Nr. 6

Tätigkeits-Bericht

Datenschutzbeauftragter des Kantons Zürich

2000

Tätigkeitsbericht

Nr. 6
2000

Der Datenschutzbeauftragte erstattet dem Regierungsrat jährlich oder nach Bedarf einen Bericht über seine Tätigkeit (§ 23 Datenschutzgesetz). Der vorliegende Tätigkeitsbericht Nr. 6 deckt den Zeitraum vom 1. Januar 2000 bis 31. Dezember 2000 ab.

Zürich, Juni 2001

Der Datenschutzbeauftragte
des Kantons Zürich
Dr. Bruno Baeriswyl

Inhaltsverzeichnis

Steigende Nachfrage nach Datenschutz

Die rasante Entwicklung der Informationstechnologie ist weiterhin die treibende Kraft im Umfeld von Datenschutz und Datensicherheit. Das Datenschutzrecht erweist sich als eigentliches Technikfolgenrecht und ist deshalb grossen Herausforderungen ausgesetzt.

Die Informations- und Kommunikationsgesellschaft bedingt für viele Verwaltungsstellen sowie für die Bürgerinnen und Bürger einen neuen Umgang mit Daten und Informationen. Die veränderten Rahmenbedingungen verlangen nach neuen Lösungen in Bezug auf den Datenschutz und die Informationssicherheit. Immer häufiger werden daher die Dienste des Datenschutzbeauftragten für umfassende Beratungen und Stellungnahmen beansprucht.

Umfassende Datenbearbeitungen

Es gibt im Wesentlichen zwei Ursachen für die zunehmende Nachfrage nach Datenschutz:

- Die neuen Technologien erlauben eine umfassende Datenbearbeitung, sowohl was die Menge als auch was die Übermittlung oder Verknüpfung dieser Daten anbelangt. Die Kosten sind in diesem Bereich kein limitierender Faktor mehr, so dass in wachsendem Ausmass die vorhandenen Möglichkeiten ausgeschöpft werden.

- Die eingesetzte Kommunikationsinfrastruktur – das Internet – stellt die notwendigen Dienste für die Verfügbarkeit der Daten bereit, gleichzeitig sind die Daten aber in Bezug auf die Vertraulichkeit oder Integrität ungeschützt. Die «Unsicherheit» in der Datenbearbeitung wächst.

Daraus ergeben sich für die Datenbearbeitungen der Verwaltung zwei wesentliche Fragen:

- Wie kann die erforderliche Transparenz für die von der Datenbearbeitung betroffenen Bürgerinnen und Bürger geschaffen werden?
- Wie können die Daten im neuen technischen Umfeld wirksam geschützt werden?

Prinzipien setzen Rahmenbedingungen

Die Prinzipien der Gesetzmässigkeit, der Zweckbindung und der Verhältnismässigkeit bilden aus datenschutzrechtlicher Sicht die Rahmenbedingungen. Die Sicherheit der Daten ist durch angemessene technische und organisatorische Massnahmen zu gewährleisten.

Diesen Ansprüchen an die Datenbearbeitung kann in der Praxis nur gerecht werden, wer sowohl die rechtlichen Rahmenbedingungen wie auch die technischen Möglichkeiten bei deren Umsetzung kritisch hinterfragt. Das Spannungsfeld zwischen den rechtlichen Vorgaben und den technischen Realisierungen, das hierbei entsteht, darf nicht ignoriert werden.
Die Grundrechte der Personen zu schützen, über die Daten bearbeitet

werden, ist oberstes Gebot und Leitlinie für die Entwicklung von Lösungen (§ 1 DSG).
Dieser Schutz ist mit rechtlichen Mitteln allein nicht mehr durchsetzbar, ebenso müssen datenschutzfreundliche Technologien hierzu beitragen.

Die Hauptthemen im vergangenen Berichtsjahr sind geprägt von dieser Ausgangslage. Dabei ist es vielfach gelungen, angemessene Lösungen umzusetzen oder mindestens Lösungsansätze zu entwickeln.

Sensibles Gesundheitswesen

Die Datenbearbeitungen im Bereich des Gesundheitswesens geben weiterhin zu zahlreichen Fragen Anlass. Wiederholt wurde der Datenschutzbeauftragte von Spitälern angefragt, wie sie sich gegenüber den Kranken- und Unfallversicherern zu verhalten hätten, die immer häufiger ausführliche Berichte über Patientinnen und Patienten verlangen (siehe S. 34). Der Datenfluss vom Spital zu den Versicherern ist sowohl auf das Prinzip der Zweckbindung als auch auf den Grundsatz der Verhältnismässigkeit hin zu prüfen. Die zu medizinischen Zwecken verfassten Austrittsberichte sind kaum geeignet, die Vergütung von Leistungen festzusetzen oder die Wirtschaftlichkeit einer Behandlung abzuklären. Aus diesen Gründen kann nur im Einzelfall und auf konkrete Frage hin eine Datenbekanntgabe erfolgen. Wir haben den Spitälern empfohlen, nur in solchen Fällen Auskunft zu erteilen.
Angesichts der Sensibilität der Datenbearbeitungen im Gesundheitswesen wären vermehrt klare gesetzliche Regelungen wünschbar, die den Datenbearbeitungen Grenzen setzen. Eine Möglichkeit hierzu bietet das in die Vernehmlassung gegebene Patientenrechtgesetz. Aus datenschutzrechtlicher Sicht vermag dieser Entwurf aber nicht zu genügen (siehe S. 10). Allzu wenig ist er auf die betroffenen Patientinnen und Patienten ausgerichtet, die grundsätzlich «Geheimnisherr» der über sie bearbeiteten Daten sind. Angesichts der technologischen Entwicklungen im Bereich des Gesundheitswesens (E-Health) muss die Transparenz für die betroffenen Personen oberstes Prinzip sein.

Ausweitung sensibler Datenbearbeitungen

Klare Rechtsgrundlagen, die neuen Datenbearbeitungsmöglichkeiten Grenzen setzen, sind auch im Polizei- und Justizbereich notwendig. Die Verwendung von DNA-Analysen in der Strafuntersuchung birgt neue Risiken für die betroffenen Personen. Da auf Bundesebene ein Gesetzesentwurf in der parlamentarischen Beratung steht, beschränkt sich die neue DNA-Analysen-Verordnung im Kanton Zürich auf sehr allgemein gehaltene Bestimmungen (siehe S. 14). Weil das Prinzip der Verhältnismässigkeit nicht konkretisiert wurde – beispielsweise durch die Begrenzung mittels eines Deliktkataloges –, fehlt für betroffene Personen jegliche Transparenz im Hinblick auf die Anordnung einer DNA-Analyse.

Die Möglichkeit, dass beliebige Personen Telefongespräche aufnehmen dürfen, soll ebenfalls ausgeweitet werden. Die neue Regelung sieht vor, dass eine erst kürzlich eingeführte Strafbestimmung wieder aufgehoben werden soll (siehe S. 13 f.). Die Gelegenheit, in einer klaren Bestimmung zu regeln, ob und zu welchem Zweck eine Aufzeichnung erfolgt, wurde mit dem präsentierten Vorschlag verfehlt.

Transparente Datenbearbeitungen

Das Prinzip der Zweckbindung verlangt, dass den betroffenen Personen klar ist, mit welchen Absichten und Zielen Datenbearbeitungen erfolgen. In zahlreichen Fällen wandten sich Personen an den Datenschutzbeauftragten, weil sie einen Missbrauch ihrer Daten befürchteten. Im Rahmen der Einführung von Qualitätsmanagementsystemen dürfen Daten nicht anderen Zwecken zugeführt werden. Durch geeignete organisatorische und technische Massnahmen ist auszuschliessen, dass die erhobenen Daten missbräuchlich verwendet werden. Dies wiederum verlangt eine transparente Gestaltung der Prozesse (siehe S. 16 f.).

Wie eine Datenbearbeitung transparent gestaltet werden kann, zeigte eine durch betroffene

Personen ausgelöste Beratungstätigkeit: Verschiedene Personen, die sich in zürcherischen Gemeinden als Wochenaufenthalter anmeldeten, sahen sich mit einem Fragebogen konfrontiert, der detaillierte Auskünfte zu ihren Lebensverhältnissen beinhaltete (siehe S. 20 f.). Tatsächlich haben die Gemeinden bei einer Wohnsitznahme die Melde- und Steuerpflicht abzuklären. Die Umsetzung der erforderlichen Abklärungen erfolgte jedoch in den einzelnen Gemeinden recht unterschiedlich. Betroffene Personen beschwerten sich über zu weit gehende Eingriffe in ihre Privatsphäre. In Zusammenarbeit mit interessierten Fachverbänden erarbeiteten wir einen Fragenkatalog, den wir den Gemeinden für die standardmässig durchzuführenden ersten Abklärungen empfohlen haben. Der Musterfragebogen erlaubt den Gemeinden, ihre Aufgaben auf verhältnismässige Weise zu erfüllen, denn die Fragen beschränken sich auf das erforderliche Minimum, das zur Aufgabenerfüllung notwendig ist. Damit wird diese Datenbearbeitung für die betroffenen Personen transparent.

Auswirkungen neuer Technologien

Sehr aufmerksam beobachten wir die Auswirkungen der neuen Technologien auf die Sicherheit der Datenbearbeitungen. Diese ist nur gewährleistet, wenn alle Komponenten eines Datenbearbeitungsprozesses einbezogen werden. Sollen sensible Patientendaten über das Internet ausgetauscht werden, ist eine umfassende Verschlüsselung notwendig (siehe S. 21). Es genügt also nicht, nur Teilstrecken der Übermittlung zu verschlüsseln und lediglich das Netzwerk zu beachten. Alle Applikationen, die sensible Daten bearbeiten, sind mit entsprechenden Massnahmen abzusichern.
Dieselbe Ausgangslage ergibt sich beim Betrieb des kantonalen Informatiknetzwerkes (siehe S. 21 f.). Im Projekt «LeuNet» steht die Auslagerung des Informatikbetriebes an eine Drittfirma im Vordergrund. Aus datenschutzrechtlicher Sicht ist der Betrieb eines Netzwerkes durch Dritte möglich. Eine solche Variante verlangt aber von den verantwortlichen Organen vermehrte Anstrengungen, umfassende Sicherheitsmassnahmen für ihre Applikationen zu treffen.

Aufbau einer Sicherheitsinfrastruktur

Der Kanton Zürich hat entschieden, für die Abdeckung der neuen Sicherheitsbedürfnisse eine Public Key Infrastructure (PKI) aufzubauen (siehe S. 30 f.). Das unter der Leitung des Datenschutzbeauftragten stehende Projekt soll für bestehende und zahlreiche neue Applikationen, wie sie im Rahmen der E-Government-Initiative entwickelt werden, die Basissicherheitsinfrastruktur bilden. Das Projekt SOPRANO hat damit wegweisende Funktion für die Art und Weise, wie Lösungen im Sicherheitsbereich vorausdenkend und umfassend angegangen werden sollen.

Durch eine permanente Beratungstätigkeit und gezielte Seminare konnten wir im vergangenen Jahr in verschiedenen weiteren Bereichen auf das zunehmende Gefährdungspotenzial der neuen Technologien reagieren. In Internet-Seminaren wurden die Informatikverantwortlichen der Gemeinden mit den neuesten Entwicklungen in puncto Datenschutz und Informationssicherheit vertraut gemacht (siehe S. 23).

Regelmässige Kontrolltätigkeit

Ein wirksamer Datenschutz erfordert systematische Kontrollen. Die Datenschutzreview ist das geeignete Mittel hierzu (siehe S. 32 f.). Bei ausgewählten Amtsstellen konnten die ersten Reviews durchgeführt werden. Das Ziel dieser Kontrollen ist einerseits die Sensibilisierung der betroffenen Stellen für bestimmte Aspekte der Datenbearbeitung und andererseits – wo notwendig – die Behebung von Mängeln im rechtlichen, organisatorischen und technischen Bereich.
Die Prüfungen sind in die Bereiche Recht und Informatiksicherheit unterteilt und lehnen sich an das Vorgehen der Informatikrevision an. Die geprüften Amtsstellen haben die Prüfungen positiv bewertet und die Empfehlungen des Datenschutzbeauftragten gut

aufgenommen. Die professionelle Aufsicht gehört zu den vertrauensbildenden Massnahmen, die unabdingbar sind für einen wirksamen Datenschutz. Im Rahmen der zur Verfügung stehenden Mittel soll sie deshalb weitergeführt werden.

Wachsendes Informationsbedürfnis

Das Informationsbedürfnis von Verwaltung und Bevölkerung ist angesichts der geschilderten rasanten technologischen Veränderungen ungebrochen hoch. Es gehört deshalb zu den ständigen Aufgaben des Datenschutzbeauftragten, die notwendige Information sicherzustellen. Um vermehrt zielgruppenspezifisch informieren zu können, wurde das Informationskonzept überarbeitet (siehe S. 39 f.). Im elektronischen Bereich erweisen sich die Homepage des Datenschutzbeauftragten (www.datenschutz.ch) und das virtuelle Datenschutzbüro (siehe S. 39) als die geeigneten Plattformen für die Vermittlung aktueller Informationen. Weitergehende Themen können in der neuen Zeitschrift «digma» publiziert oder am «Symposium on privacy and security» erörtert werden. Damit werden «Fakten» – die Zeitschrift für Datenschutz des Kantons Zürich – sowie das bisherige Symposium für Datenschutz und Informationssicherheit in neue Formen eingebunden. Die für die Informationstätigkeit vorhandenen Mittel können zukünftig besser eingesetzt werden (siehe S. 38 und S. 41).

Neuer Datenschutz

An einer Informationsveranstaltung konnten im vergangenen Jahr neue Instrumente für einen effizienten Datenschutz vorgestellt und diskutiert werden (siehe S. 28 f.). Die Erfahrungen aus fünf Jahren Datenschutzgesetz im Kanton Zürich zeigten, dass die Informatisierung der Verwaltung und die damit verbundene Zunahme der Datenbearbeitungen in allen Bereichen viele Fragen des Datenschutzes und der Informationssicherheit in den Vordergrund rückten. Um den Schutz der Privatsphäre auch unter den veränderten gesellschaftlichen und technischen Bedingungen gewährleisten zu können, wurden 10 Punkte für einen wirksamen Datenschutz erarbeitet und publiziert (siehe S. 28 f.). Sie sollen die Leitlinie für die zukünftige Entwicklung des Datenschutzes im Kanton Zürich bilden.

Veränderungen für die Zukunft

Die im vorliegenden Bericht dargestellten Tätigkeiten weisen auf das dynamische Umfeld hin, in welchem Datenschutz und Informationssicherheit zu gewährleisten sind. Durch die technische Entwicklung ergeben sich für den Datenschutz neue Herausforderungen. Bei betroffenen Personen entsteht das latente Gefühl, immer mehr Eingriffe in die Privatsphäre dulden zu müssen. Tatsächlich bringen die neuen Technologien vermehrt Risiken für den Datenschutz und die Datensicherheit mit sich. Technischer Fortschritt darf jedoch nicht automatisch zu einer Einschränkung der Privatsphäre führen.
Vermehrt wird deshalb in Zukunft auch die gesellschaftliche Rolle von Datenschutz und Sicherheit diskutiert werden müssen. In der Entwicklung der Informations- und Kommunikationsgesellschaft sind dies Schlüsselthemen.
Die Tätigkeit des Datenschutzbeauftragten soll sowohl einen Beitrag an diese zukünftigen Diskussionen leisten als auch pragmatische Lösungen für anstehende Fragen entwerfen. Ziel bleibt es, die Grundrechte der Personen, über die Daten bearbeitet werden, zu schützen. Wir richten alle unsere Anstrengungen darauf, dass dieser Schutz auch in Zukunft gewährleistet ist.

Wachsendes Bedürfnis nach umfassender Beratung

Immer häufiger werden die Dienste des Datenschutzbeauftragten für umfassende Beratungen und Stellungnahmen beansprucht.

GESUNDHEITSWESEN

1. Gesetzliche Verankerung der Patientenrechte

Mangelnde datenschutzrechtliche Bestimmungen

Im Rahmen der Totalrevision des Gesundheitsgesetzes soll auch ein Patientenrechtsgesetz geschaffen werden. Ziel ist es, die bisher nur rudimentär auf Verordnungsstufe geregelten Patientenrechte als formelles Gesetz neu zu fassen. Trotz der grossen Bedeutung datenschutzrechtlicher Aspekte (siehe auch Tätigkeitsberichte Nr. 5 [1999], S. 9 und Nr. 2 [1996], S. 40) wurden wir nicht in die Arbeiten einbezogen. Im Nachhinein stellten wir fest, dass der Entwurf eine unübersichtliche und teilweise widersprüchliche Regelung der Datenbearbeitungen enthält und einzelne Fragen unbeantwortet lässt. Unsere Anregungen wurden jedoch nicht mehr berücksichtigt; der Gesetzesentwurf wurde in die Vernehmlassung gegeben.
Im Vernehmlassungsverfahren brachten wir die folgenden Vorbehalte an:

- Der Entwurf versucht, zwischen allgemeinen Informationen über den Gesundheitszustand und Informationen aus der Krankengeschichte zu unterscheiden und beide Bereiche gesondert zu regeln. Dabei wird verkannt, dass die Krankengeschichte die Quelle aller medizinischen Informationen ist und die vorgenommene Differenzierung in der Praxis zu Unklarheiten und Rechtsunsicherheit führen wird. Insbesondere wird zu wenig klar geregelt, welche Drittpersonen (Bezugspersonen, gesetzliche Vertretung, nachbehandelndes Medizinalpersonal?) welche Informationen (Gesundheitszustand, Diagnose, Behandlungen, Berichte?) erhalten und welche Voraussetzungen dazu erfüllt sein müssen (ausdrückliche Zustimmung, vermutete Zustimmung, gesetzliches Mitteilungsrecht?). Es besteht die Gefahr, dass sich das Medizinalpersonal oft an der Grenze zur strafbaren Verletzung des medizinischen Berufsgeheimnisses nach Art. 321 Strafgesetzbuch bewegen wird.

