Nr. 7

Tätigkeits-Bericht

Datenschutzbeauftragter des Kantons Zürich

2001

Tätigkeitsbericht

Nr. 7
2001

Der Datenschutzbeauftragte erstattet dem Regierungsrat jährlich oder nach Bedarf einen Bericht über seine Tätigkeit (§ 23 Datenschutzgesetz). Der vorliegende Tätigkeitsbericht Nr. 7 deckt den Zeitraum vom 1. Januar 2001 bis 31. Dezember 2001 ab.

Zürich, Juni 2002

Der Datenschutzbeauftragte
des Kantons Zürich
Dr. Bruno Baeriswyl

Inhaltsverzeichnis

Persönliche Freiheit und Transparenz

Der Datenschutz muss auch in der Informations- und Kommunikationsgesellschaft die persönliche Freiheit der Bürgerinnen und Bürger garantieren können. Zusätzliche Informationsbedürfnisse verlangen aber auch nach mehr Transparenz. Der Staat und die Verwaltung stehen vor neuen Herausforderungen.

Die neuen Informations- und Kommunikationstechnologien bestimmen die Datenbearbeitungen der Verwaltung zunehmend. Sie ermöglichen nicht nur einen effizienteren Umgang mit Daten und Informationen, sondern auch einen vereinfachten Datenaustausch. Der Einsatz der neuen Technologien ist zudem oftmals kombiniert mit neuen Arten der Datenbearbeitung, die eine Verknüpfung von Daten unterschiedlichster Herkunft erlauben. Weitere Technologien ermöglichen flächendeckende Überwachungen wie beispielsweise die Videoüberwachung.

Dynamik der Technik

Die Risiken für die persönliche Freiheit, die von diesen Datenbearbeitungen ausgehen, sind ebenfalls zunehmend. Die Verfügbarkeit und die Kombinierbarkeit der Daten führt zu einem neuen Gefährdungspotential für die Privatheit der Bürgerinnen und Bürger. Klassifizierungen, Diskriminierungen und Kontrolle von Informationen und damit Personen werden erleichtert. Ebenso geraten Überwachungsmassnahmen, die im Interesse der inneren Sicherheit eingesetzt werden und auch die individuelle Freiheit schützen wollen, gleichzeitig in ein Spannungsfeld zum Grundrecht der persönlichen Freiheit.

Diese Interessenkonflikte und Spannungsfelder stehen heute im Zentrum der Diskussion um den Datenschutz in der Informationsgesellschaft. Im Umfeld der bestehenden Rechtsgrundlagen sind sie nur schwer unter Kontrolle zu bringen. Es scheint vielmehr, dass das Recht in diesem Bereich seine regelnde Kraft verliert und der Dynamik der Technik seinen Platz abtreten muss. Eine solche Entwicklung wird auf die Länge eine verheerende Auswirkung auf die persönliche Freiheit und die Privatsphäre der Bürgerinnen und Bürger haben.

Offene Verwaltung

Immer zentraler wird dabei auch die Frage der Transparenz des staatlichen Handelns. Das Öffentlichkeitsprinzip will den Zugang zu staatlichen Informationen erleichtern, indem die Informationen grundsätzlich öffentlich sein sollen, wenn nicht eine spezifische Vorschrift etwas anderes bestimmt. Mit dem Zugang zu Verwaltungsinformationen soll nicht nur die demokratische Kontrolle gestärkt werden, sondern auch dem wachsenden Bedürfnis von Wirtschaft und Gesellschaft nach Informationen begegnet werden. Der Zugang zu Informationen ist aber nichts anderes als die Kehrseite der Medaille, die den Schutz der Informationen oder den Daten-

schutz regelt. Es zeigt sich auch hier, dass dieses Spannungsfeld heute nach klaren Regelungen verlangt.

Informationelle Selbstbestimmung

Tatsächlich ist die Tätigkeit des Datenschutzbeauftragten immer mehr von dieser Ausgangslage geprägt. Zahlreiche Einzelfälle aus dem vergangenen Berichtsjahr sind auf dem Hintergrund dieser Situation zu sehen.
Dabei wird deutlich, dass der persönlichen Freiheit und ihrer Bedeutung für die liberale Demokratie im Alltag oftmals zu wenig Beachtung beigemessen wird. Der liberale Staat braucht autonome Bürgerinnen und Bürger, die sich ihrer Autonomie bewusst sind und diese schätzen. Die informationelle Selbstbestimmung ist Teil der persönlichen Freiheit und damit Lebensvoraussetzung für die liberale Gesellschafts- und Wirtschaftsordnung. Diese Grundauffassung kommt auch in unserer Rechtsordnung zum Ausdruck: Der Schutz der Privatheit ist bereits in der Europäischen Menschenrechtskonvention (EMRK) und in der Bundesverfassung verankert. Das Datenschutzgesetz setzt dabei die Rahmenbedingungen, wie dieser Schutz in der Praxis zu gewährleisten ist. Damit wird deutlich, wie sehr die Missachtung des Datenschutzes das Fundament unserer liberalen Demokratie in Frage stellen kann. Ohne Privatheit ist keine Selbstbestimmung mehr möglich.

Ausreichende Rechtsgrundlagen

Im Einzelfall stellt sich diese Frage oftmals bei den Rechtsgrundlagen einer Datenbearbeitung. Der Einsatz der neuen Informations- und Kommunikationstechnologien erfolgt, ohne dass die Rechtsgrundlagen konkrete Leitplanken für den Schutz der persönlichen Freiheit der betroffenen Bürgerinnen und Bürger aufweisen würden.

Die Bedeutung einer ausreichenden Rechtsgrundlage für die jeweiligen Datenbearbeitungen wird oftmals unterschätzt. Es geht dabei nicht darum, die Gesetzesmaschinerie zu ölen und für jegliche Arten von Datenbearbeitungen Rechtfertigungsgründe im Sinne von Generalklauseln zu schaffen. Tatsächlich ist einem solchen Vorgehen, obwohl auf anderer Ebene vielfach vorgelebt, nur wenig Sinn abzugewinnen. Ebenso wenig ist indessen denen zuzustimmen, die die regelnde Wirkung des Rechts zum Vornherein verneinen und sich die «Freiheit der Datenbearbeitung» durch das Fehlen von entsprechenden Rechtsgrundlagen erwirken.
Eine Betrachtung solcher Datenbearbeitungen in Bezug auf ihr Risikopotential für die persönliche Freiheit macht die Gefährdungen deutlich. Deshalb sind auf Grund einer risikobezogenen Betrachtungsweise angemessene Rechtsgrundlagen zu schaffen. Angemessen bedeutet in diesem Zusammenhang, dass die Aufgabenerfüllung unter Respektierung der Grundrechte der betroffenen Personen zu erfolgen hat. Nur mit einer solchen Rechtsgrundlage lässt sich auch eine demokratische Legitimation der Datenbearbeitungen finden.
Die Herausforderungen in diesen Bereichen sind gross, doch haben die bisherigen Bemühungen noch wenig Resultate gezeigt.

Der Einsatz von optischen Geräten zur Überwachung (siehe S. 10), die polizeilichen Datenbearbeitungen (siehe S. 11) und das geografische Informationssystem (GIS) (siehe S. 36 f.) zeugen im Besonderen von dieser Ausgangslage.

