentren an die Gemeinden und andere Stellen bedarf einer Rechtsgrundlage oder der Einwilligung der betroffenen Person (§§ 5 resp. 8 DSG). Stehen der Bekanntgabe offensichtlich schützenswerte Interessen, gesetzliche Geheimhaltungspflichten oder besondere Datenschutzvorschriften entgegen, hat sie zu unterbleiben (§ 10 DSG).

Der Bundesgesetzgeber hat die Möglichkeit der Auskunftserteilung im Arbeitslosenversicherungs- und Arbeitsvermittlungsbereich abschliessend geregelt. Die entsprechenden Gesetze und Verordnungen enthalten in detaillierter Weise Bestimmungen, unter welchen Voraussetzungen anderen Organen Auskünfte erteilt werden dürfen (Art. 97 des Arbeitslosenversicherungsgesetzes, Art. 125 der Arbeitslosenversicherungsverordnung, Art. 34 des Arbeitsvermittlungsgesetzes, Art. 57 der Arbeitsvermittlungsverordnung). Grundsätzlich erhalten nur die zuständigen Stellen anderer Sozialversicherungszweige sowie die Fürsorgebehörden diejenigen Informationen, derer sie zur Festsetzung von Leistungen, zur Verhinderung ungerechtfertigter Bezüge oder zum Rückgriff auf haftpflichtige Dritte bedürfen. Unter gewissen Voraussetzungen erhalten auch Gerichtsbehörden Auskünfte. Allen anderen Organen von Bund, Kantonen und Gemeinden sowie Privatpersonen kann eine Auskunft nur mit schriftlicher Einwilligung der betroffenen Person erteilt werden. Eine Auskunft darf immer nur einzelfallweise auf Anfrage hin gegeben werden und nur diejenigen Daten umfassen, die der Empfänger zur Erfüllung seiner Aufgaben benötigt (Prinzip der Verhältnismässigkeit, § 4 Abs. 3 DSG).

Mit dieser Regelung werden die Gemeinden im Bereich der Budgetplanung vor gewisse Probleme gestellt. Während die Arbeitslosenversicherung durch Bundesgelder und Versicherungsbeiträge gespiesen wird, werden die Fürsorgegelder primär von den Gemeinden zur Verfügung gestellt. Damit eine Gemeinde für ihr Budget im Bilde ist, wie viele Personen, die bis anhin von der Arbeitslosenversicherung unterstützt wurden, nun auf Fürsorgegelder angewiesen sein werden (sog. Ausgesteuerte), können ihr vom Regionalen Arbeitsvermittlungszentrum die diesbezüglichen Angaben in anonymisierter Form übermittelt werden, d.h. in Form einer Liste mit der Anzahl der betroffenen Personen und dem voraussichtlichen Datum der Aussteuerung. Sofern keine Rückschlüsse auf Personen mehr möglich sind, handelt es sich nicht mehr um Personendaten, weshalb sich in diesem Fall keine datenschutzrechtlichen Fragen stellen.

Zulässig ist eine Datenweitergabe, wenn die betroffene Person schriftlich einwilligt. Auf Ersuchen mehrerer Privatpersonen überprüften wir die Verwendung eines Formulars eines Arbeitsamtes, mit dem eine versicherte Person ihre Einwilligung in eine Datenbekanntgabe erteilt, sowie das zugehörige Begleitschreiben. Im Schreiben wurde in missverständlicher Weise mitgeteilt, dass die Datenschutzverordnung verlange, dass eine Einwilligung in eine Datenbekanntgabe erteilt werden müsse. Richtigerweise ist beim Fehlen einer Rechtsgrundlage eine Datenbekanntgabe in der Regel

nur möglich, wenn die betroffene Person im Einzelfall ihre Einwilligung erteilt. Dazu kann sie aber nicht gezwungen werden. Mit anderen Worten: Eine Amtsstelle kann bei Fehlen entsprechender gesetzlicher Grundlagen nicht einfach den betroffenen Personen ein Formular aushändigen und ihre Einwilligung kategorisch verlangen.

Eine Vollmacht zur Datenbekanntgabe an Dritte ist nur für den Einzelfall gültig, d.h. wenn für den Vollmachtgeber resp. die Vollmachtgeberin transparent ist, welche Daten zu welchem Zweck an welchen Empfänger resp. an welche Empfängerin weitergegeben werden. Eine wiederholte Datenbekanntgabe oder gar eine Bekanntgabe an weitere Amtsstellen ist durch die Einwilligung nicht gedeckt. Im konkreten Fall führte unsere Beratung dazu, dass das beanstandete Formular nicht weiter verwendet wurde.

2. Führen einer Bussenkontrolle

Keine Rechtsgrundlage für eine persönliche Strafkontrolle

Uns wurde die Frage vorgelegt, ob die Polizeiabteilung einer Gemeinde zulässigerweise eine Bussenkontrolliste führen könne. In diese Kontrollisten werden Angaben zur betroffenen Person sowie alle gegen diese Person ausgefällten Bussen wegen Übertretungen mit Datum, Tatbestand, Betrag, Kosten sowie allenfalls besonderen Bemerkungen eingetragen. Mit Hilfe einer solchen Liste sollte die Strafzumessung bei wiederholter Delinquenz angepasst werden.
Aufgrund des Strafsanktionscharakters von Bussen stellen die entsprechenden Angaben besonders schützenswerte Daten dar, die nur unter eingeschränkten Voraussetzungen bearbeitet werden dürfen. Eine gesetzliche Grundlage für die hier zur Diskussion stehende Frage ist insofern vorhanden, als § 340 Abs. 3 StPO vorsieht, dass Bussen- oder Einstellungsverfügungen in ein besonderes Protokoll eingetragen werden. Dieses dient nur der Verfahrensabwicklung und Geschäftskontrolle.
Es ergibt sich daraus keine Grundlage für eine Auflistung sämtlicher Bussen einer Person, sozusagen als persönliche Strafkontrolle für kommende Verfahren. Des weiteren wäre die Rechtsgleichheit tangiert, da bei den sofort bar bezahlten Bussen die Namen der Gebüssten gar nicht aufgenommen werden und deshalb auch kein Eintrag in eine Liste erfolgt.

Bei den im Protokoll gemäss § 340 Abs. 3 StPO aufgeführten Angaben ist darauf zu achten, dass im Sinne des Verhältnismässigkeitsgrundsatzes nicht mehr Daten als unbedingt nötig aufgenommen werden (beispielsweise genügen Name und Geburtsdatum zur Identifizierung einer Person, weshalb Beruf und Heimatort entbehrlich sind); ebenfalls ist vom verantwortlichen Organ zwingend festzulegen, wie lange die entsprechenden Unterlagen aufbewahrt werden, wobei eine maximal fünfjährige Aufbewahrungsdauer als verhältnismässig erscheint.

3. Einbürgerungsverfahren

Verhältnismässigkeit der Datenbearbeitung

Wir beschäftigten uns aufgrund zweier Anfragen mit der Datenbearbeitung im Einbürgerungsverfahren. Interessanterweise ging die erste Anfrage davon aus, dass insgesamt zu viele Daten preisgegeben werden müssten, während die zweite Anfrage die Möglichkeit einer erweiterten Datenbekanntgabe zur Rationalisierung des Verfahrensablaufs betraf.

In einem Einbürgerungsverfahren wird eine grosse Zahl von teilweise sehr intimen Daten und damit insgesamt ein Persönlichkeitsprofil der einbürgerungswilligen Person erhoben. Entsprechend darf eine Datenbearbeitung gemäss § 5 DSG nur unter restriktiven Voraussetzungen vorgenommen werden: Es braucht eine klare gesetzliche Grundlage, oder die Daten müssen zur Erfüllung einer gesetzlich klar umschriebenen Aufgabe unentbehrlich sein. Sowohl nach Bundes- wie nach kantonalem (und normalerweise auch nach kommunalem) Recht bezweckt das Einbürgerungsverfahren festzustellen, ob eine gesuchstellende Person eingebürgert werden kann. Entsprechend dürfen nur Daten erhoben werden, die sich auf diese Frage beziehen. Die Daten sind soweit als möglich bei der betroffenen Person selbst einzuholen (§ 7 DSG). Des weiteren ist das Verhältnismässigkeitsprinzip zu beachten: Die zur Abklärung der Einbürgerungsfähigkeit erhobenen Daten sind ausschliesslich solchen Personen bekanntzugeben, die über das Einbürgerungsgesuch zu entscheiden haben. Dabei muss der Eingriff in die Persönlichkeit der einbürgerungswilligen Personen möglichst gering gehalten werden. So reicht es aus, wenn die stimmberechtigten Bürgerinnen und Bürger auf der Gemeindekanzlei in die für die Einbürgerung relevanten Akten Einsicht nehmen können; ein Versand von Informationen bezüglich der Einbürgerungsfähigkeit wäre demgegenüber nicht verhältnismässig. Auch in der Bürgerversammlung ist die Verhältnismässigkeit zu wahren. So ist nicht bei jedem Einbürgerungsgesuch automatisch der gesamte Lebenslauf zu präsentieren. Vielmehr genügt es, wenn lediglich der Antrag als solcher verlesen wird. Nur wenn Zweifel an der Einbürgerungsfähigkeit aufkommen, soll auf Einzelheiten eingegangen und allenfalls zu gewissen Punkten nachgefragt werden können.