- Es ist klar zu regeln, wie lange Krankengeschichten aufzubewahren sind. Statt einer Mindestaufbewahrungsdauer ist eine befristete Aufbewahrungsdauer zu bestimmen, nach deren Ablauf feststeht, dass die Krankengeschichte entweder archiviert oder vernichtet wird. Wünscht die Patientin oder der Patient die weitere Aufbewahrung, kann sie/er dies verlangen (Aufbewahrung mit Einwilligung) oder sich die Krankengeschichte herausgeben lassen. Den (berechtigten) Forschungsinteressen kann Rechnung getragen werden, indem die Krankengeschichte nach Ablauf der Aufbewahrungsdauer anonymisiert wird und damit unter datenschutzrechtlichen Gesichtspunkten weiter aufbewahrt werden kann. Dazu bedarf es einer Bestimmung, wonach die Krankengeschichte so geführt werden muss, dass sie nach Ablauf der Aufbewahrungsfrist anonymisiert werden kann.

- Die im Gesetzesentwurf vorgesehenen Bestimmungen über das Auskunftsrecht weichen in verschiedenen Punkten von der Regelung des DSG ab, ohne dass hierfür öffentliche Interessen bestehen. So wird etwa das Berichtigungsrecht gänzlich ausgeschlossen, obwohl eine Einschränkung genügen würde.

- Die sensiblen Datenbearbeitungen im Gesundheitswesen verlangen nach klaren Bestimmungen. Der Entwurf des Patientenrechtsgesetzes wird diesem Anspruch nur teilweise gerecht.

2. Einsicht in Krankengeschichte verstorbener Personen

Schwierige Interessenabwägung

Nach dem Tod ihres Mannes wandte sich dessen Witwe an die Spitäler bzw. Ärzte, die ihn behandelt hatten, und bat sie um Herausgabe der lückenlosen Krankengeschichte. Die angefragten Spitäler und Ärzte beantragten bei der Gesundheitsdirektion die Entbindung von der ärztlichen Schweigepflicht. Die Anträge wurden abgelehnt, worauf die Witwe die nochmalige Überprüfung und Gutheissung wünschte. Weil die Gesundheitsdirektion ihren ablehnenden Entscheid mit datenschutzrechtlichen Argumenten begründet hatte, ersuchte sie den Datenschutzbeauftragten, die Begründung zu prüfen.
Die Praxis der Gesundheitsdirektion ist nach Auffassung des Datenschutzbeauftragten aus folgenden Gründen nicht zu beanstanden:

- Die besonders sensiblen Gesundheitsdaten sind durch die ärztliche Schweigepflicht respektive das Patientengeheimnis geschützt. Nur die betroffene Person kann als Geheimnisherr die Medizinalperson von der Schweigepflicht entbinden. Mit ihrem Tod geht diese Möglichkeit unter, die Schweigepflicht bleibt jedoch bestehen. In Frage kommt dann nur noch deren Aufhebung durch die Gesundheitsdirektion (als Aufsichtsbehörde). Diese hat in jedem Fall eine Interessenabwägung vorzunehmen und zu entscheiden, ob die Interessen der nahen Verwandten an der Kenntnis der Gesundheitsdaten schwerer wiegen als das Interesse des Verstorbenen an der weiteren Geheimhaltung seiner Daten.

- Die Patientenrechtsverordnung sieht vor, dass Drittpersonen mit dem Einverständnis des Patienten durch die behandelnden Ärzte informiert werden dürfen und dass dieses Einverständnis bei Nachfragen der engsten Angehörigen vermutet wird. Damit wird allerdings lediglich eine allgemeine Information über Krankheitszustand und -verlauf ermöglicht und keineswegs ein umfassendes Einsichtsrecht der Angehörigen in die Krankengeschichte.

- Die Hinterbliebenen sind also einerseits unter keinem Titel berechtigt, umfassend Einblick in Spital- oder Arztdossiers zu nehmen. Andererseits benötigen sie detaillierte Informationen, falls sie den Verdacht haben, die behandelnden Ärzte seien für den Tod ihres Verwandten verantwortlich. Für die Begründung einer Klage benötigen sie Kenntnisse, die ihnen die verantwortlichen staatlichen Organe zur Verfügung stellen müssen. Theoretisch erstreckt sich also das Informationsrecht der Hinterbliebenen auf Angaben bezüglich allfälliger Behandlungsfehler, während ihnen die übrigen Informationen aus der Krankengeschichte nicht zugänglich sind. Diese Trennung und Abgrenzung von Informationen ist kaum praktikabel. Die vollständige Krankengeschichte soll daher nur von einem Träger des Berufsgeheimnisses eingesehen werden. Denn wer an die ärztliche Schweigepflicht gebunden ist, kann den Hinterbliebenen die benötigten Informationen unter Respektierung der Geheimhaltungsinteressen des verstorbenen Patienten vermitteln.

- Diese Ansicht wird auch in der Lehre und der Rechtsprechung favorisiert: So hat das Obergericht des Kantons Schaffhausen entschieden, die hinterbliebenen Personen müssten einen Arzt ihres Vertrauens mit der Einsicht in die vollständige Krankengeschichte betrauen. Dieser Vertrauensarzt dürfe allerdings die Hinterbliebenen oder deren Rechtsvertreter nur insofern über den Inhalt der Krankengeschichte informieren, als daraus Schlüsse für eine allfällige Fehlbehandlung gezogen werden können (ZBl 91 S. 364 ff.). Später bezog sich in einem anderen Fall das Bundesgericht auf dieses Urteil und erklärte diese Lösung als gerechtfertigt. In der Lehre schliesslich wird dieselbe Ansicht vertreten.

In einem weiteren Fall wollte die getrennt lebende Ehefrau eines verstorbenen Unfallopfers vom Spital Auskunft über die Todesursache. Auch hier verweigerte die Gesundheitsdirektion jegliche Entbindung vom Berufsgeheimnis.

Allerdings wurde verkannt, dass die Frau keine Einsicht in die Unfallakten wünschte, sondern lediglich eine allgemeine Auskunft über die Unfallverletzungen. Das angefragte Spital hätte also prüfen müssen, ob es der (getrennt lebenden) Ehefrau in Anwendung von § 15 der Patientenrechtsverordnung die gewünschte Auskunft erteilen darf.

- Einer umfassenden Einsicht in die Krankengeschichte einer verstorbenen Person steht das Patientengeheimnis entgegen. Wollen die Angehörigen Angaben aus der Krankengeschichte – etwa um allenfalls am Tod verantwortliche Personen zur Rechenschaft zu ziehen –, hat die Gesundheitsdirektion eine Interessenabwägung vorzunehmen und bei Offenlegung einen Vertrauensarzt mit der Beschränkung der Informationen auf das Notwendige zu betrauen.

SCHULEN

3. Ärztliche Schülerkarten

Aufbewahrung und Versand nur in verschlossenen Couverts

Schülerinnen und Schüler werden im Lauf des obligatorischen Schulbesuchs mehrmals durch einen Schularzt oder eine Schulärztin untersucht. Die dabei erhobenen Daten werden in die ärztlichen Schülerkarten eingetragen. Eine Schulpflegepräsidentin erkundigte sich, ob es zulässig sei, diese Schülerkarten in offenen Couverts im Schulsekretariat aufzubewahren. Die Frage war innerhalb der Schulpflege umstritten und die Schulpflegepräsidentin stellte fest, dass auch andere Schulpflegen keine einheitliche Praxis befolgen.

Bei den auf den Schülerkarten gesammelten Angaben handelt es sich um in hohem Masse empfindliche Personendaten zur physischen und psychischen Gesundheit der untersuchten Kinder und Jugendlichen. Solche besonders schützenswerte Daten dürfen nur bearbeitet werden, wenn dafür eine gesetzliche Grundlage besteht, die Bearbeitung im Einzelfall notwendig ist oder die betroffene Person in die Bearbeitung eingewilligt hat. Für die Bearbeitung von ärztlichen Schülerdaten ist allein der Schularzt oder die Schulärztin zuständig. Andere Personen, insbesondere Sekretariatsangestellte oder Lehrkräfte, dürfen nicht die Möglichkeit haben, die Daten einzusehen.
Die Schulgemeinden sind dafür verantwortlich, dass die Schülerkarten nach den Bestimmungen des Datenschutzes aufbewahrt werden. Zudem unterstehen die Ärzte dem medizinischen Berufsgeheimnis nach Art. 321 Strafgesetzbuch.
Den besten Schutz bietet die Aufbewahrung der Schülerkarten beim zuständigen Schularzt. Müssen die Karten im Schulsekretariat oder bei einer Lehrperson aufbewahrt werden, ist es unerlässlich, dass sie vom Schularzt in einem verschlossenen Couvert zur Aufbewahrung übergeben werden.

Im gleichen Zusammenhang steht die Anfrage des Mitgliedes einer Kreisschulpflege:
Als Schülerzuteilerin hatte sie in einem an sie adressierten Couvert die ärztliche Schülerkarte eines zugezogenen Kindes erhalten. Auch hier gilt: Die besonders schützenswerten Gesundheitsdaten des Kindes dürfen nicht unbefugten Personen zur Kenntnis gelangen. Muss ein Arzt eine Schülerkarte weiterleiten, hat er sie in einem verschlossenen Couvert zuhanden des Schularztes/der Schulärztin zu verschicken.

- Bei den ärztlichen Schülerkarten handelt es sich um besonders schützenswerte Gesundheitsdaten. Sie sind verschlossen aufzubewahren und dürfen nur für schulärztliches Personal zugänglich sein.

4. Aufbewahrung von Prüfungsunterlagen

Grundsätze für Einsichtnahme und Aufbewahrungsdauer

Von verschiedener Seite wurden Fragen zum Einsichtsrecht in Prüfungsunterlagen und -protokolle gestellt. Wir nahmen in genereller Weise Stellung zum Recht, in Prüfungsunterlagen an Mittel-, Berufs- und Hochschulen Einsicht zu nehmen.
Entgegen der weit verbreiteten Meinung, das Einsichtsrecht bestehe nur im Falle einer nicht bestandenen Prüfung, erstreckt sich das Auskunftsrecht nach § 17 DSG auf sämtliche Daten über die betroffene Person – also auch auf bestandene Prüfungen. Einschränkungen gebietet das öffentliche Interesse an einem geordneten und unbeeinflussten Prüfungsverlauf; aus diesem Grund ist die Auskunft bei mehrtägigen Prüfungen und während des Korrektur- bzw. Bewertungsverfahrens aufzuschieben, damit eine rechtsgleiche Behandlung aller Kandidatinnen und Kandidaten sichergestellt ist. Das Gesuch um Einsicht in Prüfungsunterlagen unterliegt keiner Frist; es kann jederzeit gestellt werden, solange die Unterlagen aufbewahrt werden. (Selbstverständlich hat dies keinen Einfluss auf allfällige Rekursfristen bei nicht bestandenen Prüfungen.)
Die Dauer der Aufbewahrung von Prüfungen leitet sich nach dem Verhältnismässigkeitsgrundsatz davon ab, wie lange diese für die Aufgabenerfüllung benötigt werden. Dies hängt wiederum von der Art der Prüfung und dem Prüfungs- bzw. Bewertungsprozedere ab. In der Regel dürfen die Prüfungen aufbewahrt werden, bis die Gesamtnote (z.B. zum Semesterende) rechtskräftig feststeht. Die übliche Aufbewahrungsdauer von einem Jahr erscheint damit angemessen. Anschliessend sind die Unterlagen zu vernichten bzw. gemäss Archivgesetzgebung dem Staatsarchiv zur Archivierung anzubieten; möglich ist auch die Herausgabe der Prüfungen an die Schülerinnen und Schüler.

- Es ist im Einzelfall auf Grund der Ausgestaltung des Prüfungs- bzw. Bewertungsverfahrens zu entscheiden, wie lange Prüfungsunterlagen aufbewahrt werden. Solange sie aufbewahrt sind, darf die betroffene Person sie einsehen. Nach Ablauf der Aufbewahrungsdauer sind sie der betroffenen Person herauszugeben oder dem Staatsarchiv anzubieten bzw. zu vernichten.

POLIZEI UND JUSTIZ

5. Neue Regeln für die Aufzeichnung von Telefongesprächen

Vernehmlassung zur Revision des Strafgesetzbuches

Der Bund plant auf Grund eines parlamentarischen Vorstosses eine Änderung der Bestimmungen des Strafgesetzbuches (StGB), welche die Strafbarkeit von Telefonaufzeichnungen regeln. Unter dem geltenden Recht macht sich strafbar, wer ohne Einwilligung der Beteiligten Fernmeldegespräche abhört oder aufzeichnet. Ausnahmen bestehen bei Notrufen für Hilfs-, Rettungs- und Sicherheitsdienste sowie – im Rahmen des Strafprozessrechts – bei Strafuntersuchungen. Die Änderung soll die Aufzeichnung neu auch zulassen, wenn die Gesprächspartner/innen darüber informiert werden (blosse Information statt Einwilligung). Ausserdem soll die Aufzeichnung von eingehenden Anrufen zulässig sein, wenn die Aufzeichnungsmöglichkeit aus den Teilnehmerverzeichnissen (gedruckt oder elektronisch) ersichtlich ist.

Im Rahmen des kantonsinternen Mitberichtsverfahrens nahmen wir zur beabsichtigten Gesetzesänderung Stellung:

- Wir bedauern, dass der Schutz vor ungewollten Gesprächsaufzeichnungen bereits nach kurzer Zeit – die bestehende Regelung war erst 1998 mit der Liberalisierung des Fernmeldewesens eingeführt worden – wieder eingeschränkt werden soll, wodurch Eingriffe in die Privatsphäre erleichtert werden.

- Inhaltlich erscheint der Entwurf im ersten Teil als ungenügend, weil die Gesprächspartner/innen nicht nur über die Möglichkeit der Aufzeichnung, sondern auch

über deren Zweck und deren Verwendung informiert werden müssten, wollte man tatsächlich Transparenz schaffen. Ausserdem regten wir an, dass bei Zwecken, die reine Innenverhältnisse betreffen (z.B. Personalschulung, Qualifikation usw.), Alternativanschlüsse ohne Aufzeichnungsmöglichkeiten anzubieten sind.

- Schliesslich sollte die Bestimmung gestrichen werden, wonach ein entsprechender Eintrag im Teilnehmerverzeichnis genügt, um Gespräche aufnehmen zu dürfen. In vielen Fällen hat eine betroffene Person keinen Anlass abzuklären, ob ein solcher Eintrag besteht, z.B. weil die Telefonnummer bereits bekannt ist oder über Werbung vermittelt wird. Problematisch ist die Bestimmung auch, weil mit dieser Lösung Aufzeichnungen zulässig werden, die gar nicht erforderlich sind. Zudem bleibt unklar, ob im Einzelfall auch tatsächlich eine Aufzeichnung erfolgt. Für die betroffene Person geht damit jegliche Transparenz verloren.
- Für die Aufzeichnung von Telefongesprächen müssen transparente Regeln geschaffen werden, welche die Privatsphäre respektieren. Gesprächsteilnehmer/innen sollten wissen, ob und zu welchem Zweck eine Aufzeichnung erfolgt.

6. DNA-Analysen in der Strafuntersuchung

Neue kantonale Verordnung

Fehlende Rechtsgrundlagen für die Erhebung von DNA-Analysen in der Strafuntersuchung veranlassten die Direktion der Justiz und des Innern eine Arbeitsgruppe einzusetzen, die eine Verordnung über die «Erhebung und Bearbeitung von DNA-Analysen im Strafverfahren» erarbeitete. Diese wurde vom Regierungsrat auf den 1. Juni 2001 in Kraft gesetzt.

Die Ausgestaltung der zürcherischen Rechtsgrundlagen ist sehr stark geprägt von der auf den 1. Juli 2000 in Kraft getretenen Verordnung über das DNA-Profil-Informationssystem des Bundes (EDNA-Verordnung). Es handelt sich hierbei um eine befristete Rechtsgrundlage für den Betrieb einer DNA-Datenbank auf Bundesebene (der Entwurf eines entsprechenden Bundesgesetzes befindet sich in der parlamentarischen Beratung). Wir haben bereits früher auf die Sensibilität der DNA-Analysen hingewiesen (Tätigkeitsbericht Nr. 4 [1998], S. 22 ff.) und in der erwähnten Arbeitsgruppe die datenschutzrechtlichen Aspekte eingebracht. Eine gesetzliche Grundlage für die Entnahme von Proben zur Erstellung von DNA-Analysen wurde nicht geschaffen, da die Bundeslösung abgewartet werden soll. Grundsätzlich hält die Verordnung fest, dass der Kanton Zürich sich am Informationssystem des Bundes beteiligt (§ 1 DNA-Analysen-VO); daneben werden keine eigenen diesbezüglichen Datenbanken geführt. Während die bundesrechtliche EDNA-Verordnung einen Deliktskatalog aufweist, der bestimmt, wann Analysen erstellt werden dürfen, verzichtet die zürcherische Verordnung darauf: dies in Anlehnung an den Entwurf des Bundesgesetzes, der ebenfalls keinen Deliktskatalog mehr aufweist. Mit dem Verweis auf das Verhältnismässigkeitsprinzip wird die Entnahme einer Probe auf erkennungsdienstliche Anordnung hin wenig konkret geregelt (§ 2 lit. a DNA-Analysen-VO).