Videoüberwachung

Jede Überwachung mittels Videogeräten, die auf die Erkennbarkeit von Personen ausgerichtet ist, bedeutet einen Eingriff in die Grundrechte, denn jede Person hat das Recht, auch im öffentlichen Raum sich unbeobachtet bewegen zu dürfen. Eine Beobachtung des öffentlichen Raumes mit Videogeräten ist deshalb nur dann möglich, wenn sich diese Massnahme als im öffentlichen Interesse geeignet und erforderlich erweist. Die Interessenabwägung in einem Einzelfall hat auf Grund der Rahmenbedingungen, die in einer Rechtsgrundlage festzuhalten sind, zu erfolgen. Da spezifische Bestimmungen über den Einsatz von optischen Überwachungsmassnahmen im Kanton Zürich fehlen, hat bisher auch keine

grundsätzliche Diskussion zwischen den Interessen nach Überwachung und den Interessen der persönlichen Freiheit stattgefunden. Im Einzelfall ist deshalb auf das Prinzip der Verhältnismässigkeit zu verweisen, das eine Massnahme ermöglichen kann, sofern sie geeignet und erforderlich ist. Dagegen fehlt es bei dieser Betrachtung an der Gesamtsicht der Überwachungsmassnahmen: Jede einzelne Massnahme kann allein betrachtet verhältnismässig sein, doch die Gesamtheit der Massnahmen kann zu einer totalen Überwachung führen.

Polizeiliche Datenbank

Wie die Entwicklung der Technologie zu neuen Gefährdungssituationen für die persönliche Freiheit werden kann, zeigt deutlich die zentrale Datenbank der Kantonspolizei. Während die Polizei bisher verschiedene, nach unterschiedlichen Zwecken getrennte Datenbanken führte, benützt sie seit einiger Zeit ein einheitliches System, in welchem sämtliche polizeilichen Vorgänge erfasst werden. Damit stehen alle von der Polizei erfassten Informationen jederzeit für alle Zwecke zur Verfügung, und es ist nicht transparent, welche Informationen wo wiederum Verwendung finden. Hier kann allein eine Rechtsgrundlage Abhilfe schaffen, die sich darüber äussern muss, zu welchen Zwecken einzelne Informationen Verwendung finden dürfen und wie lange sie aufzubewahren sind. Solange keine diesbezüglichen Rahmenbestimmungen bestehen, geht von einer solchen Art der Datenbearbeitung ein unbestimmtes Risiko für betroffene Personen aus.

Geografisches Informationssystem

Obwohl das Risikopotential, wie es ein Datenpool für raumbezogene Daten auch in Bezug auf die Verletzung von Persönlichkeitsrechten beinhaltet, schon längst erkannt wurde, sind keine konkreten Bemühungen für die Schaffung angemessener Rechtsgrundlagen sichtbar. Da laufend neue Investitionen in diese Technologie der Datenbearbeitung erfolgen und sich der Datenpool immer mehr anfüllt, ist diese Situation unbefriedigend. Der «Freiraum», den sich die verantwortlichen Stellen mit diesem Abwarten schaffen, untergräbt die Grundrechte der betroffenen Personen. Die Risiken dieser Datenbearbeitungen für die betroffenen Personen wachsen, da es unklar bleibt, welche Datenbearbeitungen nun zulässig sind oder nicht. Bei dieser Situation kann auch kein Vertrauen in moderne Datenbearbeitungen der Verwaltung aufgebaut werden, da letztlich die Transparenz für die betroffenen Personen fehlt. Dies ist insbesondere auch im Hinblick auf den Einsatz moderner Informations- und Kommunikationstechnologien im Rahmen von E-Government keine Ausgangslage, die die Akzeptanz neuer Technologien bei den Bürgerinnen und Bürgern fördern kann (siehe S. 13).

Konzept für neue Gesetzgebung

Die Herausforderungen der neuen Informations- und Kommunikationstechnologien für den Schutz der Privatheit und die Bedürfnisse nach einem erweiterten Informationszugang haben zu einem neuen Ansatz für eine wirkungsorientierte Gesetzgebung in diesem Bereich geführt (siehe S. 31 ff.). Die gesamtheitliche Betrachtung der Informationsbearbeitung zeigt, dass der Zugang zu Informationen respektive der Schutz der Informationen zusammengehören: sie sind die Kehrseiten derselben Medaille. Bei einer solchen Betrachtungsweise können die Anliegen des Öffentlichkeitsprinzips, dessen Einführung in einer Motion verlangt wird, und die Bedürfnisse nach einem effizienten Schutz der Privatheit aufeinander abgestimmt geregelt werden. Gleichzeitig gibt dieses Gesetzgebungskonzept den Anlass, den Datenschutz technologieorientiert anzupassen und die Auswirkungen der modernen Informations- und Kommunikationstechnologien, wie sie in der Verwaltung eingesetzt werden, grundrechtskonform auszugestalten. Damit erweist sich dieses konzeptionelle Vorgehen, wie es vom Regierungsrat verabschiedet wurde, als grosse Chance, einen effizienten Datenschutz zu schaffen. Viele der anstehenden Spannungsfelder, die sich auf Grund der Entwicklung der Technologie und der Methoden der Datenbearbeitungen ergeben

haben, lassen sich damit zukunftsweisend regeln.

Informationssicherheit

Besonders ausgeprägt zeigt sich die Risikosituation auch in Bezug auf die Sicherheit der neuen Informations- und Kommunikationsmittel. Das Projekt SOPRANO (siehe S. 34 f.) hat die Einführung einer verwaltungsweiten Sicherheitsinfrastruktur zum Ziel. Damit wird bei den meisten Arten der Datenbearbeitung eine vertrauliche und authentische Kommunikation auf der Basis einer allgemeinen Sicherheitsumgebung ermöglicht. Dieses Projekt ist deshalb nicht nur wegleitend für den sicheren Einsatz von neuen Informationstechnologien beispielsweise im Rahmen von E-Government-Projekten, sondern auch in Bezug auf die konzeptionelle Ausgestaltung des Datenschutzes in der Zukunft. Wenn es gelingt, die Technik so zu gestalten, dass sie datenschutzfreundlich eingesetzt werden kann, minimieren sich die Risiken für den Umgang mit Personendaten um ein Vielfaches. Dabei hat das Recht eine datenschutzfreundliche Technikgestaltung so weit wie möglich zu verlangen.
Schliesslich zeigt sich bei den Datenschutz-Reviews (siehe S. 29 f.), wie mit wenigen zielgerichteten Massnahmen eine Grundsicherheit eines Informatiksystems erreicht werden kann. Tatsächlich zeigt sich in der Praxis, dass zahlreiche Mängel immer wieder auftauchen und durch ein vermehrtes Sicherheitsbewusstsein der verantwortlichen Stellen ohne grösseren Aufwand vermieden werden könnten. Gerade bei kleineren Amtsstellen und Gemeinden werden vielfach die Risiken, die mit dem Einsatz neuer Informationstechnologien verbunden sind, nicht wahrgenommen und so entsprechende Massnahmen vernachlässigt.