4. Datenbekanntgabe durch die Jugend- und Familienberatung

Weitergabe von Daten an die Gerichte

Im Rahmen eines Scheidungsverfahrens bzw. einer späteren Abänderungsklage obliegt es dem Gericht, über die strittige Frage der Kinderzuteilung zu entscheiden. Da sowohl Vormundschaftsbehörden als auch Beratungsstellen der Jugendsekretariate unter Umständen mit den Familien und deren sozialen Verhältnissen vertraut sind, werden diese von den Gerichten häufig beigezogen. Dabei wird entweder ein Mitarbeiter der Jugend- und Familienberatung, der als Erziehungsbeistand (i.S. von Art. 308 ZGB) tätig ist, vom Gericht ersucht, im Rahmen eines Scheidungsprozesses direkt Auskunft im Hinblick auf die Kinderzuteilungsfrage zu erteilen. Oder er wird vom Gericht gebeten, ein Kinderzuteilungs-Gutachten oder andere Berichte zu liefern, unter Verwendung der bereits über die Familie vorhandenen Daten.

Grundsätzlich erfasst das kantonale Datenschutzgesetz jede Bearbeitung von Personendaten durch öffentliche Organe. Jedoch gilt es nicht in hängigen Verfahren des Zivil-, Straf- oder Verwaltungsrechts (§ 3 Abs. 2 lit. b DSG). Vorerst ist deshalb festzuhalten, dass es nicht anwendbar ist, wenn ein Mitarbeiter oder eine Mitarbeiterin der Jugend- und Familienberatung in einem Gerichtsverfahren als Zeuge geladen wird.

Solange sie indessen nicht formell im Verfahren involviert sind, gelten die Bestimmungen des DSG. Eine Weitergabe von Personendaten erlaubt § 8 DSG nur, wenn hierfür gesetzliche Grundlagen in Form von Mitteilungsrechten und -pflichten bestehen, die Daten im Rahmen der Amtshilfe benötigt werden oder die betroffene Person eingewilligt respektive ihre Daten allgemein zugänglich gemacht hat.
Bei der Jugend- und Familienberatung fällt eine Einwilligung im Normalfall zum vornherein ausser Betracht, da in einem Streitfall kaum alle Betroffenen (Eltern, evtl. urteilsfähige Kinder) ihre Zustimmung geben werden.
Da eine gesetzliche Grundlage für die Weiterleitung von Daten fehlt, ist in bezug auf eine Auskunftserteilung gegenüber dem Gericht primär eine Amtshilfe zu prüfen. Diese darf nur auf Ersuchen der datenempfangenden Stelle erfolgen, was hier zutrifft. Ausserdem müssen die nachgefragten Informationen im Einzelfall zur Erfüllung einer öffentlichen Aufgabe benötigt werden. Die Sammlung von Beweisen im Hinblick auf die Urteilsfindung stellt eine solche öffentliche Aufgabe dar. Die Amtshilfe ist sodann subsidiärer Natur, indem keine anderen Mittel zur Verfügung stehen dürfen. Diese Voraussetzung ist zweifellos erfüllt, da in bezug auf die Kinderzuteilungsfrage nicht ausschliesslich auf die von den Prozessparteien gelieferten Informationen abgestellt werden kann. Ebenso ist das Prinzip der Zweckidentität gewahrt, da Kindesschutzmassnahmen und Scheidung – und damit die Frage nach der Zuteilung der elterlichen Gewalt – begriffsnotwendig nahe beisammen liegen. Als letztes dürfen keine besonderen Schweigepflichten eine Amtshilfe ausschliessen. Zwar auferlegt § 10 Abs. 3 des Jugendhilfegesetzes dem Personal ausdrücklich eine Schweigepflicht. Hierbei handelt es sich nicht um eine besondere, sondern lediglich um eine die allgemeine Schweigepflicht konkretisierende Norm. Eine Auskunftserteilung gegenüber dem um Amtshilfe ersuchenden Gericht ist daher grundsätzlich möglich. Kann der betroffene Mitarbeiter gegenüber dem Gericht direkt Auskunft geben, so kann er auch in Beantwortung des Amtshilfegesuches dem anfragenden Gericht ein Gutachten zustellen oder ihm entsprechende Berichte und Informationen übergeben.
Anders liegt der Fall, wenn noch kein Gesuch um Amtshilfe vorhanden ist. Dann ist zwar die Vormundschaftsbehörde, die gemäss Art. 157 ZGB die Möglichkeit hat, auf Änderung des Scheidungsurteils zu klagen, berechtigt, dem Gericht unaufgefordert die im Hinblick auf die Kinderzuteilungsfrage sachdienlichen Informationen zukommen zu lassen. Mangels ausdrücklicher gesetzlicher Grundlage steht diese Kompetenz den Jugend- und Familienberatungsstellen nicht zu. Infolgedessen wäre hier eine Informationsweitergabe nur bei Einwilligung aller betroffenen Personen zulässig.
Das Jugendamt des Kantons Zürich, das wir zur Stellungnahme einluden, beabsichtigt aufgrund unserer Ausführungen, eine entsprechende Richtlinie zuhanden der Bezirksjugendsekretariate auszuarbeiten.

5. Bekanntgabe des Stromverbrauchs an Dritte

Keine gesetzliche Grundlage

Aufgrund einer Anfrage klärten wir ab, ob die Städtischen Werke Angaben über den Stromverbrauch einer Person ohne weiteres an interessierte Drittpersonen weitergeben dürfen. Eine Datenbekanntgabe ist gemäss § 8 DSG nur zulässig, wenn hierfür eine gesetzliche Grundlage besteht oder wenn die betroffene Person ausdrücklich eingewilligt hat respektive zumindest aus den Umständen auf ihr stillschweigendes Einverständnis geschlossen werden kann oder wenn sie ihre Daten vorher schon allgemein bekanntgemacht hat.
Im konkreten Fall stellten wir fest, dass keine ausdrückliche Gesetzes-

bestimmung eine Bekanntgabe der Kennzahlen zum Stromverbrauch an Dritte generell gestattet. Eine Berechtigung zum Bezug solcher Daten liess sich im zu beurteilenden Fall auch nicht aus dem Umstand ableiten, dass die anfragende Person Eigentümerin der von der stromverbrauchenden Person bewohnten Liegenschaft war, da die Rechnungen auf die zur Miete wohnende Person lauteten und auch von ihr bezahlt wurden. Ebensowenig konnte ein Einsichtsrecht begründet werden mit dem Hinweis, dass die zur Miete wohnende Person ihre Stromkosten aufgrund einer vertrags- oder familienrechtlichen Vereinbarung von der anfragenden Drittperson zurückerstattet erhielt. Das Privatrecht schafft keine Rechtsgrundlage für Behörden und andere öffentlich-rechtliche Organe, Daten ohne weiteres an eine der beteiligten Parteien zu übermitteln. Vielmehr liegt es im Wesen des Privatrechts, dass die beteiligten Parteien die erforderlichen Angaben in bezug auf die Abwicklung eines privatrechtlichen Geschäfts grundsätzlich selber bei ihren Partnern einholen. Schliesslich lag auch keine ausdrückliche Einwilligung vor. In Betracht zu ziehen war immerhin, ob die zuständigen Behörden aus dem Umstand, dass die anfragende Person sowohl das Eigentum an der fraglichen Liegenschaft hatte sowie letzten Endes die aufgelaufenen Rechnungen faktisch bezahlte (und infolgedessen über die bisherigen Kennzahlen im Bilde war), eine stillschweigende Einwilligung ableiten durften. Von einer solchen darf nur in ganz klaren Fällen ausgegangen werden; im Zweifelsfalle ist eine ausdrückliche Einwilligung bei der betroffenen Person einzuholen.
Wir mussten daher festhalten, dass die Daten über den Stromverbrauch zu Unrecht und damit in Verletzung der geltenden Datenschutzbestimmungen an eine Drittperson weitergeleitet worden waren.

6. Datensperre bei der Einwohnerkontrolle

Rahmenbedingungen für die praktische Handhabung

Eine Gemeinde gelangte mit der Fragestellung an uns, wie Auskunftsbegehren Dritter zu handhaben seien, wenn eine Person eine Sperre ihrer Daten gemäss § 11 DSG veranlasst hat. Die Einwohnerkontrolle dieser Gemeinde erhält täglich durchschnittlich zwischen 20 und 30 Gesuche um Datenbekanntgaben, wobei rund 30 Prozent der Einwohnerinnen und Einwohner ihre Daten gesperrt haben.
Eine Datensperre gilt bezüglich aller Daten bei der entsprechenden Amtsstelle. Sie wirkt allerdings nur gegenüber Privatpersonen. Anderen Amtsstellen können die Daten trotz Sperre bekanntgegeben werden, sofern die Voraussetzungen von §§ 8–10 DSG erfüllt sind. So ist beispielsweise ein verwaltungsinterner EDV-Direktzugriff auf Einwohnerkontrolldaten erlaubt, sobald entsprechende Rechtsgrundlagen bestehen. Ebenso verhält es sich bei den Landeskirchen; diese haben gemäss § 39a des Gemeindegesetzes einen Anspruch auf Bekanntgabe derjenigen Personendaten aus dem Einwohnerkontrollregister, deren sie zur Erfassung ihrer Mitglieder bedürfen.
Die Datensperre wirkt bei Anfragen von Privatpersonen, seien dies Einzelanfragen oder Begehren um Listenauskünfte. Eine spezielle Konstellation liegt vor, wenn beispielsweise eine Kreditkartenfirma oder ein Versandhaus, etwa im Rahmen eines Vertragsabschlusses, eine Vollmacht vorlegt, nach der sie die Einwilligung der betroffenen Person für eine Datenbekanntgabe hat, aber die entsprechenden Daten gesperrt sind. Grundsätzlich steht das Verfügungsrecht über eine Datensperre der betroffenen Person zu. Sie kann die Sperre jederzeit wieder aufheben, auch nur partiell. Dies kann durch die Erteilung einer Vollmacht erfolgen, die als Einwilligung betrachtet wird. Es ist je-

