Nr. 4

Tätigkeits-Bericht

Datenschutzbeauftragter des Kantons Zürich

1998

Tätigkeitsbericht

Nr. 4
1998

Der Datenschutzbeauftragte erstattet dem Regierungsrat jährlich oder nach Bedarf einen Bericht über seine Tätigkeit (§ 23 Datenschutzgesetz). Der vorliegende Tätigkeitsbericht Nr. 4 deckt den Zeitraum vom 1. Januar 1998 bis 31. Dezember 1998 ab.

Zürich, Mai 1999

Der Datenschutzbeauftragte
des Kantons Zürich
Dr. Bruno Baeriswyl

Inhaltsverzeichnis

Die Informatisierung der Verwaltung

Die Entwicklungen im Bereich der Verwaltungsinformatik führen zu einer neuen «Qualität» der Datenbearbeitungen. Werden die datenschutzrechtlichen Grundsätze nicht beachtet, geht die technische Entwicklung zu Lasten der Grundrechte der Bürgerinnen und Bürger.

Die neuen Projekte in der kantonalen wie in den kommunalen Verwaltungen zeigen, dass die Sensibilität der Datenbearbeitungen auf Grund der technischen Möglichkeiten ständig zunimmt. Die technische Ausgangslage kann einen offensichtlich unersättlichen Hunger nach immer mehr Informationen über die einzelnen Bürgerinnen und Bürger und nach einer immer stärkeren Vernetzung dieser Daten ohne weiteres erfüllen. Die Frage, ob diese Daten im Einzelfall zur Erfüllung der Aufgaben geeignet und erforderlich sind, tritt in den Hintergrund.
Vor allem bei grossen Projekten erscheint oftmals die Dynamik der Technik der einzig bestimmende Faktor zu sein, so dass grundrechtliche Standpunkte in diesen Vorhaben einen schweren Stand haben.

Grundsätze des Datenschutzes

Vermehrt mussten wir deshalb in den Projekten, bei denen wir beigezogen wurden, auf die Grundsätze des Datenschutzrechts verweisen. Erfreulicherweise konnten in vielen Bereichen – nach teilweise sehr aufwendigen Diskussionen – entsprechende Rahmenbedingungen geschaffen werden.
Die Auswahl der Themen aus dem vorliegenden Berichtsjahr beleuchtet die verschiedenen Aspekte dieser Entwicklungen.

Outsourcing der Informatik

In der kantonalen Verwaltung wurden im vergangenen Jahr die Grundlagen gelegt für eine Privatisierung des Amtes für Informatikdienste (AID) mit dem Hintergrund, die Informatikleistungen der Verwaltung weitgehendst auszulagern (siehe S. 10). Die Auslagerung von umfassenden Informatikumgebungen an private Unternehmen bedeutet indessen einen Eingriff in die Grundrechtspositionen der Bürgerinnen und Bürger, da der Datenschutz nicht mehr auf einem gleichwertigen Niveau gewährleistet ist, wie wenn diese Daten durch die Verwaltung selber bearbeitet würden. Um für solche Fälle einen adäquaten Datenschutz gewährleisten zu können, müssen auch auf der rechtlichen Ebene die notwendigen Rahmenbedingungen geschaffen werden. Diese Schritte wurden mit einem Entwurf für ein Gesetz über die Auslagerung von Informatikdienstleistungen in die Wege geleitet.

Daten für statistische Zwecke

Die moderne Verwaltung verlangt zunehmend Daten für planerische und statistische Zwecke. Im Schulbereich werden mit der Neugestaltung der Bildungsstatistik Grundlagen geschaffen, um diesen Ansprüchen genügen zu können (siehe S. 13).
Die Sensibilität dieser Datenbearbeitungen ist allein schon durch deren Umfang gegeben. Aber auch

einzelne Datenkategorien, wie beispielsweise die Erfassung von Langzeitkarrieren der Schülerinnen und Schüler, können sensible Informationen enthalten.
Das Datenschutzrecht privilegiert Datenbearbeitungen zu statistischen, planerischen und ähnlichen Zwecken. Voraussetzung hierzu ist dabei einerseits, dass die Daten anonymisiert werden, sobald es der Zweck des Verfahrens erlaubt, und andererseits, dass diese Daten ausschliesslich zu statistischen Zwecken verwendet werden.
Die Beschäftigung mit diesem Projekt hat gezeigt, dass zur Sicherstellung dieser Grundsätze auf der rechtlichen, organisatorischen und technischen Ebene Massnahmen zu treffen sind. Nur so wird es möglich sein, dass mit dieser umfassenden Datenbearbeitung auch die Grundrechtsansprüche der betroffenen Personen gewährleistet werden können.

Sensible Organisationsstruktur

Bei organisatorischen Massnahmen können sich aus datenschutzrechtlicher Sicht sehr sensible Konstellationen ergeben. Mit der Schaffung der Direktion für Soziales und Sicherheit wurden die Polizeidirektion und die Fürsorgedirektion zusammengelegt, zwei Bereiche, die jeder für sich sehr sensible Daten bearbeitet (siehe S. 16).
Nur wenn das datenschutzrechtliche Grundprinzip der Zweckbindung strikte eingehalten wird, kann diese organisatorische Massnahme ohne Eingriffe in die Grundrechte der betroffenen Personen erfolgen. Das Prinzip der Zweckbindung besagt, dass Daten nur zu dem Zweck bearbeitet werden dürfen, der ursprünglich vorgesehen, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist (§ 4 Abs. 4 DSG).

Vernetzung raumbezogener Daten

Datensysteme, die zum Inhalt die Vernetzung von unterschiedlichsten Datensammlungen haben, bergen die Gefahr in sich, auf Grund ihrer technischen Möglichkeiten Daten über einzelne Personen zur Verfügung zu stellen, die ursprünglich nie vorgesehen waren. Zu einem solchen System entwickelt sich heute das Geografische Informationssystem der Verwaltung (GIS) (siehe S. 41).
Ausgangspunkt des GIS war, den in verschiedenen Bereichen tätigen Amtsstellen raumbezogene Daten zur Verfügung zu stellen. Das GIS-Dienstleistungszentrum soll dabei als «technische Drehscheibe» dienen, bei der jede involvierte Amtsstelle ihre eigenen Daten ablegt und von wo sie diejenigen Daten bezieht, die sie für ihre Aufgabe zusätzlich als notwendig erachtet.
Zunehmend kamen auch Personendaten dazu, so dass sich dieses System immer mehr zu einem Informationspool entwickelt, wo in Zukunft festgestellt werden kann, welche Grundstücke eine Person im Kanton Zürich besitzt, welche Schätzwerte die Gebäude haben oder ob allenfalls das Grundstück auf Grund der vorhandenen Altlasten als wertlos zu betrachten ist.
Diese zentralisierten Informationen wecken unterschiedliche Begehrlichkeiten: Auf der einen Seite möchte die Verwaltung diese Daten an Dritte verkaufen, auf der anderen wünschen interessierte private Kreise möglichst einen Online-Zugriff, so dass sie im «Selbstbedienungssystem» die sie interessierenden Daten beziehen können.
Für die betroffenen Personen geht die Transparenz über diese Datenbearbeitungen verloren: Beim überwiegenden Teil der bearbeiteten Daten stehen sie in einem hoheitlichen Verhältnis zum Staat und sind verpflichtet, einzelne Angaben gegenüber der Behörde zu geben, beispielsweise beim Eintrag eines Grundstückes in das Grundbuch. Müssen sie aber auch damit rechnen, dass diese Daten mit anderen Informationen kombiniert werden, beispielsweise mit dem Altlastenkataster, oder dass ihre Daten sogar durch den Staat kommerzialisiert werden?
Diese Problemstellungen wurden bisher im vorliegenden GIS-Projekt vernachlässigt. Das Projekt wird überwiegend mit Informatikkrediten gesteuert, so dass die rechtsstaatlichen Fragen wenig Beachtung finden.
Die GIS-Verordnung kann beim heutigen Ausmass dieser Datenbearbeitungen nicht mehr als ausreichende Rechtsgrundlage gelten. Bei einzelnen Datenbearbeitungen, insbesondere bei Datenkombinationen, scheinen entsprechende Grundlagen zu fehlen. Ebenso

wird das datenschutzrechtliche Zweckbindungsgebot umgangen.

Aufbewahrung von DNA-Analysen

Fragen in Bezug auf die gesetzlichen Grundlagen und das Prinzip der Verhältnismässigkeit stellen sich auch bei den DNA-Analysen (siehe S. 22). Das Bundesgericht hat festgehalten, dass die Aufbewahrung von DNA-Analysen einen schweren Eingriff in die Grundrechte der betroffenen Personen bedeutet. Ein solcher Eingriff erfordert deshalb eine gesetzliche Grundlage, und er muss verhältnismässig sein. Ohne diese Voraussetzungen dürfen DNA-Datenbanken nicht geführt werden.
In der Praxis zeigt sich indessen, dass EDV-Systeme solche Daten festhalten, ohne dass hierfür die rechtlichen Rahmenbedingungen bestehen. Nach dem Prinzip der Verhältnismässigkeit dürfen nur Daten aufbewahrt werden, die geeignet und erforderlich sind. Entsprechend müssten Einträge von Personen wieder gelöscht werden, die auf Grund der DNA-Analyse als Spurenleger eindeutig ausgeschlossen werden können. Technisch ist es einfacher, Daten aufzubewahren, als sie zu löschen. Die Beachtung der rechtlichen Rahmenbedingungen bei der Konfiguration von EDV-Systemen ist deshalb Voraussetzung, dass die Grundrechte der betroffenen Personen gewahrt werden können.

Internet als Kommunikationsmedium

Das Internet dient immer mehr als Informationsplattform für die Verwaltung (siehe S. 25). Die Verbreitung von Personendaten im Internet hat unter Beachtung der rechtlichen Rahmenbedingungen zu erfolgen. Da der Missbrauch von Personendaten im Internet nicht auszuschliessen ist, stellt sich bei jeder Publikation die Frage, ob personenbezogene Daten wirklich geeignet und erforderlich sind. Insbesondere ist zu beachten, dass es sich um eine weltweite Verbreitung von Daten handelt und die Daten nach deren Verbreitung kaum mehr korrigierbar oder entfernbar sind, da sie in zahlreichen Systemen gespeichert werden.
Diese Fragen stellen sich auch bei amtlichen Publikationen, beispielsweise bei Einbürgerungen, die im Amtsblatt werden, welches wiederum im Internet zugänglich gemacht wird.
Auf der anderen Seite sollen dank Internet-Angeboten die Bürgerinnen und Bürger leichter in Kontakt mit der Verwaltung treten können. Die Verwaltung hat deshalb zu gewährleisten, dass mit den notwendigen technischen Massnahmen ein Missbrauch der Daten ausgeschlossen werden kann. Der Anspruch auf Sicherheit gehört zu den datenschutzrechtlichen Grundrechten der Bürgerinnen und Bürger.

Personalinformationssystem

Den Anspruch auf Sicherheit ihrer Daten haben auch die Mitarbeiterinnen und Mitarbeiter der Verwaltung. Der Staat als Arbeitgeber hat die Privatsphäre seiner Angestellten entsprechend zu achten. Das neue kantonale Personalrecht respektiert diesen Grundsatz. Er ist auch bei der Einführung neuer elektronischer Personalinformationssysteme durch entsprechende organisatorische und technische Massnahmen sicherzustellen (siehe S. 35).
Die Sicherheit des Bearbeitens von sensiblen Personendaten in einem vernetzten System kann nur gewährleistet werden, wenn diese Daten verschlüsselt werden. Solche Anforderungen gehören deshalb zu den Eckpfeilern eines Systems, das verwaltungsweit – zentral und dezentral – Personaldaten bearbeiten will. Die betroffenen Personen haben einen Rechtsanspruch, dass ihre Daten nicht in unbefugte Hände gelangen.

Technische Entwicklungen zu Lasten der Grundrechte?

Diese Entwicklungen führten dazu, dass der Datenschutzbeauftragte vermehrt in Erinnerung rufen musste, dass die Informatisierung der Verwaltung – die Entwicklung der Technik – nicht zu Lasten der Grundrechte der Bürgerinnen und Bürger gehen darf. Die Vorteile ökonomischer oder organisatorischer Art sind nicht auf Kosten der Freiheitsrechte der betroffenen Personen zu realisieren.
Das Datenschutzgesetz beinhaltet eine Konkretisierung dieser Rechte in Bezug auf die Datenbearbeitungen, weshalb es im Rahmen der zunehmenden Informatisierung

der Verwaltung die gesetzliche Leitlinie bilden muss. Der Auftrag der Bürgerinnen und Bürger, die das Datenschutzgesetz in der Volksabstimmung mit einer Ja-Mehrheit von drei Vierteln angenommen haben, ist klar:

- Die Bürgerinnen und Bürger wollen Sicherheit: Ihre Daten sollen gegen Missbrauch geschützt werden und nicht in unbefugte Hände gelangen (§ 4 Abs. 5 DSG); die Bürgerinnen und Bürger haben auch den Anspruch, dass nur korrekte Daten über sie bearbeitet werden (§ 4 Abs. 2 DSG).
- Die Bürgerinnen und Bürger wollen Transparenz: Die Verpflichtung, der Verwaltung Daten bekannt geben zu müssen, hat sich aus einer Rechtsgrundlage zu ergeben (§ 4 Abs. 1 DSG), die auch etwas darüber aussagen muss, was mit den Daten geschieht (§ 4 Abs. 4 DSG).
- Die Bürgerinnen und Bürger legen Wert auf ihre Privatsphäre: Die Verwaltung soll nur diejenigen Daten über sie bearbeiten, die für die Aufgabenerfüllung geeignet und erforderlich sind (§ 4 Abs. 3 DSG).

Wirkung des Datenschutzrechts

Es ist die Aufgabe des Datenschutzbeauftragten, für die Gewährleistung dieser Grundrechte in der Verwaltung zu sorgen (§ 23 DSG). Die Wirkung seiner Tätigkeit lässt sich deshalb auch daran messen, wieweit die Informatisierung der Verwaltung unter der Respektierung der demokratischen Grundrechte erfolgt. Erfreulicherweise kann im jetzigen Zeitpunkt hier eine relativ positive Bilanz gezogen werden. Dies auch dank der Mitwirkung zahlreicher Verwaltungsstellen, die den Grundrechtsgehalt dieser Projekte erkannt haben und entsprechende Anstrengungen unternehmen.

Bedeutung des Datenschutzes

Die Informatisierung der Verwaltung zeigt auch, dass die Bedeutung des Datenschutzes weiter zunimmt. Diese Entwicklung darf aber nicht allein durch die Technik gesteuert sein.
Es werden sich deshalb auch vermehrt auf der rechtlichen Ebene grundsätzliche Fragen stellen: Die Informationsgesellschaft verlangt einen Ausgleich zwischen dem Schutz der Informationen und dem Zugang zu Informationen. Weiter hat ein Ausgleich zu erfolgen zwischen den individuellen Ansprüchen des Einzelnen auf Privatsphäre und den öffentlichen oder anderen privaten Interessen an mehr Daten über die einzelne Person. Aber auch auf der technischen Ebene ist an Sicherheitstechnologien zu arbeiten, die eine Gefährdung der Grundrechte ausschliessen.
Bei diesen Herausforderungen ist nicht weiter erstaunlich, dass die Geschäftslast beim Datenschutzbeauftragten auch im vergangenen Jahr kontinuierlich angestiegen ist. Die beratende und kontrollierende Funktion des Datenschutzbeauftragten trägt in ihrer präventiven Wirkung dazu bei, dass grundrechtliche Rahmenbedingungen und notwendige Interessenabwägungen Beachtung finden. Damit gewinnt die Verwaltung das Vertrauen, das notwendig ist im Verhältnis zwischen Bürgerinnen und Bürgern und dem Staat.

Zunehmende Sensibilität der Datenbearbeitungen

Sowohl organisatorische Massnahmen als auch der wachsende Umfang der Datenbearbeitungen führen zu einer zunehmenden Sensibilität der Datenbearbeitungen in der kantonalen Verwaltung.

1. Outsourcing der Informatik

Gesetz über die Auslagerung von Informatikdienstleistungen

Die im Projekt «Espresso» erarbeiteten Grundsätze für die kantonale Informatik sowie der Entscheid des Regierungsrates, das Amt für Informatikdienste des Kantons Zürich mit demjenigen des Kantons St. Gallen in einer privatrechtlichen Aktiengesellschaft zusammenzulegen, liessen auf der rechtlichen Ebene einen Handlungsbedarf erkennen, der auch durch die datenschutzrechtlichen Vorgaben hervorgerufen wurde. Nachdem sich im Rahmen des Projektes «Espresso» eine Arbeitsgruppe mit den (datenschutz)rechtlichen Fragestellungen befasst hatte, wurde einem externen Gutachter der Auftrag erteilt, die offenen rechtlichen Fragen eingehender darzustellen, um eine Entscheidungsgrundlage zu schaffen. Die wesentlichen Punkte, die sich aus datenschutzrechtlicher Sicht stellten, waren die Fragen nach den Rechtsgrundlagen für die Auslagerung gesamter Informatikleistungen, der Gewährleistung eines gleichwertigen Datenschutzes und einer entsprechenden Kontrolle, dem Umgang mit dem Amtsgeheimnis und den Spezialgeheimnissen sowie nach den zu treffenden organisatorischen und technischen Massnahmen und deren Sicherstellung. Entgegen den Schlussfolgerungen des Gutachtens ist davon auszugehen, dass ein umfassendes Informatik-Outsourcing einen Eingriff in die Grundrechtspositionen der Bürgerinnen und Bürger beinhaltet. Deshalb sind Vorkehrungen zu treffen, um im Rahmen des Legalitätsprinzips bestehende rechtliche Rahmenbedingungen zu erfüllen. Insbesondere ging das Gutachten nicht auf die Tragweite und die Bedeutung der Informatik im Rahmen der staatlichen Verwaltung ein. Es klassifizierte Informatik als administrative Hilfstätigkeit im althergebrachten Verständnis und übersah, dass die Informatik im Rahmen der staatlichen Tätigkeit eine qualitativ andere Gewichtung hat. Insbesondere sind bei Informatikleistungen die folgenden Kriterien zu beachten:

- die Sensitivität der Aufgabe: Im Zusammenhang mit Informatik ist die Sensitivität der zu bearbeitenden Daten von Bedeutung. Die Bearbeitung von Strassenunterhaltsdaten qualifiziert eine Aufgabe weniger sensibel als etwa die Bearbeitung von Gesundheitsdaten oder von Verdachtsdaten der Polizei;
- das Risikopotenzial der Tätigkeit: Das Potenzial für Eingriff in Rechte und Freiheiten Privater beispielsweise bei automatisierten Systemen;
- die Bedeutung der Tätigkeit für die (staatliche) Aufgabenerfüllung: Je weniger die Verwaltung auf eine «Hilfstätigkeit» verzichten kann oder je abhängiger eine staatliche Stelle von der Informatik ist, desto qualifizierter ist diese Tätigkeit. Die Herstellung und Ausrüstung oder der Unterhalt eines Polizeifahrzeuges beispielsweise ist – angesichts verschiedener Anbieter – von geringerer Bedeutung als der «Betrieb» des Polizeiautos: Zwar könnte die Polizei von der Fahrtüchtigkeit her wohl ebenso gut (und vielleicht kostengünstiger) einen Fahrer beispielsweise von einem Taxiunternehmen einsetzen, wegen der drohenden Abhängigkeit wird sie das kaum tun. Zahlreiche Amtsstellen können bei ihrer Aufgabenerfüllung auf die Informatik in ihrer Gesamtheit schlicht nicht mehr verzichten;
- die (relative) Austauschbarkeit der Leistungserbringer: Ob das Büromaterial von A oder B gekauft wird, oder ob das Putzinstitut C oder D die Reinigung staatlicher Gebäude besorgt, ist kaum von entscheidender Bedeutung; der Erbringer der «Informatikleistungen» für die gesamte Verwaltung ist demgegenüber weit weniger einfach austauschbar;
- die Nähe zu einer hoheitlichen Tätigkeit: In der Lehre werden gewisse Datenbearbeitungen wegen ihres nahen Bezugs zu

hoheitlichen Aufgaben als Teil der hoheitlichen Tätigkeit betrachtet (etwa bei Polizei- und Sicherheitsbehörden, Steuer- und Finanzverwaltung, mit der Folge, dass selbst statistische Bearbeitungen in diesem Bereich als hoheitliche Tätigkeit gelten).