Datenschutz am Wendepunkt

Die Entwicklungen zeigen, dass der Datenschutz an einem eigentlichen Wendepunkt angelangt ist. Auf der konzeptionellen Ebene wird er an die neuen Entwicklungen und Bedürfnisse der Informations- und Kommunikationsgesellschaft angepasst. Im technischen Bereich steht die datenschutzfreundliche Technikgestaltung im Vordergrund.
Bis diese neuen Leitlinien bestehen, wird es aber noch einige Zeit dauern. Dabei erscheint es entscheidend, dass auch in der aktuellen Situation ein grundrechtskonformer Umgang mit Personendaten garantiert wird und entsprechende angemessene Rechtsgrundlagen geschaffen werden. Ebenso sind bereits heute dem Stand der Technik entsprechende Sicherheitsmassnahmen zu treffen.
In diesem Sinne tragen die Beratungen und Stellungnahmen des Datenschutzbeauftragten, wie sie im vorliegenden Tätigkeitsbericht dargestellt werden, zu einer pragmatischen Umsetzung der Anliegen der persönlichen Freiheit bei. Wesentlicher Bestandteil ist deshalb immer die Information (siehe S. 38 ff.). Mit der Sensibilisierung für die Anliegen des Datenschutzes werden die einzelnen Verwaltungsstellen in die Lage versetzt, ihre Verantwortung im Bereich des Datenschutzes und der Informationssicherheit eigenständig wahrzunehmen. Sie haben die Verantwortung für den grundrechtskonformen Umgang mit den Daten der Bürgerinnen und Bürger. Damit können sie die notwendige Grundlage schaffen für das Vertrauen der Bürgerinnen und Bürger und die Akzeptanz der neuen Informations- und Kommunikationstechnologien, welche sie zunehmend einsetzen.

Umfangreiche Beratungstätigkeit

Die Umsetzung des Datenschutzes verlangt weiterhin eine intensive rechtliche und sicherheitstechnische Beratung.

POLIZEI UND JUSTIZ

1. Videoüberwachung

Fehlende Rechtsgrundlagen in Einzelfällen

Verschiedene Gemeinden wandten sich an uns, weil sie planten, öffentliche Gebäude oder Plätze mit Videokameras zu überwachen.

Videoüberwachung auf öffentlichen Plätzen und in öffentlichen Gebäuden stellt eine Bearbeitung von Personendaten dar, wofür eine gesetzliche Grundlage notwendig ist. Die Überwachung greift in die Grundrechte der Bürgerinnen und Bürger ein; zulässig ist ein solcher Eingriff nur, wenn er im öffentlichen Interesse liegt und verhältnismässig ist. Ein öffentliches Interesse ist zu bejahen, wenn die Überwachung geeignet ist, schwere Straftaten zu verhindern oder zumindest zu vermindern. Die Verhältnismässigkeit ist gewahrt, wenn weniger weit gehende Massnahmen versagt haben und der angestrebte Erfolg in einem vernünftigen Verhältnis zum Eingriff in die Persönlichkeitsrechte einer unbestimmten Vielzahl von Personen liegt.

Wegen mehrerer Einbrüche in Garderobenkästen eines Hallenbades wollte eine Gemeinde den Eingangsbereich mittels Videokamera überwachen. Eine andere Gemeinde plante, ihre unterirdische Bahnstation mittels Videokameras zu überwachen. Damit sollten Vandalismus bekämpft und das Sicherheitsgefühl der Passagiere erhöht werden. Wir stellten fest, dass es in beiden Fällen an einer gesetzlichen Grundlage mangelt. Ausserdem ist der angestrebte Zweck, nämlich Diebstähle zu vermeiden und Vandalismus zu unterbinden, mit anderen, weniger weit gehenden Mitteln zu erreichen, beispielsweise mit Kontrollen durch das Hallenbadpersonal, besserer Beleuchtung des unterirdischen Bahnhofs.

In einem Sportstadion sollten vier Videokameras die Stehrampe sowie den Eingangs- und Ausgangsbereich abdecken. Der Stadtrat plante, die Kameras während Heimspielen der ersten Mannschaft laufen zu lassen und die Zuschauenden darüber mittels schriftlicher Ankündigungen und mündlich über Lautsprecher zu orientieren. Die Aufnahmen sollten gespeichert und – bei Nichtgebrauch – gelöscht werden.
Eine gesetzliche Grundlage für die Überwachung besteht nicht und müsste noch geschaffen werden. Das öffentliche Interesse an der Verhinderung schwerer Straftaten ist aber hier grundsätzlich vorhanden. Die Erfahrung zeigt, dass Hooligans bei Fussballspielen immer wieder gewalttätig werden. In diesem Fall erscheint die zeitlich und örtlich beschränkte Videoüberwachung das geeignete Mittel, um gewalttätige Ausschreitungen zu verhindern, zumal andere, weniger weit gehende Massnahmen bisher versagt haben.

Die Flughafenpolizei beabsichtigt, zusammen mit der Betreiberin des Flughafens ein optisches Überwachungssystem mit systematischer Gesichtserkennung («Face Recognition») einzuführen. Begründet wurde dieses Vorhaben mit der Zunahme von illegal eingereisten Migranten, die nach der Ankunft ihre Identität und Herkunft verschleiern, um der Rückführung in ihr Herkunftsland zu entgehen. Mit dem System sollten sämtliche ankommenden Flugpassagiere erfasst und die biometrischen Messpunkte ihres Gesichts gespeichert werden. Auch für dieses System gibt es keine gesetzliche Grundlage und es mangelt sowohl am öffentlichen Interesse (illegale Einreise ist keine schwere Straftat, vor der man die Öffentlichkeit schützen muss) als auch an der Verhältnismässigkeit (erfasst werden jährlich rund 22 Millionen unverdächtige Passagiere, dem stehen im gleichen Zeitraum etwa 200 illegal eingereiste Migranten gegenüber, deren Identität und Herkunft unklar ist).

- Für die Installation von Überwachungskameras fehlt oftmals eine klare gesetzliche Grundlage. Der Eingriff in die Persönlichkeitsrechte von unzähligen Personen setzt zudem voraus, dass für die Überwachung ein öffentliches Interesse besteht und dass die Massnahme verhältnismässig ist.

2. Zentrale Polizeidatenbank

Mangelnde gesetzliche Grundlagen

Seit einiger Zeit benützt die Kantonspolizei ein Informatiksystem (Joufara II), dem auch die Städte Zürich und Winterthur angeschlossen sind oder werden. Dieses System löste bisherige, nach unterschiedlichen Zwecken getrennte Datenbanken ab. Während früher eine Geschäftskontrolle neben einer spezifischen Fahndungsdatenbank geführt wurde, stehen nun alle Informationen zentral zur Verfügung. Im Rahmen einer Überprüfung stellten wir fest, dass für das Führen einer Geschäftskontrolle ausreichende Rechtsgrundlagen bestehen. Allerdings kann auf Grund dieser Rechtsgrundlagen nicht davon ausgegangen werden, dass sämtliche Einträge in der Geschäftskontrolle auch für die Ermittlung zur Verfügung stehen. Tatsächlich ist das neue Informatiksystem nicht nach Aufgabenbereichen aufgeteilt; alle von der Polizei erfassten Informationen stehen für alle Aufgaben zu Verfügung. Damit wird es einer betroffenen Person, die beispielsweise als Anzeigeerstatterin bei der Polizei auftritt, nicht transparent, dass Informationen zu ihrer Person immer wieder in Fahnungsrecherchen auftauchen können, da eine einzige Datenbank für alle Zwecke genutzt wird. Es fehlen Rechtsgrundlagen, die Zweck, Inhalt, Art und Umfang dieser Datenbearbeitungen festlegen.