Die EDNA-Verordnung weist einen Deliktskatalog auf, nach welchem sich die Aufbewahrung von Profilen richtet. Die bezeichneten Behörden haben die Personendaten und Profile zu löschen, die nicht in das Bundessystem aufgenommen werden (§ 4 DNA-Analysen-VO). Eine Übergangsregelung sieht vor, dass die bereits bestehenden Daten nach den neuen Bestimmungen in das Bundesinformationssystem zu übertragen oder zu löschen sind.

● Die DNA-Verordnung schafft eine bisher fehlende Rechtsgrundlage für die Erhebung und Bearbeitung von DNA-Analysen in der Strafuntersuchung. Sie stellt weitgehend auf die bundesrechtlichen Bestimmungen ab, die in einer Übergangsverordnung festgehalten sind, und ist daher sehr offen formuliert. Insbesondere die Bestimmungen über die Voraussetzungen für die Erhebung respektive Löschung von Daten und Profilen sind wenig konkret. Es ist zu hoffen, dass die datenschutzrechtlichen Anliegen im Bundesgesetz konkretisiert werden.

KANTON

7. Mehr Öffentlichkeit in der öffentlichen Verwaltung

Ausgleich zwischen Informationsanspruch und Datenschutz

Die Einführung des Öffentlichkeitsprinzips in der Verwaltung ist sehr eng mit dem Datenschutz verbunden. Unser Mitbericht zum Entwurf eines Bundesgesetzes über die Öffentlichkeit der Verwaltung gab die Gelegenheit, einige grundsätzliche Fragen aufzuwerfen. Datenschutz und Informationszugang sind wie die zwei Seiten einer Medaille: Der Schutz der Daten und der Zugang zu den Informationen sind deshalb in der Praxis einheitlich und kohärent zu regeln. Der Gesetzesentwurf weist hier grundsätzliche Mängel auf; es erscheint zweifelhaft, ob damit das deklarierte Ziel der Transparenz erreicht werden kann.
Es stellt sich auch die Frage, ob die Einführung des Öffentlichkeitsprinzips nicht auf Verfassungsstufe geschehen müsste, damit es die nötige Durchsetzungskraft entfalten kann. Weiter wiesen wir darauf hin, dass der Zweckartikel kaum zu genügen vermag. In der «Erleichterung des Zugangs» kann sich der Zweck des Gesetzes wohl kaum erschöpfen. Deshalb muss das Gesetz klar deklarieren, ob es um die Transparenz im Sinne der Kontrolle der Verwaltung geht, oder ob der Zugang für die politische Meinungsbildung bezweckt wird. Geht es auch darum, der Wirtschaft Informationen, über welche die Verwaltung verfügt, zugänglich zu machen, und soll ein durchsetzbarer Anspruch auf Zugang geschaffen werden?

Es ist richtig erkannt worden, dass dem Ausgleich zwischen den Ansprüchen auf Zugang und dem Schutz der von behördlicher Datenbearbeitung betroffenen Personen – wie er im Datenschutzgesetz und in bereichsspezifischen Datenschutzregelungen in anderen Gesetzen konkretisiert wird – entscheidende Bedeutung zukommt. Unter dem Etikett der «gläsernen Verwaltung» dürfen nicht «gläserne Bürgerinnen und Bürger» geschaffen werden. Diesen Ausgleich muss das Gesetz schaffen. Dem Gesetzesentwurf mangelt es im Bereich der Schnittstelle Öffentlichkeit und Datenschutz jedoch an den notwendigen Präzisierungen. Weiter stellte sich heraus, dass gerade dort, wo überwiegende öffentliche Interessen eine Bekanntgabe von Personendaten rechtfertigen, die vorgeschlagene Regelung den Ansprüchen an die Bestimmtheit in keiner Weise genügt. Insbesondere wären die Kriterien für den Entscheid der Datenbekanntgabe zu formulieren, die Regeln für das Schlichtungsverfahren festzulegen und die Verfahrensrechte der betroffenen Personen zu definieren.

Die Behandlung von Streitigkeiten aus dem Gesetz wird sinnvollerweise in die Hände einer einzigen Schieds- und Rekurskommission gelegt und die bisherige Eidgenössische Datenschutzkommission umgewandelt in eine Eidgenössische Datenschutz- und Öffentlichkeitskommission. Unverständlich ist allerdings, dass diese Zusammenführung nicht auch bereits auf der Ebene des oder der Beauftragten stattfindet, die der Kommission vorgelagert sind. Der Entwurf verschliesst sich den guten Erfahrungen, welche mit der frühzeitigen Zusammenlegung der Verfahren und Zuständigkeiten in Ungarn, in Québec oder in den deutschen Bundesländern Brandenburg, Berlin und Schleswig-Holstein gemacht werden. Bezeichnenderweise ist in keinem Fall, wo in jüngerer Zeit das Öffentlichkeits-

prinzip eingeführt wurde, eine derartige Trennung vorgesehen. Für die Schlichtungsaufgabe wäre deshalb ebenfalls eine einzige Instanz in Form eines oder einer Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten vorzusehen.

- Im Mitbericht brachten wir zum Ausdruck, dass Datenschutz und Informationszugang eine Gemeinsamkeit besitzen: Sie setzen staatlicher Informationsmacht Grenzen. Nur wenn es gelingt, die berechtigten Ansprüche auf Datenschutz und Informationszugang als Ganzes zu betrachten, wird es möglich, eine praxistaugliche Lösung zu finden, um einen Ausgleich zwischen den verschiedenen Interessen zu schaffen.

---

8. Neue Mitarbeitende sensibilisieren

Broschüre und Merkblatt des Personalamtes

Das kantonale Personalamt entwarf eine Infobox für alle neu eintretenden Mitarbeitenden. Diese Infobox soll diverse Informationen enthalten, die für die tägliche Arbeit und das Arbeitsverhältnis wichtig oder nützlich sind, u.a. ein Merkblatt «Datenschutz» sowie einen kurzen Text dazu in der Einführungsbroschüre. Wir erhielten die Entwürfe dieser Texte zur Überprüfung, und das Personalamt hat unsere Korrekturen und Anregungen allesamt umgesetzt.

Ein weiteres Projekt des Personalamtes war die Erarbeitung eines Muster-Personaldossiers auf der Basis des Personalgesetzes von 1998. Wir nahmen Stellung zu Abschnitten des Personalhandbuches sowie zu den Mappen des Personaldossiers. Auch hier wurden unsere Anregungen umgesetzt.

- Die kurzen Informationen in der Infobox sind ein sehr nützliches Instrument, um die neuen Mitarbeitenden in einem ersten Schritt für den Datenschutz zu sensibilisieren.

---

9. Datenbearbeitungen im Qualitätsmanagement

Zweckbindung sichert den Erfolg

Im Rahmen des «New Public Management» wird in vielen Verwaltungseinheiten die Einrichtung von Qualitätsmanagementsystemen geplant. Bei der Einführung eines Qualitätsmanagements (QM) in einer Schule sah sich die Projektleitung mit Widerständen von Mitarbeitenden konfrontiert; diese befürchteten, dass die von ihnen im Rahmen des QM erhobenen Daten für die Mitarbeiterbeurteilung verwendet werden könnten.

Qualitätsmanagement erfordert meist die Erfassung, Verarbeitung und Auswertung von verschiedenen Zahlen und Daten. Dabei handelt es sich teilweise um Daten, welche einen Personenbezug – zu Mitarbeitenden oder Kundinnen und Kunden – aufweisen.

Qualitätsmanagementprozesse erfolgen in der Regel losgelöst von den einzelnen Personen; sie betreffen die Dienstleistungen, die Abläufe, die Organisation usw. Bei Datenbearbeitungen im Qualitätsmanagement handelt es sich mithin um Datenbearbeitungen zu einem nicht personenbezogenen Zweck, die nach den (erleichterten) Rahmenbedingungen des § 12 DSG zu beurteilen sind. Im Rahmen des QM dürfen bereits vorhandene Daten verwendet und ausgewertet werden, sofern sie baldmöglichst anonymisiert werden. Der QM-Prozess ist so zu gestalten, dass die Daten frühzeitig ausgewertet und dann sogleich anonymisiert werden.

Daten, welche erst im QM-Prozess neu erhoben werden (z.B. mittels Fragebogen, Interviews, Feedbackprozessen), sind zweckgebunden ausschliesslich für das QM zu verwenden. Ist auch noch eine andere Verwendung der Daten beabsichtigt, müssen die betroffenen Personen informiert werden und ihre Einwilligung ist not-

wendig. Ausserdem ist zu prüfen, ob die speziell für das QM erhobenen Daten für den anderen Zweck überhaupt geeignet sind. Weitere Fragen stellen sich, wenn es um Daten geht, welche einer besonderen Schweigepflicht unterstehen (z.B. dem medizinischen Berufsgeheimnis), und wenn diese Daten durch externe Fachleute bearbeitet werden sollen.

Auch in der kantonalen Verwaltung wurde im Rahmen der Verwaltungsreform wi*f*! ein Qualitätsmanagementprojekt gestartet. Wir haben die Projektleitung auf mögliche Probleme aufmerksam gemacht und darauf hingewiesen, dass Datenbearbeitungen im Qualitätsmanagement unter dem Blickwinkel des § 12 DSG und seiner Rahmenbedingungen zu beurteilen sind.

- QM-Projekte sollen transparent gestaltet sein. Sie müssen deklarieren, zu welchem Zweck die von den Betroffenen erhobenen Daten benötigt werden.

---

10. Elektronisches Telefon- und E-Mail-Verzeichnis
Vorarbeiten zum Aufbau eines Metadirectory

Nach einem Beschluss des strategischen Informatik-Führungsorgans startete die Abteilung für Informatikplanung der Finanzdirektion das Projekt Metadirectory. Ein Metadirectory ist ein elektronisches Adressverzeichnis, das aus verschiedenen Verzeichnissen – Telefonbuch, E-Mail-Verzeichnis, Personalinformationssystem und evtl. weiteren Quellen – gespiesen wird. Damit soll den Mitarbeitenden der Verwaltung und der Gemeinden sowie der Bevölkerung ein einheitliches und aktuelles Verzeichnis zur Verfügung stehen. Das Projekt wurde mit verschiedenen Workshops unter Beteiligung der Direktionen und von Fachleuten aus den betroffenen Bereichen gestartet.

Dabei wurden bestehende Metadirectories (Kanada, Stadt Genf) vorgeführt und das Projekt der Bundesverwaltung vorgestellt. Anschliessend haben wir zu Handen der Projektleitung die datenschutzrechtlich relevanten Fragen zusammengefasst.
Zuerst ist der genaue Zweck des Metadirectory zu definieren. Dann ist zu prüfen, welche Datenbearbeitungen und -bekanntgaben dafür verhältnismässig sind und ob die rechtlichen Grundlagen ausreichen. Zu klären ist weiter die Frage, wer für die Datenbearbeitungen im Metadirectory verantwortlich ist. Für die Gewährleistung der Sicherheit ist ein Konzept gemäss Informatiksicherheitsverordnung (ISV) erforderlich; die notwendigen organisatorischen und technischen Massnahmen sind rechtzeitig vorzusehen und umzusetzen.

Das Metadirectory ist auch bedeutsam für das Projekt SOPRANO (siehe Seite 30 f.). Der Aufbau einer Public Key Infrastructure (PKI) erfordert ein zentrales Verzeichnis, in welchem die Zertifikate mit den öffentlichen Schlüsseln abgelegt sind.
Ein Metadirectory könnte zu dieser Aufgabe beitragen.

- Beim Aufbau eines zentralen Verzeichnisses sind vor dem Hintergrund der definierten Zwecke die Fragen der Rechtsgrundlagen und der Verhältnismässigkeit zu prüfen. Weiter ist eine Verantwortungsregelung zu treffen, und es sind Sicherheitsmassnahmen vorzusehen.

GEMEINDEN

11. Einbürgerungsverfahren

Keine Publikation von Fotos

Eine politische Gemeinde gelangte an uns mit der Frage, welche Daten sie während eines Einbürgerungsverfahrens und bei der Bekanntgabe von Einbürgerungen über die betroffenen Personen publizieren dürfe. Insbesondere sollten Fotografien von einbürgerungswilligen Personen im Amtsblatt veröffentlicht werden.

Im Einbürgerungsverfahren sollen diejenigen Personen, die über die Einbürgerungsgesuche befinden, feststellen können, ob eine Person für die Einbürgerung geeignet ist. Die Einbürgerungsbehörde darf also nach dem Grundsatz der Verhältnismässigkeit nur solche Daten erheben, die entscheidend sind für die Beantwortung der Frage, ob jemand an die schweizerischen Verhältnisse assimiliert ist und damit die Voraussetzungen für die Einbürgerung erfüllt.

Verhältnismässig muss auch die Datenbekanntgabe sein: Die erhobenen Daten dürfen nur denjenigen Personen bekannt gegeben werden, die tatsächlich über das Einbürgerungsgesuch entscheiden. Es gibt keine Rechtfertigung dafür, einschlägige Angaben zu einbürgerungswilligen Personen im Amtsblatt zu veröffentlichen, diese Daten also einer unbestimmten Anzahl von Personen bekannt zu geben.

Umso weniger ist es gerechtfertigt, Fotos von einbürgerungswilligen Personen in einem für die breite Bevölkerung zugänglichen Medium zu veröffentlichen. Irrelevant ist, ob es sich um das amtliche Publikationsorgan der Gemeinde handelt, da auch dieses nicht ausschliesslich von Stimmberechtigten gelesen wird. Im Übrigen darf bezweifelt werden, dass Stimmberechtigte, die eine einbürgerungswillige Person nicht kennen, anhand einer Fotografie entscheiden können, ob diese Person assimiliert ist oder nicht. Die notwendigen Daten müssen so bekannt gegeben werden, dass der Eingriff in die Persönlichkeit der einbürgerungswilligen Person möglichst gering bleibt. Zu weit ginge es, wenn die Behörde den Stimmberechtigten Kopien der Einbürgerungsunterlagen versenden würde. Das Material, das die Stimmberechtigten erhalten, darf lediglich die Daten enthalten, die nötig sind, um die Kandidatinnen oder Kandidaten zu identifizieren und die Anträge bekannt zu geben. Der Informationsbedarf der stimmberechtigten Bürgerinnen und Bürger ist ausreichend gedeckt, wenn sie Gelegenheit haben, die für ihren Entscheid relevanten Akten vor der Abstimmung in der Gemeindekanzlei einzusehen. Dort dürfen allerdings nicht die vollständigen Akten über eine betroffene Person aufliegen, sondern nur eine Zusammenfassung der für die Entscheidung wesentlichen Fakten.

Auch an der Bürgerversammlung ist die Datenbekanntgabe auf das unbedingt erforderliche Minimum zu beschränken. Es besteht kein Grund, den Lebenslauf einer gesuchstellenden Person laut zu verlesen. Ausschliesslich der Antrag als solcher ist immer öffentlich bekannt zu geben. Und nur wenn sich Zweifel über die Einbürgerungsfähigkeit ergeben, soll auf Einzelheiten eingegangen und zu allfälligen «heiklen» Punkten nachgefragt werden können.

Gemäss kantonaler Bürgerrechtsverordnung wird jede Einbürgerung im amtlichen Publikationsorgan der Gemeinde veröffentlicht. Diese Bekanntmachung bezweckt die Orientierung der Allgemeinheit. Auch hier darf die Gemeinde nur diejenigen Daten veröffentlichen, die notwendig sind, damit eine Person identifiziert werden kann. Es genügt die Angabe von Name, Vorname, Geburtsjahr, Adresse sowie des Herkunftslandes. Die Veröffentlichung weiterer Angaben ist unverhältnismässig und daher unzulässig.

- Im Einbürgerungsverfahren ist einzig die Eignung für die Einbürgerung abzuklären. Datenerhebung und Datenbekanntgabe sind auf das unbedingt erforderliche Minimum zu beschränken. Die Veröffentlichung von Fotografien ist unverhältnismässig, eignet sich nicht als Entscheidungsgrundlage und muss daher unterbleiben.

12. Lohndaten in der Jahresrechnung

Kein Rückschluss auf Lohn einzelner Angestellter

Eine politische Gemeinde fragte uns an, wie detailliert sie die Einwohnerschaft in ihrer Jahresrechnung über die Lohngelder für ihre Angestellten informieren dürfe, ohne gegen datenschutzrechtliche Normen zu verstossen. Die gleiche Frage wurde uns aus der Sicht eines Lohnempfängers gestellt: Diesen störte die Veröffentlichung seiner individuellen Lohndaten in der Jahresrechnung der Kirchgemeinde, für die er arbeitet.

Das Arbeitsverhältnis des Gemeindepersonals ist ein öffentlich-rechtliches. Soweit die Gemeinden keine eigenen Vorschriften erlassen, gelten das kantonale Personalgesetz und seine Ausführungsbestimmungen sinngemäss für das Anstellungsverhältnis des Gemeindepersonals. Auch wenn einzelne Gemeinden eigene Vorschriften erlassen haben, verweisen diese für Aspekte des Datenschutzes in der Regel auf das übergeordnete Personalgesetz.