doch zu differenzieren, ob die Einwilligung vor oder nach der Sperre erteilt worden ist, was bedeutet, dass das Datum der Sperre vermerkt werden muss. Eine Einwilligung, die älter als die Sperrung ist, vermag diese nicht zu durchbrechen. Dagegen durchbricht eine Einwilligung, die nachher erteilt wurde, die Sperre. Es muss einer Person, die grundsätzlich ihre Daten gesperrt haben will, möglich sein, im Einzelfall in eine Datenbekanntgabe einzuwilligen, ohne das Sperrecht als Ganzes aufheben und anschliessend wieder neu einrichten zu müssen. Die Einwilligung (Vollmacht) ist vom öffentlichen Organ zu prüfen, was bedeutet, dass sie auf geeignetem Weg (in der Regel also schriftlich) eingereicht werden muss. Sie ist gültig, wenn sie sich auf einen konkreten Einzelfall – z.B. Abschluss eines Kreditkartenvertrags – bezieht, wenn die betroffene Person sich der Tragweite ihrer Einwilligung bewusst war und wenn daraus hervorgeht, welche Daten von welchen Organen bekanntgegeben werden dürfen. Inzwischen hat der Stadtrat der anfragenden Gemeinde einen Beschluss über die Abgabe von Adressen durch die Einwohnerkontrolle und die Handhabung der Datensperre gefasst, in deren Erwägungen die Ausführungen des Datenschutzbeauftragten Eingang gefunden haben.

7. Auskunftserteilung der Einwohnerkontrolle

Benutzung einer 157er Telefonnummer

Von der Stadt Uster wurden wir angefragt, ob die in § 9 DSG geregelte Auskunft durch die Einwohnerkontrolle nicht der Einfachheit halber über eine 157er Telefonnummer abgewickelt werden könnte.
Wir stellten fest, dass gegen eine Auskunftserteilung über eine kommerziell zu nutzende Telefonnummer grundsätzlich nichts einzuwenden ist, solange es sich lediglich um Auskünfte gemäss § 9 Abs. 1 DSG handelt. Angaben zu Name, Vorname, Adresse, Datum von Zu- und Wegzug sowie Beruf einer Person können, solange keine gültige Sperrung vorliegt, im Einzelfall gegenüber jedermann ohne jeglichen Interessennachweis erteilt werden.
Unzulässig ist dagegen die Abwicklung von Auskunftserteilungen gemäss § 9 Abs. 2 bis 4 DSG ausschliesslich über eine 157er Telefonnummer. Hier sind Abklärungen bezüglich der Motive beziehungsweise Interessen der anfragenden Person erforderlich, weshalb die Einwohnerkontrolle im Normalfall auf schriftliche Unterlagen angewiesen ist.
Immerhin ist nicht ausgeschlossen, dass auch bei Auskunftserteilungen gemäss § 9 Absätze 2 bis 4 DSG eine erste Kontaktnahme mit der Einwohnerkontrolle über eine 157er Telefonnummer erfolgt. Im Rahmen eines solchen Gespräches kann sie detailliert informieren, welchen Beweisanforderungen eine Anfrage genügen muss, damit sie beantwortet werden kann.
Ebenfalls datenschutzkonform kann die – nach entsprechenden Abklärungen für zulässig befundene – Auskunft wiederum über die 157er Telefonnummer erteilt werden.

8. Entlassung aus dem Amt

Keine detaillierten medizinischen Daten an andere Amtsstellen

Von einer betroffenen Person wurde uns ein Entscheid vorgelegt, worin im einzelnen die medizinischen Gründe aufgeführt waren, die zur Gutheissung ihres Entlassungsgesuchs aus dem von ihr bisher bekleideten Amt geführt haben. Störend fand sie insbesondere, dass der genannte Entscheid gemäss Verteiler nicht nur ihr selbst sowie der betroffenen Behörde, sondern auch anderen Amtsstellen zur Kenntnis gebracht worden war, wodurch sie sich öffentlich blossgestellt fühlte.

Ein Rücktritt aus einem mit Amtszwang ausgestatteten Amt verlangt den Nachweis von fundierten Rücktrittsgründen durch die gesuchstellende Person. Entsprechend ist es unumgänglich, dass bei körperlichen oder psychischen Hinderungsgründen auch Daten, die den gesundheitlichen Bereich betreffen und damit besonders schützenswert sind, innerhalb der Behörde zur Sprache gebracht werden. Jedoch besteht kein Anlass, andere Amtsstellen, wie die mit der Organisation von Neuwahlen zuständige, mit detaillierten Informationen zu bedienen; hier ist eine Mitteilung in sehr allgemein gehaltener Form absolut ausreichend.
Die von uns zur Stellungnahme eingeladene Behörde ging mit unseren Ausführungen einig. Sie ändert ihre Praxis insofern, als sensible Daten nur noch in allgemeiner Form und nicht mehr mit allen Einzelheiten vorgebracht werden; ebenso wird die mit der Ersatzwahl beauftragte Behörde künftig nur noch mit dem Dispositiv angeschrieben.

9. Begleitblatt zum Schulübertritt in die Oberstufe

Zulässigkeit der Daten auf dem Übertrittsformular

Beim Übertritt eines Schülers in die Oberstufe wird ein Begleitblatt ausgefüllt, das aufgrund seines Inhaltes der neuen Lehrkraft Informationen über den Neueintretenden gibt. Auf Anfrage der Oberstufenschulpflege einer Schulgemeinde überprüften wir, ob die Angaben des Begleitblattes den datenschutzrechtlichen Anforderungen zu genügen vermögen.
Das Begleitblatt enthält Angaben über den Schüler, die Eltern und allfällige weitere Bezugspersonen (z.B. Vormund, Pflegeeltern usw.), Anzahl der Schuljahre, Therapien, Stütz- und Fördermassnahmen sowie die Anmeldung an die Oberstufe. Es dient der neuen Lehrkraft dazu, sich ein Bild über die neuen Schüler zu machen. Dementsprechend ist bei der Datenbekanntgabe an die neue Lehrkraft zu klären, welche Angaben die Lehrperson zur Erfüllung ihrer Aufgaben benötigt.
Erforderlich und daher zulässig sind Angaben wie Name, Vorname, Geschlecht, Geburtsdatum, Adresse, Heimatort/Staatsangehörigkeit und Muttersprache des Schülers, Name, Vorname und Adresse von Eltern, Pflegeeltern, Vormund usw., Anzahl der Schuljahre sowie Zuzugsort und -datum. Die Angabe der Konfession ist nützlich für die Planung und Durchführung des Unterrichts in biblischer Geschichte und Sittenlehre (§ 11 Abs. 1 der Volksschulverordnung) sowie für die Bewilligung von Absenzen aus religiösen Gründen (§ 62 der Volksschulverordnung). Nicht erforderlich sind hingegen Angaben zum Beruf der Eltern. Solche Angaben sind zudem häufig unrichtig, was dem Prinzip der Datenrichtigkeit (§ 4 Abs. 2 DSG) widerspricht.
Ausgesprochen heikel ist die Erfassung von Daten über körperliche Besonderheiten. Solche Gesundheitsdaten sind sensibel und daher nur zu erfassen, wenn sie im Zeitpunkt des Stufenwechsels aktuell sind und ein Informationsbedarf für die neue Lehrkraft besteht. Dies ist etwa der Fall bei einer Bienenstichallergie oder bei Epilepsie, wenn mit epileptischen Anfällen des Schülers während des Schulbetriebs gerechnet werden muss. Nicht notwendig und daher unverhältnismässig ist die Erfassung von Seh-

oder Hörschwächen, die mittels Brille, Kontaktlinsen, Hörgerät usw. korrigiert sind, oder andere körperliche Besonderheiten, die sich nicht auf den Schulbetrieb auswirken.
Ebenfalls heikle Gesundheitsdaten sind Angaben über Therapien. Hier besteht jedoch unter Umständen ein Informationsbedarf, wenn therapeutische Massnahmen den Schulbetrieb betreffen. Dies ist etwa der Fall bei Legasthenie, Dyskalkulie usw. Dies gilt auch für Stütz- und Fördermassnahmen wie Deutsch für Fremdsprachige oder Schulung in der Integrativen Schulungsform. Hier sind gewisse Angaben über bereits durchgeführte Massnahmen notwendig und auch verhältnismässig, wenn sie sich auf einen begrenzten Zeitraum (z.B. die letzten zwei oder drei Jahre) beziehen.
Nebst den genannten Angaben zu den Schülern und deren Bezugspersonen enthält das Begleitblatt im unteren Viertel auch noch die Anmeldung an die Oberstufe.
Bei der Anmeldung an die Oberstufe handelt es sich um Daten, die im Dreiecksverhältnis Eltern – Schulpflege – bisherige Lehrkraft ausgetauscht werden und auf der Verordnung über den Übertritt in die Oberstufe der Volksschule beruhen. Diese Daten sind für die neue Lehrkraft nicht erforderlich und dieser demnach auch nicht bekanntzugeben. Das bedeutet, dass die Daten für die Anmeldung an die Oberstufe am besten auf einem separaten Formular erfasst werden; mindestens sind diese Angaben aber gegenüber der neuen Lehrkraft abzudecken.