In der Praxis hat sich weiter gezeigt, dass der Zugriff auf die Daten im System Joufara gesetzlich nicht näher geregelt ist, faktisch haben alle Personen, die an dieses System angeschlossen sind, auch Zugang zu allen Informationen. Dadurch wird das Prinzip der Verhältnismässigkeit verletzt, das die Datenbearbeitungen auf die für die Aufgabenerfüllung geeigneten und erforderlichen Daten beschränkt. Hinzu kommt, dass für die einzelnen Datenkategorien keine Aufbewahrungsfristen bestimmt sind. Damit verbleiben Informationen über eine verhältnismässige Aufbewahrungsdauer hinaus im aktiven Zugriff der Benutzenden.
In einer ersten Sitzung mit den betroffenen Stellen konnte über den rechtlichen Handlungsbedarf in diesem Bereich weitgehend Einigung erzielt werden.

- Zentrale Polizeidatenbanken, die nicht nach Aufgabenbereichen aufgeteilt sind, benötigen Rechtsgrundlagen, die insbesondere Art und Umfang sowie Zugriffsmöglichkeiten und Aufbewahrung der Daten detailliert regeln.

3. Aufbewahrung erkennungsdienstlicher Materialien

Keine Revision der einschlägigen Verordnung

Die Aufbewahrung erkennungsdienstlicher Unterlagen durch die Polizeiorgane gibt immer wieder zu Fragen Anlass. Insbesondere fehlen konkrete Aufbewahrungsregelungen, die je nach Abschluss des Verfahrens (Freispruch, Einstellung oder Verurteilung) differenzieren.
Grund hierfür ist die unklare Rechtslage im Kanton Zürich, da die Verordnung über die erkennungsdienstliche Behandlung von Personen vom 22. Dezember 1960 nicht mehr den datenschutzrechtlichen Anforderungen entspricht. Bereits im Tätigkeitsbericht Nr. 2 [1996], S. 11, haben wir auf den rechtlichen Handlungsbedarf hingewiesen. In der Folge fanden Gespräche mit den Polizeibehörden statt, bei welchen weitgehend eine Einigung über die materiellen Revisionspunkte der Verordnung erzielt werden konnte. Trotz neuer Fälle, bei denen erkennungsdienstliches Material von zu Unrecht verdächtigten Personen aufbewahrt blieb (Tätigkeitsbericht Nr. 4 [1998], S. 18 f.; Tätigkeitsbericht Nr. 5 [1999], S. 13 f.), erfolgte die fällige Revision der Verordnung nicht. In den Antworten auf zwei Anfragen im Kantonsrat von 1998 und 1999 hat der Regierungsrat darauf hingewiesen, dass

der Abschluss nun bevorstehe. Mit dem in der Zwischenzeit in Betrieb genommenen neuen EDV-System der Kantonspolizei (Joufara) hat sich der Handlungsbedarf verschärft (siehe S. 11).

Unterdessen sind wieder Anfragen an den Datenschutzbeauftragten gelangt. Die Revision der Verordnung über die erkennungsdienstliche Behandlung von Personen erscheint daher vordringlich.

- Die Aufbewahrung erkennungsdienstlicher Unterlagen gibt immer wieder zu Fragen Anlass, bei denen die längst fällige Revision der einschlägigen Verordnung Klarheit schaffen könnte.

4. Polizeiinterne Informationen

Versand an private E-Mail-Adresse

Der Betreiber einer Domain erhielt eine falsch adressierte und daher fehlgeleitete E-Mail eines Mitarbeiters der Kantonspolizei. Die Mail enthielt einen Registerauszug des Strassenverkehrsamtes über eine Privatperson. Der Betreiber informierte uns über den Vorfall.
Aus den Berichten der beteiligten Personen erfuhren wir einerseits, dass der Registerauszug von einem Mitarbeiter der Kantonspolizei an einen Kollegen, jedoch an dessen private E-Mail-Adresse, geschickt werden sollte, wobei ein Tippfehler zur Fehlleitung geführt hatte. Andererseits blieben die genauen Umstände und der Zweck der Datenübermittlung ungeklärt.

Wir wiesen mit Nachdruck darauf hin, dass dienstliche Informationen nur zu rein dienstlichen Zwecken verwendet werden dürfen und der Versand von Registerauszügen nur mit entsprechenden Schutzmassnahmen (Verschlüsselung) erfolgen darf – die Übermittlung an eine private Mailadresse ist grundsätzlich nicht erlaubt.

- Polizeiinterne Informationen dienen nur dienstlichen Zwecken. Sie sind zu verschlüsseln und nicht an private E-Mail-Adressen von Mitarbeitenden zu senden.

5. Falsche Zustellung einer Einstellungsverfügung

Keine Prüfung der Zustelladresse

Gegen einen Journalisten wurde bei einer Bezirksanwaltschaft von privater Seite Strafantrag wegen diverser Antragsdelikte gestellt. Zwölf Tage später zog der Geschädigte seine Strafanträge zurück. Die Bezirksanwaltschaft stellte das Strafverfahren ein und sandte die Verfügung an die Adresse des ehemaligen Arbeitgebers des Journalisten. Jenes Arbeitsverhältnis war zwei Jahre zuvor aufgelöst worden. Beim ehemaligen Arbeitgeber wurde die Sendung geöffnet und dem Journalisten nachgesandt. Er bat den Datenschutzbeauftragten, zum Sachverhalt Stellung zu nehmen und Massnahmen zu ergreifen.

Vorerst stellten wir fest, dass für Fragen im Zusammenhang mit der Postöffnung durch den ehemaligen Arbeitgeber (eine private Organisation) der Eidgenössische Datenschutzbeauftragte zuständig ist.

Die Bezirksanwaltschaft wurde zur Stellungnahme aufgefordert, woher und wie die falschen Daten des Journalisten erhoben worden waren. Sie gab an, in der Anzeige sei lediglich der Name des Journalisten enthalten gewesen, weshalb sie seine bereits in einem früheren Verfahren erfassten Angaben im Computer «abgemischt» habe. Die Strafanzeige sei dann vor der routinemässigen Überprüfung der Personalien bei der Einwohnerkontrolle zurückgezogen worden und im Sinne einer raschen Erledigung sei auf die Adresskontrolle verzichtet worden.

Wir wiesen die Bezirksanwaltschaft auf ihre in der Dienstanweisung der Staatsanwaltschaft vom 24. April 1995 («Führung der Geschäftskontrolle mit AS/400-

Justizia») festgehaltene Pflicht zur Überprüfung der Personalien zwecks Vermeidung von Fehlzustellungen hin und forderten sie auf, geeignete Massnahmen zu treffen, um ähnliche Fälle in Zukunft zu vermeiden.

- Bezirksanwaltschaften sind verpflichtet, Adressdaten vor dem Versand irgendwelcher Schriftstücke zu kontrollieren.