Es ist deshalb festzustellen, dass die Informatik nicht (mehr) der «einfachen Bedarfsverwaltung» in dem im Zeitalter der mechanischen Schreibmaschine und der manuellen Aktenführung entwickelten Sinne zugerechnet werden kann. Insbesondere steckt im Gesamtsystem Informatik – vor allem und zunehmend bei automatisierten Abläufen – das Potenzial zu Eingriffen in Rechte und Freiheiten Privater ebenso wie die Möglichkeit, Leistungen (unmittelbar) zugunsten Privater zu erbringen. Die Informatik stellt eine Form der «qualifizierten Bedarfsverwaltung» dar, und es kann deshalb bei einer umfassenden Auslagerung von Informatikleistungen nicht mehr generell vom Erfordernis einer gesetzlichen Grundlage abgesehen werden.
In Bezug auf das Datenschutzregime war festzuhalten, dass das kantonale Datenschutzgesetz nur auf öffentliche Organe anwendbar ist, wobei als öffentliche Organe Behörden oder Amtsstellen des Kantons und der Gemeinden, andere öffentliche Einrichtungen sowie Personen, die mit öffentlichen Aufgaben betraut sind, zählen (§ 2 lit. c DSG). Für ein privatrechtliches Unternehmen stellt sich deshalb die Frage, ob es mit öffentlichen Aufgaben betraut ist. Eine wirtschaftliche Betrachtung («öffentlich kontrolliert») ist beim DSG nicht massgebend. Auf ein privatrechtliches Unternehmen sind das eidgenössische DSG und dessen Bestimmungen für das Bearbeiten von Personendaten durch private Personen anwendbar.

Bei dieser Rechtslage wird offensichtlich, dass ein Outsourcing von Informatikleistungen je nach deren Umfang die Grundrechte der betroffenen Personen stark beeinträchtigt. Insbesondere werden die datenschutzrechtlichen Aufsichtsrechte eingeschränkt, und damit wird die Rechtsstellung der betroffenen Bürgerinnen und Bürger tangiert.

Die Rahmenbedingungen dieser Auslagerungen sind so zu formulieren, dass für die verantwortlichen Organe die Konsequenzen absehbar sind. Damit unterscheidet sich die Auslagerung von Informatikumgebungen auch von der einfachen Auftragsdatenbearbeitung gemäss § 13 DSG, die auf vertraglicher Ebene abgewickelt wird.
Aus datenschutzrechtlicher Sicht war es deshalb zu begrüssen, dass die verantwortlichen Stellen nicht den gutachterlichen Schlussfolgerungen gefolgt sind und sich entschieden haben, ein Gesetz über die Auslagerung von Informatikleistungen zu schaffen. Damit war die Gelegenheit offen, die materiellen Fragen in einem Gesetz zu regeln, das sowohl die Auslagerung von Informatikdienstleistungen als auch die Beteiligung an Informatikunternehmen umfassen sollte. Wir legten vor allem Wert darauf, dass insbesondere die folgenden Punkte in diesem Gesetz Berücksichtigung finden:
Die Abgrenzung der Datenbearbeitung im Auftrag (§ 13 DSG) von der Auslagerung von Informatikleistungen («Outsourcing gesamter Informatikumgebungen») sollte durch eine klare Definition der Auslagerung im Gesetz geregelt sein. Elemente einer solchen Definition sind die Tatsache der gesamthaften Auslagerung (Informatikumgebung), das Fehlen einer unmittelbaren Herrschaft über die Datenbearbeitung und die Auslagerung des «Betriebs» als Dauerprozess.
Ferner sollten materielle Kriterien für die Zulässigkeit der Auslagerung gefunden werden. Auszugehen ist dabei von der Sensibilität der zu bearbeitenden Daten, dem Risikopotenzial der Tätigkeit, der Bedeutung für die staatliche Aufgabenerfüllung, der Nähe zur hoheitlichen Tätigkeit oder der Abhängigkeit vom Leistungserbringer.
Der Regierungsrat hat eine Vorlage an das Parlament verabschiedet, die diese Anliegen teilweise aufnahm.

2. Datenbearbeitungen der Jugendsekretariate

Richtlinien für die Praxis

Bei den von den Jugendsekretariaten bearbeiteten Daten handelt es sich fast ausnahmslos um besonders schützenswerte Daten gemäss § 2 lit. d DSG. Sie dürfen nur unter den Voraussetzungen von § 5 DSG bekannt gegeben werden. Dennoch sind gerade diese Daten häufig Gegenstand von Nachfragen diverser anderer Ämter (vgl. hierzu Tätigkeitsbericht Nr. 2 [1996], S. 26 f.).
Das Amt für Jugend und Berufsberatung hat ein Projekt «Richtlinien und Leitfaden zur Datenbekanntgabe, Akteneinsicht und Aktenedition für die Bezirksjugendsekretariate» erarbeiten lassen. Das Papier umfasst einen einleitenden Teil mit grundlegenden Ausführungen zur Thematik sowie fünfzehn typische Fallkonstellationen je mit der korrekten Vorgehensweise der involvierten Personen sowie weiterführenden Bemerkungen. Wir haben dieses Projekt eng begleitet.
Wie notwendig ein klärender Leitfaden für die teilweise sehr komplexen Sachverhalte ist, zeigte sich anlässlich eines konkreten Falles: Ein südamerikanisches Gericht wandte sich mit einem Rechtshilfegesuch an ein hiesiges Bezirksgericht mit der Frage, ob die hier lebenden Grosseltern des betroffenen Kindes sinnvollerweise zu Allein- oder zumindest Miterziehenden bestimmt werden könnten. Der vom Bezirksgericht mit den Abklärungen beauftragte Mitarbeiter des zuständigen Jugendsekretariats erinnerte sich, dass der Grossvater bereits wegen sexueller Übergriffe auf seine Tochter und seine Stieftochter verurteilt worden war. (Der Mitarbeiter betreut auch die Kinder der missbrauchten Stieftochter.) Infolge Zeitablaufs ist der entsprechende Eintrag im Strafregister gelöscht. Der Mitarbeiter wandte sich daher mit der Frage an uns, ob das Wissen um die sexuellen Verfehlungen des Grossvaters dem Gericht mitgeteilt werden könne. Die Anfrage des Gerichts ist im Rahmen der Amtshilfe zu beantworten (§ 8 Abs. 1 lit. a DSG). Inhaltlich erscheint sodann ein entsprechender Hinweis bezüglich der früheren sexuellen Verfehlung des Grossvaters geeignet und erforderlich, da diese Tatsache zwar nach Löschung des Strafregistereintrags strafrechtlich nicht mehr relevant ist, für die Einräumung einer Erziehungsberechtigung dagegen noch immer eine Bedeutung haben kann. Es ist indessen offen zu deklarieren, dass die Vorfälle bereits längere Zeit zurückliegen. Ausserdem ist klar zu trennen, was Tatsachen und was blosse – pflichtgemäss vom Gutachter zu ziehende – Schlüsse sind.

3. Qualifikationssystem für Lehrkräfte an der Volksschule

Datenschutzrechtliche Rahmenbedingungen

Der Erziehungsrat erlässt gestützt auf die geltende Lehrerbesoldungsverordnung Richtlinien zur lohnwirksamen Beurteilung von Lehrkräften. Hierzu ist ein entsprechender Fragebogen sowie ein Leitfaden erstellt und anschliessend an diverse interessierte Stellen zur Vernehmlassung gegeben worden. Mehrere betroffene Personen haben uns daraufhin gebeten, die Unterlagen unter datenschutzrechtlichen Gesichtspunkten zu beurteilen, worauf wir eine ausführliche Stellungnahme zuhanden des Erziehungsrates erarbeiteten.
Obwohl Datenbearbeitungen im Rahmen von Mitarbeitendenbeurteilungen sensibel sind, finden die datenschutzrechtlichen Rahmenbedingungen in den Unterlagen nirgends Erwähnung. Ebenso wenig werden die betroffenen Schulpflegen auf den Verhältnismässigkeitsgrundsatz aufmerksam gemacht, wonach Daten nur so weit erfragt werden dürfen, als sie für die Bewertung der Lehrtätigkeit im Sinne von § 4 Abs. 3 DSG relevant sind. Vielmehr wird in teilweise missverständlicher Formulierung nahe gelegt, das Umfeld oder Privatleben einer beurteilten Lehrkraft mit zu erfassen.

Ausserdem fehlen klare Anordnungen, was mit den ausgefüllten Bogen nach erfolgter Auswertung zu geschehen hat.
Besonders heikel ist der in den Unterlagen ausgesprochene Rat, im Einzelfall aussenstehende Personen beizuziehen. Diese Datenbeschaffung ist für die betroffenen Personen nicht transparent; insbesondere fehlen hierfür klare Rechtsgrundlagen. Deshalb können, was aber in den Unterlagen unerwähnt bleibt, in solchen Fällen Informationen nur in anonymisierter Form fliessen.
Sowohl Fragebogen wie Leitfaden sind definitiv eingeführt worden, jedoch ohne unsere Ausführungen zu berücksichtigen. Wir wandten uns deshalb erneut an die Bildungsdirektion und wiesen darauf hin, dass die Lehrerqualifikationen in der Praxis von den zuständigen Schulpflegen und infolgedessen von Laienbehörden vorzunehmen sind, worauf bei der konkreten Ausgestaltung von Anweisungen und Formularen entsprechend Rücksicht zu nehmen sei. Insbesondere sind klare Handlungsanweisungen zu erteilen, welche ohne weiteres umgesetzt werden können.
Ebenso ist ausdrücklich auf die Grenzen der Datenbearbeitungen hinzuweisen.
Wird eine solche erforderliche Klarstellung in den bereitgestellten Unterlagen versäumt, muss die Verantwortung im Hinblick auf eine datenschutzkonforme Durchführung der Lehrerqualifikationen mit anderen Mitteln wahrgenommen werden.
Wir empfahlen deshalb zumindest die Schaffung eines einschlägigen, leicht verständlichen Merkblattes zuhanden der Schulpflegen.
Darin müsste mit entsprechender Deutlichkeit aufgezeigt werden, dass Daten nur dann und nur insoweit erhoben werden dürfen, als sie einen Bezug zur Gestaltung beziehungsweise Qualität des Schulunterrichts haben. Ausserdem müsste klargestellt werden, dass ein Beizug von Dritten nur unter Wahrung des Amtsgeheimnisses zulässig ist. Schliesslich wäre unmissverständlich auszuführen, was mit den diversen Unterlagen nach Durchführung der Qualifikation zu geschehen hat.
In der Zwischenzeit hat die Bildungsdirektion einen Entwurf zu einem solchen Merkblatt erstellt.

4. Daten für die Bildungsstatistik

Bearbeitung innerhalb der gesetzlichen Rahmenbedingungen

Eine betroffene Person hat das von der Bildungsdirektion im Rahmen der kantonalen Mittelschulstatistik herausgegebene Formular mit Fragen insbesondere zu beruflicher Tätigkeit, Stellung und Ausbildung von Vater und Mutter der Schulkinder als zu weit gehend beanstandet. Wir haben Mängel in Bezug auf den Datenschutz festgestellt, weshalb wir an die zuständige Abteilung für Bildungsplanung gelangten. Daraufhin hat sich ergeben, dass die Umfrage in der beanstandeten Form zum letzten Mal durchgeführt worden ist, da eine umfassende Neugestaltung des Erhebungsverfahrens bevorsteht. Der konkrete Fall gab Anstoss zu einer intensiven Zusammenarbeit mit der Bildungsdirektion im Hinblick auf die Neugestaltung der Schulstatistik. Dabei haben wir die datenschutzrechtlichen Anforderungen an schulstatistische Untersuchungen hervorgehoben: Für jede Datenkategorie muss eine entsprechende Rechtsgrundlage vorliegen. Fehlt eine solche, können Erhebungen lediglich auf der Basis von Freiwilligkeit erfolgen. Des Weiteren ist die Zweckgebundenheit der zu statistischen Zwecken erfassten Daten zu garantieren, weshalb eine Verwendung beispielsweise für Unterrichtszwecke und die Einspeisung in die Datenbanken der Schulverwaltung zu verhindern ist. Ausserdem sind gemäss § 12 Abs. 1 lit. a DSG – als Korrelat zur Lockerung gewisser datenschutzrechtlicher Grundsätze bei Datenbearbeitungen zu statistischen Zwecken – die erhobenen Daten so bald als möglich zu anonymisieren.
Im gegenwärtigen Zeitpunkt ist diese Neugestaltung der Schulstatistik noch nicht abgeschlossen.

5. Fragebogen bei Bewerbungen

Beachtung der Verhältnismässigkeit und Transparenz

Das Personalamt der kantonalen Verwaltung führt einen Fragebogen für Stellenbewerberinnen und -bewerber. Auf Grund einer Beanstandung der Fragen zum Gesundheitszustand legte es uns den Fragebogen zu einer umfassenden Überprüfung vor.
Auszugehen ist vom Zweck der Datenbearbeitung: die Abklärung der Eignung einer Person für die ausgeschriebene Stelle. Die Fragen haben sich auf die für diesen Zweck geeigneten und erforderlichen Angaben zu beschränken. Die Angabe der Konfession ist nur bei so genannten Tendenzbetrieben zulässig, die auf einer konfessionellen Anschauung gründen (z.B. Landeskirchen).
Das Verlangen einer kurzen handschriftlichen Bewerbung mutet im Rahmen der fortschreitenden Büroautomation antiquiert an; die Handschrift ist kaum mehr geeignet, die Sorgfalt der Arbeitsweise zu prüfen. Soll aus einer Handschriftenprobe dagegen ein graphologisches Gutachten erstellt werden, muss ausdrücklich darauf hingewiesen werden. Für die Besetzung der Stelle ebenfalls unerheblich sind Angaben zur Kündigungsfrist am bisherigen Arbeitsplatz und zu bisherigen Lohnbezügen. Gefragt werden darf nach dem möglichen Eintrittstermin und nach den Lohnvorstellungen für die zu besetzende Stelle.
In Bezug auf die Frage nach einem allfälligen Wohnsitzwechsel war auf die Praxis des Bundesgerichts zu verweisen, die eine Einschränkung der Niederlassungsfreiheit durch Wohnsitzpflicht nur zulässt, wenn zwingende Gründe des Dienstes oder das Erfordernis besonderer Beziehungen zur Bevölkerung es verlangen; rein fiskalische Motive sind dagegen unzulässig. Besteht eine Wohnsitzpflicht, ist bereits bei der Stellenausschreibung darauf hinzuweisen. Die von der betroffenen Person beanstandeten Fragen zum Gesundheitszustand waren dagegen – abgesehen von der Frage nach Rentenbezügen – nicht zu bemängeln. Bei Datenerhebungen mittels Fragebogen müssen Rechtsgrundlage und Zweck des Bearbeitens bekannt gegeben werden (§ 7 Abs. 2 DSG). Dies kann direkt auf dem Fragebogen oder auf einem Beiblatt (z.B. Merkblatt oder Erläuterungsblatt zum Fragebogen) erfolgen. Das Personalamt passte den Fragebogen entsprechend unseren Hinweisen an.
In einem anderen Fall wandte sich eine betroffene Person an den Datenschutzbeauftragten, weil sie sich bei der Bewerbung für einen Einsatz in einem Beschäftigungsprogramm für arbeitslose Personen in ihren Persönlichkeitsrechten beeinträchtigt fühlte. Wir unterzogen auch diesen Personalbogen einer Prüfung und kamen zum Schluss, dass ein solcher Personalbogen nach den gleichen Grundsätzen zu beurteilen ist wie eine Stellenbewerbung. Es darf daher nur nach Daten gefragt werden, welche zur Abklärung der Eignung der sich bewerbenden Person für die vorgesehene Stelle geeignet und erforderlich sind. Unzulässig sind etwa Fragen nach Hobbys, finanzieller Unterstützung durch Dritte, Rentenbezügen oder detaillierten Angaben zur Gesundheit. Nach dem Führerausweis, einem eigenen Fahrzeug und der Bereitschaft, dieses für berufliche Zwecke einzusetzen darf gefragt werden, wenn dies für das Arbeitsverhältnis erforderlich ist. Die Trägerschaft des Beschäftigungsprogramms passte den Fragebogen nach unseren Vorgaben an. Das Amt für Wirtschaft und Arbeit, das wir mit einer anonymisierten Kopie unserer Stellungnahme und des beanstandeten Fragebogens bedient hatten, informierte von sich aus sämtliche Trägerschaften und forderte sie auf, ihre Unterlagen, falls nötig, ebenfalls anzupassen.
Ein weiterer Fall betraf die Frage nach der Aufbewahrung von Bewerbungsformularen. Anlässlich einer Rechtsauskunft an eine betroffene Person hielten wir fest, dass solche Formulare von abgewiesenen Stellenbewerberinnen und -bewerbern zu vernichten sind, sobald keine Ansprüche aus der Bewerbung (z.B. auf Grund des Bundesgesetzes über die Gleichstellung von Frau und Mann) mehr geltend gemacht werden können. Wurden die Bewerbungsunterlagen bereits vorher zurückgegeben, rechtfertigt sich auch eine weitere Aufbewahrung der Formulare nicht.