Laut Personalgesetz dürfen Personendaten der Angestellten nur bekannt gegeben werden, wenn eine gesetzliche Grundlage es erlaubt, oder wenn es im Einzelfall zur Erfüllung einer öffentlichen Aufgabe der Empfänger notwendig ist. Empfänger der Personendaten sind die Stimmberechtigten in ihrer Eigenschaft als Teilnehmende an der Gemeindeversammlung. Es stellt sich die Frage, ob die Stimmberechtigten für die Abnahme der Jahresrechnung die Löhne der einzelnen Gemeindeangestellten kennen müssen. Dies ist nicht der Fall. Allgemein üblich und absolut ausreichend ist die Aufschlüsselung der Lohngelder nach funktionalen Aspekten wie «allgemeine Verwaltung», «öffentliche Sicherheit», «Kultur und Freizeit». Die Bekanntgabe der konkreten Löhne tangiert die Persönlichkeitsrechte der Angestellten und steht in keinem angemessenen Verhältnis zum Anspruch der Stimmberechtigten auf Kenntnis der Gemeindeausgaben. Zudem unterliegen die Besoldungen der Angestellten der Schweigepflicht gemäss § 71 Gemeindegesetz.

Beim Mitarbeiter einer Kirchgemeinde nannte die Jahresrechnung im Bereich «Seelsorge und Gottesdienst» neun Posten, welche je die individuellen Besoldungen der Angestellten enthielten. Hier gilt das Gleiche wie oben ausgeführt: Die Stimmberechtigten können ihre politischen Rechte in der Gemeindeversammlung auch wahrnehmen, wenn ihnen unter dem Titel «Seelsorge und Gottesdienst» der gesamte Besoldungsaufwand als Total bekannt gegeben wird. Damit ist ein Rückschluss auf Lohndaten einzelner Angestellter nicht möglich. Die Auflistung aller neun Posten stellt einen zu weit gehenden Eingriff in die Persönlichkeitsrechte der Mitarbeitenden dar und verletzt den Grundsatz der Verhältnismässigkeit.

- Der Besoldungsaufwand für das Gemeindepersonal darf in der Jahresrechnung der Gemeinde nicht detailliert und personenbezogen aufgeschlüsselt sein. Es genügt, wenn die Personalkosten auf die einzelnen Verwaltungsbereiche verteilt sind.

13. Abfassung von Schulpflegeprotokollen

Vollständige Namen nur in bestimmten Fällen

Im Zusammenhang mit der Abfassung ihrer Protokolle stellte sich für eine Schulpflege die Frage, ob sie Personennamen (zum Beispiel bei Zuweisungen zu Sonderschulmassnahmen) ausschreiben oder ob sie nur die Initialen oder andere Abkürzungen verwenden solle.

Das Gemeindegesetz (GG) äussert sich in § 68 zur Protokollführung: Über Verhandlungen jeder Gemeindebehörde ist ein Protokoll zu führen, das zwingend sämtliche Beschlüsse, die Präsidialverfügungen und auf Verlangen die Anträge einzelner Mitglieder oder Minderheiten enthalten muss. Die Behörde darf sich also darauf beschränken, lediglich ihre Beschlüsse zu protokollieren, diese müssen aber vollständig, das heisst mit allen relevanten Einzelheiten, abgefasst sein.
Im Übrigen sind die Bestimmungen des Datenschutzgesetzes anwendbar: Personendaten dürfen gestützt auf § 4 Abs. 3 DSG nur dann ins

Protokoll aufgenommen werden, wenn und so weit sie zur Erfüllung einer öffentlichen Aufgabe geeignet und erforderlich sind.
Sofern es sich bei Zuweisungen zu Sonderschulmassnahmen und Ähnlichem um Entscheidungen der Behörde handelt, kommt § 68 GG zur Anwendung. Die von der Massnahme betroffene Person wird mit vollständigem Namen aufgeführt. Handelt es sich jedoch lediglich um Diskussionen oder Voten einzelner Schulpflegemitglieder, tritt die datenschutzrechtliche Bestimmung in den Vordergrund: in solchen Fällen ist vorerst zu klären, ob das Gesagte überhaupt schriftlich fixiert sein muss. Erscheint es wahrscheinlich, dass später eine Rekonstruktion des Gesprächs notwendig wird, genügt es in der Regel vollauf, wenn die Person, über die gesprochen wurde, mit den Initialen bezeichnet wird. Falls auch die Initialen Rückschlüsse für die mit der Situation näher Vertrauten zulassen, ist die anonyme Bezeichnung «ein Schulkind» oder «eine Lehrkraft» zu wählen.

- Ob in Schulpflegeprotokollen die vollständigen Namen zu nennen sind oder lediglich die Initialen oder gänzlich anonymisierte Bezeichnungen von Personen, die Gegenstand von Beschlüssen oder Diskussionen waren, muss nach dem Grundsatz der Verhältnismässigkeit im Einzelfall entschieden werden.

14. Abklärungen für Wochenaufenthalt

Verhältnismässiger Fragenkatalog

Betroffene Personen hatten beanstandet, dass in Formularen zur Abklärung des Wochenaufenthalts zu viele Daten erhoben würden (siehe bereits Tätigkeitsbericht Nr. 1 [1995], S. 21 f.).

Zur Abklärung der Melde- und Steuerpflicht darf die Gemeinde Fragen über die Gründe für die Anmeldung als Wochenaufenthalter/in und die Beibehaltung des bisherigen Wohnsitzes stellen. Weiter darf sie fragen, wie lange der Wochenaufenthalt voraussichtlich dauern wird, wie häufig eine Rückkehr an den Wohnort erfolgt und in welcher Gemeinde die Steuern bezahlt werden. Zulässig sind auch Fragen nach den persönlichen Beziehungen zu Wohnort und Wochenaufenthaltsort (Beziehungen zu Ehegatten bzw. Lebenspartner/in, zu Kindern, zu Eltern bzw. Geschwistern, zum Freundes- und Bekanntenkreis) und zur Wohnsituation an den beiden Orten (Wohneigentum, Mietwohnung, möbliertes Zimmer, zur alleinigen Benützung oder mit anderen Personen). Ebenfalls verhältnismässig sind Fragen zur Erwerbstätigkeit (selbständig oder unselbständig unter Angabe der Betriebsstätte bzw. des Arbeitsortes und Arbeitgebers) oder zu einer aktuellen Ausbildung (Studium, Lehre usw.), deren voraussichtlicher Dauer und der Ausbildungsstätte.
Nicht gefragt werden darf hingegen, mit welchem Verkehrsmittel die Fahrten zwischen Wohnort und Wochenaufenthaltsort zurückgelegt werden, wie viele Zimmer die Mietwohnung hat, ob es sich um eigene oder vom Vermieter zur Verfügung gestellte Möbel handelt oder wo sich der Hausarzt und Zahnarzt befinden. Auch Fragen zu Mitgliedschaften in Vereinen, zu Freizeit- oder politischen Aktivitäten und zur Arbeitsplatzsituation (wie z.B. Dauer des Arbeitsweges, gewähltes Verkehrsmittel, Beschäftigungsgrad) sind nicht erforderlich und daher unverhältnismässig.

Ergeben sich im Einzelfall Unklarheiten, kann die Gemeinde bei der betroffenen Person weitere Auskünfte einholen, soweit dies notwendig ist. Auch kann die Richtigkeit einzelner Angaben stichprobenweise überprüft werden.

Eine Umfrage über die Praxis der Gemeinden in der Schweiz ergab ein uneinheitliches Bild. Wir haben deshalb einen Fragebogen entworfen und interessierten Kreisen zu einer Vernehmlassung zugestellt. Anschliessend diskutierten wir den Entwurf mit dem Verband der Steuerämter des Kantons Zürich, dem Steueramt der Stadt Zürich und dem kantonalen Steueramt weiter;

daraus ergab sich ein Muster-Fragebogen, den wir den Gemeinden für die standardmässig durchzuführenden ersten Abklärungen empfohlen haben. Der vollständige Fragebogen wurde in «Fakten» Nr. 3/2000, S. 9 f. veröffentlicht.

- Die Abklärung des Wochenaufenthaltes tangiert die Privatsphäre der betroffenen Personen. Der mit Vertretern der Steuerbehörden erarbeitete Muster-Fragebogen ermöglicht den Gemeinden, ihre Aufgaben (Abklärung der Melde- und Steuerpflicht) auf verhältnismässige Weise zu erfüllen.

INFORMATIONSSICHERHEIT

15. Patientendaten über Internet

Anforderungen an den Schutz sensibler Daten

Zum Austausch von Patientendaten über kantonale oder kommunale Netzwerke zwischen Spitälern sowie mit der elektronischen Post (E-Mail) über das Internet hat der Datenschutzbeauftragte sowohl aus rechtlicher als auch aus technischer Sicht schon mehrmals Stellung genommen.
Die von den Verwaltungsstellen erarbeiteten Lösungen, die wir beurteilen mussten, wiesen häufig folgende Mängel auf:

- Meistens wurden in Teilbereichen Lösungen vorgeschlagen, die nicht in ein Gesamtkonzept von technischen und organisatorischen Massnahmen eingebettet waren: Zum Beispiel erfolgte die Verschlüsselung nur auf Teilstrecken bei den Kommunikationsnetzen oder der Fokus der Lösung wurde einseitig auf die Schlüssellänge der Verschlüsselungsalgorithmen gesetzt.
- Die Massnahmen zur Sicherung wurden nicht flächendeckend getroffen: Offensichtliche Probleme in den Kommunikationsverbindungen wie Notverbindungen und Zugriffe für die Fernwartung wurden angegangen, für den Verkehr über das bestehende Netzwerk wurden jedoch keine weiteren Massnahmen getroffen.
- Die Diskussion über die Sicherheit erfolgte immer auf Stufe Netzwerk oder höchstens im E-Mail-Bereich mit dem Thema Standardsoftware: Zu sichern sind jedoch die Applikationen, welche die sensiblen Daten bearbeiten.
- Patientendaten sind nach dem aktuellen Stand der Technik auf allen Netzwerken (Wide-Area-Netzwerke, WAN), auf den lokalen Netzwerken und in der elektronischen Post verschlüsselt von Applikation zu Applikation («End-to-End») zu übertragen. Neue Möglichkeiten, um diese Forderung umzusetzen, wird das Projekt SOPRANO bieten (siehe auch Seite 30 f.).

16. Betrieb des kantonalen Informatiknetzwerkes

Arbeitsgruppe «LeuNet» erarbeitet Strategien

Das Projekt «LeuNet» hat zum Ziel, eine Strategie für den Betrieb des kantonalen Netzwerkes zu erarbeiten und zu implementieren. Der Datenschutzbeauftragte ist im Fachausschuss des Projektes vertreten. Kernpunkt der bisherigen Arbeiten war die Frage, wie weit der Betrieb des Netzwerkes an eine beliebige Drittfirma ausgelagert werden kann und entsprechend eine Ausschreibung stattzufinden hat. Aus datenschutzrechtlicher Sicht haben wir hierzu Stellung bezogen. Neben dem Datenschutzgesetz (DSG) sind die Informatiksicherheitsverordnung (ISV) und das Gesetz über die Auslagerung von Informatikdienstleistungen (Auslagerungsgesetz) zu berücksichtigen. Die im Projekt «LeuNet» erarbeiteten Strategievarianten unterschieden grundsätzlich zwischen Eigenbetrieb und Fremdbetrieb eines Netzes. Als Zwischenvariante erwies sich der

Betrieb durch eine Aktiengesellschaft, die der öffentlichen Hand gehört (abraxas AG). Für die Beurteilung betrachteten wir lediglich den Fremdbetrieb respektive die Variante mit der Firma abraxas. Aus datenschutzrechtlicher Sicht und unter Berücksichtigung der Informatiksicherheit handelt es sich hierbei um die sensibelsten Varianten.
Die Wahl der Strategievarianten ist nur dann von datenschutzrechtlichen Rahmenbedingungen abhängig, wenn der Netzwerkbetreiber Personendaten bearbeitet. Ein Netzwerkbetreiber stellt in erster Linie eine Infrastruktur zur Verfügung. Diese Kommunikationsinfrastruktur lässt sich jedoch nicht betreiben, ohne dass personenbezogene Daten bearbeitet werden (Berechtigungen, Abrechnungen etc.). So genannte Administrations- und Verbindungsdaten bilden die Voraussetzung für die Datenkommunikation. Aus den Verbindungsdaten lassen sich auch weitere Schlüsse ziehen (Beispiel: Kommunikationsverhalten). Es ist deshalb davon auszugehen, dass auch ein Netzwerkbetreiber Personendaten bearbeitet.
Die Verbindungsdaten sind zu unterscheiden von den Inhaltsdaten, den eigentlichen Daten, die über die Kommunikationsinfrastruktur verteilt werden. Diese werden von den einzelnen Benutzern der Infrastruktur (Amtsstellen etc.) nach ihren Bedürfnissen übertragen. Für das Bearbeiten der Inhaltsdaten bleiben die Benutzer verantwortlich.

Das Bearbeiten von Personendaten durch Dritte richtet sich nach § 13 DSG und den Bestimmungen des Auslagerungsgesetzes. Dabei sind der Schutz und die Sicherheit der Daten im gleichen Mass zu gewährleisten, wie wenn die Daten verwaltungsintern bearbeitet würden. Das Auslagerungsgesetz differenziert für die zu treffenden Massnahmen nach den Eigentumsverhältnissen des Dritten: Private Unternehmen mit Stimmenmehrheit und Kapitalmehrheit der öffentlichen Hand gelten diesbezüglich nicht als Dritte (§ 2 Abs. 2 Auslagerungsgesetz). Sie unterstehen deshalb bei der Bearbeitung von sensiblen Daten nicht den restriktiven Bestimmungen von § 2 Abs. 1 und § 3 Auslagerungsgesetz.

In Bezug auf die Firma abraxas als mögliche Netzwerkbetreiberin sind aus datenschutzrechtlicher Sicht und aus Sicht des Auslagerungsgesetzes keine zusätzlichen Massnahmen erforderlich, welche die generell bei der Bearbeitung von Personendaten durch Dritte notwendigen übertreffen.
Soll eine beliebige Drittfirma die Daten bearbeiten, stellt sich aus Sicht des Auslagerungsgesetzes die Frage, ob es sich um sensible Daten handelt, so dass zusätzlich zu den Anforderungen von § 2 besondere Massnahmen gemäss § 3 Auslagerungsgesetz zu treffen sind. Die Frage, ob sensible Daten bearbeitet werden, kann nicht abschliessend beantwortet werden. Dies, weil einerseits die im Rahmen des Netzwerkbetriebes notwendigen Daten nicht generell, sondern erst auf Grund bestimmter Konfigurationen im Einzelfall definiert sind; andererseits, weil es möglich ist, mit Kombinationen aus den Verbindungsdaten wiederum sensible Informationen zu gewinnen (Profile).

Aus diesen Erwägungen ergibt sich, dass der Netzwerkbetrieb durch einen privaten Dritten grundsätzlich ohne sensible Daten auskommen kann, zur Absicherung einer anderweitigen sensiblen Verwendung hingegen entsprechende Massnahmen notwendig sein werden (z.B.: allgemeine Geschäftsbedingungen in Bezug auf Datenschutz und Informationssicherheit; regelmässige Datenschutzreviews).

- Aus datenschutzrechtlicher Sicht ist der Betrieb eines Netzwerkes auch durch Dritte möglich. Eine solche Variante verlangt aber vermehrte Anstrengungen der verantwortlichen Organe, die Anforderungen gemäss Informatiksicherheitsverordnung umzusetzen. Insbesondere müssen geeignete Verschlüsselungsmassnahmen die Vertraulichkeit der bearbeiteten Daten gewährleisten.

17. Internet-Seminar für Gemeinden

Anleitung für sicheren Web-Auftritt

Das vom Datenschutzbeauftragten erarbeitete Seminar für die Informatik-Verantwortlichen der Gemeinden (siehe auch Tätigkeitsbericht Nr. 5 [1999], S. 31), das die konzeptionellen und technischen Anforderungen beim Aufbau eines Internetauftritts behandelt, wurde im Rahmen eines Weiterbildungsseminars für Gemeinden insgesamt fünfmal durchgeführt. Es vermittelte den Teilnehmenden im rechtlichen, organisatorischen und technischen Bereich das nötige Rüstzeug, um Datenschutz und Informatiksicherheit genügend berücksichtigen oder verbessern zu können. Eine Umfrage unter den Teilnehmenden zeigte auf, dass für die Bereiche Technik und Recht ein grosser Informationsbedarf besteht. Erstmals wurden die aus Recht, Organisation und Technik stammenden aktuellen Themen beim Aufbau eines Web-Auftritts in einer einzigen Veranstaltung zusammengeführt. Die ausführliche Seminardokumentation mit Checklisten in den Bereichen Organisation des Web-Auftritts, Internet-Server-Sicherheit (Web-Server und E-Mail) und Netzwerksicherheit (lokale Netzwerke und Fremdzugriffe via Internet) sowie mit weiteren Unterlagen (Fachartikel, Glossar, Internet-Links) wurde von den Teilnehmenden sehr gut aufgenommen. Wir konnten den Kurs für eine Arbeitsgruppe von Gemeinden aus dem Bezirk Affoltern anpassen. Er kann somit im Sinne einer Sensibilisierung auf datenschutzrechtliche Aspekte weiter verwendet werden.