KANTON

6. E-Government und Datenschutz

Kategorisierung der Projekte nach Sensibilität

In regelmässigen Tranchen bewilligt der Regierungsrat im Rahmen der E-Government-Strategie Teilprojekte auf der Stufe Direktion oder Amt. Ziel dieser Projekte ist die Verbesserung des «Service Public» unter Einsatz moderner Informations- und Kommunikationstechnologie. Damit sind unmittelbar auch Fragen des Datenschutzes und der Informationssicherheit angesprochen. Die Sensibilität der einzelnen Projekte in Bezug auf diese Fragen ist jedoch unterschiedlich. Auf Grund dieser Ausgangslage und unter Berücksichtigung der dem Datenschutzbeauftragten nur beschränkt zur Verfügung stehenden Ressourcen erfolgt die Mitwirkung in diesen Projekten auf Grund einer vorgängigen Klassifizierung nach deren Relevanz in Bezug auf den Datenschutz und die Informationssicherheit. Aus datenschutzrechtlicher oder sicherheitstechnischer Sicht sind diejenigen Projekte am sensibelsten, die besonders schützenswerte Personendaten bearbeiten oder die Übermittlung von personenbezogenen Daten beispielsweise über das Internet vorsehen.
Von besonderer Bedeutung sind daher zurzeit die Projekte E-Voting, Bildungsstatistik, E-Workpermits und E-Procurement.
Durch die vorgesehene Interaktion der Bürgerinnen und Bürger mit dem Staat in weiteren Projekten werden Fragen des Datenschutzes und der Sicherheit weiter in den Vordergrund treten. Bereits heute zeigt sich bei vielen interaktiven E-Business-Lösungen, dass das Vertrauen in Bezug auf den korrekten Umgang mit Personendaten entscheidend ist für die Akzeptanz der neuen Informations- und Kommunikationstechnologien. Auch im E-Government-Bereich wird dies nicht anders sein. Datenschutz und -sicherheit sind deshalb notwendige Elemente für das Vertrauen in die neuen Informations- und Kommunikationsinfrastrukturen der Verwaltung.

- Datenschutz und Informationssicherheit sind Kernelemente des Vertrauens der Bürgerinnen und Bürger in die neuen Informations- und Kommunikationstechnologien, die im Rahmen von E-Government-Projekten eingesetzt werden.

7. Transparenz der Datenbearbeitungen

Mitberichte in Vernehmlassungsverfahren

In verschiedenen Vernehmlassungsverfahren nahmen wir zu bundesrechtlichen und kantonalen Erlassen aus datenschutzrechtlicher Sicht Stellung.

- Im Vorentwurf zu einer Schweizerischen Strafprozessordnung und einem Schweizerischen Jugendstrafverfahren sind zu verschiedenen Themen (z.B. Protokollierung, Archivierung, Mitteilungen an andere Behörden) Abläufe mittels neuerer Technologien vorgesehen. Wir haben auf die mit der Digitalisierung grundsätzlich verbundenen Risiken und die notwendigen Sicherheitsvorkehrungen hingewiesen. Beim Thema Akten und Akteneinsicht taucht ebenfalls die Problematik der Archivierung in elektronischer Form auf, die jedoch im Entwurf nicht ausdrücklich geregelt ist. Im Entwurf wird auch auf die aus dem DNA-Profil-Gesetz zu übernehmenden Gesetzesbestimmun-

gen verwiesen. Weder zu diesem noch zur DNA-Datenbank wurde eine Vernehmlassung durchgeführt. Durch die gegenseitigen Rückverweisungen war es nicht möglich, zu dieser äusserst wichtigen Frage Stellung zu nehmen. Eine Aufzählung der Delikte, bei denen eine DNA-Analyse erfolgen kann, fehlt im aktuellen Entwurf. Weiter sind die Aufbewahrungsfristen und die Voraussetzungen für die Löschung von Material explizit zu regeln. Als schwer wiegender Eingriff in die persönliche Freiheit muss zudem der Einsatz der DNA-Analyse im Jugendstrafverfahren speziell geregelt werden.

- Nach der Teilrevision des Zollgesetzes im Jahr 2000 stand bereits die nächste Überarbeitung, nämlich die Totalrevision an. Vorgesehen ist damit auch eine Erweiterung der Befugnisse für Datenbearbeitungen, welche mit einem neuen Aufgabenverständnis begründet wird. Einige dieser neuen Regelungen geben keine genügenden Antworten zu Zweck und Umfang der Datenbearbeitungen und erfüllen somit die Anforderungen an die Transparenz für die betroffenen Personen nicht. Besonders heikel sind die Bestimmungen, welche das Abnehmen von biometrischen Daten für die Bestimmung der Identität von Personen erlauben. Weiter werden die Befugnisse der Zollbehörden für den Einsatz von optischen und anderen Überwachungsgeräten erweitert. Hier erscheint ein Hinweis notwendig, dass technische Überwachungsmassnahmen nur in den Fällen in Betracht kommen, in denen andere Möglichkeiten ausgeschlossen sind. Deshalb ist eine abschliessende Aufzählung über die zulässigen Zwecke, bei denen die Einrichtung von Überwachungssystemen erfolgen kann, notwendig.

- Das Bundesgesetz über die elektronische Signatur (BGES) regelt die Vergabe und die Verwaltung von anerkannten digitalen Zertifikaten und sieht vor, dass digitale Signaturen zum Einsatz kommen können, wo heute zu einem gültigen Vertragsschluss eine handschriftliche Unterzeichnung notwendig ist.
  Zu diesem Zweck scheint der Gesetzesentwurf ein taugliches Mittel zu sein, wobei die praktische Verbreitung der im Rahmen des BGES anerkannten digitalen Signaturen jedoch gering sein dürfte. Die Kundin und der Kunde wird betreffend Sicherheit umfassend in die Pflicht genommen. Es fehlen jedoch geeignete Massnahmen, welche die Geheimhaltung der privaten Schlüssel gewährleisten könnten, so dass ein verantwortungsbewusster Kunde von den im Gesetz vorgeschlagenen Zertifikaten kaum Gebrauch machen wird. Für die Kantone bedeuten die mangelnden Schutzmechanismen bei Missbrauch im BGES, dass sie im Bereich der Einführung von E-Government-Projekten nicht auf die Lösungen des BGES zurückverweisen dürfen.
  Zur generellen Verbreitung der digitalen Signatur ist aber zusätzlich zum vorgesehenen Gesetz erforderlich, dass der Bund (wohl in Zusammenarbeit mit internationalen Gremien) benutzerfreundliche Technologien fördert und technische Komponenten zertifizieren hilft. Bereits eingeleitete Aktivitäten in diese Richtung – etwa im Projekt «Guichet virtuel» – sind zu verstärken. Viel häufiger und wichtiger wird der Einsatz der digitalen Signatur aber zur Identifikation oder für sichere E-Mail oder zum Abschluss formloser Verträge sein. Hier wird sie zu einem zentralen Instrument des Datenschutzes und der Informationssicherheit (Wahrung von Integrität und Vertraulichkeit nebst Gewährleistung der Authentizität).

- In Mitberichten nehmen wir die Gelegenheit wahr, auf unpräzise und missverständliche Formulierungen aufmerksam zu machen. Damit kann die Transparenz der Datenbearbeitungen erhöht werden.

8. Frist für Auskunfterteilung

Zuständigkeit des Bezirksrats für Aufsichtsbeschwerde

Eine Mutter verlangte bei der Schulpflege Einsicht in die vollständigen Akten ihrer beiden Töchter. Anschliessend reichte sie beim Bezirksrat eine Aufsichtsbeschwerde gegen die Schulpflege ein mit der Begründung, diese habe ihr nur schleppend und unvollständig Akteneinsicht gewährt. Der Bezirksrat vertrat die Ansicht, der Datenschutzbeauftragte sei für die Beurteilung der Aufsichtsbeschwerde zuständig, und überwies das Geschäft an uns.
Wir stellten fest, dass der Datenschutzbeauftragte keine Spezialaufsicht im Sinne von § 141 Abs. 3 Gemeindegesetz ausübt. Laut § 141 Abs. 1 Gemeindegesetz und § 10 Gesetz über die Bezirksverwaltung ist der Bezirksrat für die Bearbeitung der Aufsichtsbeschwerde zuständig.