6. Strafentscheide an die Gesundheitsdirektion

Mitteilungen in Ausnahmefällen zulässig

Auf Grund einer Anfrage der Verwaltungskommission des Obergerichts beurteilten wir, ob und gegebenenfalls in welchem Umfang die Strafverfolgungsbehörden Delikte betreffend das Medizinalwesen beziehungsweise von Medizinalpersonen an die Gesundheitsdirektion weitermelden dürfen.
Mitteilungen von Strafentscheiden betreffen gemäss § 2 lit. d Ziff. 4 DSG besonders schützenswerte Personendaten, weshalb die Gesundheitsdirektion nur bei Vorliegen klarer Rechtsgrundlagen darüber informiert werden kann. Eine Aufsichtsfunktion (vgl. Tätigkeitsbericht Nr. 3 [1997], S. 11 f.) beziehungsweise die Zuständigkeit zum Vollzug des Gesundheitsgesetzes reichen deshalb für sich allein für eine Datenbekanntgabe nicht aus.
Gemäss Gesundheitsgesetz (§§ 7 ff.) ist die Gesundheitsdirektion zuständig für Bewilligungen zur Ausübung gewisser Berufe im Gesundheitswesen. Sie ist dabei ausdrücklich ermächtigt, die Bewilligung bei Vorliegen gewisser Umstände zu entziehen. Infolgedessen sind ihr alle diejenigen Delikte zu melden, welche auf Grund ihrer Art und Schwere einen Entzug einer solchen Bewilligung zur Folge haben könnten.
Des Weiteren ist die Gesundheitsdirektion ermächtigt, die den Medizinalpersonen gemäss Art. 9 des Betäubungsmittelgesetzes zustehende Befugnis zum Bezug, zur Lagerung, Verwendung oder Abgabe von Betäubungsmitteln bei Betäubungsmittelabhängigkeit oder gewissen Widerhandlungen gegen das genannte Gesetz zu entziehen. Ihr sind infolgedessen alle diejenigen Fälle zu melden, welche zu einem Entzug dieser Befugnis führen könnten.
Weitere Meldepflichten resultieren aus §§ 8 a und 9 der Verordnung über den Verkehr mit Heilmitteln, welche unter gewissen Voraussetzungen zur Abgabe von Betäubungsmitteln an betäubungsmittelabhängige Personen ermächtigen. So sind einerseits die in einem Behandlungsprogramm stehenden Personen der Gesundheitsdirektion zu melden. Eine Meldepflicht resultiert andererseits aus dem Umstand, dass die Gesundheitsdirektion sowohl Ärztinnen und Ärzte wie Patientinnen und Patienten, welche wiederholt und schwer gegen die Richtlinien verstossen haben, von der weiteren Behandlung mit Betäubungsmitteln ausschliessen kann. Damit wird zwangsläufig vorausgesetzt, dass die Strafverfolgungsbehörden die Gesundheitsdirektion über einschlägige Sachverhalte informieren.
Weitere Melderechte sind nicht ersichtlich. Insbesondere ergibt sich aus Art. 15 des Betäubungsmittelgesetzes, wonach Fälle von Betäubungsmittelmissbrauch der für die Betreuung zuständigen Behörde beziehungsweise einer anderen Behandlungs- oder Fürsorgestelle gemeldet werden können, keine dem Präzisierungsgrad von § 5 DSG entsprechende Rechtsgrundlage für eine Mitteilung an die Gesundheitsdirektion.

7. Bekanntgabe von Daten ausländischer Personen

Leitfaden der Fremdenpolizei

Die Fremdenpolizei bearbeitet beim Vollzug des Ausländer- und Asylrechts Daten über ausländische Personen. Sie ist häufig Anlaufstelle von Gesuchen Dritter um die Bekanntgabe von Daten über ausländische Personen. Wir begrüssten die Absicht der Fremdenpolizei, zur einheitlichen Umsetzung des DSG interne Richtlinien über die Datenbearbeitung zu erarbeiten.
Die verschiedenen Behörden, welche Aufgaben im Ausländer- und Asylwesen erfüllen, sind grundsätzlich zur Zusammenarbeit berechtigt. Personendaten dürfen in dem Mass ausgetauscht werden, als es für die empfangende Stelle zur Erfüllung ihrer ausländer- und asylrechtlichen Aufgaben geeignet und erforderlich ist (Grundsatz der Verhältnismässigkeit; § 4 Abs. 3 DSG). Ein solcher Datenaustausch

erfolgt z.B. mit den Arbeitsmarktbehörden (Ausländerbeschäftigung) oder mit den Einwohnerkontrollen (Meldewesen).
In Bezug auf den Datenaustausch mit Polizeibehörden sind Differenzierungen erforderlich. Bei Vorgängen im Zusammenhang mit dem Vollzug des Ausländer- und Asylrechts ist die Bekanntgabe zulässig, soweit die Polizei in Erfüllung fremdenpolizeilicher Aufgaben handelt (z.B. Festnahme und Überstellung in Ausschaffungshaft, Vollzug der Ausschaffung, Ausweisung oder Wegweisung). Im Rahmen von polizeilichen Ermittlungen sind Daten nach dem Verhältnismässigkeitsprinzip unter den Voraussetzungen der Amtshilfe weiterzugeben. Diese Grundsätze gelten auch für die Bekanntgabe an die Strafuntersuchungsorgane (Bezirksanwaltschaften, Jugendanwaltschaften).
Die Mehrzahl der ausländischen Personen ist sozialversicherungspflichtig (Krankenversicherung, Alters- und Hinterlassenenvorsorge usw.). Den einzelnen Trägern der Sozialversicherung sind auf Anfrage Auskünfte zu erteilen, welche für die Festsetzung, Änderung oder Rückforderung von Leistungen, die Verhinderung ungerechtfertigter Bezüge oder den Rückgriff auf haftpflichtige Dritte notwendig sind. Dabei sind allenfalls auch Daten einer Person bekannt zu geben, welche eine so genannte Garantieerklärung – eine Art Bürgschaft für Forderungen gegenüber der ausländischen Person – abgegeben hat.
Eine Pflicht zur Leistung von Amtshilfe im Einzelfall besteht auch gegenüber den Steuerbehörden, etwa im Bereich der Quellenbesteuerung ausländischer Personen.
Bei Anfragen aus dem Ausland (Botschaften und Konsulate, ausländische Gerichts- und Verwaltungsbehörden usw.) handelt es sich um eine Datenbekanntgabe ins Ausland, welche im Bundesrecht eine besondere Regelung erfahren hat (Art. 6 Bundesgesetz über den Datenschutz). Im Kanton Zürich fehlt eine solche Bestimmung. Die Interessenabwägung, die das verantwortliche Organ vornehmen muss (§ 10 DSG), führt allenfalls zu Einschränkungen. Eine Datenbekanntgabe ins Ausland ist im Ausländer- und noch verstärkt im Asylbereich besonders sensibel.
Wir empfahlen der Fremdenpolizei deshalb, solche Anfragen generell an die zuständigen Bundesbehörden zu verweisen, denen zusätzliche Beurteilungsgrundlagen zur Verfügung stehen.
Mangels Rechtsgrundlagen ist für Auskünfte an Private eine Einwilligung der betroffenen Person erforderlich. Allenfalls kann diese nach den Umständen vorausgesetzt werden, z.B. wenn eine angehörige Person mit dem Ausweis der betroffenen Person am Schalter der Fremdenpolizei vorspricht und in deren Namen eine Verlängerung der Aufenthaltsbewilligung beantragt oder wenn sich der (potenzielle) Arbeitgeber nach dem Stand des Verfahrens erkundigt und präzise Angaben zum Sachverhalt machen kann.

8. Schutz der sensiblen Daten im Fürsorgebereich

Zusammenlegung der Fürsorgedirektion mit der Polizeidirektion

Die Zusammenlegung der Fürsorgedirektion mit der Polizeidirektion (und der Militärdirektion) zur Direktion für Soziales und Sicherheit hat bei betroffenen Personen zu Befürchtungen Anlass gegeben, Fürsorgedaten könnten nun in «falsche Hände» geraten.
Wir haben bei verschiedenen Gelegenheiten auf die Sensibilität dieser organisatorischen Änderungen hingewiesen, die nur unter strenger Beachtung der datenschutzrechtlichen Grundsätze und mit entsprechenden organisatorischen und technischen Massnahmen ohne Risiken für die Grundrechte der betroffenen Personen umgesetzt werden können.
Personendaten, die im Polizei- und Sozialbereich bearbeitet werden, sind sensibel und werden vom DSG als besonders schützenswert bezeichnet (§ 2 lit. d DSG). Die Voraussetzung für deren Bearbeitung ist deshalb eine klare gesetzliche Grundlage (§ 5 DSG).
Im vorliegenden Zusammenhang speziell zu beachten ist das Prinzip der Zweckbindung (§ 4 Abs. 4

DSG): Daten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich ist oder gesetzlich vorgesehen wird. Damit sind grundsätzlich Polizei- und Sozialdaten auseinander zu halten. Hinzu kommt das Amtsgeheimnis, das auch zwischen den verschiedenen Verwaltungsabteilungen zu beachten ist. Allerdings gilt es gegenüber der vorgesetzten Behörde grundsätzlich nicht, die somit Informationen von beiden Bereichen erhält. Sie hat sich jedoch an das Zweckbindungsgebot zu halten. Der Fürsorgebereich ist nicht wie beispielsweise der Sozialversicherungsbereich durch ein Spezialgeheimnis geschützt. Im Rahmen der Amtshilfepflicht haben deshalb Fürsorgebehörden den Polizeistellen bei Vorliegen der erforderlichen Voraussetzungen im Einzelfall Auskunft zu erteilen.

Durch die organisatorische Zusammenlegung von sensiblen Datenbearbeitungen aus unterschiedlichen Bereichen wird das Risikopotenzial für Datenschutzverletzungen erhöht. Dieses ist daher mit angemessenen Massnahmen gegen das unbefugte Bearbeiten aufzufangen. Die unabhängige Aufsicht und Kontrolle ist entsprechend zu verstärken.

9. Verdeckte Ermittlung

Schranken der Überwachungsmassnahmen

Die staatliche Überwachung und insbesondere die verdeckte Ermittlung soll neu in der Strafprozessordnung ausdrücklich geregelt werden. Im Hinblick auf die Bedeutung der Vorlage haben wir eine ausführliche Stellungnahme zu den im Entwurf vorliegenden Bestimmungen abgegeben.
Dem polizeilichen Ermittlungsverfahren kommt eine selbständige Bedeutung zu, weshalb es nicht als Teil des hängigen Strafverfahrens betrachtet werden kann und deshalb in den Geltungsbereich des Datenschutzgesetzes fällt (§ 3 Abs. 2 lit. b e contrario). Auch das anschliessende Strafverfahren kann nicht losgelöst von der Datenschutzgesetzgebung betrachtet werden, da die Datenschutzbestimmungen weitgehend eine Konkretisierung der verfassungsmässigen Rechte in diesem Bereich darstellen.

In allen Verfahrensstadien fallen Daten hinsichtlich strafrechtlicher Verfolgungen und Sanktionen an, die besonders schützenswert sind (§ 2 lit. d Ziff. 4 DSG). Überwachungsmassnahmen durch staatliche Organe stellen einen schweren Eingriff in die Privatsphäre der betroffenen Personen dar, weshalb sie einer klaren respektive formellgesetzlichen Rechtsgrundlage bedürfen. Insbesondere müssen die Voraussetzungen sowie die Art und Weise der Datenbearbeitung im Rahmen der Zweckbestimmung klar umschrieben werden. Die vorgeschlagenen Bestimmungen der StPO entsprechen diesen Anforderungen jedoch nicht: Während die bisherige gesetzliche Regelung sowohl in Bezug auf die zu überwachenden Personen und die einzusetzenden Überwachungsmittel als auch in Bezug auf die Eingriffsbereiche klare Abgrenzungen enthält, lässt die neu vorgeschlagene Formulierung vieles offen. Beispielsweise könnte neuerdings eine Vielzahl von Personen von Überwachungsmassnahmen betroffen sein (z.B. bei einer Internet-Überwachung), ebenso wie Personen mit einem Zeugnisverweigerungsrecht gemäss § 130 StPO. Auch die neu in die StPO aufzunehmende Verwertbarkeit von Zufallsfunden (welche Frage bis anhin offen geblieben war) erscheint rechtsstaatlich fragwürdig, da mit dem unbeschränkten Einsatz von Überwachungsmitteln in allen gesetzlich geschützten Geheim- und Privatbereichen sowie der Ausdehnung der Verwertung auf Dritte kaum mehr von «Zufallsfunden» gesprochen werden kann.
Der Einsatz verdeckter Ermittler und Ermittlerinnen beinhaltet einen schwereren Eingriff in die persönliche Freiheit als die Telefonüberwachung, weshalb er mindestens auf deren Mindeststandard abgestützt werden muss.

Die vorgeschlagenen ergänzenden Bestimmungen der StPO sind jedoch nicht in der erforderlichen Klarheit abgefasst, so dass sie einen solch schweren Eingriff in die persönliche Freiheit nicht zu rechtfertigen vermögen. Festzuhalten gewesen wäre sowohl der Deliktskatalog wie das Vorhandensein eines dringenden Tatverdachts und auch die Genehmigung und Terminierung des Einsatzes. Geregelt werden müsste ebenso, was mit den nicht zu den Untersuchungsakten genommenen Aufzeichnungen zu geschehen hat. Die überarbeitete Fassung der einschlägigen Bestimmungen der StPO liegt zwischenzeitlich in einem Antrag an den Gesetzgeber vor. Darin sind jedoch weder im erforderlichen Detaillierungsgrad die Zielpersonen noch die Überwachungsmittel oder der Eingriffsbereich von Massnahmen gegen den gesetzlich geschützten Geheim- und Privatbereich festgehalten worden. Ebenso fehlt im Hinblick auf die Verwertung von Zufallsfunden nach wie vor ein Deliktskatalog. Dieselbe Feststellung gilt in Bezug auf die verdeckte Ermittlung, da offen bleibt, in welchen Fällen beziehungsweise über welchen Zeitraum eine solche zulässigerweise durchgeführt werden darf.

10. Aufbewahrung von erkennungsdienstlichem Material

Vernichtung bei erwiesener Nichttäterschaft

Eine zu Unrecht eines bestimmten Delikts verdächtigte und erkennungsdienstlich behandelte Person ersuchte sowohl die Kantonspolizei wie die zuständige Bezirksanwaltschaft um Vernichtung der angefallenen Unterlagen. Während die Erstere dem Begehren ohne weiteres stattgab und auch beim Bundesamt für Polizeiwesen diesbezüglich vorstellig zu werden versprach, weigerte sich Letztere unter Hinweis auf eine allgemein einzuhaltende zwanzigjährige Archivierungsfrist. Die betroffene Person wandte sich daraufhin an die Justizdirektion, welche uns um einen Mitbericht ersuchte.

Wie sich aus § 3 Abs. 2 lit. b DSG e contrario ergibt, kommt das Datenschutzgesetz nach Abschluss eines hängigen Verfahrens der Strafrechtspflege zur Anwendung. Entsprechend dürfen Daten ab diesem Zeitpunkt nur unter Beachtung der Grundsätze des DSG aufbewahrt werden.
Das Archivrecht kommt so lange nicht zur Anwendung, als das Daten bearbeitende Organ ungehindert Zugriff auf das entsprechende Material hat. Archivrechtliche Fragen stellen sich ausserdem erst in Bezug auf solche Akten, welche grundsätzlich aufbewahrt werden dürfen.
Für die Aufbewahrung von Untersuchungsakten bestehen keine klaren gesetzlichen Grundlagen im Sinne von § 5 DSG. Entsprechend dürfen sie nur aufbewahrt werden, soweit dies zur Erfüllung einer gesetzlich klar umschriebenen Aufgabe unentbehrlich ist. Dabei kann die «Verordnung des Obergerichts über die Archive der Gerichte, der Friedensrichter-, Gemeindeammann-, Stadtammann- und der Betreibungsämter» als Auslegungshilfe bezüglich der bestehenden gesetzlichen Aufgaben dienen. Dies gilt jedoch nur so lange, als nicht anders lautende Rechtsvorschriften bestehen.

Der § 8 der Verordnung über die erkennungsdienstliche Behandlung von Personen hält fest, dass zu Unrecht erhobenes erkennungsdienstliches Material zu vernichten ist sowie Registraturhinweise zu entfernen sind (vgl. Tätigkeitsbericht Nr. 2 [1996], S. 11); der Sachverhalt darf auch nicht auf Umwegen erschliessbar bleiben. Entsprechend hat die Kantonspolizei korrekterweise nicht nur die eigenen Daten zum Vorfall vernichtet, sondern auch beim Bund für eine Löschung gesorgt. Würde nun aber die zuständige Bezirksanwaltschaft, welche den Fall formell durch Einstellung des Verfahrens zum Abschluss bringt, ihre Daten weiterhin aufbewahren, wäre der Schutz der zu Unrecht erkennungsdienstlich behandelten Personen nicht gewährleistet.
Auch eine Abwägung der beteiligten Interessen ergibt nichts

Gegenteiliges: Zwar müssen die Bezirksanwaltschaften die Rechtmässigkeit ihres Handelns belegen, doch darf dies nicht zu Lasten der zu Unrecht in ein Verfahren verwickelten Personen geschehen. Ausserdem hat eine Kontrolle der Rechtmässigkeit des bezirksanwaltschaftlichen Handelns möglichst frühzeitig anzusetzen, weshalb kein Grund für eine prinzipielle Aufbewahrungsfrist von zwanzig Jahren ersichtlich ist.

In der Folge hat die Justizdirektion der betroffenen Person mitgeteilt, dass sie veranlassen werde, dass die angefallenen Akten (mit Ausnahme der Spruchbuchausfertigung des Entscheids und der notwendigen Geschäftskontrolldaten) nach erfolgter Prüfung des Rechenschaftsberichts der zuständigen Bezirksanwaltschaft vernichtet beziehungsweise gelöscht werden. Diese Praxis wird zu überprüfen sein, sobald die Verordnung über den Erkennungsdienst der fälligen Revision unterzogen worden ist.

11. Verdacht auf Kindsmisshandlung

Mitteilungsrechte der Polizei

Die Polizei hat die zuständige Vormundschaftsbehörde von Amtes wegen über vormundschaftsrechtlich relevante Sachverhalte zu informieren. An dieser liegt es sodann abzuklären, ob und gegebenenfalls mit welchen Massnahmen einzuschreiten ist.
In der Praxis wird jedoch teilweise nur zögernd interveniert. Der Bezirksrat als Aufsichtsbehörde erster Instanz über die Vormundschaftsbehörden wird dagegen über mögliche Kindesschutzfälle nur dann in Kenntnis gesetzt, wenn vormundschaftliche Massnahmen getroffen wurden, nicht aber bei Untätigbleiben der Vormundschaftsbehörde.
Aufgeworfen wurde deshalb die Frage, ob nicht auch der Bezirksrat neben den zuständigen Vormundschaftsbehörden mit Mitteilungen der Polizei über mögliche Kindesschutzfälle bedient werden könnte.