- Die Informatikverantwortlichen der Gemeinden müssen regelmässig mit den neusten Entwicklungen in puncto Datenschutz und Informationssicherheit vertraut gemacht werden. Damit kann gewährleistet werden, dass sie diese angemessen berücksichtigen.

18. Schwerpunkte der IT-Sicherheitsberatung

Zunehmendes Gefährdungspotenzial

Ein wichtiger Teil der Arbeit in der IT-Sicherheitsberatung war neben der Beratung der Amtsstellen die Beantwortung der E-Mail-Anfragen von Bürgerinnen und Bürgern. Diese wünschten hauptsächlich Auskünfte zu unseren Web-Angeboten «Browser-Test» und «Sicher ist sicher». Einige der daraus resultierenden Anregungen konnten wir bereits im neuen Testwerkzeug «Browser-Diagnose» umsetzen.

In der Beratungstätigkeit dominierten die folgenden Themen:

- Die Umleitung von E-Mail vom Arbeitsplatz auf andere E-Mail-Anbieter (Provider) ausserhalb des kantonalen Netzes (KZHNETZ). Umgekehrt auch der Zugriff auf die eigene E-Mail vom Internet über den kantonalen Firewall (bisher vom Netzwerkbetreiber aus Sicherheitsgründen nicht eingerichtet). Die Umleitung von E-Mail kann temporär und in Ausnahmefällen bei der tiefen Sicherheitsstufe S1 gemäss Informatiksicherheitsverordnung (ISV) eingerichtet werden. Sicherheitsmassnahmen für die Stufen S2 und S3 wird erst das Projekt SOPRANO (siehe Seite 30 f.) bereitstellen.

- Zugriff auf Server der kantonalen Verwaltung vom Internet zu Servicezwecken (Remote Access [RAS]).
  Der Zugriff auf die Server muss mit organisatorischen und technischen Massnahmen gesichert werden. Dazu gehören einerseits Massnahmen zur Authentisierung und Vertraulichkeit der RAS-Kommunikationsstrecke, andererseits verbindlich formulierte Bedingungen in den Verträgen mit den Dienstleistern, insbesondere betreffend die Gewährleistung der Geheimhaltung.

- Virenbekämpfung beim Secure Messaging im Hinblick auf die PKI-Lösung (Projekt SOPRA-NO), Eskalationsverfahren für die Zusammenarbeit zwischen den Direktionen. Im Zusammenhang mit verschlüsselten E-Mails kommt dem Schutz gegen schädigende Programmteile auf dem Client eine zentrale Rolle zu, da die Eingriffsmöglichkeiten auf Firewall, E-Mail-Server etc. nicht mehr vorhanden sind und ersetzt werden müssen. Die Schutzmechanismen der Virenscanner müssen auch zuverlässig die schädigenden aktiven Komponenten auf dem Internet (Macros, Java etc.) erkennen und beheben, da die Bedrohung in diesem Bereich stark zugenommen hat.

- Angesichts des zunehmenden Gefährdungspotenzials wird die IT-Sicherheit immer bedeutender. Die IT-Sicherheitsberatung stellt deshalb den betroffenen Stellen die notwendigen Hilfsmittel zur Verfügung.

ARCHIVE

19. Archivierung von psychiatrischen Krankengeschichten

Offene Fragen in der Praxis

Das Staatsarchiv gelangte mit der Frage an uns, wie die Aufbewahrung und Archivierung von Krankengeschichten der Psychiatrie zu handhaben sei. Derzeit bestehen zwischen dem Staatsarchiv und psychiatrischen Kliniken diverse Vereinbarungen über die Aktenablieferung und die Aufbewahrung der Krankengeschichten. Dabei handelt es sich nicht um eine tatsächliche Archivierung, mit welcher die übliche Zweckänderung einhergeht, sondern lediglich um eine Aufbewahrung durch das Staatsarchiv im Auftrag der Kliniken. Diese wollen nach wie vor auf die Krankengeschichten zurückgreifen können. Eine klare Regelung dieser unüblichen Situation fehlt jedoch.

Die Patientenrechtsverordnung sieht vor, dass die Kliniken die Krankengeschichten mindestens zehn Jahre aufbewahren; in den meisten Fällen wird aber entschieden, die Akten länger aufzubewahren. Im psychiatrischen Bereich besteht dieses Bedürfnis, weil die Krankengeschichten häufig für spätere Behandlungen wieder benötigt werden.

Rechtlich ist die Aufbewahrung durch das Staatsarchiv im Auftrag der Kliniken problematisch. Da eine klare Regelung fehlt, ist für die betroffenen Personen nicht transparent, wie lange ihre Daten für die Aufgabenerfüllung der Klinik tatsächlich aufbewahrt werden. Offen ist deshalb auch, ob und zu welchem Zeitpunkt die Krankengeschichten archiviert werden. Das von den Kliniken und der Gesundheitsdirektion anerkannte Recht der Patientinnen und Patienten, der Archivierung ihrer Daten zu widersprechen, können die Betroffenen im Ergebnis nicht wahrnehmen.
Ungelöst sind auch die folgenden Fragen:

- Gilt für das Staatsarchiv das medizinische Berufsgeheimnis, wenn es im Auftrag der Klinik Krankengeschichten aufbewahrt?
- Ab welchem Zeitpunkt gilt für die Krankengeschichten das Archivrecht mit all seinen Rechtsfolgen, insbesondere Zweckänderung der Datenbearbeitung und Verbot, die Akten zur Aufgabenerfüllung wieder an die Klinik herauszugeben?
- Wie verhält es sich mit dem medizinischen Berufsgeheimnis, wenn die Krankengeschichten archiviert werden? Geht es unter, geht es auf das Staatsarchiv über?

Wir kamen deshalb mit dem Staatsarchiv überein, für die Bearbeitung und Lösung dieser Fragen aus Vertretern der Gesundheitsdirektion und der betroffenen Kliniken eine Arbeitsgruppe zu bilden. Angesichts der speziellen Bedürfnisse im psychiatrischen Bereich wäre eine Sonderlösung gemäss § 18 Archivgesetz möglich. Die Gesundheitsdirektion entschied jedoch, die Fragen nicht gesondert zu behandeln, sondern

bei der Ausarbeitung eines Patientenrechtgesetzes anzugehen. Im Einzelfall sollen provisorische Lösungen im Sinne der bereits bestehenden Praxis getroffen werden.

- Bei der Archivierung von Krankengeschichten sind einige Fragen nach wie vor unbeantwortet, weil die vorgesehene (rudimentäre) Regelung im Bereich der Aufbewahrung, Herausgabe und Archivierung der Krankengeschichten nicht genügt.

---

20. Richtlinien für Gemeindearchive

Vernehmlassung zum Entwurf des Staatsarchivs

Das Archivgesetz sieht vor, dass verschiedene öffentliche Organe – etwa die Gemeinden – eigene Archive führen. Diese Archive werden in fachlicher Hinsicht vom Staatsarchiv beaufsichtigt und beraten. Nachdem das Staatsarchiv Richtlinien für die Gemeindearchive entworfen hatte, äusserten wir uns zu einigen Punkten, die sich auf die Schnittstellen zwischen Datenschutz und Archiv beziehen.

Nach dem Grundsatz von § 14 DSG sind Personendaten zu vernichten, wenn sie nicht mehr zur Aufgabenerfüllung und zu Beweis- und Sicherungszwecken (z.B. während einer noch laufenden Verjährungsfrist) benötigt werden. Vor der Vernichtung ist zu prüfen, ob die Akten archivwürdig und deshalb – unter archivarischen Gesichtspunkten – weiter aufzubewahren sind. Diesen Entscheid fällt das für die Akten zuständige Archiv. Die Richtlinien nehmen diese Grundsätze auf und äussern sich weiter zu Fragen der Schutzfristen von archivierten Akten, der vorzeitigen Einsichtnahme vor Ablauf der Schutzfrist und der Rückführung von archivierten Akten an das Organ, das die Akten ursprünglich bearbeitet hatte.

Mit der Archivierung werden Akten und Daten, die ihren ursprünglichen Zweck erfüllt haben, für eine dauerhafte Überlieferung aufbewahrt. Es findet eine Zweckänderung im Sinne von § 4 Absatz 4 DSG statt, für die das Archivrecht die gesetzliche Grundlage liefert. Das öffentliche Organ kann nicht mehr auf die archivierten Akten zugreifen; deren Aufbewahrung dient nun einem anderen Zweck. Nur in Ausnahmefällen, die das Archivrecht festlegt, darf das öffentliche Organ archivierte Akten wieder verwenden; den Entscheid darüber fällt das Archiv. In den meisten Gemeinden gibt es keine organisatorische und personelle Trennung von Verwaltung und Archiv. Es besteht daher die Gefahr, dass archivierte Akten an das ursprüngliche Organ zurückgehen, ohne dass eine Interessenabwägung vorgenommen und ein eigentlicher Entscheid über die Rückführung gefällt wurde. Die Richtlinien sehen daher vor, dass die Gemeinden organisatorische Massnahmen ergreifen, die gewährleisten, dass die gesetzlichen Bestimmungen eingehalten werden. Sie haben eine verantwortliche Person und eine Stellvertretung zu bestimmen, die über solche Fälle entscheidet.
Wird in archivierte Akten Einsicht gewährt, ist darüber eine schriftliche Kontrolle zu führen. Diese enthält Angaben über die eingesehenen Akten, die Person, die Einsicht nimmt, sowie den Zeitpunkt und die Gründe der Einsicht.

Schliesslich enthalten die Richtlinien einige praktische Hinweise für organisatorische und technische Massnahmen, damit eine sichere und dauerhafte Aufbewahrung gewährleistet werden kann.

- Mit den Richtlinien für Gemeindearchive steht den Gemeinden ein gutes, praxisnahes Hilfsmittel zur Verfügung, das es ihnen ermöglicht, ihre archivarischen Aufgaben im Rahmen der rechtlichen Vorgaben zu erfüllen.

21. Vorzeitige Archiveinsicht
Konsequenzen bei Verstoss gegen Auflagen

Die im Staatsarchiv archivierten Akten unterliegen einer Schutzfrist, während der sie der Öffentlichkeit grundsätzlich nicht zur Verfügung stehen. Aus wichtigen Gründen kann das Staatsarchiv jedoch eine vorzeitige Einsichtnahme bewilligen; dazu hat es verschiedene Interessen gegeneinander abzuwägen.

Das Staatsarchiv wollte in diesem Zusammenhang von uns wissen, welche Sanktionen es aussprechen könne, wenn eine Person, der die vorzeitige Archiveinsicht bewilligt wurde, die dabei ausgesprochenen Auflagen missachtet hat.
Der Entscheid des Staatsarchivs, dass einer anfragenden Person vor Ablauf der Schutzfrist Einsicht gewährt wird, erfolgt in Form einer Verfügung. Es bleibt also kein Raum für zivilrechtliche Vereinbarungen. Deshalb sind im Rahmen der Verfügung allfällige Auflagen durch das Archiv einseitig anzuordnen. Daraus folgt auch, dass dem Archiv keine zivilrechtlichen Sanktionsmittel zur Verfügung stehen. Nur eine betroffene Person kann allenfalls nach Art. 28 Zivilgesetzbuch und Art. 15 Bundesdatenschutzgesetz (BDSG) wegen Verletzung ihrer Persönlichkeitsrechte zivilrechtlich gegen die Gesuchstellerin bzw. den Gesuchsteller vorgehen.
Hingegen bietet das Strafrecht eine Sanktionsmöglichkeit für das Archiv an. In Frage kommt insbesondere die Bestimmung des Strafgesetzbuches über den Ungehorsam gegen amtliche Verfügungen (Art. 292 StGB). Dazu muss das Staatsarchiv die Verfügung über die Einsichtnahme mit der Strafandrohung von Art. 292 StGB verbinden; verstösst die gesuchstellende Person dann tatsächlich gegen Auflagen aus der Verfügung, kann gegen sie Anzeige erstattet werden. Rein theoretischer Natur sind andere Strafbestimmungen wie Art. 35 BDSG; deren Voraussetzungen dürften in der Praxis kaum je erfüllt sein.
Im Vordergrund stehen somit verwaltungsrechtliche Sanktionen. Die Archivverordnung sieht vor, dass das Benützungsrecht des Archivs bei schweren Verstössen gegen die Benützungsordnung entzogen oder eingeschränkt werden kann. Denkbar ist etwa, dass eine Person nach einem Verstoss mit einer befristeten Benutzungssperre belegt wird. Eine weitere Möglichkeit besteht darin, in Zukunft die Auflagen zu verschärfen. Beispielsweise könnte das Archiv verlangen, dass eine Publikation, die im Zusammenhang mit der vorzeitigen Archiveinsicht erfolgen soll, vorgängig zur Genehmigung vorzulegen ist.

- Das Staatsarchiv kann bei der Bewilligung der vorzeitigen Archiveinsicht Auflagen machen. Bei Verstössen stehen nur in beschränktem Mass Sanktionen zur Verfügung.

22. Kosten für das Auskunftsrecht?

Keine gesetzgeberische Lösung im Kanton Zürich

Regelmässig werden wir angefragt, ob und wenn ja in welcher Höhe für die Wahrnehmung des Auskunftsrechts durch eine betroffene Person Gebühren erhoben werden dürfen. Eine Verwaltungsstelle verlangt beispielsweise pauschal 60 Franken für die Abgabe von Rapportkopien; unter gewissen Umständen ist die Gebühr sogar höher.

Das Auskunftsrecht wird als «Kern des Datenschutzes» bezeichnet; es ist das zentrale Recht, welches es einer Person ermöglicht, zu erfahren, welche Daten über sie bearbeitet werden. Gestützt auf die Auskunft kann sie allenfalls weitere Ansprüche wie das Recht auf Berichtigung oder Unterlassung geltend machen. Wenn Auskünfte kostenpflichtig sind, können betroffene Personen von der Ausübung ihrer Rechte abgehalten werden. Sie erhalten weder Kenntnis von den Datenbearbeitungen noch die Möglichkeit, ihre weiteren Rechte wahrzunehmen. Der Gesetzgeber entschied deshalb auf Bundesebene ausdrücklich, dass Auskünfte unentgeltlich sind. Nur im Ausnahmefall – insbesondere bei einem besonders grossen Arbeitsaufwand – darf eine Gebühr erhoben werden. Damit die Ausnahme nicht zur Regel wird, hat die Eidgenössische Datenschutzkommission (ein Spezialverwaltungsgericht des Bundes) in einem Leitentscheid umschrieben, was als besonders grosser Aufwand gilt. Der übliche Aufwand, der entsteht, wenn ein Dossier hervorgeholt und kopiert wird, fällt nicht darunter.
Der Kanton Zürich hat keine Regeln über die Kosten für Auskünfte aufgestellt. Wegen dieser Gesetzeslücke ist davon auszugehen, dass Kosten nach dem Gebührenrecht auferlegt werden dürfen, sofern sie nicht die Wahrnehmung des Auskunftsrechts unverhältnismässig einschränken. Die einleitend erwähnte Praxis der Kostenauflage ist problematisch. Wir regten daher an, diese Praxis zu ändern, doch entschied sich die Verwaltungsstelle für die Beibehaltung.

- In Anlehnung an die Bundesgesetzgebung sollten auch die kantonalen und kommunalen Amtsstellen für die Wahrnehmung des Auskunftsrechtes keine Gebühren erheben. Eine gerichtliche Klärung dieser Grundsatzfrage ist noch nicht erfolgt.

23. Datensperre im Steuerwesen

Weisung der Finanzdirektion angepasst

Mit dem neuen Steuergesetz, das Anfang 1999 in Kraft trat, erhielten steuerpflichtige Personen das Recht, die Bekanntgabe ihrer Daten – insbesondere das Ausstellen von Steuerausweisen – sperren zu lassen (siehe Tätigkeitsbericht Nr. 3 [1997], S. 41). In einer Weisung über die Führung der Steuerregister regelte die Finanzdirektion die Modalitäten der Datensperre. Die Weisung sah vor, dass die Datensperre durchbrochen werden kann, wenn der Gesuchsteller nachweist, dass er mit der betroffenen Person in wirtschaftlichem Kontakt steht oder einen solchen Kontakt aufnehmen möchte. Damit hätten auch die Prüfung der Kreditwürdigkeit und ähnliche Anliegen interessierter Personen eine Sperre durchbrechen können. Gemäss § 11 Absatz 2 DSG kann eine Datensperre nur durchbrochen werden, wenn sie die gesuchstellende Person an der Verfolgung eigener Rechte gegenüber der betroffenen Person hindert.
Die Weisung der Finanzdirektion war zu weit gefasst und stellte sich in dieser Hinsicht als gesetzeswidrig heraus; sie wurde geändert.

- Die Voraussetzungen, unter denen eine Datensperre durchbrochen werden kann, dürfen nicht zu weit gefasst sein: Nur die Verfolgung eigener Rechte ist hinreichend.

Neuer Datenschutz

An einer Informationsveranstaltung und Medienorientierung wurden neue Instrumente für einen effizienten Datenschutz vorgestellt und diskutiert.