10. Kommunale Datenschutzaufsichtsstellen

Erste Datenschutzbeauftragte ernannt

§ 22 DSG sieht vor, dass Gemeinden und öffentliche Einrichtungen mit Zustimmung des Regierungsrates eine eigene Aufsichtsstelle bestellen oder vom Regierungsrat zur Einrichtung einer solchen verpflichtet werden können. Wo eine solche Aufsichtsstelle eingerichtet ist, kommt dem kantonalen Datenschutzbeauftragten die Oberaufsicht zu.
Der Regierungsrat hat 1996 bei interessierten Kreisen eine Vernehmlassung durchgeführt zur Frage, aufgrund welcher Kriterien eine Gemeinde eine eigene Aufsichtsstelle führen oder eventuell hierzu verpflichtet werden sollte. Nach Auswertung der Antworten hat der Regierungsrat festgestellt, dass die grösseren Gemeinden über eine eigene Aufsichtsstelle verfügen sollten. Er hat deshalb die Städte Zürich und Winterthur mit Beschluss vom 27. November 1996 zur Führung einer Datenschutz-Aufsichtsstelle gemäss § 23 ff. DSG verpflichtet und ihnen zum Erlass der notwendigen Gemeindebestimmungen und zur Umsetzung eine Frist bis zum 31. Dezember 1997 angesetzt. Den übrigen grösseren Gemeinden wurde empfohlen, eine eigene Aufsichtsstelle zu bestellen und dem Regierungsrat den Antrag zur Genehmigung einzureichen.
1996 haben die Städte Dietikon und Dübendorf einen Antrag an den Regierungsrat für eine eigene Aufsichtsstelle gestellt. Der Regierungsrat hat mit Beschluss vom 7. Februar 1996 respektive 27. November 1996 der Errichtung dieser Aufsichtsstellen zugestimmt. Er legte dabei Wert darauf, dass diese Stellen verwaltungsunabhängig ausgestaltet und der Exekutive oder der Gemeindeversammlung direkt unterstellt werden, damit sie ihre Aufgaben gemäss § 23 ff. wahrnehmen können.
Die Stadt Uster hat 1996 eine Übergangslösung für die Einführung des Datenschutzgesetzes beschlossen, die ebenfalls zur Einrichtung einer eigenen Aufsichtsstelle führen soll.

11. Datenschutz-Musterreglemente für die Gemeinden

Konkretisierung des Datenschutzes auf Gemeindeebene

Eine Arbeitsgruppe, bestehend aus Vertretern des Verbandes Zürcherischer Gemeindeschreiber und Verwaltungsbeamter (VZGV), des Verbandes Zürcher Einwohnerkontrollen (VZE) sowie dem Datenschutzbeauftragten erarbeitete ein Datenschutz-Musterreglement für die Gemeinden. Das Musterreglement soll in Ergänzung der Gesetzesvorschriften ermöglichen, in bezug auf den Datenschutz auf Gemeindestufe notwendige Konkretisierungen vorzunehmen und organisatorische Verantwortlichkeiten festzulegen. Es eignet sich insbesondere für kleinere und mittlere Gemeinden, die Handlungsanleitungen bezüglich des Datenschutzes für immer wieder auftretende Verwaltungsabläufe benötigen. Durch eine Anpassung an die konkreten Bedürfnisse kann auf einfache Art und Weise eine klare Regelung des Datenschutzes auf kommunaler Ebene erreicht werden. Zwar besteht keine Verpflichtung der Gemeinden zum Erlass eines solchen Reglements. Indes kann ein Datenschutzreglement nicht zuletzt auch dazu dienen, im Umgang mit betroffenen Personen, den Einwohnerinnen und Einwohnern, Klarheit und Vertrauen in bezug auf Datenbearbeitungen durch Gemeindebehörden zu schaffen. Das Musterreglement enthält zudem einen Vertragsvorschlag für eine Datenbearbeitung durch Dritte im Sinne von § 13 DSG sowie das Muster einer Vereinbarung zwischen verantwortlichem Organ und einem Herausgeber von Adressbüchern und Nachschlagewerken gestützt auf § 5 f. DSV. Das Datenschutz-Musterreglement wurde allen Gemeinden im Kanton Zürich zur Verfügung gestellt. Es kann auch beim Datenschutzbeauftragten bezogen werden.

12. Datenschutz im kirchlichen Bereich

Arbeitsgruppe zusammen mit den anerkannten Landeskirchen

Diverse offene Fragen betrafen den Datentransfer der politischen Gemeinden, der Schulgemeinden und der Spitäler mit den Kirchgemeinden. Da es sich hierbei insgesamt um komplexe und relativ weitreichende Probleme sowie um Angaben über die Religion und damit um besonders schützenswerte Daten gemäss § 2 lit. d Ziff. 1 DSG handelt, wurden diese Fragen im Rahmen der gemeinsamen Arbeitsgruppe besprochen (siehe Tätigkeitsbericht Nr. 1 [1995], S. 20 f.).
In bezug auf den Datentransfer zwischen einer Gemeinde (das heisst der zuständigen Einwohnerkontrolle) und den anerkannten Landeskirchen (sowie allenfalls weiteren nach § 39 Absatz 2 Gemeindegesetz anerkannten religiösen Gemeinschaften) zwecks Erfassung der zugehörigen Mitglieder wurde in einem ersten Schritt, in enger Zusammenarbeit mit Pilotgemeinden, eine bilaterale Mustervereinbarung über den Datenaustausch zwischen der politischen Gemeinde und der römisch-katholischen respektive der evangelisch-reformierten Kirchgemeinde erarbeitet. Damit sind gute Grundlagen vorhanden für den Aufbau einer kantonalen Vereinbarung zwischen den politischen Gemeinden und den anerkannten Kirchgemeinden. Der Datenaustausch zwischen Schulgemeinde und Kirche wirft ebenfalls Fragen auf. Wir stellten fest, dass die Schulgemeinde zwar eine Rechtsgrundlage hat, um die benötigten Daten den Kirchen herauszugeben, dass sie aber zur Erhebung der Religion ihrer Schülerinnen und Schüler gesetzlich nicht verpflichtet ist. Diese Frage wird von einer Kontaktgruppe für den konfessionell-kooperativen Religionsunterricht weiter besprochen werden.
Zu Diskussionen Anlass gab auch die Frage, ob und gegebenenfalls unter welchen Umständen die Spitäler die Daten der als Patientinnen und Patienten eingelieferten

Kirchenmitglieder an die für die Seelsorge zuständige Stelle weiterzumelden haben. Mit dem DSG nicht vereinbar wäre zum vornherein, dass die Spitäler, wie teilweise praktiziert worden ist, eine integrale Liste aller Neueintritte an die anerkannten Kirchen überweisen, da für die Weitergabe von Daten von Nichtmitgliedern eindeutig keine Rechtsgrundlage besteht. Da ein Spital jedoch nur die zur Abwicklung der medizinischen Behandlung notwendigen Angaben bearbeiten darf, liegt es nicht im Rahmen seiner Befugnisse, zuhanden der zuständigen Kirchen die Religion zu erheben. Folgerichtig muss es in dem bei Spitaleintritt auszufüllenden Formular ausdrücklich darauf hinweisen, dass die Angabe der Religion zum Zwecke der Spitalseelsorge auf freiwilliger Basis beruht.

---

13. Bedarfsplan für Spitex-Basisdienste

Starke Eingriffe in die Privatsphäre

Um die spezifischen Bedürfnisse einer hilfsbedürftigen Person abklären und so eine wirkungsvolle und rationelle Hilfe und Pflege organisieren zu können, hat die Gesundheitsdirektion, Abteilung Spitalexterne Dienste (Spitex), ein mehrseitiges Formular erarbeitet, den sogenannten «Bedarfsplan für Spitex-Basisdienste». Dieser Bedarfsplan wird mit dem Arbeitsbuch «Spitex bedarfsgerecht» den Spitex-Diensten im ganzen Kanton abgegeben. Im Formular werden sehr viele Fragen gestellt zur pflegebedürftigen Person, ihren gesundheitsspezifischen Problemen, ihrem Umfeld sowie ihren psychischen Befindlichkeiten.
Dieser Fragebogen wurde uns von verschiedener Seite zur Begutachtung vorgelegt; es wurde die Befürchtung geäussert, mit den teilweise ausführlichen Fragen werde unnötig in die Persönlichkeitsrechte der betroffenen Personen eingegriffen.
Wir prüften den Bedarfsplan, unter Einbezug des mitgelieferten, relativ ausführlichen Arbeitsbuches, auf seine Vereinbarkeit mit dem Datenschutz. Einleitend stellten wir fest, dass Spitex, trotz der privatrechtlichen Ausgestaltung der jeweiligen Pflegeverhältnisse, dem Geltungsbereich des Datenschutzgesetzes unterliegt, da die Besorgung einer ausreichenden spitalexternen Pflege aufgrund von § 59 des Gesundheitsgesetzes eine öffentliche Aufgabe darstellt.
Eine gesetzliche Grundlage zur Erhebung von besonders schützenswerten Daten, zu denen solche aus dem Gesundheits- und dem persönlichen Geheimbereich zählen, fehlt. Eine Datenbearbeitung ist deshalb nur mit der Einwilligung der betroffenen Person möglich. Auch wenn diese Voraussetzung gegeben ist, dürfen nur diejenigen Angaben erfasst werden, die zur Abwicklung der Spitex-Dienste im konkreten Pflegefall geeignet und unbedingt erforderlich sind (Prinzip der Verhältnismässigkeit). Entsprechend sind je nach der vorliegenden Pflegesituation ganze Abschnitte des Fragebogens leer zu lassen. Keinesfalls darf «auf Vorrat» nach Informationen gefragt werden, die sich später einmal als nützlich erweisen könnten. Des weiteren ist weder im Bedarfsplan noch im Arbeitshandbuch eine Aufbewahrungsfrist für die ausgefüllten Fragebogen vorgesehen. Eine solche Frist ist gemäss § 14 Abs. 2 DSG vom verantwortlichen Organ zwingend für jede Datensammlung festzulegen. Auf die datenschutzrechtlichen Erfordernisse wird weder im Arbeitsbuch noch in dem als Muster ausgefüllten Bedarfsplan eingegangen. Wir haben die zuständige Gesundheitsdirektion aufgefordert, auf geeignete Art ausdrücklich auf den Datenschutz der pflegebedürftigen Personen hinzuweisen sowie den Fragebogen entsprechend anzupassen.
Ein Merkblatt «Datenschutz», das in Zusammenarbeit mit dem Datenschutzbeauftragten entstanden ist und die wichtigsten datenschutzrechtlichen Grundsätze festhält, wurde den betroffenen Spitex-Organisationen und -Mitarbeitenden abgegeben. In bezug auf den Fragebogen haben wir konkrete Vorschläge unterbreitet, die bisher aber noch nicht umgesetzt worden sind.