Nachdem der Bezirksrat die Aufsichtsbeschwerde behandelt und der Frau einen Entscheid zugestellt hatte, wandte sich diese nochmals direkt an uns. Sie nahm Bezug auf Art. 1 Abs. 4 der Verordnung zum Datenschutzgesetz des Bundes (VDSG). Darin wird der Inhaber einer Datensammlung verpflichtet, die Auskunft (Akteneinsicht) oder den begründeten Entscheid über die Einschränkung des Auskunftsrechts innert 30 Tagen seit Eingang des Auskunftsbegehrens zu erteilen. Da sie erst 33 Tage nach ihrem Begehren an die Schulpflege die gewünschte Akteneinsicht erhalten hatte, bat die Frau den Datenschutzbeauftragten bezüglich der nicht eingehaltenen Frist um eine Stellungnahme.

Die 30-tägige Frist gilt für den Bereich der Bundesgesetzgebung und ist für den Kanton Zürich nicht verbindlich. Sie kann daher nur indirekt herangezogen werden. Als Grundsatz gilt, dass die Auskunfterteilung nicht bewusst verzögert werden darf. Sie hat aber auch nicht automatisch Priorität vor allen anderen Aufgaben der Verwaltungsstelle. Über die Priorität entscheidet im Einzelfall die Interessenabwägung zwischen möglichst rascher Auskunft und Aufwand für die Auskunftserteilung. Das Gesuch um Akteneinsicht ging Mitte Dezember ein; wegen der darauf folgenden Feiertage ist es verständlich, dass die Erledigung der Geschäfte sich etwas verzögerte. Die Zeitspanne von 33 Tagen zwischen dem Akteneinsichtsgesuch und der Erledigung ist deshalb nicht übersetzt.

- Für eine Aufsichtsbeschwerde, mit der die Missachtung datenschutzrechtlicher Bestimmungen durch eine Gemeinde gerügt wird, ist der Bezirksrat zuständig. Das Datenschutzgesetz des Kantons Zürich kennt keine Frist für die Auskunfterteilung. Die 30-tägige Frist in der Verordnung zum Datenschutzgesetz des Bundes kann als Richtlinie herangezogen werden.

GEMEINDEN

9. Datensperre beim Steuerregister

Anforderungen an die Durchbrechung

In verschiedener Hinsicht gab die Datensperre beim Steuerregister zu Fragen und Beanstandungen Anlass:

In einer Zeitschrift waren über einen Arzt Steuerdaten veröffentlicht worden, weshalb er sich bei verschiedenen Stellen über die Praxis der Steuerämter, Medienvertretern Steuerauskünfte zu geben, beschwerte. Er machte insbesondere geltend, Medienanfragen nach den Steuerdaten eines gewöhnlichen Bürgers seien immer abzulehnen, weil dessen Interesse an der Geheimhaltung seiner Steuerdaten offensichtlich und schützenswert sei. So könnten irreführende Publikationen (Persönlichkeitsverletzungen) verhindert werden. Der Arzt vermutete schliesslich, die Instruktionen der Gemeindesteuerämter durch den Kanton seien nicht ausreichend.

Grundsätzlich sind die Steuerämter nach Steuergesetz berechtigt, Steuerausweise auszustellen. Die Ausstellung von Steuerausweisen an private Dritte kann verhindert werden, indem betroffene Personen eine Datensperre nach § 11 DSG einrichten. Besteht keine Datensperre, lehnt das Steueramt die Bekanntgabe der Daten nur ab, wenn wesentliche öffentliche Interessen oder offensichtlich schützenswerte Interessen der betroffenen Personen es verlangen (§ 10 lit. a DSG). Anfragen von Medien, welche keine Personen des öffentlichen Lebens oder der Zeitgeschichte betreffen, sind nicht zum Vornherein abschlägig zu beantworten. Auch die Tatsache, dass Medienanfragen in der Regel im Zusammenhang mit einer beabsichtigten Publikation erfolgen, bedeutet nicht, dass automatisch die Interessen an einer Verweigerung der Auskunft überwiegen; dies würde nicht nur den Einzelfall ausser Acht lassen, sondern könnte als Eingriff in die Medienfreiheit gewertet werden.

Wird ein Steuerausweis ausgestellt, ist es Sache der anfragenden Person bzw. Organisation, bei der Bearbeitung der Daten die Persönlichkeit der betroffenen Person nicht widerrechtlich zu verletzen. Auch die Presse ist bei ihrer Berichterstattung an den Persönlichkeitsschutz nach dem Datenschutzgesetz bzw. nach Art. 28 ff. Zivilgesetzbuch (ZGB) gebunden; im Falle einer widerrechtlichen Persönlichkeitsverletzung besteht der zivilrechtliche Rechtsschutz.

Die Weisung der Finanzdirektion über die Führung der Steuerregister in den Gemeinden enthält den Hinweis, dass auch bei Fehlen einer Datensperre § 10 lit. a DSG anzuwenden ist. Sie ist also korrekt und vollständig abgefasst.

Zwei Gemeinden benützten im Bestätigungsschreiben an Steuerpflichtige, die ihre Daten sperren liessen, eine nicht mehr gültige Formulierung: «Einem allfälligen Begehren um Ausstellung von Steuerausweisen wird ... entsprochen, wenn der Antragsteller ... belegen kann, dass er eine (wirtschaftliche) Beziehung konkret aufnehmen will ...» Wir machten die Gemeinden darauf aufmerksam, dass die Datensperre nur durchbrochen werden kann, wenn eine antragstellende Person glaubhaft macht, dass die Datensperre sie in der Verfolgung eigener Rechte gegenüber dem Steuerpflichtigen behindert. Die Absicht, eine wirtschaftliche Beziehung aufzunehmen, reicht für die Durchbrechung der Datensperre nicht. Die Steuerverwaltungen änderten daraufhin den Wortlaut der Bestätigung.

Ein Steueramt fragte uns, ob es verpflichtet sei, einem Gericht im Kanton Tessin die Steuerdaten eines Ehepaares herauszugeben, das seine Daten sperren liess. Die Datensperre wirkt nur gegenüber privaten Personen und Organisationen, nicht aber gegenüber einem Gericht. Ob das Steueramt die gewünschte Auskunft erteilen muss, entscheidet die Finanzdirektion (Ziff. 4 der Verfügung der Finanzdirektion über Auskünfte aus Steuerakten an Verwaltungs- und Gerichtsbehörden vom 7. Dezember 1998). Die Frage war deshalb der Finanzdirektion zu unterbreiten.

Die Weisung der Finanzdirektion vom 22. Dezember 2000 über die Führung der Steuerregister in den Gemeinden enthält Regeln für das konkrete Vorgehen bei einer Durchbrechung der Datensperre. Ein Kantonsrat erkundigte sich in einer Anfrage nach der Gewährung des rechtlichen Gehörs derjenigen Person, die ihre Daten sperren liess. In unserem Mitbericht für das kantonale Steueramt verwiesen wir auf diverse frühere Stellungnahmen und bestätigten, dass ein korrekter Umgang mit dem Sperrrecht – wie dies die entsprechende Weisung der Finanzdirektion vorsieht – kein Grundrecht verletzt.

- Jede Person kann ihre Steuerdaten sperren lassen. Die Durchbrechung der Sperre ist unter den im DSG genannten Voraussetzungen möglich.