Für eine regelmässige Weitergabe dieser – besonders schützenswerten – Daten ist eine klare gesetzliche Grundlage erforderlich (§ 8 Abs. 1 in Verbindung mit § 5 lit. a DSG). Im Einzelfall ist die Bekanntgabe möglich, wenn die Daten für die Erfüllung einer gesetzlich klar umschriebenen Aufgabe des Empfängers unentbehrlich sind (§ 8 Abs. 1 lit. a in Verb. mit § 5 lit. b DSG) oder wenn eine klare Einwilligung der betroffenen Person vorliegt (§ 8 Abs. 1 lit. b in Verb. mit § 5 lit. c DSG).
Der § 60 EG zum ZGB verpflichtet die Polizeiorgane, allfällige Gefährdungen des Kindeswohls an die jeweilige Vormundschaftsbehörde weiterzumelden (vgl. hierzu Tätigkeitsbericht Nr. 3 [1997], S. 29). Diese muss den Bezirksrat von den angeordneten Massnahmen in Kenntnis setzen beziehungsweise gegebenenfalls bei ihm den Entzug der elterlichen Gewalt beantragen. Erachtet sie dagegen eine Massnahme als unnötig, hat sie dem Bezirksrat den Vorfall nicht zu melden. Dies stellt jedoch keine gesetzliche Grundlage in dem von § 5 DSG geforderten Präzisierungsgrad für einen direkten Datentransfer von der Polizei an den Bezirksrat dar.
Der Bezirksrat seinerseits hat auf Grund seiner Aufsichtsfunktion eine gewisse Kontrolle über die ihm unterstellten Vormundschaftsbehörden. Jedoch ergibt sich auch daraus keine Rechtsgrundlage für die geplante Meldepraxis.

Unsere Schlussfolgerungen legten wir der Verwaltungskommission des Obergerichts als der in zweiter Instanz zuständigen Aufsichtsbehörde im Vormundschaftswesen zu einer Stellungnahme vor. Sie erachtete § 60 EG zum ZGB als ausreichende Norm für eine Datenweitergabe von der Polizei an den Bezirksrat. Auf Grund der obigen Ausführungen konnten wir diese Auffassung nicht teilen. Entsprechend haben wir die Polizei darauf hingewiesen, dass Kindsschutzfälle nur durch die Vormundschaftsbehörde und nur für einen von vornherein begrenzten Zeitraum an den Bezirksrat weitergemeldet werden können. Dabei handelt

es sich um eine aufsichtsrechtliche Massnahme, welche für die Polizei keine Auswirkungen hat.

Für den in Frage stehenden Informationsfluss müsste dagegen eine Gesetzesänderung vorgenommen werden, was im Zusammenhang mit laufenden Gesetzesrevisionen in Angriff genommen worden ist.

12. Verfahrenskontrolle bei der Fremdenpolizei

Begutachtung aus datenschutzrechtlicher Sicht

Die Fremdenpolizei führt eine eigene Geschäftskontrolle, die sie uns für eine datenschutzrechtliche Begutachtung vorführte. Das System machte insgesamt einen guten Eindruck, weshalb wir uns auf die Abklärung einiger offener Punkte insbesondere in Bezug auf die Datenübernahme aus dem ZAR/AUPER-System des Bundes und der Erweiterung der Zugriffsberechtigungen beschränken konnten.

In der Geschäftskontrolle werden bei der Eröffnung eines neuen Geschäftes die Angaben wie Name, Vorname, Geburtsdatum und Staatsangehörigkeit automatisch aus dem System ZAR (Zentrales Ausländerregister) oder AUPER (Automatische Personenregistratur) des Bundes übernommen. Mit dem ZAR- resp. AUPER-System besteht eine direkte Zugriffsmöglichkeit und die Daten werden aus der Bildschirmmaske kopiert. Die Suche nach den Datenkategorien erfolgt über eine Bearbeitungsnummer. Dieser Sachverhalt war unter zwei Aspekten zu betrachten: Erstens stellte sich die Frage, wieweit die Fremdenpolizei im Bereich des Vollzugs des Ausländer- und des Asylwesens zur Führung einer eigenen Geschäftskontrolle berechtigt ist, und zweitens, ob in diesem Fall Daten aus den erwähnten Systemen übernommen werden dürfen.
Es ist davon auszugehen, dass die bundesrechtlichen Bestimmungen die Führung einer eigenen Geschäftskontrolle der kantonalen Fremdenpolizei nicht vorsehen. Der eidgenössische Datenschutzbeauftragte hat in einer Stellungnahme vom 14. Dezember 1994 klar abgegrenzt, inwieweit die kantonale Fremdenpolizei Zugriff auf das zentrale Ausländerregister (ZAR) erhält (VPB 60 [1996], Nr. 10). Vorab aus der gestützt auf Art. 7 Abs. 4 ZAR-Verordnung erlassenen Weisung leitet der eidgenössische Datenschutzbeauftragte ab, dass die Daten das ZAR grundsätzlich nicht verlassen sollen und nicht in grösserem Umfang in andere EDV-Systeme übernommen werden dürfen. Vielmehr werden die Daten des ZAR der kantonalen Fremdenpolizei für die Geschäftskontrolle zugänglich gemacht. Dass der ZAR-Verordnung dieser Grundsatz zu Grunde liegt, geht auch aus Art. 19 ZAR-Verordnung hervor. Dort wird lediglich die Archivierung und Löschung der Daten im ZAR geregelt, während kantonale Datenbearbeitungen unerwähnt bleiben.

Allerdings wird auf Grund der bundesrechtlichen Bestimmungen auch nicht ausgeschlossen, dass eine kantonale Fremdenpolizei eine eigene Geschäftskontrolle führen darf. Die Bekanntgabe der Daten erfolgt für die Erfüllung der Aufgaben nach dem ANAG, und es wird nicht differenziert, was weiter mit den abgerufenen Daten geschehen soll.
Das Führen einer eigenen Geschäftskontrolle erfordert somit eine genügende Rechtsgrundlage auf kantonaler Ebene. Wir gehen grundsätzlich davon aus, dass die Organisation einer Amtsstelle auch das Führen einer eigenen Geschäftskontrolle beinhaltet. Allerdings ist die Datenbearbeitung auf die für die Erfüllung der Aufgaben notwendigen und geeigneten Daten zu beschränken. Sofern indessen besonders schützenswerte Personendaten bearbeitet werden, ist eine genügende gesetzliche Grundlage gemäss § 5 lit. a DSG zu schaffen. Es kann deshalb davon ausgegangen werden, dass Daten aus dem ZAR- oder dem AUPER-System für eine eigene Geschäftskontrolle verwendet werden dürfen. Diese Daten stehen zur Erfüllung der Aufgaben nach dem Ausländer- beziehungsweise Asylrecht zur Verfügung. Die bundesrechtlichen Bestimmungen schränken insoweit die Organisationsautonomie der kantonalen Fremdenpolizei nicht ein.

Der Fremdenpolizei lagen Anträge der Kantonspolizei und der Stadtpolizei Zürich vor, welche eine direkte Zugriffsmöglichkeit auf die Verfahrenskontrolle wünschen. Dabei handelt es sich um andere Stellen als diejenigen, die schon bisher auf Grund ihrer Aufgaben beim Vollzug des Ausländerrechts diesen Zugriff haben. Auf Grund der verfassungsrechtlichen Anforderungen an die Bestimmtheit einer Rechtsgrundlage muss die Möglichkeit des Abrufverfahrens, welches eine besondere Gefahr der Persönlichkeitsverletzung aufweist, in einem Gesetz im materiellen Sinne ausdrücklich vorgesehen sein. Bei besonders schützenswerten Daten ist ein Gesetz im formellen Sinne notwendig. Dabei sind mindestens die Tatsache des Abrufverfahrens, die berechtigten Behörden und der Umfang der abrufbaren Daten festzuhalten. Des Weiteren ist festzuhalten, dass auch aus einer bestimmten Zweckverwendung von Daten nicht ohne weiteres darauf geschlossen werden darf, dass diese von einer anderen Verwaltungsbehörde bezogen respektive bekannt gegeben werden dürfen.
Wir sahen keine Rechtsgrundlage, welche diese Zugriffsmöglichkeiten im Abrufverfahren gestatten würde. Entweder wäre diesbezüglich eine entsprechende Rechtsgrundlage zu schaffen, oder es ist auf die Möglichkeit des Abrufverfahrens zu verzichten.

13. Neue Archivgesetzgebung

Spezialgesetzliche Datenschutzbestimmungen

Auf den 1. Januar 1999 sind das neue Archivgesetz vom 24. September 1995 und die Archivverordnung vom 9. Dezember 1998 in Kraft gesetzt worden. Damit wird das Datenschutzgesetz mit spezialgesetzlichen Bestimmungen für das Aufbewahren von Daten, die für die Erfüllung der ursprünglichen Verwaltungsaufgaben nicht mehr notwendig sind, ergänzt.
Wir haben im vergangenen Jahr insbesondere zur Archivverordnung Stellung bezogen. Mit der Archivierung geht eine Zweckänderung in der ursprünglichen Datenbearbeitung einher. Die Akten und Daten werden im Archiv aufbewahrt zur Bewahrung, Erschliessung und Vermittlung einer dauerhaften dokumentarischen Überlieferung, die rechtlichen, administrativen, kulturellen und wissenschaftlichen Zwecken dient (§ 4 Archivgesetz). Die Akten unterliegen im Staatsarchiv einer Schutzfrist, die generell 30 Jahre von ihrer Anlage an beträgt (§ 10 Archivgesetz). Personendaten unterliegen einer Schutzfrist von 30 Jahren seit dem Tod der betroffenen Person oder, falls der Tod ungewiss ist, 100 Jahren seit deren Geburt (§ 10 Archivgesetz). Sind weder Todes- noch Geburtsdatum einer Person feststellbar, endet die Schutzfrist 80 Jahre nach der Anlage der Akten (§ 4 Abs. 2 Archivverordnung). Das Staatsarchiv hat neu zu beurteilen, ob vor Ablauf dieser Schutzfristen im Einzelfall Einsicht in bestimmte Akten oder Daten gewährt werden kann (§ 10 Abs. 4 Archivverordnung). Die Archivverordnung weist hierzu auf mögliche überwiegende Interessen für eine Durchbrechung der Schutzfristen hin (§ 10 Abs. 3 lit. a und b Archivverordnung). Mit dieser Regelung wird die Archivverordnung den Anliegen des Datenschutzes gerecht, die eine klare Zweckbestimmung aller Datenbearbeitungen vorsehen. Allgemein sind Daten nur so lange zu bearbeiten, wie sie für die Erfüllung der Verwaltungsaufgaben geeignet und erforderlich sind (Prinzip der Verhältnismässigkeit; § 4 Abs. 3 DSG). Deshalb sind sie nach Ablauf einer bestimmten Zeit zu archivieren oder zu vernichten (§ 14 DSG). Die öffentlichen Organe haben neu eine Anbietungspflicht gegenüber dem Staatsarchiv (§ 8 Archivgesetz). Der Datenschutzbeauftragte ist auch Mitglied der Archivkommission. Diese wird zunächst die Aufgabe haben, klare Rahmenbestimmungen für die Ablieferung von Akten beim Staatsarchiv zu erarbeiten. Hierzu wird sie geeignete Richtlinien und Weisungen für die öffentlichen Organe erarbeiten.

Sensible DNA-Analysen und ihre Verwendung

Die Möglichkeit der «Entschlüsselung des Menschen» schreitet auf Grund der technischen Entwicklungen rasant voran. DNA-Analysen im Bereich der Strafverfolgung sind ein Teilaspekt davon.

Auf Grund einer Anfrage im Kantonsrat hatten wir Gelegenheit, in einem Mitbericht zu Fragen von DNA-Untersuchungen Stellung zu nehmen. Ausserdem beschäftigte sich die 5. Schweizerische Konferenz der Datenschutzbeauftragten, die am 13. Oktober 1998 in Fribourg stattfand, mit den rechtlichen Rahmenbedingungen für die Errichtung von DNA-Datenbanken. Diese Konferenz verabschiedete auch eine diesbezügliche Resolution (siehe Kasten).

Rechtliche Grundlagen

Eine DNA-Analyse ist grundsätzlich wie jede andere Art der Bearbeitung von Personendaten im Rahmen von § 4 DSG erlaubt. Da es sich bei den anlässlich einer Deliktsbegehung gewonnenen Informationen zudem um besonders schützenswerte Daten i.S. von § 2 lit. d Ziff. 4 DSG handelt, sind bei deren Bearbeitung die qualifizierten Anforderungen von § 5 DSG zu beachten. Insbesondere braucht es eine klare gesetzliche Grundlage, damit die Abnahme von Proben sowie deren Auswertung statthaft ist. Eine solche findet sich in § 156 Strafprozessordnung (StPO). Diese Bestimmung gelangt vor allem zur Anwendung, wenn eine Blutentnahme durch eine Medizinalperson erforderlich ist. Im Normalfall genügt heute jedoch eine Speichelprobe, welche ohne Beizug einer ärztlichen Fachperson ohne weiteres durch die Polizei abgenommen werden kann. Sie kann infolgedessen in den in § 3 der Verordnung über den Erkennungsdienst umschriebenen Fällen zur Anwendung kommen. Voraussetzung hierfür sind demnach entweder ein Tatverdacht oder die Einwilligung der zu untersuchenden Person (wobei es nicht genügt, wenn lediglich gegen die geplante Massnahme nicht opponiert wird; vielmehr ist eine ausdrückliche Einwilligung verlangt).

Tatverdacht massgebend

DNA-Analysen dürfen ausschliesslich im Hinblick auf die Ermittlung einer konkreten Täterschaft und damit zum Zwecke der Identifikation von Spuren erstellt werden. Dagegen wäre es unzulässig, wenn die nicht codierenden Teile der DNA nach weiteren Hinweisen auf die Persönlichkeit einer überprüften Person hin untersucht würden und beispielsweise nach Informationen zum genetischen Potenzial, zur Veranlagung respektive zum Gesundheitszustand geforscht würde. Von ausschlaggebender Bedeutung ist ausserdem § 14 DSG, wonach Daten von Personen, welche sich anhand des Genmusters eindeutig als Nichttäter erwiesen haben, von Amtes wegen vernichtet werden müssen.

Massenuntersuchungen

Eine DNA-Analyse kommt in Betracht, wenn entweder ein Tatverdacht auf eine zu untersuchende Person fällt oder eine Einwilligung der betroffenen Person vorliegt. Da aber bei einer Eingrenzung der Täterschaft auf eine bestimmte Region oder Ortschaft noch nicht ein eigentlicher Tatverdacht in der erforderlichen Deutlichkeit vorliegt, ist eine zwangsweise Aufbietung aller im betreffenden Gebiet lebenden Personen ausgeschlossen. Deshalb bleibt nur die Möglichkeit, auf freiwilliger Basis zu den entsprechenden Speichelproben zu gelangen. Jedoch ist als Folge der Unschuldsvermutung darauf zu achten, dass die Nichterteilung der Einwilligung keine Folgen nach sich zieht, insbesondere also nicht als Tatverdacht gewertet wird. Im Übrigen stellt sich auch die Frage, ob generell (nicht im Einzelfall) erteilte Einwilligungen eine Rechtsgrundlage ersetzen können.

Rechtsgrundlagen schaffen

Eine zum Zwecke der Identifizierung vorgenommene Analyse der nicht codierenden Teile der DNA einer unter Tatverdacht stehenden Person ist im konkreten Verdachtsfall auf Grund der bestehenden gesetzlichen Regelungen zulässig. Wir empfahlen indessen, die Besonderheiten dieses Verfahrens, insbesondere angesichts des erheblichen Missbrauchspotenzials, einer ausdrücklichen gesetzlichen Bestimmung zu unterwerfen.

DNA-Datenbanken in der Strafverfolgung: Ja, aber …

Strafverfolgungsorgane setzen seit geraumer Zeit DNA-Analysen als Mittel zur Aufklärung von Straftaten ein. In den Kantonen werden heute schon DNA-Datenbanken angelegt und das zu Grunde liegende menschliche Zellmaterial wird aufbewahrt.
Die aus dem Zellmaterial gewonnenen DNA-Identifizierungsmuster werden auch «genetische Fingerprints» genannt. Sie sind aber weit mehr als «gewöhnliche» Fingerabdrücke. Aus ihnen lassen sich bereits heute Informationen z.B. über Verwandtschaft gewinnen. Angesichts der weltweiten intensiven Forschung zur Entschlüsselung des gesamten menschlichen Genoms ist zudem nicht auszuschliessen, dass künftig aus den genetischen Fingerprints Informationen über die genetische Disposition sichtbar werden. Wird zudem das menschliche Zellmaterial aufbewahrt, so können daraus jederzeit auch Informationen über Krankheiten sowie Krankheits- und Erbanlagen erhoben werden. DNA-Analysen beinhalten somit Risiken und Gefahren für die Grundrechte der betroffenen Menschen.
Die Schaffung einer DNA-Datenbank und die Aufbewahrung menschlichen Zellmaterials über den Abschluss des Strafverfahrens hinaus stellen nach der Rechtsprechung des Bundesgerichts einen schweren Eingriff in die Grundrechte dar: Deshalb sind DNA-Datenbanken klaren Regeln zu unterwerfen.
Die Datenschutzbeauftragten von Bund, Kantonen und Gemeinden fordern daher, dass DNA-Datenbanken erst und nur dann aufgebaut werden und menschliches Zellmaterial erst und nur dann aufbewahrt wird, wenn angemessene gesetzliche Grundlagen bestehen.
Zum Schutz der Grundrechte der betroffenen Personen haben diese gesetzlichen Grundlagen für die Schaffung von DNA-Datenbanken zur Speicherung von DNA-Identifizierungsmustern Folgendes zu garantieren:
In eine DNA-Datenbank dürfen nur Identifizierungsmuster aufgenommen werden,

- die entweder von Zellmaterial gewonnen wurden, dessen Entnahme richterlich angeordnet oder mindestens gerichtlich überprüfbar war, und
- die nicht aus Massenscreenings stammen, oder
- die von Tatortspuren stammen, die noch nicht bestimmten Personen zugeordnet werden konnten.

Im Falle eines rechtskräftigen Freispruchs oder wenn das Verfahren nicht eröffnet oder rechtskräftig eingestellt wird, sind die in diesen Verfahren gewonnenen Identifizierungsmuster der entsprechenden Personen grundsätzlich sofort zu vernichten.
Die in eine DNA-Datenbank aufgenommenen Identifizierungsmuster dürfen ausschliesslich zum Zwecke der Strafverfolgung weiterverwendet werden.
Die Aufbewahrungsdauer ist durch angemessene Prüf- oder Löschfristen zu begrenzen, wobei die Art und Schwere des Delikts sowie das Alter der betroffenen Person berücksichtigt werden können.
An die Institute, die mit der Analyse der Körperzellen betraut werden, an die angewandten Verfahren (z.B. Anzahl der erhobenen Merkmale) und an die Datensicherheit sind aus datenschutzrechtlichen Gründen höchste Anforderungen bezüglich der Qualitätssicherung zu stellen.
Zum Schutz der Grundrechte der betroffenen Personen fordern die Datenschutzbeauftragten bezüglich des menschlichen Zellmaterials:
Grundsätzlich ist das menschliche Zellmaterial (inkl. Zwischen- und Restprodukte) nach rechtskräftigem Abschluss des Strafverfahrens oder wenn ein Strafverfahren nicht eröffnet oder rechtskräftig eingestellt wird, sofort und von Amtes wegen zu vernichten.
Darüber hinaus darf menschliches Zellmaterial nur und erst aufbewahrt werden, wenn eine klare gesetzliche Grundlage dies vorsieht. Dabei ist die Verwendung ausschliesslich auf die Zwecke der Nachführung der DNA-Datenbank bei Technologiewechsel und der Verifikation zu begrenzen.
Wenn das Material auf Grund einer klaren gesetzlichen Grundlage aufbewahrt werden kann, muss es unter der Obhut eines unabhängigen «Custos» stehen und getrennt von unmittelbar identifizierenden Informationen aufbewahrt werden.
Die Datenschutzbeauftragten bekräftigen ihre Bereitschaft, bei den entsprechenden Gesetzgebungsprojekten aktiv und konstruktiv mitzuarbeiten.