Schritte in Richtung Datensicherheit

Auf konzeptioneller Ebene wie auch in bezug auf die Kontrolle der rechtmässigen Datenbearbeitung und der Datensicherheit sind erste Ansätze realisiert worden.

1. Überwachung und Kontrolle der Datenbearbeitungen

Konzept für einen Datenschutz-Review

Die Aufsicht und Kontrolle der Datenbearbeitungen durch den Datenschutzbeauftragten erfordern auf der methodischen Ebene ein Vorgehen, das einerseits erlaubt, die Zulässigkeit der Bearbeitung und die angemessenen technischen und organisatorischen Massnahmen zu überprüfen, und andererseits der betroffenen Verwaltungsstelle die notwendige Transparenz in bezug auf fehlende oder zu schaffende Voraussetzungen für eine korrekte Datenbearbeitung gibt.
In Zusammenarbeit mit dem Amt für Informatikdienste (Interne Revision), dem Informatikdepartement der ETH Zürich und dem Datenschutzbeauftragten des Kantons Bern konnte ein Konzept für eine systematische und periodische Aufsichts- und Kontrolltätigkeit entwickelt werden. Dieses Verfahren sieht in einem ersten Schritt eine Priorisierung vor, um angesichts der beschränkten Ressourcen die Aufsichtstätigkeit auf die sensiblen Datenbearbeitungen fokussieren zu können. Die Überprüfung erfolgt sodann in vier Phasen, wobei aufgrund entsprechender Checklisten in den beiden ersten Phasen die rechtlichen Grundlagen sowie das Vorhandensein der Grundschutzmassnahmen überprüft werden. Die Datenbearbeitungen werden fünf verschiedenen Szenarien zugeteilt (Workstation, Terminal, Client/Server an einem Standort, Client/Server mit mehreren Standorten, Client/Server mit weltweitem Netzverbund), die unterschiedlicher organisatorischer und technischer Datensicherheitsmassnahmen (Grundschutz) bedürfen. In Schritt drei und vier werden im einzelnen die Art der Massnahmen wie auch die über den Grundschutz hinausgehenden Massnahmen betrachtet. Mit dem ersten Teil dieses Vorgehens ist es sehr rasch möglich, einen Überblick über die Datenbearbeitung zu gewinnen und summarisch zu prüfen, ob die Bearbeitung im einzelnen rechtlich zulässig ist und die angemessenen organisatorischen und technischen Massnahmen getroffen wurden. Werden in diesem Schritt keine gravierenden Mängel festgestellt, wird ein entsprechender Bericht verfasst und die Verwaltungsstelle aufgefordert, eventuell festgestellte kleinere Schwachstellen zu beseitigen. Sofern allerdings in dieser ersten Überprüfung schwerwiegende rechtliche oder organisatorische und technische Mängel festgestellt werden, ergehen unmittelbar Empfehlungen an die verantwortliche Stelle und eine weitergehende Abklärung erfolgt. Die Methode wurde anhand der Überprüfung einer kommunalen und einer kantonalen Verwaltungsstelle in der Praxis getestet. Sie erwies sich sowohl für die betroffene Verwaltungsstelle wie auch für den Datenschutzbeauftragten als ein Hilfsmittel, das für beide Seiten eine transparente Beurteilung der Datenbearbeitungen zulässt.

2. Sicherheit von Informatiksystemen und -anwendungen

Richtlinien für die kantonale Verwaltung

Die Arbeitsgruppe Planung und Steuerung für Informatik und Kommunikation (AGIK) hat 1996 die Arbeiten für Richtlinien bezüglich der Sicherheit von Informatiksystemen und -anwendungen in der kantonalen Verwaltung in Angriff genommen. Ein Kernteam, bestehend aus Vertretern des Amts für Informatikplanung (AIP), dem Datenschutzbeauftragten und fallweise zugezogenen externen Beratern hat ein Konzept zuhanden der Arbeitsgruppe Datensicherheit erarbeitet. Dieses sieht vor, dass

Daten, Informationen und Programme, die mit Systemen der elektronischen Datenverarbeitung bearbeitet werden, in drei Sicherheitsstufen zu klassifizieren sind. Für die Einteilung werden neben datenschutzrechtlichen Kriterien weitere betriebswirtschaftliche Elemente berücksichtigt. Jede Sicherheitsstufe verlangt entsprechende Sicherheitsmassnahmen im Sinne eines Grundschutzes. Für die Klassifizierung der Daten sowie für die Realisierung der notwendigen Massnahmen ist die einzelne Direktion verantwortlich. Sie hat auch sicherzustellen, dass das Sicherheitskonzept periodisch überprüft wird. Das Konzept soll von der AGIK verabschiedet und mittels Verordnung vom Regierungsrat für verbindlich erklärt werden.
Das Projekt schliesst aus datenschutzrechtlicher Sicht eine Lücke in bezug auf die organisatorischen und technischen Massnahmen der Datensicherheit. Bisher fehlte es in der kantonalen Verwaltung an den notwendigen Grundlagen auf konzeptioneller und strategischer Ebene. Bei der Erarbeitung des Konzeptes zeigte sich, dass die datenschutzrechtlichen Anforderungen eine gute Basis für eine generelle Sicherheitsstrategie der Verwaltung bilden können. In diesem Sinne konnten datenschutzrechtliche Anforderungen und weitere betriebsspezifische Bedürfnisse in bezug auf die Datensicherheit in diesem Konzept vereinigt werden.
Damit die Informatiksicherheit nicht isoliert dasteht, hat der Regierungsrat auch einen Auftrag für eine Gebäude- und Informationssicherheitspolitik erteilt.

3. Missachtung der Datensperre bei der Adressbuchherausgabe

Ungenügende Datensicherheitsmassnahmen

Daten, die bei einer Einwohnerkontrolle gemäss § 11 DSG gesperrt werden, dürfen bei der Herausgabe eines Adressbuches nicht verwendet werden. Ungenügende organisatorische Massnahmen führten dazu, dass ein solches Adressbuch mit den Angaben über die gesperrten Personen veröffentlicht wurde. Von einer betroffenen Person wurden wir darauf aufmerksam gemacht, dass sie im Adressbuch der Stadt Zürich, das von einer privaten Firma herausgegeben wird, verzeichnet sei, obwohl sie ihre Daten bei der Einwohnerkontrolle hat sperren lassen. Unsere Abklärungen bei der verantwortlichen Stelle ergaben, dass die gesperrten Adressen nicht nur in diesem Einzelfall, sondern in über 200 Fällen publiziert worden waren. Es stellte sich heraus, dass dieser Fehler bei der elektronischen Aufbereitung der Adressen für die Weitergabe an den Herausgeber erfolgte, da die Programmierungen für diesen Datenaustausch keinem Test und keiner Schlusskontrolle unterlagen. Mit diesem Vorfall wurde der zuständigen Datenverarbeitungsstelle aufgezeigt, dass organisatorische Mängel in der Abwicklung der Datenbearbeitung bestehen. Es muss deshalb davon ausgegangen werden, dass die angemessenen organisatorischen und technischen Massnahmen gegen das unbefugte Bearbeiten gemäss § 4 Abs. 5 DSG zu diesem Zeitpunkt nicht vorhanden waren. Zwischenzeitlich wurden entsprechende Massnahmen getroffen.

Die Wichtigkeit angemessener organisatorischer und technischer Massnahmen zeigt sich auch darin, dass eine Datensperre für die betroffene Person eine grosse Bedeutung haben kann und der Schaden der Durchbrechung im Einzelfall kaum berechenbar ist. Während einzelne der betroffenen Personen allenfalls eine Datensperre nur beantragten, um nicht belästigt zu werden, hatte ein Grossteil der betroffenen Personen auch wegen einer Gefahr an Leib und Leben eine solche Sperre einrichten lassen. Im Falle eines Flüchtlings aus dem Iran, der aufgrund einer nicht auszuschliessenden persönlichen Gefährdung seine kürzlich gekaufte Eigentumswohnung wieder verkaufen wollte, sah sich die Stadt Zürich mit direkten Haftungsansprüchen konfrontiert.