10. Datenaustausch zwischen Sozialbehörden und Betreibungsamt

Grundsätze für Datenaustausch und Ausstandsregelungen

Im Verhältnis zwischen Sozialbehörden und Betreibungsamt stellt sich die Frage, ob die Sozialbehörden dem Betreibungsamt melden müssen, wenn sie dem Klienten gemäss den Richtlinien der Schweizerischen Konferenz für Sozialhilfe (SKOS) einen Anteil Erwerbseinkommen über dem sozialrechtlichen Bedarf als Motivation zusprechen wollen, und ob andererseits das Betreibungsamt das Sozialamt informieren muss, wenn es beabsichtigt, einen solchen Einkommensanteil zu pfänden.
Eine besondere Problematik ergibt sich bei Betreibungsbeamten, die gleichzeitig Mitglieder einer Sozialbehörde sind. Es stellt sich die Frage, ob in das Wahlgesetz eine Unvereinbarkeitsbestimmung aufzunehmen ist.

Das Schuldbetreibungs- und Konkursgesetz (SchKG) enthält eine Auskunftspflicht der Behörden im Pfändungsverfahren und im Konkursverfahren. Diese Pflicht gilt auch für die Sozialhilfebehörden. Zu melden sind sämtliche Unterstützungsleistungen. Demgegenüber hat das Betreibungsamt weder die Pflicht noch das Recht, dem Sozialamt zu melden, ob es Einkommen (wieder) pfändet oder nicht.

Im Ergebnis kann diese Konstellation allenfalls dazu führen, dass das Sozialamt einer Person Beiträge zuspricht, die ihr dann sogleich wieder weggepfändet werden, was indirekt einer Schuldensanierung durch das Gemeinwesen gleichkommt. Dies ist allerdings nicht auf datenschutzrechtliche Bestimmungen zurückzuführen, sondern auf die unterschiedliche Berechnung des Existenzminimums im Bereich der Sozialhilfe und des Betreibungswesens. Um diesen Konflikt zu beseitigen, müssten die Existenzminima gesetzlich neu geregelt werden.

Sowohl das Gemeindegesetz als auch das SchKG enthalten Ausstandsregelungen. Das Gemeindegesetz verweist diesbezüglich seit der Revision von 1997 auf die Bestimmungen des Verwaltungsrechtspflegegesetzes (VRG). In den Ausstand zu treten haben Personen, «wenn sie in der Sache persönlich befangen erscheinen». Das SchKG bestimmt, dass Mitarbeiter von Betreibungsbehörden in den Ausstand zu treten haben «in Sachen, in denen sie aus anderen Gründen befangen sein könnten». Ob ein solcher Grund vorliegt, muss jeweils im Einzelfall entschieden werden.

Es ist offensichtlich, dass ein gewisser Interessenkonflikt besteht, wenn die beiden Funktionen gleichzeitig in sich überschneidender Zuständigkeit ausgeübt werden. So dürfte ein Ausstandsgrund gegeben sein, wenn das Mitglied einer Sozialbehörde zuvor als Betreibungsbeamter Betreibungshandlungen gegen einen Sozialhilfeempfänger vornahm. Das Gleiche gilt umgekehrt, wenn ein Betreibungsbeamter zuvor als Mitglied einer Sozialhilfebehörde über Unterstützungsleistungen befand. Insofern bietet das geltende Recht Mittel und Wege, um im Einzelfall solche Konfliktsituationen zu umgehen. Demgegenüber würde eine Unvereinbarkeitsbestimmung im Wahlgesetz derartige Interessenkonflikte zum Vornherein ausschliessen.

- Die Sozialbehörden haben dem Betreibungsamt alle Leistungen zu melden, die sie einem Schuldner zukommen lassen. Die Ausstandsregelungen sind speziell zu beachten, wenn Mitglieder einer Sozialbehörde gleichzeitig Betreibungsbeamte sind.

11. Spitalrechnungen an die Gemeinde

Unverhältnismässige Angaben

Ein öffentliches Spital stellte dem Zivilstandsamt einer Gemeinde Rechnung für die Bestattung eines verstorbenen Einwohners. Das Rechnungsformular enthielt neben den Bestattungskosten weitere, zum Teil äusserst sensible Angaben zur verstorbenen Person (Diagnose, Versicherungsstatus bei der Krankenkasse, behandelnde Station des Spitals, Tagestaxe, Kosten zu Lasten Patient und Versicherer). Das Zivilstandsamt, das lediglich die Bestattungskosten übernimmt, benötigt diese Angaben nicht. Die Gemeinde bat uns um Vermittlung.

Wir machten das Spital auf die unverhältnismässige Datenbearbeitung aufmerksam und empfahlen, künftig zwei getrennte Rechnungen zu erstellen: eine für die Versicherung und eine für das Zivilstandsamt, auf der nur die zur Bezahlung der Bestattungskosten benötigten Personendaten aufgeführt sind. Das Spital befolgte diese Empfehlung.

- Die Weitergabe überflüssiger Daten ist unzulässig. Spitäler haben auf ihren Rechnungen nur die für den Adressaten wesentlichen Daten anzugeben.

12. Erfassung anderer Konfessionen durch die Einwohnerkontrolle

Keine gesetzliche Grundlage

Die Einwohnerkontrolle einer Gemeinde war vom Statistischen Amt aufgefordert worden, künftig bei den Mitgliedern der evangelisch-reformierten Kirche abzuklären, ob diese der französischen Kirchgemeinde angehören. Sie forderte daraufhin alle mit dem Code «übrige Konfessionen» erfassten Einwohnerinnen und Einwohner auf, unter 14 namentlich aufgeführten Konfessionen die zutreffende anzukreuzen. Eine betroffene Person wollte von uns wissen, ob diese Abklärung zulässig sei.

Für jede von der Einwohnerkontrolle erfasste Datenkategorie ist eine gesetzliche Grundlage notwendig und es dürfen nur diejenigen Daten bearbeitet werden, die für die Erfüllung der Aufgaben geeignet und erforderlich sind. Gemäss §39a Abs. 1 Gemeindegesetz erhalten die staatlich anerkannten Kirchen (evangelisch-reformiert, römisch-katholisch, christ-katholisch) aus dem Einwohnerregister die Mitteilungen, die sie zur Erfassung ihrer Mitglieder benötigen. Die Einwohnerkontrollen sind also verpflichtet, diejenigen Personen zu erfassen, die einer der drei Landeskirchen angehören. Für die Erfassung anderer Konfessionen gibt es keine gesetzliche Grundlage.
Die Einwohnerkontrolle wurde von uns entsprechend aufgeklärt und informierte alle angeschriebenen Personen, dass die Fragebogen, auf denen die französische Kirche nicht angekreuzt war, vernichtet worden seien.

- Die Einwohnerkontrollen sind gesetzlich verpflichtet, die Mitglieder der drei Landeskirchen zu erfassen. Weitere Daten über die Zugehörigkeit zu anderen Konfessionen sind nicht zu erheben.