(Resolution verabschiedet von der 5. Schweizerischen Konferenz der Datenschutzbeauftragten am 13. Oktober 1998 in Fribourg)

Damit wäre sowohl für die in der praktischen Anwendung tätigen wie für die zu untersuchenden Personen mit der von § 5 DSG geforderten Deutlichkeit festgelegt, wann eine solche Untersuchung bei wem zulässig ist, was untersucht und was wie lange aufbewahrt wird. Insbesondere müsste klar geregelt werden, wann im Einzelfall eine Einwilligung der betroffenen Personen einen entsprechenden Tatverdacht ersetzen könnte. Auch wäre in diesem Zusammenhang zu verdeutlichen, welche Konsequenzen die Unschuldsvermutung im Falle einer Nicht-Einwilligung hätte. Zudem wären die Aufbewahrung und speziell die Frage, ob neben den gewonnenen Codes auch das Probenmaterial aufbewahrt werden dürfte, zu regeln.

Auf Grund der gesetzlichen Unschuldsvermutung erscheint des Weiteren die Schaffung einer Rechtsgrundlage, welche grossflächige Untersuchungen ermöglichen würde, rechtsstaatlich ausgeschlossen.

DNA-Datenbank

Eine gesetzliche Regelung ist demgegenüber unumgänglich, sofern eine eigentliche DNA-Datenbank geführt werden soll (siehe Kasten S. 23). Hier müsste zumindest umschrieben werden, ab welchem Zeitpunkt und in welcher Art welche Daten gespeichert sind, wie im gewählten Computersystem nach Spurenlegern gesucht werden kann, wer Zugriff erhält und wer als verantwortliches Organ zu gelten hat. Da sich allfällige Bestimmungen über eine DNA-Datenbank im Rahmen des geltenden Rechts zu halten haben, dürfte jedoch beispielsweise auf einen Zusammenhang der gewonnenen Analyseergebnisse mit einem Strafverfahren nicht verzichtet werden.

Praxis der DNA-Analyse

Der Regierungsrat hat in der Beantwortung der erwähnten kantonsrätlichen Anfrage (RRB 1643/1998; KR-Nr. 136/1998) auf die Sensibilität der DNA-Analysen hingewiesen und insbesondere betont, dass solche Untersuchungen nur unter strenger Beachtung des Prinzips der Verhältnismässigkeit vorzunehmen sind. Er befürwortete auch die Schaffung einer ausdrücklichen gesetzlichen Grundlage.
Des Weiteren untersuchten wir auch gestützt auf § 24 DSG die Praxis der DNA-Analysen. Die Ergebnisse veranlassten uns, Empfehlungen in Bezug auf die Anpassung der herrschenden Praxis an die bestehenden gesetzlichen Grundlagen abzugeben.

Der Anschluss von Behörden an das Internet

Immer mehr öffentliche Organe schliessen sich an das weltweite Internet an. Dem Datenschutz und der Informationssicherheit wird dabei häufig nicht die notwendige Beachtung geschenkt.

Das Internet ist für viele Private zu einem wichtigen Medium für die Beschaffung und den Austausch von Informationen sowie für das Angebot und die Nutzung kommerzieller Dienstleistungen geworden. Auch kantonale Behörden, Gemeinden, Schulen, Spitäler usw. suchen vermehrt den Anschluss an das Internet. Punktuell mussten wir dabei feststellen, dass Rahmenbedingungen des Datenschutzes und der Informationssicherheit nicht beachtet werden. Eine systematische Überprüfung war auf Grund des damit verbundenen Aufwandes mit den zur Verfügung stehenden Ressourcen bisher nicht möglich. Es ist jedoch angesichts der mangelnden Sensibilität im Umgang mit diesem Medium geplant, vermehrt anlassunabhängige Kontrollen durchzuführen.

Sicherheitskonzept

Das Internet ist ein öffentliches, globales und unstrukturiertes Netz. Dadurch entstehen spezifische Risiken, die erkannt werden müssen und gegen die es Massnahmen zu ergreifen gilt. Die Erstellung eines Sicherheitskonzeptes ist dafür unumgänglich. Das hohe Gefahrenpotenzial des Anschlusses an das Internet erfordert Abschottungsmassnahmen wie beispielsweise Firewalls. Werden im eigenen Netzwerk sensible Personendaten bearbeitet, ist auch eine Chiffrierung einzurichten. Das Sicherheitskonzept hat auf Grund von Risikoanalysen die erforderlichen Massnahmen im Einzelnen vorzusehen. Die kantonale Informatiksicherheitsverordnung (ISV) setzt für bestehende Informatiksysteme und -anwendungen hierfür eine Frist bis zum 31. März 2000 fest (siehe dazu S. 35). Die Massnahmen haben dem Stand der Technik zu entsprechen und sind periodisch zu überprüfen (§ 1 Abs. 2 DSV; § 17 ISV).

Rechtsfragen

Die Bearbeitung von Personendaten im Internet (z.B. Veröffentlichung von Daten im World Wide Web, Datenaustausch mittels E-Mail) ist heute noch nicht ausdrücklich geregelt. Ob aus bestehenden Rechtsgrundlagen Entsprechendes hergeleitet werden kann, muss im Einzelfall geklärt werden. Ist die Bearbeitung vom Grundsatz her zulässig, müssen die Rahmenbedingungen, insbesondere die Grundsätze der Verhältnismässigkeit, der Integrität und der Sicherheit, beachtet werden.

Internet-Anschluss zu welchem Zweck?

Damit diese Rahmenbedingungen im Einzelnen umgesetzt werden können, muss sich das verantwortliche Organ über den Zweck des Anschlusses ans Internet klar werden. Es hat zu beurteilen, ob ein solcher Anschluss zur Erfüllung der

Welches ist der Nutzen des Internets?

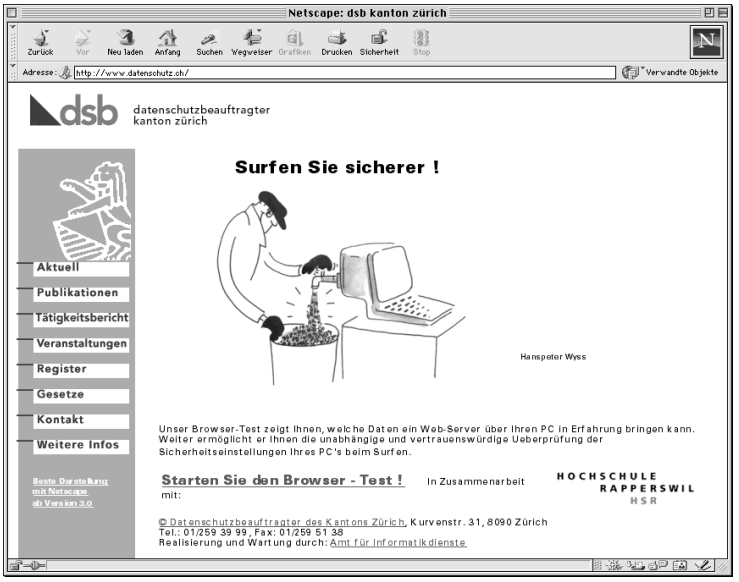
Das World Wide Web eignet sich, Informationen von allgemeinem Interesse zu verbreiten, z.B. die eigene Amtsstelle, Gemeinde, Anstalt usw. zu porträtieren, auf kulturelle und politische Anlässe aufmerksam zu machen oder Amtsadressen und Öffnungszeiten zu veröffentlichen. Mangels Rechtsverbindlichkeit eignet es sich nur bedingt zur Veröffentlichung von amtlichen Mitteilungen.
Das World Wide Web enthält ein grosses Informationsvolumen, weshalb öffentliche Organe es auch als Informationsquelle oder für Ausbildungszwecke nutzen können.
Einen schnellen und umfangreichen Austausch von Informationen ermöglicht der E-Mail-Dienst. Für Behörden steht derzeit noch der formlose Informationsaustausch (z.B. Erteilung einfacher Auskünfte) im Vordergrund. Technische Mechanismen für die Wahrung der Vertraulichkeit und Authentizität bei der Entgegennahme von Anmeldungen, Gesuchen, Anträgen usw. sind zwar bereits teilweise vorhanden, doch fehlen derzeit noch Normen, welche die Rechtsverbindlichkeit gewährleisten.

gesetzlichen Aufgaben notwendig ist. Auf dieser Basis ist eine Differenzierung vorzunehmen, und es sind die Dienste festzulegen, welche benötigt werden. In rechtlicher Hinsicht ist schliesslich zu klären, welche Bearbeitung von Personendaten im Internet (Veröffentlichung im World Wide Web, Austausch mittels E-Mail usw.) zulässig ist.

Veröffentlichung von Daten

Das World Wide Web ist eine neue Form für die Publikation von Informationen. Im Unterschied zu anderen Medien können Informationen im World Wide Web kontinuierlich zugänglich gemacht werden. Sie sind nach bestimmten Kriterien recherchierbar und erschliessbar, etwa durch Suchfunktionen (z.B. Volltextsuche über das eigene Angebot, kommerzielle oder nicht kommerzielle Suchmaschinen Dritter).
Wer Personendaten im World Wide Web zum Abruf bereithalten will, muss klären, ob eine Veröffentlichung durch Rechtsgrundlagen gedeckt ist. Bestehen gesetzliche Grundlagen, sind sie daraufhin zu prüfen, ob diese Form der Veröffentlichung dem Zweck der Bekanntgabe der Daten entspricht und verhältnismässig ist. Sofern die Zulässigkeit der Veröffentlichung als grundsätzlich gegeben scheint, kann es sich als notwendig erweisen, den Zugang zu Informationen durch eine Suchfunktion auf bestimmte Kriterien zu begrenzen. Auch sind die Daten allenfalls nach einer bestimmten Zeit wieder zu löschen, wenn kein öffentliches

Homepage des Datenschutzbeauftragten



Homepage:
http://www.datenschutz.ch
http://www.zh.ch/dsb

E-Mail-Adresse:
datenschutz@dsb.zh.ch

Wo liegen die Gefahren des Internets?

Auf Grund der Struktur des Internets gibt es keine Instanz, welche die Übersicht und Kontrolle über das ganze Netz und damit auch eine Gesamtverantwortung innehat. Die Verantwortung bleibt bei jeder einzelnen angeschlossenen Stelle, die sich dieser Situation oft zu wenig bewusst ist.
Die Übermittlung der Daten erfolgt auf Wegen, die weder voraussehbar noch vorherbestimmbar sind. Sie ist deshalb auch nicht kontrollierbar. Die Daten können von Dritten abgehört und manipuliert werden. Auch die Authentizität der Daten ist nur mit besonderen Massnahmen gewährleistet.
Die Verbreitung von Daten über Internet-Dienste wie das WWW erfolgt global. Die Daten gelangen auch in Staaten, die keinen dem schweizerischen gleichwertigen Persönlichkeitsschutz kennen. Die Durchsetzung von Rechtsansprüchen im Ausland ist faktisch erschwert oder gar nicht möglich. Datenschutzrechtliche Ansprüche nach der schweizerischen Rechtsordnung können dadurch ausgehöhlt werden.

Im Internet sind die Daten beliebig verwendbar und können auf vielfältige Weise kombiniert werden. Die nicht transparente Nutzung solcher Möglichkeiten widerspricht dem datenschutzrechtlichen Zweckbindungsgebot und verstösst gegen den Grundsatz von Treu und Glauben. Durch die Kombination mit anderen Daten können Daten auch eine andere Qualität erhalten, was zu einer erhöhten Gefährdung der Persönlichkeitsrechte führen kann.
Daten, die im Internet verbreitet werden, sind «ewig», da deren weitere Speicherung nicht mehr beeinflusst werden kann. Fristen für die Löschung von Daten und Schutzfristen des Archivrechts können unterlaufen werden.
Das Internet ist weltweit öffentlich zugänglich. Dabei können Personen mit böswilligen Absichten auch ohne besondere Kenntnisse und Ausrüstungen in ungeschützte Systeme eindringen. Besondere Sicherheitsmassnahmen zum Schutz der eigenen Programme und Dateien sind deshalb unerlässlich.

Interesse an einer unbegrenzten und dauernden Zugänglichkeit besteht.

E-Mail

Als praktisch erweist sich der elektronische Postdienst des Internets (E-Mail). Daten dürfen Dritten auch über E-Mail verschickt werden, sofern die Voraussetzungen für die Bekanntgabe von Daten gemäss §§ 8 ff. DSG erfüllt sind. Weiter ist zu berücksichtigen, dass das Verschicken einer ungesicherten E-Mail dem Versand einer Postkarte gleichkommt und diese von jedermann mitgelesen werden kann.
Vertrauliche Daten müssen daher verschlüsselt werden, wenn sie via E-Mail ausgetauscht werden. Sollen auch die Authentizität, die Richtigkeit des Inhalts sowie die Nicht-Abstreitbarkeit der Kommunikationsbeziehungen sichergestellt werden, ist eine digitale Signatur notwendig (siehe dazu auch S. 34). Auf Grund der Rechtslage kann eine Behörde derzeit noch keine rechtsverbindlichen Erklärungen mittels E-Mail abgeben.

Daten über Mitarbeitende

Daten über Mitarbeiterinnen und Mitarbeiter sind im Rahmen der dienstlichen Verrichtungen durch das DSG geschützt. Sie dürfen nur bearbeitet werden, soweit es zur Erfüllung der Aufgaben der Behörden oder zur Durchführung des Arbeitsverhältnisses geeignet und erforderlich ist. Nicht erforderlich ist die Veröffentlichung vollständiger Mitarbeiterverzeichnisse im World Wide Web. Die globale Verbreitung dieser Daten widerspricht dem lokal beschränkten Zweck einer solchen Publikation.
Das öffentliche Interesse bzw. die gesetzlichen Aufgaben erstrecken sich nur auf die Veröffentlichung der amtlichen Adresse sowie allenfalls die Angabe des Namens des Leiters bzw. der Leiterin der Amtsstelle oder Abteilung.

Instruktion notwendig

Der Umgang mit dem Internet, insbesondere auch in Bezug auf die Beachtung der Sicherheitsaspekte und der datenschutzrechtlichen Anforderungen, erfordert eine entsprechende Ausbildung. Wer Mitarbeiterinnen und Mitarbeiter mit einem Internet-Anschluss ausstattet, ist daher zu einer angemessenen Instruktion durch eine entsprechende Schulung verpflichtet. Auch sollten klare Richtlinien in Form von Weisungen über den Umgang mit dem Internet bzw. den einzelnen Diensten vorgegeben werden.

Umfang der Datenbearbeitung und -weitergabe

Praxisbezogene Richtlinien und Beratungen schaffen mehr Sicherheit im Umgang mit Personendaten auf Gemeindeebene.

1. Rundschreiben an die Einwohnerkontrollen

Liste der zulässigen Datenkategorien und Mutationsmeldungen

Unsicherheit herrschte bei den Einwohnerkontrollen sowohl bezüglich der zulässigerweise geführten Datenkategorien wie auch bezüglich des Empfängerkreises von periodischen Mutationsmeldungen. Dies zeigte sich in der grossen Zahl von entsprechenden Anfragen beim Datenschutzbeauftragten. Eine Durchsicht der Register der Datensammlungen der Gemeinden bestätigte einen Handlungsbedarf.

In einem Rundschreiben an alle Einwohnerkontrollen konnten wir diese zentralen Fragen beantworten.
Grundsätzlich darf eine Einwohnerkontrolle Daten bearbeiten, wenn eine gesetzliche Grundlage vorliegt und die Daten zur Erfüllung einer Aufgabe tatsächlich gebraucht werden. Vom Gesetz vorgegebene Aufgabe ist primär die Kontrolle der auf dem Gemeindegebiet niedergelassenen beziehungsweise sich aufhaltenden Personen, weshalb in erster Linie die zur Identifizierung erforderlichen Angaben benötigt werden. Darüber hinaus sind im Rahmen von § 38 Abs. 3 Gemeindegesetz auch für andere Ämter die für deren Aufgabenerfüllung notwendigen Angaben zu erfassen.

Gestützt auf § 4 Abs. 2 DSG dürfen nur richtige Daten bearbeitet werden. Das sind etwa Daten, welche definitionsgemäss nicht mehr ändern (wie beispielsweise das Geburtsdatum). Bei veränderlichen Angaben muss demgegenüber die Zulässigkeit der Erfassung mit der Pflicht zur Meldung von Änderungen korrelieren. Infolgedessen sind im Normalfall insbesondere der Beruf beziehungsweise der Arbeitgeber einer Person nicht zu erheben.

Zulässigerweise dürfen folgende Datenkategorien erfasst werden:
- Name und gegebenenfalls Frauenname
- sämtliche Vornamen sowie der Rufname
- korrekte Anrede
- genaue Adresse
- Wohnungsnummer (im Hinblick auf die Volkszählung 2000)
- AHV-Nummer
- Personalien der Eltern
- das Bestehen vormundschaftlicher Massnahmen sowie die Nennung der gesetzlichen Vertretung
- Zuzugsdatum und -ort
- Wegzugsdatum und -ort beziehungsweise Sterbedatum und -ort
- Geburtsdatum
- Geschlecht
- Zivilstand
- Familienbezug der unmündigen Kinder
- Traudatum und -ort beziehungsweise Scheidungsdatum und -ort respektive Datum und Ort der gerichtlichen Trennung beziehungsweise Todesdatum des Ehepartners
- Nationalität
- Heimatort
- Geburtsort
- Niederlassungsstatus
- gesetzlicher Wohnsitz bei auswärtigem Aufenthaltsort respektive Aufenthaltsort bei Vorliegen des gesetzlichen Wohnsitzes
- Konfession
- Eintrag Zivilschutz, sofern die Einwohnerkontrolle das Meldewesen für den Zivilschutz besorgt
- Eintrag über die Erfüllung der Krankenversicherungspflicht
- Datum der Hinterlegung des Heimatscheins beziehungsweise des Heimatausweises sowie Ausstellungsdatum und -ort des Heimatscheins

Bei ausländischen Personen kann zusätzlich erfasst werden:
- ZAR-Nummer und Fremdenpolizei-Nummer
- fremdenpolizeilicher Status
- Datum des Ablaufs der fremdenpolizeilichen Bewilligung
- Einreisedatum in die Schweiz
- sowie (nur bei gewissen Kategorien von Ausländern) Beruf und Arbeitgeber

Wir wiesen darauf hin, dass einerseits gemäss kommunalem Recht allenfalls weitere Datenkategorien zulässig sind und dass

sich eine Einwohnerkontrolle andererseits auf Grund ihrer vorgegebenen Organisationsstruktur beziehungsweise ihrer konkreten Bedürfnisse auf einen Teil der aufgeführten Daten beschränken kann.