4. Fernwartung von Informatiksystemen

Angemessene technische und organisatorische Massnahmen notwendig

Aufgrund der Anfragen des Fürsorgeamtes einer Gemeinde sowie einer Klinik verfassten wir Empfehlungen bezüglich datenschutzrechtlicher Anforderungen an die Fernwartung von Informatiksystemen mit sensiblen Personendaten.

§§ 1 und 2 der Datenschutzverordnung verlangen, dass das verantwortliche Organ die zur Gewährleistung der Datensicherheit geeigneten organisatorischen und technischen Massnahmen trifft. Aufgrund des Verhältnismässigkeitsprinzips sind um so höhere Anforderungen an diese Massnahmen zu stellen, je sensibler die Daten sind. Ein blosser Datenschutzvermerk in den Arbeitsverträgen der von der Fernwartungsfirma angestellten Mitarbeiter ist als Sicherheitsmassnahme nicht geeignet. Vielmehr ist bereits die Kenntnisnahme der Daten durch diese auszuschliessen.

Die Fernwartung von Informatiksystemen mit besonders schützenswerten Personendaten kann nur unter Beachtung der folgenden grundsätzlichen Überlegungen aus datenschutzrechtlicher Sicht zugelassen werden:

- Um die Nutzung der Fernwartungsverbindung durch Unbefugte auszuschliessen, darf die Dialogverbindung ausschliesslich durch Verantwortliche des zu wartenden Rechners aufgebaut werden können. Der Verbindungsaufbau sollte im Normalfall automatisch über festgelegte Nummern erfolgen, die im System hinterlegt sind. Der Wartungstechniker muss sich darüber hinaus bei jedem Wartungsvorgang durch ein vereinbartes Passwort autorisieren.
- Fernwartungsaktivitäten sollen lokal mitverfolgt und gegebenenfalls unterbrochen werden können. Hierzu muss beim verantwortlichen Organ vor Ort eine fachkundige Person anwesend sein.
- Der Zugriff auf personenbezogene Daten ist zu verhindern, indem Daten nur auf Verzeichnissen oder Datenträger gespeichert werden, die während des Wartungsvorgangs nicht verfügbar sind. Werden Test- und Serviceprogramme des Herstellers auf das System übernommen, sind diese unter einer besonderen Kennzeichnung abzulegen.
- Der Wartungstechniker darf keinen Systemverwalterstatus erlangen können. Sofern eine physikalische Abkoppelung der Dateien mit personenbezogenen Daten nicht möglich ist, ist das Einspielen von Änderungen in das Betriebssystem und in die systemnahe Software durch die Fernwartung abzulehnen und ausschliesslich vor Ort durchzuführen. Die Übernahme der Änderungen ist erst nach Freigabe des verantwortlichen Organs vorzunehmen. Applikationsprogramme dürfen durch die Fernwartung nicht aktiviert werden können.
- Fernwartungsaktivitäten sind revisionssicher aufzuzeichnen. Die Protokolle müssen durch entsprechende Programme ausgewertet werden können und vor Manipulationen geschützt sein.
- Der Personenbezug der gespeicherten Daten ist im weiteren durch geeignete Anonymisierung aufzuheben. Hierzu sind Namen und weitere, die Person unmittelbar identifizierende Daten von anderen anwendungsspezifischen Daten getrennt zu speichern. Während der Fernwartungstechniker lediglich Zugriff auf anonymisierte Daten hat, ist die Verknüpfung der Dateien zu Anwendungszwecken nur dem verantwortlichen Organ erlaubt.
- Mit der beauftragten Fernwartungsfirma ist eine vertragliche Vereinbarung abzuschliessen, die einen Hinweis auf die Strafbestimmung von § 26 DSG enthält.

Unter Beachtung dieser Grundsätze und dem Vorbehalt besonderer Geheimhaltungsvorschriften kann eine Fernwartung installiert werden.

5. Internet-Informationsangebot

Personendaten nur mit Einwilligung

Der Regierungsrat hat beschlossen, im Internet ein eigenes Informationsangebot der kantonalen Verwaltung aufzubauen. Vom Amt für Informatikdienste (AID) wird ein WWW-Server ausserhalb des mit einem Firewall abgesicherten kantonalen Netzwerkes betrieben. Für die Gestaltung des Angebotes wurde unter der Leitung der Staatskanzlei eine Arbeitsgruppe eingesetzt. Zuhanden dieser Arbeitsgruppe nahmen wir bezüglich der Frage des Datenschutzes Stellung. Das Anbieten von personenbezogenen Informationen im Internet ist aus datenschutzrechtlicher Sicht kritisch. Da solche Informationen praktisch weltweit verbreitet werden, ist ein Missbrauch dieser Daten nicht auszuschliessen und eine Ahndung von Missbräuchen kaum möglich. Wir verlangten deshalb, dass Informationen, die von der kantonalen Verwaltung auf dem Internet zur Verfügung gestellt werden, soweit zu anonymisieren sind, dass keine Rückschlüsse auf bestimmte oder bestimmbare Personen möglich sind. Sofern personenbezogene Informationen angeboten werden sollen (z.B. Kontaktpersonen, Adresslisten) ist sicherzustellen, dass die betroffenen Personen mit einer Bekanntgabe ihrer Daten via Internet ausdrücklich einverstanden sind. Dies bedeutet auch, dass sie über die Datenschutz-Risiken vorgängig aufgeklärt werden.

6. Aus dem Papierkorb

Mangelnde Sorgfalt bei der Papierentsorgung

Dem Datenschutzbeauftragten wurde eine beachtliche Anzahl von personenbezogenen Dokumenten aus den verschiedensten Amtsstellen und Verwaltungsabteilungen des Kantons zugestellt, die auf dem Weg zur Vernichtung in die Hände von unbefugten Dritten gelangt waren. Dabei handelte es sich nicht nur um allgemeine Personendaten, sondern teilweise sogar um besonders schützenswerte Daten über strafrechtliche Verfolgungen und Sanktionen.
Hinterher liess sich zwar nicht mehr eruieren, wo genau (Papierkorb, Container, Altstoffhändler) die Dokumente zur Kenntnis unbefugter Dritter gelangt sind. Unabhängig davon sind jedoch in allen Fällen das Datenschutzgesetz wie auch das Amtsgeheimnis tangiert.
Wir wandten uns an die betroffenen Amtsstellen und forderten sie auf, zum Sachverhalt Stellung zu nehmen. Aus den Antworten ging hervor, dass eine Sensibilisierung stattgefunden hatte und dass für eine praktische Realisierung einer datenschutzkonformen Entsorgung vertraulicher Akten vermehrt Bemühungen unternommen werden.
Wir schlossen den Vorfall ab, indem wir uns an alle betroffenen Amtsstellen wandten und sie auf die Wichtigkeit einer datenschutzkonformen Entsorgung und Vernichtung personenbezogener Akten hinwiesen. So müssen nicht nur die zur Zeit noch benötigten Unterlagen durch angemessene organisatorische und technische Massnahmen gegen das unbefugte Bearbeiten geschützt werden (§ 4 Absatz 5 DSG, §§ 1 und 2 DSV). Vielmehr ist dieser Schutz auch für die zur Makulatur gewordenen Unterlagen zu gewährleisten. Dabei kann die Verantwortung für eine datenschutzkonforme Behandlung von nicht mehr benötigten Unterlagen nicht delegiert und beispielsweise auf das Reinigungspersonal übertragen werden; sie verbleibt bis zum Moment der physischen Vernichtung beim datenverarbeitenden Organ.
In bezug auf Einzelheiten und organisatorische Vorgehensweisen einer datenschutzkonformen Aktenentsorgung verwiesen wir auf das Kreisschreiben der Staatskanzlei betreffend Vernichtung vertraulicher Akten vom 4. Dezember 1995. Es skizziert einen korrekten sowie praktikablen Weg zur Entsorgung vertraulichen Aktenmaterials.

Bedürfnis nach kompetenten Informationen

Mit Veranstaltungen, Seminaren, Referaten und Publikationen trugen wir weiter zur Sensibilisierung für die Anliegen des Datenschutzes bei.

1. Symposium für Datenschutz und Informationssicherheit

Rechtliche und sicherheitstechnische Aspekte

Der Datenschutzbeauftragte hat in Zusammenarbeit mit dem Departement Informatik der Eidgenössischen Technischen Hochschule (ETH) am 3. Oktober 1996 das 1. Symposium für Datenschutz und Informationssicherheit veranstaltet. Unter dem Titel «Vernetzte Informationstechnologie kontra Persönlichkeitsschutz?» wurden datenschutzrechtliche Fragestellungen und Lösungsansätze für die Datensicherheit vorgestellt. Im Zeitalter globaler Vernetzung der Informations- und Kommunikationstechnologien stellen sich nebst Fragen nach der Rechtmässigkeit immer mehr auch Fragen nach der Sicherheit. Dank der Zusammenarbeit mit der ETH konnten beide Aspekte zusammengeführt werden. Thematische Schwerpunkte des Symposiums waren das Internet, technische und rechtliche Aspekte der Chipkarte, Datenschutzfragen im New Public Management und die europäische Rechtsentwicklung. Als Referenten wirkten neben den Veranstaltern Dozenten vom Interkantonalen Technikum Rapperswil (ITR) und der Hochschule St.Gallen (HSG) sowie Datenschutzbeauftragte aus der Schweiz und dem Ausland.
Über 250 Teilnehmerinnen und Teilnehmer haben an dieser Veranstaltung teilgenommen. Das Echo war sehr positiv, und die grosse Teilnehmerzahl bestätigte das wachsende Bedürfnis nach praxisbezogener Information in diesem Bereich. Die Veranstaltung war auch in finanzieller Hinsicht erfolgreich; es konnte sogar ein Gewinn zuhanden der Staatskasse ausgewiesen werden. Das 2. Symposium für Datenschutz und Informationssicherheit, das am 11. September 1997 wiederum an der ETH Zürich stattfinden wird, hat das Thema «Konzepte und Technologien für einen wirksamen Datenschutz».