Fünf Jahre Datenschutzgesetz im Kanton Zürich waren Anlass für einen Rückblick und insbesondere einen Ausblick auf die Rolle des Datenschutzes in der Informations- und Kommunikationsgesellschaft. Die Informatisierung der Verwaltung und die damit verbundene Zunahme der Datenbearbeitungen in allen Bereichen rückt zahlreiche Fragen des Datenschutzes und der Informationssicherheit in den Vordergrund. Datenschutzrecht ist Technikfolgerecht. Angesichts der rasanten Entwicklungen im Bereich der Informations- und Kommunikationstechnologien erstaunt es nicht, dass die bisherigen Konzepte nicht mehr der heutigen technologischen Realität entsprechen.

Auf Grund der entstandenen Spannungsfelder zwischen (datenschutz)rechtlichen Rahmenbedingungen und der technischen Entwicklung gilt es deshalb, die Anforderungen an den Schutz der

10 Punkte für einen wirksamen Datenschutz

1. Verwesentlichung des Datenschutzgesetzes
Das Datenschutzgesetz hat das verfassungsmässige Recht auf Datenschutz zu konkretisieren, indem die Grundprinzipien materiell ausgestaltet werden und das Gesetz von den administrativen Bestimmungen entlastet wird.
Die Grundprinzipien des Datenschutzes wie das Prinzip der Gesetzmässigkeit, der Verhältnismässigkeit oder der Zweckbindung sind so auszugestalten, dass die Datenbearbeitungen auf Grund ihrer Risiken für die Privatsphäre qualifiziert werden können. Definitionskataloge oder Verpflichtungen zur Führung von Registern, die ohne Auswirkung auf den Grundrechtsschutz bleiben, sind zu überdenken.

2. Materielle Regelungen
Das Datenschutzgesetz soll Regelungen enthalten, die auf Grund der Sensibilität der Informationen und der Art und Weise ihrer Bearbeitung für alle Bereiche die materiellen Voraussetzungen der Datenbearbeitungen umfassen.
Automatisierte Verfahren oder interaktive Anwendungen (z.B.: E-Voting) oder neue Methoden der Datenbearbeitung (z.B.: Data Warehousing, Data Mining) wie auch die Auslagerung von Datenbearbeitungen (z.B.: Outsourcing) verlangen klare Regelungen über die Voraussetzungen für deren Einführung und deren Kontrolle beim Betrieb.

3. Informationszugang und Informationsschutz
Das Datenschutzgesetz hat sowohl den Schutz wie auch den Zugang zu Informationen, die in gegenseitiger Abhängigkeit stehen, einheitlich zu regeln.
Die Interessenabwägung zwischen Datenschutz und Informationszugang oder Schutz der Privatsphäre und Veröffentlichung von Daten (z.B.: geografische Informationssysteme) ist konzeptuell einheitlich zu betrachten, da es sich um zwei Seiten der gleichen Medaille handelt und nur so Konflikte in der Praxis vermieden werden können. Umfang und Grenzen der Kommerzialisierung von Daten sind auszudiskutieren.

4. Neue Technologien
Der Einsatz neuer Technologien, die umfassende Eingriffe in die Privatsphäre der Bürgerinnen und Bürger zulassen, ist ausdrücklich zu regeln.
Insbesondere Überwachungstechnologien (z.B.: Videogeräte im öffentlichen Raum, Software im Internet) sind wegen der Risiken für die betroffenen Personen nicht ohne besondere Voraussetzungen einzuführen.
Es sind Technikfolgenabschätzungen vorzusehen und Rahmenbedingungen zu schaffen.

5. Recht und Technik
Die Wirksamkeit des Datenschutzrechts ist durch die Einführung von datenschutzfreundlichen Technologien zu verstärken. Die datenschutzfreundliche Gestaltung von Informations- und Kommunikationstechnologien ist durch Anreizsysteme und Förderungsmassnahmen zu unterstützen.
Der Einbezug technischer Elemente zum Schutz der Privatsphäre (z.B.: Verschlüsselungstechnologie) ist als gleichwertiges Element bei der Ausgestaltung der Datenschutzkonzepte zu betrachten. Deren Einbezug ist

Privatsphäre der Bürgerinnen und Bürger unter den veränderten gesellschaftlichen und technischen Bedingungen neu zu definieren.

Die Beiträge der Informationsveranstaltung sind in «Fakten» Nr. 2/2000 publiziert. Auf der Grundlage der verschiedenen Beiträge und Diskussionen wurden die 10 Punkte für einen wirksamen Datenschutz entwickelt (siehe Kasten).

Damit wurden die Grundlagen für einen angemessenen und effizienten Datenschutz im Kanton Zürich erarbeitet. Es geht nun darum, im Einzelnen die notwendigen Schritte für einen wirksamen Datenschutz in die Praxis umzusetzen. Handlungsbedarf besteht nicht zuletzt auch im Hinblick auf «E-Government». Grundvoraussetzung dafür ist das Vertrauen der Bevölkerung in die «elektronische Verwaltung». Dieses Vertrauen kann nur vermittelt werden, wenn die Rahmenbedingungen für den Schutz der Privatsphäre an die Gegebenheiten der Informationsgesellschaft angepasst und konsequent umgesetzt werden.

vorzuschreiben oder kann in einzelnen Bereichen als marktwirtschaftliches Element der Verantwortung des Datenbearbeiters übertragen werden.

6. Informationssicherheit
Das Konzept der Informationssicherheit ist auf Standards aufzubauen, wobei sowohl der Einsatz von Sicherheitselementen bei den Datenbearbeitern (Sicherheitsinfrastruktur) als auch die Verwendung von Selbstschutzinstrumenten (Systemeinstellungen) bei den Benutzerinnen und Benutzern vorzusehen und zu regeln sind.
Konzepte zur Informationssicherheit haben Prinzipien wie die Datenvermeidung oder -sparsamkeit zu konkretisieren oder anonyme oder pseudonyme Nutzungen von Systemen vorzusehen.

7. Auditierung und Zertifizierung
Die Auditierung und Zertifizierung von Systemen und Anwendungen ist für alle Datenbearbeiter vorzusehen und für sensible Datenbearbeitungen vorzuschreiben.
Eine Überprüfung von Systemen und Anwendungen vor deren Einführung auf ihre rechtliche und technische Vereinbarkeit mit den Prinzipien des Datenschutzes und der datenschutzfreundlichen Systemgestaltung führt zu einer klaren Umsetzungsstrategie des Datenschutzes in der Praxis. Damit verbunden ist eine Zertifizierung im Sinne eines Qualitätssiegels.

8. Informations- und Ausbildungsmassnahmen
Das Konzept des wirksamen Datenschutzes und die Förderung von datenschutzfreundlichen Technologien ist zu unterstützen durch Informations- und Ausbildungsmassnahmen.
Die Information über die Bedeutung der Privatsphäre in der Informations- und Kommunikationsgesellschaft, aber auch die Ausbildung über neue Technologien (z.B.: Einsatz von Verschlüsselungstechnologien) sind als dauernde Begleitmassnahmen vorzusehen.

9. Datenschutz- und Sicherheits-Kompetenzzentrum
Die Aufgaben und Funktionen des Datenschutzbeauftragten sind mit Beratungs-, Informations-, Dokumentations- sowie Zertifizierungsleistungen im Sinne eines Dienstleistungszentrums zu erweitern, was personelle, technische, organisatorische und finanzielle Mittel notwendig macht, die verhältnismässig zu den Vorhaben im Bereich der Datenbearbeitungen sind.
Die Ausrichtung im Sinne eines Dienstleistungszentrums entspricht den Anliegen der modernen Verwaltungsführung und ermöglicht eine raschere Orientierung an den Bedürfnissen der Datenbearbeiter und der betroffenen Personen. Neben dem Dienstleistungsangebot sind aber auch die Aufsicht und Kontrolle zu verstärken, um gleichzeitig den Bürgerinnen und Bürgern als Vermittlungs- und Vertrauensstelle zur Verfügung stehen zu können.

10. Datenschutz und E-Government
Die Umsetzung eines wirksamen Datenschutzes ist nicht nur im Hinblick auf die Bewahrung der Grundrechte, sondern auch in Bezug auf die Akzeptanz der neuen Informations- und Kommunikationstechniken als Teil der Entwicklung zum E-Government zu verstehen.
Die Anliegen eines wirksamen Datenschutzes sind in allen Teilbereichen der modernen Verwaltung, die die neuen Technologien nutzt, mitzuberücksichtigen.
Der daraus sich ergebende Handlungsbedarf auf gesetzgeberischer oder organisatorischer und technischer Ebene ist von den jeweiligen Verantwortlichen auch im Interesse der Vertrauensbildung gegenüber den Bürgerinnen und Bürgern wahrzunehmen.

Aufbau einer Sicherheitsinfrastruktur

Die Einführung einer kantonsweiten Public Key Infrastructure (PKI) für die sichere Datenkommunikation läuft nach Plan.

Im Tätigkeitsbericht Nr. 5 (1999), S. 22 f. berichteten wir ausführlich über die Vorbereitungsarbeiten im Projekt SOPRANO. Zur Abdeckung der Bedürfnisse einer verwaltungsweiten Sicherheitsstrategie in der kantonalen Verwaltung soll eine Public Key Infrastructure (PKI) eingeführt werden.

Für den Aufbau der zentralen Infrastruktur sollte das Projekt SOPRANO unter Leitung des Datenschutzbeauftragten weitergeführt werden und die hierfür notwendigen Mittel sollten im Rahmen eines wi*f*!-Projektes bereitgestellt werden.

Nachdem grundsätzlich die Notwendigkeit einer verlässlichen Sicherheits-Infrastruktur für die Kommunikation im Internet anerkannt wurde, erfolgte die Neupositionierung des Projektes SOPRANO als Teil des wi*f*!-Programmes und als sicherheitstechnische Grundlage der E-Government-Initiative des Kantons Zürich.

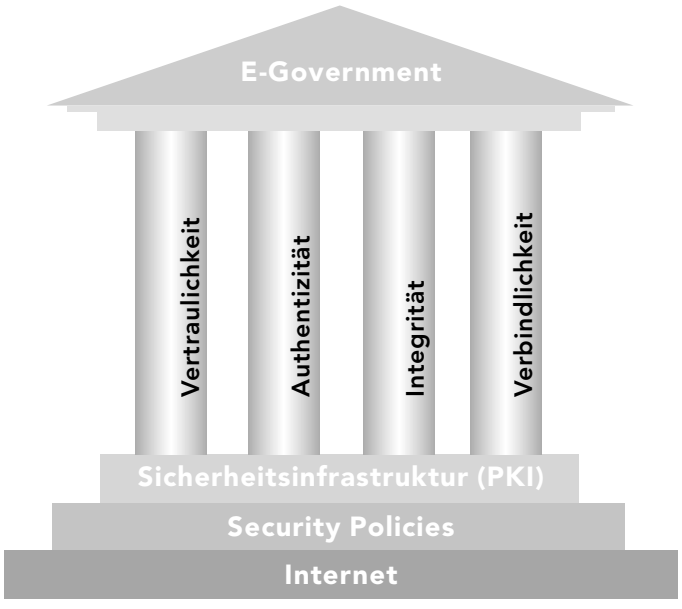
Mit Beschluss des Regierungsrates wurden die Ziele festgesetzt, die entsprechenden Mittel gesprochen und dem Datenschutzbeauftragten die Weiterführung des Projekts übertragen.
Um den Erfolg sicherzustellen, wurde das Projekt in folgende Schritte unterteilt:

- Projekt-Initialisierung
- Evaluation Produkte und Anbieter
- Ausschreibung Betreiber der Sicherheitsinfrastruktur
- Rollen und Verantwortlichkeiten
- Policies und Prozesse
- Implementierung Certification Authorities
- Pilotprojekt
- Planung Koordinationsstelle
- Planung Folgeprojekte

Für das gesamte Projekt wurde ein Projekthandbuch geschaffen. Dieses richtet sich an alle Projektbeteiligten und regelt die gesamte Projektorganisation. Neben den Beschreibungen der einzelnen Schritte wurden Termine und Meilensteine gesetzt sowie eine adäquate Projektorganisation erstellt. Das Projekt wird dabei von einer externen Firma unterstützt.

Die ersten Schritte wurden im Jahr 2000 mit einer Marktanalyse und der Festsetzung einer Strategie für den Aufbau einer PKI in die Wege geleitet. Sorgfältig mussten die sehr speziellen und vielseitigen Anforderungen des Kantons evaluiert werden. Daraus entstand eine Strategie, die wie folgt aussieht:
Die kantonale Verwaltung baut eine eigene Certification Authority

Vier Säulen für ein sicheres E-Government



(CA) auf, welche von einer kantonsinternen/-nahen Stelle betrieben wird. Die Policy wird nach eigenen Anforderungen definiert. Das Know-how wird aufgebaut und verbleibt im Kanton. Der Kanton hat die volle Kontrolle über die Funktionalität (Verwendungs- und Einsatzzweck) und den Sicherheitsstandard der Infrastruktur. Die kantonale Verwaltung und die Gemeinden akzeptieren Zertifikate von Drittanbietern (öffentliche CA), sofern diese den gesetzlichen Mindestanforderungen genügen.

Die Vorteile und besonderen Merkmale der gewählten Strategie sind:

- Bedürfnisgerechte Funktionalität
- Gestaltungsfreiheit für verwaltungsinterne Policy und Abläufe
- Kontrolle über verwaltungsinterne Sicherheitsstandards
- Aufbau von Know-how für zukünftige Integrationsprojekte
- Hohe Akzeptanz im E-Government-Umfeld
- Externe Zertifikate für Bürger/in

Als nächste Schritte im Projekt SOPRANO folgen die Installation und Durchführung von Pilotprojekten, um die detaillierten Anforderungen an den Betrieb und die Abläufe genau festlegen zu können. Ab 2002 soll die endgültige und flächendeckende Einführung erfolgen.

- Das Projekt SOPRANO wird planmässig umgesetzt. Die erarbeitete Strategie beinhaltet die Installation einer eigenen Certification Authority (CA) mit dezentralen Registration Authorities (RA) in den Direktionen/Ämtern und Gemeinden. Für die sichere Kommunikation mit der Bürgerin/dem Bürger sollen die am Markt erhältlichen Zertifikate akzeptiert werden.

Aufsicht und Sensibilisierung

Ein wirksamer Datenschutz erfordert systematische Kontrollen. Die Datenschutzreview erweist sich als geeignetes Mittel dafür.

Der Datenschutzbeauftragte hat bei ausgewählten Amtsstellen (siehe Tätigkeitsbericht Nr. 5, [1999], S. 32 und Nr. 2 [1996], S. 34) die ersten Datenschutzreviews durchgeführt.
Mit den Reviews sollen in einem bestimmten, möglichst kurzen Zeitrahmen Resultate erzielt werden: Die geprüften Stellen sollen für bestimmte Aspekte des Datenschutzes sensibilisiert werden, ihre Datenbearbeitungen an die rechtlichen Rahmenbedingungen anpassen und – wo notwendig – Verbesserungen im organisatorischen und technischen Bereich vornehmen. Diese Ziele erreichen wir, indem wir den Prüfungsumfang im Voraus festlegen, die Prüfung auf Bereiche mit sensiblen Datenbearbeitungen ausrichten und uns auf Teilaspekte beschränken.

Die Prüfungen sind in zwei Bereiche unterteilt:

Im Bereich Recht prüfen wir, ob die registrierten Datensammlungen rechtmässig geführt werden und inwieweit die rechtlichen Rahmenbedingungen für die an den IT-Systemen eingerichteten Zugriffsrechte von externen Stellen erfüllt sind. Als Externe gelten alle nicht unmittelbar zur Organisationseinheit gehörenden Stellen, zum Beispiel andere Amtsstellen, Abteilungen innerhalb der Amtsstelle sowie externe Dritte wie Fernwartungsfirmen oder andere Dienstleister. Werden externe Dienstleister beigezogen, prüfen wir das Vertragswerk; das Augenmerk gilt dabei den Regelungen über Geheimhaltung, Datenschutz und Informationssicherheit.

Im Bereich Informatiksicherheit überprüfen wir zuerst die uns von der Amtsstelle oder Gemeinde zugesandte Basisdokumentation gemäss «Leitfaden zur Umsetzung der Informatiksicherheitsverordnung» (System- und Risikoanalyse, Schutzziele und Massnahmenpläne gemäss Sicherheitsstufe).

Anschliessend kontrollieren wir vor Ort eine Auswahl der wichtigsten Grundschutzmassnahmen wie Verantwortlichkeiten Informatikbetrieb, Regelung des Passwortgebrauchs, regelmässiger Einsatz von Virenprogrammen. Ebenfalls vor Ort vergleichen wir stichprobenweise, ob der tatsächlich eingerichtete Zugriff auf Daten und Systeme mit dem von der Amtsstelle vorgelegten Zugriffskonzept übereinstimmt.

Der Ablauf der Review ist an das Vorgehen bei einer Informatikrevision angelehnt:

Wir studieren die angeforderten Unterlagen, zum Beispiel die Dokumentation gemäss «Leitfaden zur Umsetzung der Informatiksicherheitsverordnung», Verträge mit allfälligen Dienstleistungserbringern für Hard- und Software sowie Netzwerkdienstleistungen, das Register der Datensammlungen.

Anschliessend informieren wir in einem persönlichen Gespräch die verantwortliche Person in der Amtstelle, die Ansprechperson und die Mitarbeitenden bei der Review über den Ablauf der Prüfung und beantworten allfällige Fragen.