Automatische Mutationsmeldungen sind grundsätzlich nur zulässig aus dem Bestand der eigenen Daten; aus Datensammlungen anderer Amtsstellen dürfen demgegenüber keine Informationen weitergegeben werden. Konkret sind gemäss eidgenössischem beziehungsweise kantonalem Recht Meldungen je mit den vom empfangenden Amt benötigten Informationen insbesondere an das Steueramt, an die Militärsektion/den Sektionschef, die Zivilschutzstelle, die anerkannten Kirchen, die Schulpflegen, die AHV-Zweigstellen sowie an die Fremdenpolizei zulässig. Nach kommunalem Recht kommen allenfalls weitere regelmässige Datenempfänger in Betracht. Liegen die Voraussetzungen für eine automatische Datenbekanntgabe dagegen nicht vor, kann eine Auskunft höchstens im Einzelfall im Rahmen einer Amtshilfe erteilt werden. Für eine regelmässige Datenbekanntgabe an die örtlich zuständige Polizeistelle, die Poststelle oder die gemeindeeigene Bibliothek fehlen demgegenüber die Voraussetzungen.

2. Daten über Schülerinnen und Schüler

Beurteilung des Umfangs der Bearbeitung und der Weitergabe

Diverse Anfragen betrafen Datenbearbeitungen über Schulkinder sowie über Lehrpersonal. Wir hielten grundsätzlich fest, dass gemäss § 4 Abs. 2 und 3 DSG Daten nur insoweit bearbeitet werden dürfen, als sie zur konkreten Aufgabenerfüllung geeignet und erforderlich sowie aktuell sind.
Die Führung von Akten über die Schulkinder obliegt der Schul pflege. Sie muss gemäss § 6 DSG für eine den Anforderungen der Datensicherheit genügende Aufbewahrung besorgt sein. Sie hat abzuklären, ob und in welchem Umfang einer Lehrkraft zur Gestaltung des Unterrichts Einblick in ein Dossier eines Schulkindes zu geben ist. Dabei kann es insbesondere bei Gesundheitsdaten, also besonders schützenswerten Daten, allenfalls genügen, wenn eine Lehrkraft über gewisse unterrichtsrelevante Besonderheiten eines Schulkindes orientiert wird, ohne dass ihr die genaue Ursache beziehungsweise die medizinische Diagnose im Einzelnen offen gelegt werden müsste. Aus diesem Grunde dürfen Lehrkräfte auch nicht untereinander Daten über Schulkinder beliebig austauschen.
Angaben bezüglich der Schulkinder müssen stets auf dem aktuellen Stand sein. Infolgedessen sind Unterlagen über Ereignisse, welche für den Unterricht nicht mehr relevant sind, auszusondern.
Ausserdem besteht für die urteilsfähigen Schulkinder (beziehungsweise bei urteilsunfähigen Kindern für deren gesetzliche Vertretung) ein Auskunftsrecht für die über sie geführten Daten gemäss § 17 DSG. Davon ausgenommen sind lediglich reine Gedächtnisstützen der einzelnen Lehrpersonen, welche aber als persönliche Hilfsmittel keiner anderen Lehrkraft und keinem Mitglied der Schulpflege zugänglich gemacht werden dürfen.

In diesem Sinne beurteilten wir auch ein von der Bildungsdirektion geplantes Formular, welches ein Schulkind während der gesamten Schulzeit hätte begleiten sollen (zum Datentransfer bei Schulübertritt an die Oberstufe vgl. Tätigkeitsbericht Nr. 2 [1996], S. 30 f.).
Wir stellten fest, dass ein ausreichender Grund fehlt, um bei allen Schulkindern von vornherein beispielsweise die Konfession, die Berufe der Eltern oder Angaben zum Hausarzt oder zur Hausärztin zu erfassen. Problematisch erschien eine Rubrik für unterrichtsrelevante Besonderheiten, da die stete Nachführung solcher Einträge beziehungsweise die Löschung nicht mehr aktueller Angaben nicht garantiert war.
Ausserdem waren sowohl der Zweck des Formulars sowie die einzelnen Zugriffsberechtigungen nicht klar umschrieben. Nicht

zuletzt war eine den Sicherheitsanforderungen genügende Aufbewahrung solcher teilweise sehr heiklen Daten nicht gewährleistet.
Im Gespräch mit der Bildungsdirektion wurden der Verzicht auf die unzulässigen Rubriken sowie eine datenschutzkonforme Neufassung des Formulars in Aussicht gestellt.

3. Steuerdaten für andere Verwaltungszweige

Umsetzung des Zweckbindungsgebots

In kleinen Gemeinden sind die Aufgaben häufig auf einige wenige Mitarbeitende verteilt, die verschiedene Funktionen in Personalunion ausüben. Dies kann zu Schwierigkeiten in Bezug auf die Verwendung von Personendaten führen.
Der Grundsatz der Zweckbindung bestimmt, dass Daten nur zu einem Zweck bearbeitet werden dürfen, der bei der Beschaffung angegeben wurde oder der gesetzlich vorgesehen wird (§ 4 Abs. 4 DSG).
Die konkrete Anfrage betraf den Fall, dass ein Bezüger von Leistungen der Sozialhilfe verdächtigt wurde, einem Nebenverdienst nachzugehen, den er gegenüber den Sozialhilfebehörden nicht deklarierte. Die zu Steuerzwecken bearbeiteten Daten durften nicht den Zwecken der Sozialhilfe zugeführt werden, da eine entsprechende Rechtsgrundlage fehlt. Ausserdem stand einem Beizug der Steuerakten durch die Sozialhilfebehörde das Steuergeheimnis (§ 82 des bisherigen bzw. § 120 des neuen, am 1. Januar 1999 in Kraft getretenen Steuergesetzes) entgegen.
Die Fragestellung war auf andere Weise zu lösen. Gemäss § 18 des Sozialhilfegesetzes muss die betroffene Person diejenigen Auskünfte geben und Unterlagen einreichen, die für die Gewährung von wirtschaftlicher Hilfe erforderlich sind. Diese Mitwirkungspflicht der Hilfe suchenden Personen ermöglichte es, die fraglichen Unterlagen direkt von der betroffenen Person einzuverlangen. Dieses Vorgehen entspricht auch dem Grundsatz, dass Daten in der Regel direkt bei der betroffenen Person zu beschaffen sind (§ 7 Abs. 1 DSG).
Ebenso war in einem Fall zu verfahren, in dem eine betroffene Person die Bezahlung der Kehrichtgebühr für Gewerbetreibende mit dem Argument verweigerte, sie mache auch keine Erträge bzw. Verluste aus dem Gewerbe mehr geltend. Aus den erwähnten Gründen war auch hier eine Einsichtnahme in die Steuerakten ausgeschlossen. Sieht das kommunale Kehrichtgebührenrecht eine Bemessung auf Grund der in der Steuererklärung deklarierten Erträge bzw. Verluste vor, kann die betroffene Person zu entsprechenden Nachweisen verpflichtet werden, wenn sie behauptet, die Bemessungsgrundlagen hätten sich in ihrem Fall geändert.

4. Abklärungen bei Entmündigungsfällen

Datenbeschaffung durch die Vormundschaftsbehörde

Die Abklärung eines Entmündigungsfalles tangiert zwangsläufig sehr weit gehend persönliche Bereiche der betroffenen Person. Die Vormundschaftsbehörde muss deshalb eine grosse Zahl von Informationen zusammentragen, bevor sie bei dem für Entmündigungen zuständigen Bezirksrat einen entsprechenden Antrag stellen kann. Eine Vormundschaftsbehörde bat uns abzuklären, in welchem Masse sie berechtigt ist, Informationen bei anderen staatlichen Stellen einzuholen.
Da bei Bevormundungsfällen zu einem grossen Teil besonders schützenswerte Daten (namentlich in Bezug auf die psychische Gesundheit) betroffen sind, darf ein Datentransfer gemäss § 5 DSG nur unter qualifizierten Bedingungen erfolgen: Entweder liegt eine klare gesetzliche Grundlage vor,

oder die Daten sind zur Erfüllung einer gesetzlich klar umschriebenen Aufgabe unentbehrlich, oder die betroffene Person hat eingewilligt. Letzteres ist auch in Bezug auf Personen, bei welchen konkrete Entmündigungsgründe abgeklärt werden müssen, denkbar, da ihre Willensäusserungen bis zum Zeitpunkt der vollzogenen Entmündigung rechtsbeachtlich sind, sofern sie urteilsfähig sind. Ausserdem braucht eine Einwilligung nicht ausdrücklich gegeben worden zu sein, sondern kann sich ebenso aus den konkreten Umständen herleiten. Hat sich die betroffene Person jedoch klar negativ geäussert, kann ihr nicht mehr unterstellt werden, sie würde bei vernünftiger Beurteilung der Lage einwilligen.
Eine Rechtsgrundlage im erforderlichen Präzisierungsgrad ist für den vorliegenden Fall nicht gegeben. Dagegen kann eine Vormundschaftsbehörde amtshilfeweise (§ 8 lit. a DSG) die im Hinblick auf ein allfälliges Entmündigungsverfahren benötigten Informationen bei anderen Stellen einholen, da sie nur in Kenntnis aller relevanten Umstände über einen Entmündigungsantrag beim Bezirksrat gemäss § 83 EG zum ZGB entscheiden kann. Beispielsweise kann sie bei einem medizinischen Gutachter, welcher sich bereits mit dem Fall befasst hat, nicht nur Auskunft über das Resultat seiner Abklärungen verlangen, sondern auch Einblick in alle für die Frage der Entmündigung relevanten Aktenstücke nehmen. Nur so kann sie prüfen, ob die von der Gutachtensperson gezogenen Schlussfolgerungen auch unter rechtlichen Gesichtspunkten stichhaltig sind.

5. Fragebogen über den Gesundheitszustand

Konkrete Durchführung der Untersuchung ausschlaggebend

Von einer betroffenen Person wurden wir auf den «Fragebogen über den Gesundheitszustand» eines schulärztlichen Dienstes hingewiesen. Auf dem mehrseitigen Formular werden die unterschiedlichsten Fragen zur aktuellen Lebenssituation des Schulkindes gestellt. Angesprochen wird beispielsweise die momentane physische und psychische Empfindlichkeit, die Sexualität, die Ernährung, der Konsum von erlaubten und verbotenen Drogen oder die Gewaltbereitschaft innerhalb der Schule sowie der Familie. Die betroffene Person hat Bedenken sowohl hinsichtlich der Rechtsgrundlage wie hinsichtlich der Verhältnismässigkeit der teilweise sehr weit gehenden Fragen geäussert.
Das Verhältnismässigkeitsprinzip gebietet, dass nur die zur Aufgabenerfüllung geeigneten und erforderlichen Daten (§ 4 Abs. 3 DSG) bearbeitet werden. Bei systematischen Datenerhebungen und namentlich bei Fragebogen müssen zudem gemäss § 7 Abs. 2 DSG sowohl der Bearbeitungszweck wie die Rechtsgrundlage bekannt gegeben werden.
Der Fragebogen war zwar mit einem Beiblatt versehen, welches über die konkreten Aufgaben einer schulärztlichen Untersuchung informierte und auf die Wichtigkeit der medizinischen Vorsorge hinwies. Ausserdem wurde darin die ärztliche Schweigepflicht ausdrücklich erwähnt. Jedoch liess er weder eine Rechtsgrundlage für die Befragung noch deren Zweck transparent werden. Offen blieb, ob und gegebenenfalls bei wem die gemachten Angaben gespeichert werden und ob sogar eine Weiterleitung von strafrechtlich relevanten Informationen (verbotener Drogenkonsum, Gewalt in der Familie) an andere Amtsstellen stattfindet. Infolgedessen fehlten die Voraussetzungen gemäss § 5 DSG für eine Bearbeitung solcher besonders schützenswerter Personendaten.

Ein direkter Kontakt mit dem schulärztlichen Dienst ergab, dass diverse Fassungen des genannten Beiblattes kursieren. Insbesondere wird in anderen Varianten ausdrücklich darauf hingewiesen, dass der (nicht unbedingt vollständig) ausgefüllte Fragebogen niemandem abgegeben werden muss. Wie
uns versichert wurde, soll den zu untersuchenden Schülerinnen und Schülern damit lediglich eine Art private Gedankenstütze in Bezug

auf mögliche Gesprächsthemen in die Hand gegeben werden.
Uns wurde ausserdem eine Neuformulierung des Beiblattes in Aussicht gestellt, worin der Fragebogen ausdrücklich als eine auf freiwilliger Basis zu erstellende eigene Gedächtnisstütze deklariert wird.

Problematisch bleibt jedoch, dass die Datenschutzkonformität der Untersuchung erheblich von den konkreten Umständen abhängt: So hat es bereits einen gewissen Einfluss, mit welchen begleitenden Bemerkungen die Lehrkraft die Blätter an die Schülerinnen und Schüler abgibt. Ausschlaggebend ist aber vor allem, dass nicht Unbefugte in die ausgefüllten Fragebogen Einblick verlangen beziehungsweise sich Kenntnis davon verschaffen.

6. Auszug über die Telefongebühren

Nur ausnahmsweise detaillierte Auswertungen für Amtsstellen

Auf Grund des neuen Fernmeldegesetzes (FMG), das seit dem 1. Januar 1998 in Kraft ist, steht den Kundinnen und Kunden einer Fernmeldediensteanbieterin («Telefongesellschaft») das Recht zu, Auskunft über die für die Rechnungsstellung verwendeten Daten zu verlangen. Die Auskunft enthält die Rufnummern der Teilnehmenden (anrufende und angerufene Person), Zeitpunkt und Dauer der Verbindungen und die Höhe der Gebühren. Eine Schulbehörde verlangte bei der Fernmeldediensteanbieterin einen solchen Gebührenauszug zu einem bestimmten Anschluss.

Öffentliche Organe, welche von ihrer Fernmeldediensteanbieterin detaillierte Abrechnungen verlangen wollen, haben zusätzlich die Anforderungen des DSG zu beachten. Der Betrieb eines Telefonanschlusses ist in der Regel durch die Aufgabenumschreibung eines öffentlichen Organs gedeckt und gehört zu den üblichen Arbeitsinstrumenten. Auswertungen der Telekommunikationsverbindungen dürfen jedoch nur unter bestimmten Voraussetzungen verlangt werden. Insbesondere ist zu berücksichtigen, dass dabei auch die Persönlichkeitsrechte der angerufenen Drittpersonen tangiert werden.

- Eine Auswertung der Daten ist möglich, wenn alle Beteiligten eingewilligt haben. Dieser Fall kommt jedoch nur theoretisch in Betracht.
- Eine moderne Telefonanlage ist vergleichbar mit jedem anderen EDV-System bzw. -Netzwerk, in welchem sicherheitsrelevante Ereignisse vorfallen können. Diese Problematik stellt sich jedoch nur, wenn das öffentliche Organ die Anlage selbst betreibt, was vorliegend nicht der Fall war (zu den Rahmenbedingungen beim Betrieb einer eigenen Teilnehmervermittlungsanlage vgl. Tätigkeitsberichte Nr. 1 [1995], S. 31, und Nr. 3 [1997], S. 23 f.). Eine Auswertung aus Sicherheitsgründen ist ausserdem unter sicherheitsspezifischen Aspekten vorzunehmen.
- Für eine allfällige interne Weiterverrechnung von Gebühren ist normalerweise kein detaillierter Auszug erforderlich. Für die Zuordnung an einzelne Kostenträger des öffentlichen Organs genügen die allgemeinen Gebührenrechnungen der Fernmeldediensteanbieterin, die keine Angaben über die einzelnen Kommunikationsverbindungen enthalten.
- Hinsichtlich der privaten Benutzung des Telefons durch Mitarbeitende ist im Einzelfall zu differenzieren. Ist privates Telefonieren nicht grundsätzlich verboten, widerspricht es Treu und Glauben, dennoch Kontrollen durchzuführen. Selbst wenn ein Verbot ausgesprochen wurde, gehört es zu den Persönlichkeitsrechten des Arbeitnehmers bzw. der Arbeitnehmerin, dass er oder sie am Arbeitsplatz in Pausen und in dringenden Fällen unbeaufsichtigt telefonieren kann. Auch wenn dazu ein separater Anschluss zur Verfügung steht, dürfen beim «Diensttelefon» nicht einfach Kontrollen bzw. Auswertungen durchgeführt werden. Lediglich stichprobeweise darf der Tele-

fonverkehr ausgewertet werden, sofern die Betroffenen vorgängig über die Möglichkeit solcher Kontrollen informiert wurden. Der Grundsatz der Verhältnismässigkeit erfordert zudem, dass vorher erfolglos andere Führungs- und Kontrollinstrumente eingesetzt worden sind, welche die Persönlichkeitsrechte weniger stark tangieren.

- Bei Verdacht auf Missbräuche (z.B. übermässiges Telefonieren während der Arbeitszeit) – dieser Verdacht muss sich aus konkreten Anhaltspunkten ergeben – sind einzelfallweise Kontrollen möglich. Aus Gründen der Verhältnismässigkeit muss jedoch immer eine vorgängige Abmahnung erfolgen, d.h., Kontrollen sind vorher anzukündigen und nur für die Zukunft vorzunehmen. Zeitlich haben sie sich auf einen verhältnismässigen Zeitraum (ein bis drei Monate) zu beschränken. Auch ist auf eine möglichst schonende Auswertung hinsichtlich der Daten von unbeteiligten bzw. unverdächtigen Personen zu achten.

Zuständig für Kontrollen ist die personalrechtlich vorgesetzte Person. Die Kontrolle selbst sollte vom Amts- oder Abteilungschef bzw. dem Vorsteher der Organisationseinheit angeordnet werden. Der Fernmeldedienstanbieterin sollte deshalb mitgeteilt werden, welche Personen das Recht haben, einen Auszug zu verlangen.
Ein detaillierter Gebührenauszug darf durch öffentliche Organe deshalb nur unter diesen eingeschränkten Voraussetzungen bei der Fernmeldedienstanbieterin eingefordert werden.