2. Seminare und Referate

Sensibilisierung für die Anliegen des Datenschutzes

Im Rahmen des Angebots der kantonalen Aus- und Weiterbildung führten wir ganztägige Seminare zum Datenschutz durch. Diese Seminare wurden in zwei unterschiedlichen Formen angeboten und richteten sich einerseits an Führungskräfte der Verwaltung, die in ihren Bereichen die Verantwortung für die Umsetzung des Datenschutzgesetzes tragen, und andererseits an Mitarbeiterinnen und Mitarbeiter, die in ihrer täglichen Arbeit mit Datenschutzfragen konfrontiert werden. Anhand von Fallbeispielen wurden die Grundanliegen des Datenschutzes vermittelt, und die Teilnehmerinnen und Teilnehmer gewannen einen Überblick über datenschutzrechtliche Lösungsansätze in ihren Bereichen. Die Seminare fanden ein grosses Interesse und wurden sehr positiv beurteilt. Das Angebot soll deshalb in diesem Rahmen beibehalten werden. Des weiteren gestalteten wir für verschiedene Bereiche halbtägige Spezialseminare. Diese Veranstaltungen ermöglichten es, noch spezifischer auf die Bedürfnisse der einzelnen Direktionen oder Abteilungen einzugehen. Einen Schwerpunkt bildeten dabei Seminare im Bereich des Gesundheitswesens.
Daneben hielten wir zahlreiche Referate bei Direktionen, Ämtern oder Verbänden zu spezifischen Fragestellungen. Ausgangspunkt für solche Referate waren vielfach konkrete Fälle, die das Bedürfnis und die Notwendigkeit nach eingehenderen datenschutzrechtlichen Informationen aufzeigten.

3. Publikationen des Datenschutzbeauftragten

«Fakten» – die Zeitschrift für Datenschutz des Kantons Zürich

1996 publizierten wir vier Nummern unserer Zeitschrift «Fakten». Die Sondernummer Fakten 1/1996 präsentiert die Studie von Prof. Dr. U. Maurer, ETH Zürich, über «Sicherheit in Datennetzen». Diese Sondernummer fand grosses Interesse und wird mittlerweile in verschiedenen Projekten der Verwaltung, wo es um Fragen der Informatiksicherheit geht, als Referenz beigezogen. Eine zweite Sondernummer (Fakten 4/1996; «Beiträge '96 zum Datenschutz») beinhaltet Artikel verschiedener Autorinnen und Autoren zu Fragen des Datenschutzes im Bereich des Gesundheitswesens, der Polizei, des New Public Managements und der Europäischen Union (EU).
Fakten 2/1996 beschäftigt sich schwerpunktmässig mit den Gesprächsaufzeichnungen und -protokollierungen in den modernen, digitalen Telefonzentralen.
Fakten 3/1996 stellt den Umgang mit sensiblen Daten am Beispiel der Schulpsychologischen Dienste dar.
Die Zahl der Interessentinnen und Interessenten für Fakten wächst laufend, obwohl wir bisher keine Werbeanstrengungen unternehmen konnten. Es zeigt sich, dass diese Publikation auch zu Ausbildungszwecken und für die Dokumentation von Fragen des Datenschutzes sehr gut geeignet ist. «Fakten» soll deshalb auch in Zukunft diesen Bedürfnissen entsprechen.

4. Dritte nationale Konferenz der Datenschutzbeauftragten in Zürich

Informationsaustausch und Verabschiedung einer Resolution

Nachdem die Konferenz der Datenschutzbeauftragten zweimal vom Eidgenössischen Datenschutzbeauftragten veranstaltet worden war, hatten wir die Gelegenheit, als erster Kanton diesen Anlass zu organisieren. Die 3. Konferenz der Datenschutzbeauftragten fand am 2. Oktober 1996 statt und vereinigte Vertreterinnen und Vertreter aus Bund und 19 Kantonen.
Im Mittelpunkt der Diskussionen standen die Datenbearbeitungen von besonders schützenswerten Personendaten im Gesundheitswesen. In jüngster Zeit fallen in diesem Gebiet an verschiedenen Stellen – insbesondere bei den Krankenkassen sowie bei den kantonalen und eidgenössischen Statistik- und Gesundheitsbehörden – beträchtliche Datenmengen an. Nach zwei Referaten zu diesem Themenbereich verabschiedete die Konferenz einstimmig eine Resolution, die alle Akteure des Gesundheitswesens (Krankenkassen, Gesundheitsbehörden, Statistikbehörden) auffordert, den Aspekten des Persönlichkeitsschutzes vermehrt Rechnung zu tragen, indem die Menge der bekanntgegebenen Gesundheitsdaten im Einzelfall auf das notwendige Mindestmass begrenzt werden (Verhältnismässigkeit) und dafür gesorgt wird, dass medizinische Daten nur unter Arztpersonal und dessen Hilfspersonen zirkulieren und die Dauer jeglicher Aufbewahrung von Personendaten limitiert wird.
Weitere Schwerpunkte der Konferenz waren der Revisionsentwurf des Volkszählungsgesetzes, die Behandlung erkennungsdienstlicher Unterlagen der Polizei und der Datenschutz in Archiven. Diskutiert wurden zudem der Datenaustausch zwischen kantonalen und kommunalen Ämtern, die Vertrauenswürdigkeit von EDV-Systemen und die Problematik der Fernwartung von Informatiksystemen.
Die 3. nationale Konferenz der Datenschutzbeauftragten kann als weiterer Schritt zu einer engen Zusammenarbeit der schweizerischen Datenschutzbeauftragten gewertet werden.

Datenschutz in Bewegung

In verschiedenen Bereichen, die wir im letzten Tätigkeitsbericht (Nr. 1, 1995) aufgegriffen haben, sind seither Entwicklungen eingetreten.

1. Datenschutz im Gesundheitswesen

Kreisschreiben der Gesundheitsdirektion

Im letztjährigen Tätigkeitsbericht Nr. 1 (1995), S. 10, haben wir berichtet, dass die Gesundheitsdirektion die Anwendbarkeit des Datenschutzgesetzes im Bereich der staatlichen und vom Staat unterstützten Krankenhäuser lange Zeit ablehnte. Weitere Gespräche mit Vertretern aus dem Gesundheitsbereich sowie eine Anfrage im Kantonsrat (Revision der Patientenrechtverordnung und der Verordnung über den Datenschutz in den kantonalen Krankenhäusern; KR-Nr. 25/1996, 24. April 1996) haben 1996 zu einer vermehrten Beachtung der datenschutzrechtlichen Bestimmungen im Bereich des Gesundheitswesen geführt.

Die Patientenrechtverordnung wurde mit einem Kreisschreiben der Gesundheitsdirektion vom 18. November 1996 präzisiert, und die veraltete Verordnung über den Datenschutz in den kantonalen Krankenhäusern ist auf den 31. Dezember 1996 aufgehoben worden. Damit ist eine gute Grundlage für einen datenschutzkonformen Umgang mit den sensiblen Gesundheitsdaten geschaffen. Allerdings sind zwei wichtige Punkte, nämlich der Herausgabeanspruch der Patientinnen und Patienten auf ihre Krankengeschichte respektive die Frage des Eigentums an der Krankengeschichte sowie das Einsichtsrecht in Drittunterlagen, die sich in der Krankengeschichte befinden, offen geblieben. Diesbezüglich werden sich in der Praxis weiterhin Schwierigkeiten ergeben.

Zu hoffen bleibt, dass die Bemühungen der Gesundheitsdirektion in bezug auf den Datenschutz nicht an diesem Punkt stehen bleiben, sondern dass mit entsprechenden Massnahmen (z.B. Ausbildung) die Sensibilisierung für die Anliegen des Datenschutzes in diesem sehr sensiblen Bereich vorangetrieben wird. Mit Weisung vom 18. Oktober 1996 hat die Gesundheitsdirektion die Krankenhäuser verpflichtet, spitalinterne Datenschutzbeauftragte zu bestimmen. Im weiteren wurde eine Arbeitsgruppe zur Koordination der Datenschutz- und Datensicherheitsmassnahmen in den Krankenhäusern eingesetzt.

2. Vollzug des neuen Krankenversicherungsgesetzes

Bundesrechtswidrige Lösungen

Die kantonale Einführungsverordnung zum neuen Krankenversicherungsgesetz (EVO KVG), die am 1. Januar 1996 in Kraft trat, führte zu einem Datenaustausch zwischen Gesundheitsdirektion, Sozialversicherungsanstalt, Gemeinden und Versicherern (Krankenkassen), von dem sämtliche Einwohnerinnen und Einwohner betroffen sind. Aufgrund verschiedener Anfragen betroffener Personen und in Zusammenarbeit mit dem Eidgenössischen Datenschutzbeauftragten überprüften wir die Verfahren der Obligatoriumsabklärung und der Prämienverbilligung sowie Aspekte der Datensicherheit.