Nach erfolgter Prüfung vor Ort erstellen wir einen Bericht, der den Prüfungsumfang, die Abgrenzungen, die geprüften Punkte und Resultate sowie, falls nötig,

Häufiges Problem: «Alle dürfen alles»

In den geprüften Verwaltungsstellen war ein Zugriffskonzept meistens nur im Ansatz vorhanden. Der Datenschutzbeauftragte hat unter Zuhilfenahme von ausgewählten Massnahmen aus dem «Leitfaden zur Umsetzung der Informatiksicherheitsverordnung» eine Checkliste für die Erstellung eines angemessenen Zugriffskonzepts erarbeitet. Mit dieser Checkliste können die Administratoren eine praxisgerechte Dokumentation erarbeiten, die bei Änderungen einfach und schnell nachgeführt werden kann.

Hilfestellung für IT-Sicherheit

Der Datenschutzbeauftragte bot nach den Prüfungen Hinweise und Hilfestellung für die Umsetzung der Massnahmen und zur Sensibilisierung der Mitarbeitenden an. Das Kompetenzzentrum für IT-Sicherheit, das im Laufe des Jahres 2001 seine Arbeit aufnehmen soll, hat auch die Aufgabe, die Verwaltung im Bereich Informationssicherheit fachlich zu unterstützen.

Empfehlungen enthält. In der Schlussbesprechung stellen wir den Berichtsentwurf mit entsprechenden Erläuterungen vor und klären die letzten offenen Fragen mit den Verantwortlichen der geprüften Amtsstelle.

Im Sinne eines Informationsflusses informiert die geprüfte Amtsstelle den Datenschutzbeauftragten innert einer vorher festgesetzten Frist über die getroffenen Massnahmen gemäss den Empfehlungen des Berichts.

Nach den bisher durchgeführten Reviews stellen wir Mängel mit entsprechendem Handlungsbedarf hauptsächlich in den folgenden Bereichen fest:

- Das Erstellen und Umsetzen des Massnahmeplans im Rahmen der Informatiksicherheitsverordnung erfolgt teilweise zu rudimentär.
- Verantwortlichkeiten werden zu wenig detailliert zugewiesen.
- Es fehlt an einer Dokumentation der Zugriffsberechtigungen in Form eines Zugriffskonzepts.
- Die Verträge mit Dienstleistern sind oft ungenügend. Insbesondere bezüglich der Bestimmungen über die Art, den Zweck und den Umfang der Datenbearbeitungen, über Geheimhaltung, Datenschutz sowie Daten- und Informationssicherheit müssen die Verträge optimiert werden.

● Die geprüften Amtsstellen haben die Prüfung positiv bewertet und die Anregungen und Empfehlungen des Datenschutzbeauftragten gut aufgenommen. Das Ziel der Sensibilisierung für datenschutzrechtliche Fragen und technische Massnahmen für IT-Sicherheit wurde erreicht.

Gesetzliche Grundlagen der Review

Der Datenschutzbeauftragte überwacht die Anwendung der Vorschriften über den Datenschutz (§ 23 lit. a DSG). Er kann ungeachtet allfälliger Geheimhaltungspflichten bei öffentlichen Organen oder beauftragten Dritten schriftlich oder mündlich Auskünfte über das Bearbeiten von Personendaten einholen, Einsicht in Unterlagen und Akten nehmen und sich Bearbeitungen vorführen lassen, soweit es für seine Tätigkeit notwendig ist (§ 24 DSG). Gemäss § 11 Abs. 2 Datenschutzverordnung (DSV) sind die verantwortlichen Organe verpflichtet, an der Feststellung des Sachverhaltes mitzuwirken.

Diese umfassenden Auskunfts- und Einsichtsbefugnisse des Datenschutzbeauftragten werden durch eine entsprechende Schweigepflicht abgesichert. So sind der Datenschutzbeauftragte und seine Mitarbeitenden hinsichtlich Personendaten, die sie bei ihrer Tätigkeit zur Kenntnis nehmen, zur gleichen Verschwiegenheit verpflichtet wie das bearbeitende Organ (§ 25 Abs. 1 DSG).

Lösungsansätze und offene Fragen

In verschiedenen Bereichen finden umfangreiche Datenbearbeitungen statt, die weder verhältnismässig sind noch auf gesetzlichen Grundlagen beruhen. Teilweise wurden Lösungsansätze entwickelt.

1. Spitalberichte an Kranken- und Unfallversicherer

Unverhältnismässige Datenbekanntgaben

Mehrere Spitäler gelangten mit der Frage an uns, wie sie sich gegenüber den Kranken- und Unfallversicherern zu verhalten hätten, die immer häufiger ausführliche Berichte von ihnen verlangen (siehe auch Tätigkeitsbericht Nr. 3 [1997], S. 20 f.). Tendenziell fordern die Versicherer gehäuft detaillierte Diagnosen, Röntgenbilder, Operations-, Labor- und Austrittsberichte von den Leistungserbringern (speziell von den Spitälern). Begründet werden die Anfragen meistens mit Allgemeinplätzen wie «zur Vervollständigung unserer Akten» oder «zur Begleichung der Rechnung». Austrittsberichte werden von gewissen Versicherern systematisch verlangt.
Da es sich um eine gesamtschweizerische Tendenz handelt, das Kranken- und Unfallversicherungsrecht auf Bundesebene geregelt ist und die Versicherer unter die Aufsicht des Bundes fallen, baten wir auch den Eidgenössischen Datenschutzbeauftragten um eine Beurteilung. Dieser bestätigte unsere Auffassung.

Aus rechtlicher Sicht gilt: Berichte werden nicht für die Versicherungen, sondern für das Medizinalpersonal angefertigt und sie enthalten entsprechende Informationen. Die Weitergabe solcher Berichte an Versicherer widerspricht daher dem Grundsatz der Zweckbindung. In den Berichten sind ausserdem mehr Daten enthalten, als vom Versicherer tatsächlich benötigt werden. Damit ist auch der Grundsatz der Verhältnismässigkeit verletzt.
Die medizinischen Daten sind weder geeignet noch erforderlich, um Vergütungen festzusetzen und die Wirtschaftlichkeit von Leistungen zu überprüfen. Sofern im Einzelfall zusätzliche Daten benötigt werden – z.B. um abzuklären, weshalb eine bestimmte Behandlung ungewöhnlich viel kostet –, kann der Versicherer mit konkreten Fragen zu den benötigten Informationen gelangen.
Versicherer sollen also zusätzliche Informationen nur erhalten, wenn sie auf den Einzelfall bezogen konkret nachfragen und das Spital – wiederum auf den Einzelfall bezogen – die Frage beantworten kann. Wird die Frage in einem Austritts- oder einem anderen Bericht beantwortet, kann dieser Teil des Berichts (aber nur dieser) zur Beantwortung verwendet werden.
Problematisch ist das Vorgehen der Kranken- und Unfallversicherer auch deshalb, weil die Fülle der verlangten Informationen durch die vertrauensärztlichen Dienste der Versicherer gar nicht mehr bewältigt werden kann und direkt in die administrative Sachbearbeitung der Versicherer gelangt. Dadurch wird das medizinische Berufsgeheimnis (Art. 321 Strafgesetzbuch) ausgehöhlt und die Funktion des Vertrauensarztes in Frage gestellt.

- Wir haben den Spitälern empfohlen, den Versicherern nur im Einzelfall detaillierte Diagnosen oder Berichte auszuhändigen.
  Die Versicherer haben ihre Anfragen schriftlich zu begründen und darzulegen, warum sie auf die zusätzlichen Daten angewiesen sind.

2. Gesetz zur Bewirtschaftung raumbezogener Daten

Regierungsrat erkennt Regelungsbedarf

Im Tätigkeitsbericht Nr. 5 (1999), S. 19 ff. berichteten wir über die Problematik der Datenbearbeitungen im Zusammenhang mit geografischen Informationssystemen und wiesen auf die fehlenden gesetzlichen Grundlagen hin.
Im letzten Jahr fanden in verschiedener Hinsicht Entwicklungen statt.

Mehrere Amtsstellen wandten sich an uns und wollten in konkreten Fällen wissen, ob bestimmte Daten in der geplanten Weise im Internet veröffentlicht werden dürften. Obwohl die Projekte nur geringfügige Eingriffe in die Persönlichkeitsrechte zur Folge hätten, brachten wir mangels gesetzlicher Grundlagen Vorbehalte an und mussten die Frage der Zulässigkeit letztlich offen lassen.

Eine Bank wollte Daten über die Gebäudeschätzungen der Gebäudeversicherung erwerben. Für das Hypothekargeschäft erhält die Bank bereits heute – jeweils auf Grund einer Einwilligung der betroffenen Person im Einzelfall – die Schätzwerte der Gebäudeversicherung. Laut Projekt sollten der Bank in einer Initialladung alle definierten Daten (Gebäude mit Katasternummer, Erstellungsjahr, Basiswert, Schätzwert und Versicherungssumme, Schätzungsdatum und -grund sowie Eigentümerangaben) geliefert werden und sie sollte regelmässig über Mutationen informiert werden.

Wir wiesen darauf hin, dass dafür die Einwilligung aller Grundeigentümer erforderlich ist, weil gesetzliche Grundlagen für eine umfassende und regelmässige Datenübermittlung fehlen.
Ausserdem ist die Gebäudeversicherung als verantwortliches Organ in die Diskussion einzubeziehen. Die geplante Lösung ist zudem unverhältnismässig, weil für das Hypothekargeschäft weit weniger Daten benötigt werden, als laut Projekt übermittelt werden sollten.
Zu bedenken ist in einem solchen Fall schliesslich, dass nach dem Grundsatz der Gleichbehandlung alle Banken ein gleiches Recht zum Bezug der Daten hätten, womit faktisch ein öffentliches Register geschaffen würde.
Die Gebäudeversicherung teilte unsere Bedenken.
Das Projekt wird weiterverfolgt und es soll ein elektronisches Verfahren entwickelt werden, das eine Abbildung des Status quo der Einzelanfragen (die sich auf Einwilligungen der Betroffenen stützen) darstellt. Unerlässlich sind auch geeignete Kontrollmechanismen, die gewährleisten, dass nur die zulässigen Daten bearbeitet werden.

Die Beispiele belegen den Handlungs- bzw. Regelungsbedarf im Bereich der Geodatenbearbeitungen. Der Regierungsrat hat deshalb beschlossen, die notwendigen gesetzlichen Grundlagen zu schaffen. Hintergrund dafür ist das Projekt für ein Gebäude- und Wohnungsregister (GWR). Im Rahmen der Volkszählung 2000 erstellt der Bund unter Mitwirkung der Kantone ein Gebäude- und Wohnungsregister. Weil das GWR einem zweiten Gebäuderegister im Kanton Zürich entspräche, soll das bestehende System so ausgebaut werden, dass es den Anforderungen des Bundes an das GWR genügt.
Wir hielten fest, dass für die Verwendung des GWR für kantonale Zwecke keine gesetzlichen Grundlagen bestehen. Die bundesrechtlichen Grundlagen genügen nicht, da sie nur die Bearbeitung der Daten für Aufgaben des Bundes regeln.
Der Regierungsrat beschloss dann, das bestehende System in ein vom Bund anerkanntes GWR zu überführen. Gleichzeitig beauftragte er die Baudirektion, mit den betroffenen Stellen die notwendigen Rechtsgrundlagen für die Datenbearbeitungen im Bereich der Bewirtschaftung raumbezogener Daten zu schaffen.

- Die Gesetzgebung im Geodatenbereich ist nach den Grundsätzen der Datenvermeidung und Datensparsamkeit zu konzipieren und sollte folgende Punkte regeln: Zweck, Art und Umfang der Datenbearbeitungen, Kombinationen, Verantwortungen, Datenaustausch und Veröffentlichungen, Kommerzialisierung und Rechtsansprüche Betroffener.

3. Datenbearbeitungen im kirchlichen Bereich

Datenschutzreglement in Kraft getreten

Die bereits 1995 begonnenen Arbeiten betreffend Datenbearbeitungen im kirchlichen Bereich (vgl. Tätigkeitsberichte Nr. 1 [1995], S. 20 f., Nr. 2 [1996], S. 32 f. und Nr. 3 [1997], S. 42) konnten im Berichtsjahr abgeschlossen werden.

In den Ordnungen der beiden (grössten) Landeskirchen wurden per 1. Juli 2000 gesetzliche Grundlagen für den Datenschutz geschaffen (Art. 18a der Kirchenordnung der evangelisch-reformierten Landeskirche, Art. 4a der Kirchenordnung der römisch-katholischen Körperschaft). Zudem trat auf denselben Zeitpunkt – als Ergänzung zur staatlichen Datenschutzgesetzgebung – das Kirchliche Datenschutzreglement in Kraft, welches ebenfalls in der Gesetzessammlung veröffentlicht ist und für alle Landeskirchen Geltung hat.

Weiter schufen die Landeskirchen in Zusammenarbeit mit dem Datenschutzbeauftragten und der Gesundheitsdirektion Empfehlungen für den Datenschutz in der Spitalseelsorge an den öffentlich-rechtlichen Spitälern im Kanton Zürich. Für die Spitalaufnahme erarbeiteten sie ein Musterformular, in welchem Patientinnen und Patienten für die Spitalseelsorge freiwillig die Konfession angeben können.

- Mit den kirchlichen Datenschutzbestimmungen konnten die Grundlagen geschaffen werden für den Umgang mit Personendaten in diesem sensiblen Bereich.

4. Volkszählung 2000

Fragen der Kontrolle im Vordergrund

Am 5. Dezember 2000 war der Stichtag der Volkszählung 2000. Die Aufgabe des kantonalen Datenschutzbeauftragten lag vor allem in der Beratung und Kontrolle der involvierten kommunalen und kantonalen Stellen. Da die Mehrzahl der zürcherischen Gemeinden einen Teil der Datenbearbeitungen im Rahmen der Volkszählung an ein Dienstleistungszentrum auslagerte, gehörte auch die Kontrolle dieser Datenbearbeitungen zu den Aufgaben des kantonalen Datenschutzbeauftragten.
Im Tätigkeitsbericht Nr. 5 (1999), S. 14 konnten wir über die Vorbereitungen zur Volkszählung berichten. Zahlreiche Gemeinden wandten sich im Jahre 2000 mit Fragen zur Volkszählung an den Datenschutzbeauftragten. Wir verteilten ein Merkblatt an alle zürcherischen Gemeinden und informierten sie über die Aufgaben und Verantwortungen im Bereich des Datenschutzes. Weiter wurden die Aufbewahrung und Vernichtung der Erhebungspapiere und elektronischen Datenträger sowie die Informatiksicherheit thematisiert. Schliesslich gaben wir den Gemeinden ein Merkblatt zur Einhaltung des Datenschutzes bei der Erhebung der Kollektivhaushalte ab.

Die meisten Zürcher Gemeinden haben einen Teil ihrer Aufgaben dem externen Dienstleistungszentrum übertragen. Bezüglich dieser ausgelagerten Aufgabenbereiche hatte das Dienstleistungszentrum die zürcherischen Datenschutzbestimmungen zu beachten.
Da auch die Gemeinden anderer Kantone ihre Daten durch dasselbe Dienstleistungszentrum bearbeiten liessen, stellten sich für alle kantonalen Aufsichtsbehörden dieselben Fragen der Datenschutzkontrolle. Eine wirksame Datenschutzaufsicht ist ein entscheidender Faktor dafür, dass überhaupt ein Dienstleistungszentrum eingesetzt werden kann. Die Sicherstellung des Datenschutzes erfordert eine umfassende, anspruchsvolle und aufwändige Überprüfung von Konzepten und Massnahmeplänen, von Organisationen und Abläufen.
Nur eine unabhängige Datenschutzkontrolle im Sinne einer umfassenden, prozessorientierten Informatikrevision, die allerdings die rechtlichen Fragen nicht ausklammert, kann dies gewährleisten.

Aus diesem Grunde fanden sich die Datenschutzbeauftragten schon früh zu einer Arbeitsgruppe zusammen, die dem Bundesamt für Statistik als dem für die Durchführung der Volkszählung verantwortlichen Organ bezüglich Datenschutz Anregungen unterbreitete.
Konkret lautete der Vorschlag, das Dienstleistungszentrum sei zu verpflichten, ein unabhängiges Datenschutzkontrollorgan einzurichten. Darüber hinaus schlossen sich die Datenschutzbeauftragten zu einem Aufsichtsgremium zusammen, das die Berichte dieses Kontrollorgans überprüfen sollte und auch eine eigene Kontrolltätigkeit entwickeln konnte. Diesem Gremium gehörten die Kantone Basel-Stadt, Freiburg, Zürich und der Eidgenössische Datenschutzbeauftragte an. Damit sollten die Anliegen aller kantonalen Datenschutzbehörden abgedeckt werden.

Im Verlaufe der Arbeiten zeigte sich, dass die vom Dienstleistungszentrum berufene Datenschutztreuhandstelle den Anforderungen keineswegs zu genügen vermochte. Die Bemühungen des Aufsichtsgremiums, eine eigenständige Informatikrevision beim Dienstleistungszentrum durchzuführen, wurden durch das Verhalten der beteiligten Stellen kompromittiert. Zudem nahm auch der Eidgenössische Datenschutzbeauftragte Abstand von der gemeinsamen Position der kantonalen Datenschutzbeauftragten und desavouierte damit eine effiziente Kontrolltätigkeit.
Nach Abschluss der Erhebung durch die Gemeinden ging die aufsichtsrechtliche Verantwortung vollständig an den Bund über.
Die kantonalen Aufsichtsbehörden sind wieder involviert, wenn es um die Nachführung der Einwohnerregister geht.