7. Krankengeschichten im Altpapier

Verletzung von Datenschutz und Berufsgeheimnis

Interessierte Personen übergaben uns eine grosse Anzahl von teilweise vollständigen Akten (inklusive dazugehöriger Röntgenbilder) aus der Schulzahnklinik einer Gemeinde. Diese waren für die gewöhnliche Papiersammlung bereitgestellt worden. Daraus konnten neben Angaben zum Zahnzustand der behandelten Kinder auch Informationen zu den erziehungsberechtigten Personen sowie teilweise weitere Angaben beispielsweise zum Schulverlauf entnommen werden.
Wir machten die zuständige Schulpflege darauf aufmerksam, dass die in § 4 Abs. 5 DSG vorgeschriebenen Datensicherheitsmassnahmen auch bei nicht mehr gebrauchten Unterlagen mit Personendaten beachtet werden müssen (vgl. zur Pflicht einer datenschutzkonformen Entsorgung Tätigkeitsbericht Nr. 2 [1996], S. 37, sowie Nr. 1 [1995], S. 30 f.). Dies gilt insbesondere in Bezug auf Angaben zur Gesundheit, die zu den besonders schützenswerten Daten gemäss § 2 lit. d Ziff. 2 DSG zählen. Entsprechend sind bei medizinischen Akten, welche zudem durch das Berufsgeheimnis nach Art. 321 Strafgesetzbuch (StGB) abgesichert sind, bei jeder Art des Bearbeitens und damit auch hinsichtlich der Vernichtung qualifizierte Anforderungen zu beachten: Sie sind korrekterweise von dem gemäss § 6 DSG verantwortlichen Organ zu shreddern oder auf andere ebenso sichere Art und Weise zu entsorgen.
Die Antwort der betroffenen Schulpflege mussten wir zum Anlass nehmen, nochmals auf die Wichtigkeit eines datenschutzkonformen Umgangs mit Personendaten und insbesondere auf die Pflicht zur fachgerechten Entsorgung hinzuweisen. Ausserdem gaben wir die Empfehlung ab zu analysieren, ob sich generell ein Handlungsbedarf in Bezug auf einen datenschutzkonformen Umgang mit Personendaten im Bereich der Schule aufzeige. In der Folge erging der Auftrag an ein Schulpflegemitglied, die schulärztlichen Reihenuntersuchungen kritisch auf datenschutzrechtliche Mängel hin zu durchleuchten.

Infrastruktur für Sicherheit

Die Schaffung eines angemessenen, dem Stand der Technik entsprechenden Sicherheitsstandards ist eine der grossen Herausforderungen im Bereich der Informatik.

1. Digitale Signaturen für die Verwaltung

Start eines Pilotprojekts

Verschiedene Anfragen nach Lösungsmöglichkeiten im Bereich der sicheren Kommunikation und die Aufgaben im Rahmen der Umsetzung der Informatiksicherheitsverordnung (siehe S. 35) führten dazu, dass wir uns eingehender mit der Frage des Einsatzes von digitalen Signaturen in der Verwaltung beschäftigten.

Die digitale Signatur, basierend auf einem kryptographischen Verfahren, stellt sich heute als eine Schlüsseltechnologie dar, die es ermöglicht, verschiedene Risiken der Informatik, die durch die weltweite Vernetzung der Systeme drastisch zugenommen haben, abzudecken. Mit dem Einsatz von digitalen Signaturen ist es möglich, Daten vertraulich zu übermitteln, die Authentizität der Kommunikation sowie die Integrität des Inhaltes sicherzustellen. Ebenso kann mit der digital signierten Kommunikation erreicht werden, dass ein stattgefundener Datenaustausch nicht abgestritten werden kann. Damit kommt die Technologie der digitalen Signatur in idealer Weise den Anforderungen des Datenschutzgesetzes entgegen, das insbesondere bei sensiblen Daten einen vertraulichen, authentischen und integren Datenaustausch zwischen den involvierten Stellen verlangt.
Digitale Signaturen werden deshalb in der Verwaltung insbesondere dort eine Rolle spielen, wo Daten zwischen Amtsstellen elektronisch ausgetauscht werden, im Verhältnis zwischen kantonalen und kommunalen Stellen oder in der Kommunikation zwischen der Verwaltung und Unternehmungen oder Bürgerinnen und Bürgern.
Klare Bedürfnisse haben sich bereits gezeigt beim Austausch von E-Mails oder vertraulicher Berichte im Gesundheitswesen. Der zunehmende elektronische Datenaustausch wird auch immer mehr das Verhältnis zwischen Staat und Bürgerinnen und Bürgern betreffen, beispielsweise beim elektronischen Einreichen von Steuererklärungen, Gesuchen usw. In all diesen Fällen ist entscheidend, dass die teilweise sensiblen Daten angemessen geschützt werden.
Der Datenschutzbeauftragte war deshalb zusammen mit der Abteilung für Informatikplanung (AIP) und der Informatikrevision des Amts für Informatikdienste (AID) mitverantwortlich für einen Antrag an die Arbeitsgruppe für die Planung und Steuerung der Informatik (AGIK) zur Schaffung von Grundlagen für den Einsatz von digitalen Signaturen in der kantonalen Verwaltung.

In einem ersten Schritt wurde entschieden, in einem Pilotprojekt den Einsatz von digitalen Signaturen in der Verwaltung zu prüfen. Schwerpunkt in diesem Projekt ist die Sicherstellung der vertraulichen, integren und authentischen Kommunikation mittels E-Mail, weshalb primär die beiden in der kantonalen Verwaltung zum Einsatz gelangenden E-Mail-Systeme diesbezüglich getestet werden sollen. Mit dem Universitätsspital nimmt auch ein Betrieb an diesem Pilotversuch teil, der sehr sensible Daten aus dem Gesundheitsbereich bearbeitet und ein grosses Bedürfnis nach einem sicheren elektronischen Austausch solcher Daten hat. In Bezug auf die Infrastruktur, welche für den Einsatz von digitalen Signaturen notwendig ist, wurde in diesem Projekt die Zusammenarbeit mit einer externen Firma gewählt, die eine Public-Key-Infrastruktur (PKI) anbietet

Die Erfahrungen dieses Pilotprojekts sollen in die Formulierung einer verwaltungsweiten Sicherheitspolitik einfliessen. Diese hat zum Ziel, die sichere Kommunikation zwischen den verschiedenen Verwaltungsstellen und dieser Stellen mit interessierten Dritten und den Bürgerinnen und Bürgern auf der Basis einer Public-Key-Infrastruktur zu ermöglichen.

2. Umsetzung der Informatiksicherheitsverordnung

Leitfaden für öffentliche Organe

Die Informatiksicherheitsverordnung (ISV) setzt die Leitlinien für ein einheitliches und angemessenes Sicherheitsniveau bei den Informatiksystemen der kantonalen Verwaltung und derjenigen Stellen, die mit dieser Daten austauschen (vgl. Tätigkeitsbericht Nr. 3 [1997], S. 36). Ein Kernteam bestehend aus der Abteilung für Informatikplanung (AIP), der Informatikrevision des Amts für Informatikdienste (AID) und dem Datenschutzbeauftragten übernahm die Aufgabe, den Amtsstellen die notwendigen Hilfsmittel zur Verfügung zu stellen, um eine rasche und effiziente Umsetzung der notwendigen Sicherheitsmassnahmen zu gewährleisten.
In einem ersten Schritt wurde den Amtsstellen ein Paket von Sofortmassnahmen angeboten, welches ihnen ermöglichte, die wichtigsten Grundschutzmassnahmen umgehend und kostengünstig zu realisieren. Für die weiteren Schritte wurde ein Leitfaden erstellt, der für alle Stellen elektronisch erhältlich ist. Dieser ist nach den Vorgaben der ISV aufgebaut und beinhaltet die notwendigen Angaben für eine Risikoanalyse, das Erarbeiten der Schutzziele sowie die Erstellung entsprechender Massnahmenpakete. Als Grundlage für diesen Leitfaden diente in Bezug auf die Massnahmenpakete das vom deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn, herausgegebene IT-Grundschutzhandbuch.
An Informationsveranstaltungen und durch Publikationen wurden die verantwortlichen Organe auf die notwendigen Aktivitäten zur Umsetzung der ISV aufmerksam gemacht. Einzelne Direktionen wie beispielsweise die Direktion der Justiz und des Innern hatten in Bezug auf die Sicherheit der Informatik bereits Anstrengungen unternommen, so dass in deren Bereich die Umsetzung der ISV überwiegend abgeschlossen ist. Die ISV gibt für die bestehenden Informatiksysteme eine Umsetzungsfrist bis zum 31. März 2000 vor. Diese Frist sollte ausreichend sein, um in allen Bereichen die angemessenen Sicherheitsmassnahmen treffen zu können.
Gemäss § 18 ISV haben die verantwortlichen Organe die Angemessenheit der Sicherheitsmassnahmen regelmässig durch unabhängige interne oder externe Stellen überprüfen zu lassen. Der Datenschutzbeauftragte kann solche Überprüfungen vornehmen, aber auch anlassunabhängige Kontrollen durchführen.

3. PALAS – neues Personalverwaltungssystem

Sensible Datenbearbeitungen im Personalbereich

Nachdem der Kanton Zürich ein neues Personalrecht geschaffen hat (vgl. Tätigkeitsberichte Nr. 1 [1995], S. 14, und Nr. 3 [1997], S. 41), sollte auch ein den modernen Anforderungen des Personalwesens angepasstes Personalinformationssystem eingeführt werden. Auch dieses System hat den datenschutzrechtlichen Rahmenbedingungen insbesondere in Bezug auf die Sicherheit zu genügen.

An die Stelle des bisherigen Personalinformationssystems soll ein System treten, das auch vermehrt die Bedürfnisse der dezentralen Personalstellen in den einzelnen Direktionen abdeckt. Mit einer zentralen und verschiedenen dezentralen Komponenten war klar, dass ein reger Datenaustausch in diesem Verbund stattfinden wird. Da mit diesem Personalsystem beabsichtigt ist, teilweise besonders schützenswerte Personaldaten zu bearbeiten, mussten von Anfang an die Anforderungen an die Sicherheit angemessen berücksichtigt werden. In der Ausschreibung des Projektes wurde deshalb festgehalten, dass die Vertraulichkeit und die Authentizität des Datenverkehrs im gesamten System gewährleistet werden müsse. Idealerweise geschieht dies heutzutage mit einer Chiffrierung der Daten auf der Anwendungsebene. Anscheinend waren aber solche modernen

Anwendungen im Personalbereich im Markt (noch) nicht erhältlich; auf jeden Fall entschieden sich die verantwortlichen Stellen für ein System, das diesen Anforderungen nicht genügte.
Wir legten deshalb Wert darauf, dass in der Vorstudie, welche der Realisation des Gesamtsystems voranging, die Frage der angemessenen Sicherheit der Personaldaten nochmals überprüft wurde. Schliesslich lag eine Lösung vor, die als Minimalvariante eine Verschlüsselung der Verbindungen vorsah, eventuell den Einsatz eines Verschlüsselungsprozessors auf der Ebene des Zentralsystems oder den Einsatz von digitalen Signaturen. Da letztere Lösung auch für die übrigen Bereiche der Verwaltung von Interesse wäre, wurde entschieden, diese Frage koordiniert anzugehen (siehe S. 34). Die neue Personalanwendung wird in Etappen eingeführt werden.

4. Sicherheit der Akten

Richtlinien und Anforderungen an die papiergebundene Information

Eine Arbeitsgruppe unter der Verantwortung der Direktion der Justiz und des Innern sowie der Staatskanzlei beschäftigte sich mit der Erarbeitung von Sicherheitsrichtlinien und -anforderungen für die papiergebundene Information.
In Ergänzung zum Konzept der Gebäudesicherheit und zur Informatiksicherheitsverordnung (siehe S. 35) sollten diese Richtlinien die Anforderungen für den richtigen Umgang mit Dokumenten, Akten usw. in der Verwaltung einheitlich regeln.

In Koordination mit den beiden erwähnten Projekten und in Anlehnung an die Informatiksicherheitsverordnung wurden drei Sicherheitsstufen definiert, abhängig von den möglichen Negativfolgen, die eine unbefugte Offenlegung der Informationen hervorrufen würde. Im Weiteren wurden die grundsätzlichen Sicherheitsanforderungen an die Informationen respektive Informationssammlungen festgehalten. Neben der Betrachtung der allgemeinen Informationsbearbeitung wurden insbesondere Anweisungen verfasst für den Versand und die Verpackung, die Aufbewahrung am Arbeitsplatz, die Mitnahme, die Zwischenarchivierung sowie die Vernichtung und Entsorgung von Dokumenten.
Die Richtlinien sind vom Regierungsrat für verbindlich erklärt worden. Die Amtsstellen haben Massnahmenpläne zu erstellen, die periodisch auf ihre Einhaltung und die Angemessenheit der getroffenen Massnahmen hin zu überprüfen sind.
Mit diesen Richtlinien liegen für die Verwaltungsstellen weitere praxisbezogene Handlungsanweisungen vor, um sie bei der Umsetzung der Informationssicherheit zu unterstützen.

5. Messung der Patientenzufriedenheit

Organisatorische Massnahmen zur Sicherstellung des Datenschutzes

Im Rahmen eines Spitalreformprojektes plante die Gesundheitsdirektion als flankierende Massnahme zur Einführung einer leistungsorientierten Spitalfinanzierung die Ergebnisqualität der Spitalleistung zu erfassen und dabei auch auf eine Messung der Patientenzufriedenheit abzustellen. Ein solches Projekt wurde dem Datenschutzbeauftragten zur Beurteilung vorgelegt.
Das Projekt sah die wöchentliche Lieferung der Adressdateien der Patientinnen und Patienten mit zusätzlichen Angaben unter anderen zum Austrittsdatum durch die betroffenen Spitäler an eine Drittfirma vor, die mit der Befragung beauftragt wurde. Die Adressdaten werden dabei für den Versand eines Fragebogens und – falls dieser nicht innert einer bestimmten Frist zurückgesandt wird – einer Erinnerung verwendet. Anschliessend sollten diese Daten vernichtet werden. Der Fragebogen selber kann anonym ausgefüllt

werden, wobei auch auf den Zweck der Befragung und die Freiwilligkeit hingewiesen wird.
Aus datenschutzrechtlicher Sicht war festzuhalten, dass Daten aus dem Gesundheitsbereich zu den besonders schützenswerten Personendaten gehören (§ 2 lit. d Ziff. 2 DSG) und zusätzlich durch das Patientengeheimnis auch strafrechtlich geschützt sind (Art. 321 Strafgesetzbuch [StGB]).
Eine Bekanntgabe oder Weitergabe von Gesundheitsdaten einer Person (worunter auch bereits die Tatsache des Aufenthaltes in einem bestimmten Krankenhaus fällt) verlangt deshalb eine klare Rechtsgrundlage (§ 8 DSG in Verb. mit § 5 DSG; Art. 321 Abs. 3 StGB) oder im Einzelfall die Einwilligung der betroffenen Person (§ 8 lit. b DSG; Art. 321 Abs. 2 StGB).

Auch für nicht personenbezogene Zwecke wie Forschung, Planung und Statistik dürfen Personendaten nur weitergegeben werden, sofern keine Geheimhaltungspflicht dies ausschliesst (§ 12 Abs. 2 lit. b DSG; Art. 321bis StGB).
Sofern keine Personendaten weitergegeben werden, d.h. die Daten so anonymisiert werden, dass der Datenempfänger keinen Rückschluss auf eine bestimmte Person ziehen kann, sind diese (datenschutz)rechtlichen Voraussetzungen unbeachtlich.

Mit einer Änderung des Ablaufschemas der Befragung – es werden keine Patientennamen mehr bekannt gegeben, sondern nur noch Patientennummern, wobei die Verbindung zu einem bestimmten Namen einzig beim Spital bleibt – konnte garantiert werden, dass keine Personendaten den Bereich der Krankenhäuser verliessen, weshalb die Frage nach der klaren Rechtsgrundlage oder dem Vorliegen einer Einwilligung der betroffenen Personen obsolet wurde. Ob eine klare Rechtsgrundlage für das ursprünglich gewählte Vorgehen bestand oder ob Einwilligungen der betroffenen Personen vorlagen, war zum Beurteilungszeitpunkt offen.

Das nunmehr gewählte Vorgehen zeigt auf, wie bei einem an sich sensiblen Datenfluss, der hohe Risiken für die Verletzung von Persönlichkeitsrechten betroffener Personen beinhalten kann, mit organisatorischen Massnahmen diese Risiken sehr stark minimiert werden können.

Vermittlung von aktuellen Informationen

Das Bedürfnis nach aktuellen und kompetenten Informationen im Bereich von Datenschutz und Informationssicherheit wächst dauernd.

1. Drittes Symposium für Datenschutz und Informationssicherheit

Wachsende Aktualität und zunehmendes Interesse

Bereits zum dritten Mal führten wir zusammen mit der ETH Zürich das Symposium für Datenschutz und Informationssicherheit durch. Dabei zeigte sich, dass die Fragestellungen in diesem Bereich zunehmend an Aktualität gewinnen und auf ein immer breiteres Echo stossen: Rund 350 Personen nahmen an diesem Symposium teil.

Thematische Schwerpunkte wurden durch Referate zu spezifischen Fragen im Gesundheitsbereich, zur Sicherheit als Erfolgskomponente, zur EU-Datenschutzrichtlinie und zur allgemeinen Situation im Bereich Datenschutz und Informationssicherheit abgedeckt. Regierungsrat Dr. Markus Notter begrüsste die Teilnehmerinnen und Teilnehmer und wies auf die Bedeutung und Wichtigkeit einer konsequenten Umsetzung des Datenschutzgesetzes zur Sicherstellung der Grundrechte der betroffenen Personen in einer Zeit der zunehmenden Informatisierung der Gesellschaft hin. Damit wurde auch das Spannungsfeld zwischen Recht und Technik angeschnitten, das sich einerseits – aus rechtlicher Sicht – bei der Frage zeigt, wie die Technologieentwicklung mit rechtlichen Rahmenbedingungen grundrechtskonform genutzt werden kann, und wo andererseits – aus informationstechnischer Sicht – sich gerade die Frage stellt, wie eine vertrauenswürdige Sicherheitsinfrastruktur zu diesem Zweck aufgebaut werden kann. Diese Standortbestimmung wurde von den beiden Veranstaltern, Prof. Dr. Ueli Maurer und Dr. Bruno Baeriswyl, vorgenommen. Zu den Entwicklungen der Datenschutzkonzepte und deren absehbaren Neuerungen referierte Prof. Dr. Spiros Simitis. Das Referat zu Datenschutz und Datensicherheit als Qualitätsmerkmal (Prof. Dr. Alfred Büllesbach) und ein Praxisbericht zur Umsetzung eines Sicherheitskonzeptes in einer Bank (PD Dr. Hannes P. Lubich) zeigten auf, wie diese Elemente wachsende Bedeutung in einem wettbewerbsorientierten Markt haben.
Neue Bedingungen für den internationalen Datenaustausch beinhaltet die EU-Richtlinie, zu deren aktuellem Umsetzungsstand sich Dr. Ulf Brühann äusserte.
Im Bereich des Gesundheitswesens lagen die Schwerpunkte bei der Telemedizin (Dr. Joachim Jacob), den Datenflüssen im schweizerischen Gesundheitswesen (lic. iur. Michael Schnyder) sowie der Sicherheit von klinischen Informationssystemen (Dr. Ross J. Anderson).
Prof. Dr. Marlis Buchmann rundete die Beiträge mit einer soziologischen Analyse der Wechselbeziehung zwischen Technologie und Menschenbild ab.