Im Verfahren der Obligatoriumsabklärung reichten die Krankenkassen die Daten ihrer Mitglieder der Gesundheitsdirektion ein. Diese Daten wurden mit den Daten aus den Einwohnerkontrollregistern abgeglichen, um festzustellen, bei welchen Personen keine obligatorische Krankenversicherung bestand. Diese Personen wurden aufgefordert, sich zu versichern, oder wurden zwangsversichert.

Das Krankenversicherungsgesetz (KVG) enthält keine Grundlage, welche die Kantone berechtigt, von den Krankenkassen die Bekanntgabe von Daten all ihrer Mitglieder zu verlangen. Die Krankenkassen, die im Bereich des Vollzugs des Versicherungsobligatoriums als Bundesorgane zu betrachten sind,

verfügen über keine Rechtsgrundlage zur Datenbekanntgabe. Die Einführung der Versicherungspflicht sollte nach der Meinung des Gesetzgebers auch nicht zu einer Aufblähung der Verwaltung führen, weshalb eine flächendeckende Abklärung unverhältnismässig ist. Das Verfahren gemäss § 2 EVO KVG erscheint deshalb als bundesrechtswidrig. Gemäss Angaben der Gesundheitsdirektion wird es nicht mehr weitergeführt.
Die Auszahlung der individuellen Prämienverbilligung richtet sich nach § 5 Abs. 3 EVO KVG. Die Sozialversicherungsanstalt resp. die Stadt Zürich teilen den Versicherten die Höhe der Beträge der individuellen Prämienverbilligung mit, überweisen diese aber direkt den Krankenkassen, welche die Beträge den jeweiligen Prämienkonti der Versicherten gutzuschreiben haben. Gemäss Art. 65 Abs. 1 KVG gewähren die Kantone den Versicherten, die in bescheidenen wirtschaftlichen Verhältnissen leben, Prämienverbilligungen. Durch die Auszahlung an die Krankenkassen gelangen diesen Daten über die wirtschaftlichen Verhältnisse ihrer Mitglieder zur Kenntnis. Eine solche Datenbekanntgabe ist durch keine gesetzliche Grundlage abgedeckt. Sie ist auch nicht erforderlich für die Aufgabenerfüllung der Krankenkassen und deshalb unverhältnismässig. Das Verfahren im Bereich der individuellen Prämienverbilligung muss deshalb angepasst werden. Da bisher der Auszahlungsmodus nicht geändert wurde, bleibt den betroffenen Personen nur die Möglichkeit des Rechtswegs.
Im Tätigkeitsbericht Nr. 1 (1995), S. 10, haben wir auf das fehlende Datensicherheitskonzept beim Vollzug des KVG hingewiesen. Anlass zur Überprüfung der Datensicherheitsmassnahmen bildete 1996 die Mitteilung an eine Privatperson, dass sie aufgrund eines steuerbaren Einkommens und eines steuerbaren Vermögens von Fr. 0.00 Anspruch auf Prämienverbilligung habe. Im gleichen Schreiben waren auch drei weitere Personen erwähnt, die mit dieser Person offensichtlich nichts zu tun haben. Bei einer Überprüfung der uns zur Verfügung gestellten Unterlagen zur Datensicherheit mussten wir feststellen, dass offensichtlich kein Sicherheitskonzept für die betreffende Anwendung besteht. Wir haben diesbezüglich weiter interveniert.

3. Steuerausweise und Privatsphäre

Sperrecht im neuen Steuergesetz vorgesehen

Im Tätigkeitsbericht Nr. 1 (1995), S. 12, haben wir die Problematik der Bekanntgabe von Steuerdaten an private Personen und Organisationen dargestellt. Unterdessen hat sowohl bezüglich der Revision des Steuergesetzes (StG) als auch bezüglich der bestehenden Rechtslage eine Entwicklung stattgefunden.
Die Revision des StG wurde in der Zwischenzeit vom Kantonsrat beraten und beschlossen. Die Möglichkeit der Ausstellung von Steuerausweisen an Dritte wurde beibehalten. Im Sinne der Auffassung des Datenschutzbeauftragten ist im neuen StG indessen ein Sperrecht gemäss § 11 DSG vorgesehen. Das neue StG bedarf noch der Zustimmung des Stimmvolkes.
Unter der aktuellen Rechtslage ist derzeit ein Rechtsmittelverfahren hängig. Eine private Person wollte im Sinne von § 11 DSG ihre Steuerdaten beim Steueramt ihrer Wohngemeinde sperren lassen, was dieses ablehnte. Ein Rekurs gegen diese Verfügung wurde abgewiesen. Die Angelegenheit ist derzeit vor der dritten Instanz hängig. Nach unserer Auffassung besteht unter dem geltenden Steuergesetz zur Ausstellung von Steuerausweisen keine ausreichende Rechtsgrundlage im Sinne von § 8 DSG, die den Anforderungen von Art. 8 der Europäischen Menschenrechtskonvention (EMRK) genügen würde. Zumindest wäre ein Sperrrecht für die betroffenen Personen gemäss § 11 DSG anzuerkennen: § 83 StG ist keine verpflichtende Norm für das Steueramt zur Datenbekanntgabe, sondern lediglich eine Ermächtigung zur Ausstellung von Steuerausweisen.

4. Datensperre für Motorfahrzeughalter

SVG-Revision und CD-ROM

Die Veröffentlichung von Daten über Motorfahrzeughalter durch das Strassenverkehrsamt hat mit dem Einbezug neuer Medien (Tel.-Nr. 111 und Videotex), die eine Auskunftsmöglichkeit rund um die Uhr anbieten, zu einem erhöhten Risiko von Persönlichkeitsverletzungen geführt, da solchermassen bekanntgegebene Daten ohne weiteres auch in anderem Zusammenhang als mit dem Strassenverkehr Verwendung finden können (z.B. Ausspionieren der Privatsphäre, Belästigungen, Erleichterung krimineller Handlungen). Diese Gefahr des Missbrauchs führte zu einer starken Sensibilisierung der Öffentlichkeit, und viele betroffene Personen haben von der Möglichkeit der Datensperre gemäss § 11 DSG Gebrauch gemacht (vgl. Tätigkeitsbericht Nr. 1 [1995], S. 11).
Die Teilrevision des Strassenverkehrsgesetzes (SVG), über die 1996 ein Vernehmlassungsverfahren durchgeführt wurde, sieht nun zum besseren Schutz der Persönlichkeit der Fahrzeughalter den Verzicht auf die Publikation der Fahrzeughalterverzeichnisse vor. In unserer Stellungnahme im Mitberichtsverfahren haben wir diesen Vorschlag grundsätzlich begrüsst, wobei wir für den Fall der Beibehaltung der Publikationsmöglichkeit im Sinne einer einheitlichen Bestimmung für die ganze Schweiz auch ein vorbehaltloses Sperrecht auf bundesrechtlicher Ebene vorgeschlagen haben. Im weiteren wiesen wir in bezug auf vorgesehene direkte «Online-Zugriffe» auf ungenügende gesetzliche Grundlagen sowie offene Datensicherheitsfragen hin. Der Regierungsrat hat unsere Vorbehalte in seiner Vernehmlassungsantwort integriert.

1996 hat eine private Firma das Fahrzeughalterregister des Kantons Zürich (und fast sämtlicher übriger Kantone) auf einer CD-ROM angeboten. Diese Bearbeitung der Motorfahrzeughalterdaten ist durch die gesetzlichen Bestimmungen nicht abgedeckt und beinhaltet eine Zweckentfremdung der Daten. Die CD-ROM lässt sich nach verschiedenen Kriterien auswerten, obwohl die gesetzlichen Bestimmungen nur die Angabe von Name und Adresse eines Fahrzeughalters (Kontrollschild) zulassen. Sie verstösst auch gegen das Prinzip der Verhältnismässigkeit und teilweise gegen den Grundsatz der Integrität. Der Eidgenössische Datenschutzbeauftragte, der für die Datenbearbeitungen durch private Personen zuständig ist, hat deshalb in einer Empfehlung die betroffene Firma aufgefordert, die Produktion und den Vertrieb dieser CD-ROM einzustellen.

Datenschutzbeauftragter
des Kantons Zürich
Kaspar Escher-Haus
8090 Zürich
Tel.: 01 / 259 39 99
Fax: 01 / 259 51 38

Datenschutzbeauftragter:
Dr. iur. Bruno Baeriswyl

Jur. Sekretär(in):
lic.iur. Peter Meyer (bis 30.6.1996)
Dr. iur. Esther Knellwolf (ab 1.7.1996)

Auditor:
lic.iur. Daniel Geisseler (bis 30.9.1996)
lic.iur. Marco Fey (ab 1.10.1996)

Sekretariat:
Regula Rüeger

Tätigkeitsbericht Nr. 2 (1996)

Konzeption und Produktion:
Frontpage AG, Zürich

Druck:
KDMZ
Gedruckt auf Recyclingpapier

Bezug:
Druckschriftenverkauf
Neumühlequai 8
8090 Zürich
Tel.: 01 / 259 20 28
Fax: 01 / 259 51 45