- Bei der Volkszählung zeigte sich, dass Kontrollen grosser Informatiksysteme nur nach professionellen Methoden, wie sie die Informatikrevision zur Verfügung stellt, wirksam erfolgen können. Fehlen solche Kontrollen, sind keine Aussagen über die Vertrauenswürdigkeit von Datenbearbeitungen möglich. Alle Datenschutzbeauftragten sollten über solche Kontrollisnstrumente verfügen und sie nutzen. Im Rahmen der Datenschutzreviews gelangen sie im Kanton Zürich systematisch zur Anwendung.

Neues Informationskonzept

Mit einem zielgruppenspezifischen Angebot befriedigt der Datenschutzbeauftragte das Informationsbedürfnis von Verwaltung und Bevölkerung.

1. Fünftes Symposium für Datenschutz und Informationssicherheit

«Die Entschlüsselung des Menschen» als Schwerpunkt

Das jährliche Symposium, das der Datenschutzbeauftragte zusammen mit dem Departement Informatik der ETH Zürich organisiert, fand im Oktober 2000 zum fünften Mal statt. Im Mittelpunkt stand das Thema Genforschung mit seinen (datenschutz)rechtlichen Implikationen. Einleitende Worte sprachen die Regierungspräsidentin des Kantons Zürich, Rita Fuhrer, und der Vizepräsident der ETH Zürich, Prof. Dr. Albert Waldvogel.
Prof. Dr. Hansjakob Müller, Leiter der Abteilung Medizinische Genetik des Universitäts-Kinderspitals beider Basel, verschaffte den Anwesenden einen Überblick über den aktuellen Stand der Genforschung beim Menschen und illustrierte das Potenzial der Genforschung für die Prävention und Heilung von Krankheiten.
Das Spannungsfeld zwischen biotechnologischen Möglichkeiten und ethischen Schranken leuchtete Prof. Dr. Bartha M. Knoppers aus. Sie präsidiert die Ethikkommission der «Human Genome Organisation» und trat dezidiert dafür ein, dass eine gesellschaftliche Diskussion über die ethischen und rechtlichen Rahmenbedingungen stattfindet. Prof. Dr. Hansjürgen Garstka, Berliner Beauftragter für Datenschutz und Akteneinsicht, setzte sich mit den datenschutzrechtlichen Aspekten der Genforschung auseinander. Er wies vor allem auf die ungelösten Fragen hin: Was darf mit Daten aus Gentests gemacht werden? Sollen (bestimmte) Personen oder Personengruppen – z.B. von Versicherungen oder Arbeitgebern – zu einem Gentest gezwungen werden können? Anschliessend diskutierten die Referentin und die Referenten unter Leitung von Helen Issler, Redaktionsleiterin von «Menschen Technik Wissenschaft» des Schweizer Fernsehens DRS, in einem Podiumsgespräch weiter.

Im zweiten Teil der Veranstaltung sprach Prof. Dr. Rainer J. Schweizer, Präsident der Eidgenössischen Datenschutzkommission, über aktuelle Rechtsfragen im Bereich des Datenschutzes. Anhand der Praxis des Bundesgerichts und der Datenschutzkommission erläuterte er, wie bestimmte Fragen gelöst wurden und welche Bereiche einer Klärung bedürfen.
Nick Mansfield, Chefberater für IT-Security bei Shell, erläuterte am Beispiel der Shell-Lösung, wie multinationale Unternehmen im Zeitalter von «Informationskriegen» und Industriespionage Verteidigungsstrategien – u.a. im Bereich des E-Commerce – entwickeln können.

Zum Abschluss warf Prof. Dr. Bernt Schiele, Professor für Computerwissenschaft an der ETH Zürich, einen Blick in die (nicht mehr so ferne) Zukunft. Er zeigte auf, dass in der Informationstechnologie ein Quantensprung bevorsteht, wenn unsichtbare Rechner und neue Services zum Alltag werden.

Zum zweiten Mal gab es die parallel zur Veranstaltung organisierte Fachausstellung, an der sich interessierte Personen über Lösungen im Bereich der Informatiksicherheit informieren konnten. Das Symposium hat mittlerweile eine neue Trägerschaft; es wird in Zukunft von der Stiftung für Datenschutz und Informationssicherheit durchgeführt. Neu wird es zwei Tage dauern, damit noch mehr Praxisbezug möglich wird. Das «Symposium on Privacy and Security» findet am 1./2. November 2001 in Zürich statt.

- Das Symposium für Datenschutz und Informationssicherheit spricht jedes Jahr viele Teilnehmer an. So ist es möglich, wichtige Standpunkte des Datenschutzes und der Informationssicherheit zu thematisieren.

2. Virtuelles Datenschutzbüro

Internationale Internetplattform der Datenschutzbeauftragten

Im Jahr 2000 konnte ein neue Dienstleistung von Datenschutzbeauftragten aus der ganzen Welt der Öffentlichkeit vorgestellt werden: das virtuelle Datenschutzbüro. Dieser Service wurde auf Initiative des Unabhängigen Landeszentrums für Datenschutz des Bundeslandes Schleswig-Holstein als gemeinsames Projekt verschiedener Datenschutzbehörden lanciert.

Neben interessanten Informationen finden sich im virtuellen Datenschutzbüro Diskussionsforen zu aktuellen Datenschutzthemen sowie ein Newsticker. Ausserdem wird ein Bereich mit Datenschutz-Tools eingerichtet, die sich Internet-Nutzerinnen und -Nutzer kostenlos herunterladen können. Das virtuelle Datenschutzbüro soll als weltweite Plattform für Projekte dienen und die Vernetzung der Datenschutzbeauftragten ermöglichen, denn gemeinsam und arbeitsteilig lassen sich die Themen viel besser bearbeiten.
Transparenz ist das zentrale Motto im Datenschutzbüro. Das bedeutet: Offenheit für Konzepte, offene Diskussionen und Einsatz von so genannter Open-Source-Software, die ihre Vertrauenswürdigkeit überprüfbar macht, indem ihr Quellcode offen gelegt und damit für jede(n) einsehbar wird. Im virtuellen Datenschutzbüro sollen sich auch Teams zusammenfinden, die gemeinsam neue datenschutzfördernde Techniken (Privacy Enhancing Technologies) für Nutzerinnen und Nutzer entwickeln.
Die beteiligten Datenschutzbeauftragten betrachten das virtuelle Datenschutzbüro als Antwort auf die Herausforderungen für die Privatsphäre, die neue Technologien wie das Internet mit sich bringen. Zugleich wollen sie mit der Kooperation im virtuellen Datenschutzbüro durch Arbeitsteilung, Spezialisierung und systematische Bündelung ihrer Ressourcen ihre Effizienz steigern.

- Der Datenschutzbeauftragte des Kantons Zürich stellt mit dem Portal «www.datenschutz.ch» einen direkten Einstieg ins virtuelle Datenschutzbüro zur Verfügung und ist seinerseits mit Beiträgen im virtuellen Datenschutzbüro vertreten. Das Internet-Angebot unter «www.datenschutz.ch» wird in Zukunft weiter ausgebaut und mit dem virtuellen Datenschutzbüro abgestimmt werden.

3. Neue Formen der Information

Sensibilisierung für die Anliegen des Datenschutzes

Die Information und Sensibilisierung für die Anliegen des Datenschutzes gehört zu den ständigen Aufgaben des Datenschutzbeauftragten. Es gilt, den Informationsbedürfnissen der Verwaltung und der Bürgerinnen und Bürger Rechnung zu tragen.
Diese Bedürfnisse sind in den letzten Jahren stetig gestiegen: Es werden immer mehr und immer detailliertere Informationen verlangt. Gleichzeitig werden höhere Ansprüche an die Aktualität gestellt. Es war deshalb ein neues Informationskonzept notwendig, das diese Bedürfnisse befriedigen kann und gleichzeitig die beschränkten Ressourcen des Datenschutzbeauftragten berücksichtigt. Im Zentrum stand die Vernetzung der Informationen: Die bestehenden Kommunikationsmittel und -plattformen sollten so verstärkt werden, dass die Informationen mit möglichst wenig zusätzlichem Aufwand für mehrere Zielgruppen genutzt werden können. Dabei wird dem Nutzen von Synergien grosse Bedeutung zugemessen. Dies bedingt, dass die Informationen von Anfang an entsprechend aufbereitet werden.
Diese grundsätzlichen Überlegungen werden im Jahre 2001 erste Auswirkungen zeigen. «Fakten» – die Zeitschrift für Datenschutz des Kantons Zürich – wird in dieser Form nicht mehr herausgegeben (eine inhaltliche Übersicht über alle in «Fakten» erschienenen Beiträge wurde in «Fakten» Nr. 4/2000 publiziert). Informationen, die

bisher in «Fakten» erschienen, sollen in zwei neuen Gefässen publiziert werden:

- «digma» – die Zeitschrift für Datenrecht und Informationssicherheit – erscheint seit Frühjahr 2001 im Verlag Schulthess Juristische Medien AG Zürich. Dank einer breit abgestützten Herausgeberschaft aus Juristen und Informatikern sowie einer professionellen Redaktion wird es möglich sein, umfassende Informationen im Bereich des Datenschutzes und der Informationssicherheit effizient aufzubereiten.

- «www.datenschutz.ch» – die Homepage des Datenschutzbeauftragten des Kantons Zürich – wird neu gestaltet. In Zukunft werden wir vermehrt aktuelle Informationen zielgruppengerecht publizieren können. Wir werden häufig gestellte Fragen (FAQ) beantworten und noch mehr Informationen, insbesondere im Bereich der Informationssicherheit, bereitstellen. Die einzelnen Benutzerinnen und Benutzer werden die Informationen nach ihrem jeweiligen Tätigkeitsgebiet aufbereitet vorfinden. Vermehrt wollen wir auch gezielt Lösungen aus einzelnen Bereichen präsentieren.

Daneben führen wir die Sensibilisierung und Information durch Ausbildungs- und Weiterbildungsmöglichkeiten im Rahmen von Seminaren und Referaten fort.

- Die vermehrte Nutzung der neuen Medien in der Verwaltung und durch die Bürgerinnen und Bürger macht eine ständige Überprüfung des Informationskonzepts zur Pflicht. Aus diesem Grunde haben wir neue Angebote entwickelt, die noch besser die Bedürfnisse der Verwaltung und der Bevölkerung nach Informationen zu Datenschutz und Informationssicherheit abdecken.

Eine Probenummer von «digma» kann beim Datenschutzbeauftragten bestellt werden, wo auch alle Ausgaben von «Fakten» noch erhältlich sind.

4. Von «Fakten» zu «digma»

Neue Zeitschrift zu Datenrecht und Informationssicherheit

Wie im letzten Jahr konnten wir vier Nummern von «Fakten» herausgeben:

- Das Heft 1/2000 befasst sich umfassend mit dem Thema Durchbrechung einer Datensperre. Es enthält zudem Empfehlungen für die korrekte Bildung und Verwendung von Passwörtern.
- Die Sondernummer 2/2000 enthält die Beiträge der Veranstaltung «Neuer Datenschutz» und ein 10-Punkte-Programm für einen wirksamen Datenschutz (siehe auch Seite 28 f.).
- Schwerpunktthema des dritten Heftes waren Empfehlungen für den Gebrauch des Internets an den Schulen.
- Den Abschluss bildet das Heft 4/2000 mit einer Inhalts- und einer Themenübersicht über sämtliche Nummern von 1995–2000.
  Mit dieser Nummer haben wir die Publikation von «Fakten» eingestellt.

Seit dem Frühjahr 2001 erscheint unter dem Namen «digma» eine neue Zeitschrift für Datenrecht und Informationssicherheit, die von Wissenschaftlern und Praktikern aus Recht und Technologie in einem Fachverlag herausgegeben wird. Wir sind an dieser Zeitschrift beteiligt und werden wichtige Themen und Aspekte einbringen.

- Da die Herausgabe von «Fakten» immer mehr Ressourcen beim Datenschutzbeauftragten beanspruchte, um den zunehmenden Informationsbedürfnissen zu genügen, stellt die Zeitschrift «digma» eine sehr gute Nachfolgerin dar.

5. Zusammenarbeit der Datenschutzbeauftragten

Gründung der Vereinigung DSB+CPD.CH

Die Zusammenarbeit zwischen den Datenschutzbeauftragten dient einerseits dem Meinungsaustausch, andererseits aber auch der Ausarbeitung von gemeinsamen Lösungen. Wir haben deshalb immer grossen Wert auf diese Zusammenarbeit gelegt, um Synergien zu schaffen und die beschränkten Ressourcen besser nutzen zu können.

Auf kantonaler Ebene finden regelmässig Sitzungen der kommunalen Datenschutzbeauftragten statt, an denen auch der kantonale Datenschutzbeauftragte teilnimmt. Hier werden vor allem Themen besprochen, die auf kommunaler Ebene anstehen.

Auf nationaler Ebene wurde im vergangenen Jahr die Vereinigung der schweizerischen Datenschutzbeauftragten (DSB+CPD.CH) gegründet. Zurzeit sind mit Ausnahme des Kantons Wallis alle kantonalen Datenschutzbehörden wie auch der Eidgenössische Datenschutzbeauftragte Mitglied. Durch Informations- und Erfahrungsaustausch, Weiterbildung und Unterstützung bei der Meinungsbildung soll die Kompetenz der Mitglieder auf dem Gebiete des Datenschutzes verbessert und ein effizienter Einsatz der überall knappen Mittel erreicht werden.
Die Vereinigung nimmt in Vernehmlassungsverfahren Stellung zu Datenschutzfragen und stellt den Mitgliedern Grundlagen für die kantonsinterne Ausarbeitung von Stellungnahmen zur Verfügung. Im letzten Jahr wurden unter anderem die Revision des Ausländergesetzes, die Entwürfe für ein Ausweisgesetz und ein Öffentlichkeitsgesetz unter die Lupe genommen.

In Weiterbildungsveranstaltungen setzen sich die Mitglieder der Vereinigung mit aktuellen Fragen des Datenschutzes auseinander, zum Beispiel mit «Internet in der Schule» und «Datenschutzaufsicht – Funktion, Instrumente und Ressourcen für neue Herausforderungen». An der 7. Schweizerischen Konferenz der Datenschutzbeauftragten in Basel widmeten sie sich den Themen «Data ware-

housing und Data mining im öffentlichen und privaten Bereich» und «E-Government – Neue Herausforderungen für den Datenschutz».

Das Büro der Vereinigung wurde im Jahre 2000 präsidiert vom Datenschutzbeauftragten des Kantons Basel-Landschaft; nach dessen Rücktritt als Datenschutzbeauftragter übernahm der Datenschutzbeauftragte des Kantons Bern das Präsidium; der Datenschutzbeauftragte des Kantons Zürich ist Mitglied des Büros.

- Dank der Zusammenarbeit mit anderen Datenschutzbeauftragten ist es möglich, zahlreiche Fragen des Datenschutzes umfassend und effizient zu bearbeiten. Die gewonnenen Synergien fliessen direkt in die eigene Informations-, Beratungs- und Kontrolltätigkeit.

---

6. «Sicher ist sicher…»
Erfolgreiche Aktion weitergeführt

Die unverändert grosse Nachfrage nach der Broschüre mit Sicherheitstipps für den PC-Arbeitsplatz und dem dazugehörigen Mousepad führte zu einer zweiten Auflage der Aktion «Sicher ist sicher…» (siehe Tätigkeitsbericht Nr. 5 [1999], S. 34 f.). Mit einem neuen Cartoon und einer leicht angepassten Broschüre wollen wir weiterhin auf Gefahren und Risiken aufmerksam machen, die der Einsatz von Informatik mit sich bringt, und den PC-Benutzenden praktische Tipps zur Verbesserung der Sicherheit an ihrem PC-Arbeitsplatz geben. Aktualisiert wurden insbesondere die Hinweise auf Virenschutzprogramme und auf Sicherheitsmassnahmen bei der Nutzung des Internets. Die Broschüre steht auch im Internet zur Verfügung; es besteht zudem die Möglichkeit, direkt Fragen zu einzelnen Bereichen zu stellen.

- Mit dem Mousepad und der Broschüre der Aktion «Sicher ist sicher…» steht den PC-Anwenderinnen und -Anwendern in Verwaltung, Gemeinden, Schulen und Spitälern ein praxisnahes Hilfsmittel zur Verbesserung der Sicherheit am PC-Arbeitsplatz zur Verfügung.

Datenschutzbeauftragter
Kanton Zürich
Postfach
8090 Zürich
Tel.: +41 1 259 39 99
Fax: +41 1 259 51 38
E-Mail: datenschutz@dsb.zh.ch
Web: www.datenschutz.ch
www.zh.ch/dsb

Datenschutzbeauftragter:
Dr. iur. Bruno Baeriswyl

Juristisches Sekretariat:
lic. iur. Marco Fey
(ab 1.6.2001 Stellvertreter des
Datenschutzbeauftragten)
lic. iur. Barbara Mathis Aeppli (ab 1.10.2000)
lic. iur. Joëlle Kupfer-Matey (ab 1.3.2001)
lic. iur. Barbara Egli Vetsch (ab 1.5.2001)

IT-Sicherheitsberatung und -Revision:
Andrea C. Mazzocco, CISA

Projektleitung SOPRANO:
René Müller (ab 1.3.2001)

Sekretariat:
Tanja Blass

Tätigkeitsbericht Nr. 6 (2000)
ISSN 1422-5816

Konzeption und Produktion:
Frontpage 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