Das 4. Symposium für Datenschutz und Informationssicherheit findet am 28. Oktober 1999 statt.

2. Sensibilisierung für die Anliegen des Datenschutzes

Effiziente Gestaltung der Informationen

Die Information über die Anliegen des Datenschutzes und der Informationssicherheit gehört zu den wichtigsten Aufgabenschwerpunkten des Datenschutzbeauftragten. Bisher konnte dem wachsenden Bedürfnis nach Informationen in diesem Bereich in unterschiedlicher Form begegnet werden.
«Fakten» – die Zeitschrift für Datenschutz des Kantons Zürich wurde auch 1998 vierteljährlich herausgegeben. Die praxisbezogenen Beiträge stiessen sowohl in der kantonalen als auch in den kommunalen Verwaltungen auf grosses Interesse.
Die Broschüre «In punkto Datenschutz», die Informationen für die öffentlichen Organe und für

betroffene Personen enthält, war innert kurzer Zeit vergriffen, weshalb eine zweite Auflage gedruckt werden musste.
Die Homepage des Datenschutzbeauftragten (www.zh.ch/dsb oder www.datenschutz.ch) wurde laufend aktualisiert, was ein sehr positives Echo bei den Benutzerinnen und Benutzern hervorrief.
Auch die Seminare, die der Datenschutzbeauftragte im Rahmen der Aus- und Weiterbildung durchführte, erhielten durchwegs gute bis sehr gute Qualifikationen. Diese Seminare sind ein wichtiger Beitrag für die verantwortlichen Organe, praxisbezogen auf die wichtigsten Problembereiche hingewiesen zu werden und Lösungsansätze kennen lernen zu können.
Mit Referaten und Beiträgen in Fachzeitschriften und Zeitungen nahmen wir weiter zu Schwerpunkten des Datenschutzes Stellung.

Auf Grund der wachsenden Nachfrage nach kompetenten Informationen und der beschränkten Ressourcen des Datenschutzbeauftragten wurde nach einer Optimierung der Informationsvermittlung gesucht. Überlegungen hierzu zeigten, dass die Informationen zukünftig zielgruppenspezifischer aufbereitet werden müssen, was bedeutet, dass neben den bisherigen Mitteln auch neue Medien und Formen als Träger von Informationen zu Datenschutz und Informationssicherheit in Betracht zu ziehen sind. Erste diesbezügliche Projekte wurden in Angriff genommen, so dass bereits im 1999 neu gestaltete Seminare im Rahmen der kantonalen Aus- und Weiterbildung angeboten werden können.

3. Register der Datensammlungen

Veröffentlichung im Internet

Öffentliche Organe, welche Personendaten bearbeiten, sind verpflichtet, ein öffentliches Register der von ihnen angelegten Datensammlungen zu führen (§ 15 Abs. 1 DSG). Im kantonalen Bereich werden die Register vom Datenschutzbeauftragten auch zentral geführt (§ 16 DSG), und dieses zentrale Register ist zu veröffentlichen. Im Tätigkeitsbericht Nr. 2 (1996), S. 21 ff., haben wir über die Zielsetzungen und den Stand der Registrierung berichtet.
Inzwischen haben wir die Register – soweit sie von den verantwortlichen Organen vollständig erfasst sind – im Internet veröffentlicht und auf unserer Homepage zum Abruf bereitgestellt.
Jede interessierte Person kann ausserdem beim Datenschutzbeauftragten Einsicht in das zentrale Register nehmen oder Auszüge daraus bestellen. Dadurch erhalten betroffene Personen Transparenz über die Bearbeitung ihrer Daten durch kantonale Behörden und können bei verantwortlichen Organen ihr Auskunftsrecht gemäss § 17 DSG geltend machen.

Die Form der Veröffentlichung des zentralen Registers im Internet ermöglicht, dass die Publikation mit geringem Aufwand regelmässig aktualisiert werden kann. Die Reorganisation der Verwaltungsstrukturen hat zu einem Nachführungsbedarf geführt, dem namentlich die Direktion für Soziales und Sicherheit in vorbildlicher Weise nachgekommen ist.
Bei anderen Direktionen mussten oder müssen Anpassungen durch uns vorgenommen werden. Zwei Direktionen haben die Registrierung ihrer Datensammlungen bis Ende des Berichtsjahres nicht abgeschlossen, obschon die Frist dazu bereits am 31. Dezember 1996 abgelaufen war.

Für die Gemeinden hatte der Regierungsrat die Frist für die Registrierung bis zum 30. Juni 1997 verlängert. Der Grossteil der Gemeinden ist der Registrierungspflicht nachgekommen.
Im Rahmen der Aufsicht über die Gemeinden kontrollieren die Bezirksräte teilweise auch, ob ein Register der Datensammlungen vorhanden ist. Dabei wurde festgestellt, dass Register bestehen, welche den gesetzlichen Anforderungen nicht genügen.
In einzelnen Gemeinden musste gar beanstandet werden, dass das Register gänzlich fehlte.

Transparenz in Recht und Praxis

Bei sensiblen Datenbearbeitungen, die bereits früher Gegenstand unserer Tätigkeitsberichte waren, stellen sich weiterhin Fragen in Bezug auf die Rechtsgrundlage und die Praxis.

1. Datenbearbeitungen über arbeitslose Personen

Missachtung der Schweigepflicht

Die Thematik der Weitergabe von Listen über arbeitslose Personen an die Gemeinden beschäftigte uns im Berichtsjahr erneut. Die Gemeinden haben seit der 1995 erfolgten Änderung im Arbeitslosenversicherungsrecht keine direkten Aufgaben im Arbeitslosenversicherungs- und Arbeitsvermittlungsbereich mehr zu erfüllen. Sie dürfen von den Organen der Arbeitslosenversicherung und der Arbeitsvermittlung Daten über arbeitslose Personen auf Grund einer konkreten Anfrage im begründeten Einzelfall, auf Grund einer schriftlichen Einwilligung der betroffenen Person oder in anonymisierter Form erhalten (siehe Tätigkeitsbericht Nr. 2 [1996], S. 24 f.).
Die regelmässige Weitergabe von Listen über arbeitslose Personen, deren Rahmenfrist für den Bezug von Leistungen abläuft (auch «Aussteuerung» genannt), ist nicht erforderlich. Für die Budgetplanung der Gemeinden sind anonymisierte Listen ausreichend. Das Sozialhilfegesetz und das (kantonale) Gesetz über Leistungen an Arbeitslose gehen zudem vom Grundsatz aus, dass die Hilfe suchende Person von sich aus ein Gesuch einzureichen und die erforderlichen Angaben zu machen hat. Die betroffenen Personen werden in den Beratungsgesprächen vom Regionalen Arbeitsvermittlungszentrum (RAV) auf diese Möglichkeiten hingewiesen.

Von dritter Seite wurden wir darauf aufmerksam gemacht, dass ein RAV den Gemeinden seines Zuständigkeitsbereiches dennoch Listen über arbeitslose Personen weiterleitet, deren Rahmenfrist für den Bezug von Leistungen abläuft. Die Listen enthielten im konkreten Fall nicht nur Daten über die in der jeweiligen Gemeinde wohnhaften Personen, sondern auch über andernorts Ansässige, was – selbst wenn Rechtsgrundlagen bestünden – eine unverhältnismässige Datenbekanntgabe darstellte. Die fragliche Weitergabe der Listen ist aber bereits mangels Rechtsgrundlagen als rechtswidrig zu bezeichnen.
Unsere Intervention beim Amt für Wirtschaft und Arbeit (AWA) führte dazu, dass das betreffende RAV zur Einhaltung der gesetzlichen Vorschriften angewiesen wurde.

Gegen Ende des Berichtsjahres wiesen uns dann aber sowohl betroffene Personen als auch ein Mitarbeiter einer Sozialhilfebehörde darauf hin, dass Gemeinden von den RAVs weiterhin bzw. erneut regelmässig Listen der arbeitslos gemeldeten Personen erhielten. Die Beanstandungen bezogen sich diesmal auf verschiedene (andere) RAVs und Gemeinden. Unsere Abklärungen ergaben, dass diese neuerlichen Mitteilungen der RAVs auf eine «Praxisänderung» des Bundesamtes für Wirtschaft und Arbeit zurückzuführen waren. Wir wandten uns darauf an den eidgenössischen Datenschutzbeauftragten. Die Frage, wie diese «Praxisänderung» zu begründen ist, befindet sich in Abklärung. Fest steht bisher nur, dass keine Rechtsänderung erfolgt ist, welche die «Praxisänderung» rechtfertigen könnte.

Ein ähnlicher Fall betraf einen Verein, der Beschäftigungsprogramme durchführt. Die Geschäftsleitung fragte, ob den Mitgliedgemeinden des Trägervereins mitgeteilt werden dürfe, welche ihrer Einwohnerinnen und Einwohner an einem Arbeitseinsatz teilnehmen. Da auch Trägerschaften solcher Programme unter der Schweigepflicht nach Art. 97 Arbeitslosenversicherungsgesetz stehen, gelten hier die gleichen Voraussetzungen wie im vorstehend dargelegten Fall. Aus der Mitgliedschaft im Verein können die Gemeinden allenfalls einen Anspruch auf anonymisierte Angaben ableiten; die Vereinsmitgliedschaft vermag jedoch keine zwingenden Rechtsnormen zu durchbrechen. Erhält eine

Person, die von einer Gemeinde delegiert wird, bei der Mitarbeit im Verein Kenntnis von Personendaten, steht sie ebenfalls unter der erwähnten Schweigepflicht. Auch das Zweckbindungsgebot nach § 4 Abs. 4 DSG verbietet in diesem Fall, dass Informationen an die Gemeindebehörden weitergegeben werden.

2. Verordnung über geografische Informationssysteme

Wenig transparente Rechtslage

Bei der Beurteilung des Projekts des GIS-Dienstleistungszentrums (GIS-DLZ) über die Zusammenführung von geografischen Daten verschiedener öffentlicher Organe hatten wir darauf hingewiesen, dass Rechtsgrundlagen fehlten (vgl. Tätigkeitsbericht Nr. 2 [1996], S. 16 f.). Der Regierungsrat hat daraufhin eine Verordnung über geografische Daten und Informationssysteme in der kantonalen Verwaltung (GIS-Verordnung) erlassen.
Die GIS-Verordnung statuiert eine Koordinations- und Informationspflicht, die integrierte und koordinierte Lösungen für eine kostengünstige Bearbeitung und Nutzung von raumbezogenen Daten fördern soll. Sie regelt ausserdem die Organisation der GIS-Organe und das Verfahren. Die Bestimmungen über die Verantwortung gehen davon aus, dass für den Datenschutz und die Datensicherheit dasjenige Organ verantwortlich ist, welches die Daten zur Erfüllung seiner gesetzlichen Aufgaben bearbeitet; die Bearbeitung der Daten bzw. der Umgang mit den einzelnen Datenkategorien (Pläne, Kataster usw.) richtet sich nach dem bereichsspezifischen Recht (z.B. Planungs- und Baugesetz).
Das GIS-DLZ ist grundsätzlich wie ein beauftragter Dritter im Sinne von § 13 DSG zu betrachten, wobei es gewisse Kompetenzen in Bezug auf den Erlass technischer und administrativer Vorschriften hat. Es kann jedoch keine Bearbeitungen aus eigenem Recht vornehmen. Widersprüchlich ist daher die Regelung der GIS-Verordnung über die Datenabgabe, die selber materielle Vorschriften aufstellt. Das Verhältnis dieser Bestimmungen zu den bereichsspezifischen Rechtsgrundlagen, die teilweise in übergeordneten Erlassen stehen (Bundesrecht, kantonale Gesetze), wurde trotz Anregungen unsererseits bisher nicht umfassend untersucht.
Problematisch ist im Weiteren die technisch realisierte Zusammenführung der verschiedenen Daten und Datenkategorien. Dadurch entstehen Kombinationsmöglichkeiten, welche unter Umständen dem Zweckbindungsgebot nach § 4 Abs. 4 DSG widersprechen. Auch in dieser Hinsicht ist die Rechtslage nicht geklärt.
Als weiterer Aspekt tritt die Frage der Kommerzialisierung von Verwaltungsdaten hinzu. Personenbezogene Daten werden durch Gemeinwesen meist auf Grund von Mitwirkungspflichten der Betroffenen beziehungsweise auf Grund eines hoheitlichen Rechtsverhältnisses bearbeitet. Die Behörden trifft deshalb eine besondere Verantwortung im Umgang mit diesen Daten. Auch hier verlangt das datenschutzrechtliche Zweckbindungsgebot entsprechende Vorgehensweisen (Erlass von im öffentlichen Interesse liegenden Rechtsgrundlagen durch das zuständige Legislativorgan, Wahrung der Verhältnismässigkeit, Schutzmassnahmen für die betroffenen Personen zur Wahrung ihrer Persönlichkeitsrechte).
All diese Aspekte wurden bisher zu wenig beachtet, obwohl wir wiederholt darauf hingewiesen hatten.
Die Problematiken der Datenbearbeitungen und -bekanntgaben im Rahmen des GIS zeigten sich anlässlich einer Anfrage. Die GIS-Verordnung sieht vor, dass der Datenschutzbeauftragte die Zulässigkeit der Abgabe von GIS-Daten an private Dritte im Online-Verfahren begutachtet. Die Anfrage betraf die Frage, ob interessierten Banken zur Abwicklung von Hypothekargeschäften Daten über die Schätzwerte der Gebäudeversicherungen im Online-Verfahren bekannt gegeben werden dürfen. Dabei sollte die Bank technisch Zugriff auf sämtliche Daten er-

halten und eine Verpflichtungserklärung abgeben, nur diejenigen Daten abzurufen, für welche eine schriftliche Zustimmung der betroffenen Person vorliegt. Der Abruf sollte protokolliert und stichprobenweise überprüft werden, wobei bei Verstössen entsprechende Sanktionen vorgesehen werden sollten (Sperrung, Konventionalstrafe). Die vorgesehene Lösung vermochte jedoch weder rechtlich noch technisch zu genügen. Bereits die Einrichtung einer Online-Zugriffsmöglichkeit stellt begrifflich eine Datenbekanntgabe dar, da das verantwortliche Organ die Herrschaft über die Bekanntgabe verliert. Die Voraussetzungen für die Bekanntgabe müssen daher bereits bei der Erteilung der Zugriffsberechtigungen erfüllt sein. Die Protokollierung der Zugriffe und entsprechende Kontrollen stellen angemessene Sicherheitsmassnahmen im Sinne von § 4 Abs. 5 DSG dar, vermögen aber für sich allein nicht zu genügen. Eine nachträgliche, stichprobenweise Kontrolle der Protokolle kann Missbräuche nicht mehr verhindern und nur in beschränktem Umfang aufdecken. Ausserdem kann dem Benutzenden bei einem unzulässigen Abruf von Daten kaum nachgewiesen werden, ob tatsächlich eine Missbrauchsabsicht oder lediglich eine unbeabsichtigte Fehlmanipulation vorgelegen hat.
Wir gaben deshalb verschiedene Empfehlungen ab und verlangten insbesondere, dass die Zugriffsmöglichkeiten auf Daten derjenigen Personen beschränkt werden, welche ihre Einwilligung erteilt haben, und dass selbst in diesen Fällen der Zugriff zeitlich (Dauer der Berechtigung) und/oder quantitativ (Anzahl der Abrufe der gleichen Daten) beschränkt wird.

Auch diese Anfrage hat den Handlungsbedarf im Bereich des GIS aufgezeigt, da keine Rechtsgrundlagen für die Datenbekanntgabe im Abrufverfahren bestehen und die Einrichtung und Ausgestaltung von Abrufverfahren auf der Grundlage von einzelfallweisen Einwilligungen kaum in effizienter Weise möglich ist.

3. Erklärung betreffend VPM-Mitgliedschaft

Rechtswidrige Praxis von Schulbehörden

In zwei Fällen wurden wir von betroffenen Personen informiert, dass sie im Anstellungsgespräch nach einer eventuellen Mitgliedschaft im «Verein zur Förderung der psychologischen Menschenkenntnis (VPM)» gefragt wurden respektive eine Erklärung unterzeichnen sollten, dass sie nicht Mitglied in diesem Verein seien, wobei eine Falschaussage gegebenenfalls die Auflösung des Anstellungsverhältnisses zur Folge haben könne.
Im Tätigkeitsbericht Nr. 3 [1997], S. 13 f., haben wir bereits in Bezug auf die Rechtslage bei der Frage nach einer eventuellen Vereinszugehörigkeit eines Stellenbewerbers oder einer Stellenbewerberin zusammenfassend Stellung bezogen. Diese Ausführungen basierten auf unserem Bericht vom 5. August 1997 an den Regierungsrat zur Zulässigkeit der Bearbeitung einer bestimmten Datenkategorie («Vereinszugehörigkeit») im Rahmen des Arbeitsverhältnisses. Nach diesen Ausführungen ist die einleitend geschilderte Praxis als rechtswidrig zu bezeichnen, da sich auf Grund der allgemeinen Fragen zur Eignung im Bewerbungsverfahren keine Hinweise ergaben, dass eine mangelnde Eignung allenfalls auf eine bestimmte Vereinszugehörigkeit zurückzuführen ist.
Zu Recht wandten sich die betroffenen Personen an den Datenschutzbeauftragten, der die verantwortlichen Organe auf die rechtswidrige Praxis hinwies. Durch diese Vermittlung konnte erreicht werden, dass auf die genannten Erklärungen verzichtet wurde, wobei in beiden Fällen ein Anstellungsverhältnis mit den betroffenen Personen zu Stande kam. Des Weiteren hat die Bildungsdirektion als Aufsichtsbehörde ihrerseits gegenüber einer betroffenen Person ihr Bedauern über dieses Vorgehen der Schulbehörde ausgedrückt.

Datenschutzbeauftragter
Kanton Zürich
Kurvenstrasse 31
8090 Zürich
Tel.: 01/259 39 99
Fax: 01/259 51 38
E-Mail: datenschutz@dsb.zh.ch
Homepage:
http://www.datenschutz.ch
http://www.zh.ch/dsb

Datenschutzbeauftragter:
Dr. iur. Bruno Baeriswyl

Juristisches Sekretariat:
Dr. iur. Esther Knellwolf
lic. iur. Marco Fey (ab 1.7.1999)

IT-Sicherheitsberatung und -Revision:
Andrea C. Mazzocco, CISA
(ab 1.7.1999)

Sekretariat:
Tanja Blass (ab 1.1.1999)

Tätigkeitsbericht Nr. 4 (1998)
ISSN 1422-5816

Konzeption und Produktion:
Homepage AG, Zürich

Druck:
KDMZ
Gedruckt auf Recyclingpapier

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