13. Beschränkte Einsicht in Vormundschaftsakten

Verweigerte Einsicht mit Kostenfolge

Die Eltern einer Adoptivtochter wurden wegen angeblich falscher Behandlung ihres Kindes bei der Vormundschaftsbehörde angezeigt. Diese weigerte sich, die Namen der Informanten bekannt zu geben, worauf die Eltern den Datenschutzbeauftragten um Beratung und später Vermittlung baten.
In der Folge erliess die Vormundschaftsbehörde einen formellen Beschluss und begründete ihre Haltung mit dem Argument, sie sei auf Angaben aus der Bevölkerung angewiesen. Den Anzeigenden sei Anonymität zuzusichern, weil diese sonst nicht mehr bereit seien, eventuelle Missstände zu melden. Die Kosten des Beschlusses (245 Franken) wurden der Familie auferlegt, weil sie mit ihrem Begehren um vollständige Akteneinsicht unterlegen war.
Bei der Bekanntgabe von Informanten und Informantinnen sind einerseits das Informationsbedürfnis der betroffenen Personen, andererseits die Geheimhaltungsinteressen der Informierenden zu berücksichtigen. Überwiegt das Informationsbedürfnis – davon ist auszugehen, wenn Aussagen die persönliche Geheimsphäre und den guten Ruf der Betroffenen tangieren – ist die Bekanntgabe zulässig. Bestehen aber zum Vornherein Anhaltspunkte, dass den Informierenden durch Bekanntgabe ihrer Namen und Aussagen erhebliche Nachteile drohen, darf die Behörde die Auskunft verweigern. Konkrete Anhaltspunkte für die Gefahr einer rechtswidrigen Beeinträchtigung der Informierenden durch die Eltern des Mädchens nannte die Vormundschaftsbehörde nicht; trotzdem beharrte sie auf ihrem Entscheid. Die Eltern verzichteten auf weitere rechtliche Schritte.

Auf Grund der Vermittlung des Datenschutzbeauftragten wurde wenigstens erreicht, dass der Familie die Kosten des Beschlusses erlassen wurden. Das Datenschutzgesetz des Kantons Zürich spricht sich zwar nicht über die Kosten des Auskunftsrechts aus. Wir empfehlen dennoch, in Anlehnung an die eidgenössische Regelung (Art. 8 Abs. 5 EDSG) keine Kosten zu erheben (vgl. auch Tätigkeitsbericht Nr. 6 [2000], S. 27). Der Grundsatz der Kostenlosigkeit muss erst recht gelten, wenn die Auskunft verweigert oder nur eingeschränkt erteilt wird.

- Die Verweigerung des Einsichtsrechts setzt voraus, dass konkrete Anhaltspunkte für die Gefahr einer rechtswidrigen Beeinträchtigung der Informierenden durch die Gesuchsteller bestehen. Bei der Verweigerung des Auskunftsrechts sollten keine Kosten erhoben werden.

14. Steuerabzug für Beiträge an politische Parteien

Bekanntgabe der Partei

Ein Bürger wollte wissen, ob er den Steuerbehörden bekannt geben müsse, welche politische Partei er finanziell unterstütze. Seit Jahrzehnten sei sein Abzug in der Steuererklärung ohne weiteres akzeptiert worden, der neue Steuerkommissär verlange jetzt schriftliche Belege.
Steuerpflichtige dürfen bis zu 1500 Franken Beiträge an politische Parteien, die im Kantonsrat vertreten sind, abziehen. Sie müssen das amtliche Formular für die Steuererklärung wahrheitsgemäss und vollständig ausfüllen und alles tun, um eine vollständige und richtige Einschätzung zu ermöglichen, insbesondere haben sie auf Verlangen der Steuerbehörden Auskunft zu erteilen und Belege vorzuweisen (§§ 133 Abs. 2 und 135 Abs. 1 und 2 Steuergesetz). Gestützt auf diese allgemeine Mitwirkungspflicht der Steuerpflichtigen kann das Steueramt einen Nachweis für den geltend gemachten Steuerabzug und die Bekanntgabe der unterstützten Partei verlangen.

- Steuerpflichtige haben im Rahmen ihrer Mitwirkungspflicht für die Höhe ihrer Beiträge und die Identität der unterstützten politischen Partei den Nachweis zu erbringen.

15. Einsicht in Gutachten

Interessenabwägung durch auftraggebende Behörde

Eine Vormundschaftsbehörde liess eine von ihr betreute Familie durch den Kinder- und Jugendpsychiatrischen Dienst begutachten. Die Familie wollte das Gutachten anschliessend bei der Vormundschaftsbehörde einsehen, doch diese stellte sich auf den Standpunkt, der Kinder- und Jugendpsychiatrische Dienst sei für die Frage der Akteneinsicht zuständig. Dort verweigerte man der Familie die Auskunft mit der Begründung, das Gutachten sei im Auftrag der Vormundschaftsbehörde erstellt worden und es obliege deshalb ihr, über Art und Umfang der Einsicht zu entscheiden.

Der Datenschutzbeauftragte intervenierte auf Wunsch der Familie bei der Vormundschaftsbehörde und stellte fest, dass das Datenschutzgesetz (DSG) die Einsicht in die eigenen Akten als Grundsatz postuliert, von dem nur in Ausnahmefällen abgewichen werden kann: «Die Auskunft darf aufgeschoben, eingeschränkt oder verweigert werden, wenn eine gesetzliche Bestimmung, überwiegende öffentliche Interessen oder überwiegende schützenswerte Interessen Dritter dies verlangen» (§ 18 Abs. 1 DSG). Will die Vormundschaftsbehörde die Akteneinsicht verweigern, muss sie eine begründete Verfügung erlassen (§ 20 Abs. 1 DSG), gegen die der Rechtsmittelweg offen steht.
In der Folge erklärte sich die Vormundschaftsbehörde bereit, der Familie eine Kopie des Gutachtens auszuhändigen.

- Die Einsicht in ein Auftragsgutachten kann durch die auftraggebende Stelle gewährt werden.

GESUNDHEIT

16. Merkblatt Austritts- und Operationsberichte

Wegleitung für Spitäler und Heime

Im Berichtsjahr hat die Vereinigung der Schweizerischen Datenschutzbeauftragten DSB+CPD.CH (siehe dazu Tätigkeitsbericht Nr. 6 [2000], S. 41 f.) ein Merkblatt über Austritts- und Operationsberichte veröffentlicht. Das Merkblatt richtet sich an die Spitäler und Heime; es beantwortet die Frage, ob und wann Spitäler und Heime Austritts- oder Operationsberichte an Kranken-, Unfall- oder andere Versicherungen senden dürfen. Das Merkblatt wurde durch die Arbeitsgruppe «Gesundheit» der DSB+CPD.CH, in welcher wir mitwirken, erarbeitet und mit Vertretern und Vertreterinnen des Schweizerischen Versicherungsverbands (SVV) diskutiert. Der SVV hat die vorgeschlagene Lösung akzeptiert.

Das Merkblatt definiert, was die Berichte beinhalten und was den Versicherern bekannt gegeben werden darf. Weiter enthält es Empfehlungen für das Vorgehen der Spitäler und Heime: In einem ersten Schritt (Regelfall) senden die Spitäler und Heime dem Versicherer eine detaillierte und verständliche Rechnung. Benötigt der Versicherer im Einzelfall zusätzliche Angaben, kann er in einem zweiten Schritt dem Spital oder Heim schriftlich spezifische, auf den konkreten Fall bezogene Fragen stellen. Genügen auch diese Angaben ausnahmsweise nicht, kann der Versicherer in einem dritten Schritt zu Handen des beratenden Arztes bzw. des Vertrauensärztlichen Dienstes einen Austritts- oder Operationsbericht verlangen. Dabei ist die Notwendigkeit dieses Vorgehens schriftlich zu begründen. Das Merkblatt sieht vor, dass die versicherte Person in jedem Fall darüber informiert werden muss,

welche Informationen an den Versicherer gehen. Wir haben das Merkblatt allen Spitälern und Heimen im Kanton Zürich zugestellt und empfohlen, nach dessen Regeln vorzugehen.

- Das Merkblatt über Austritts- und Operationsberichte bietet den Spitälern und Heimen eine nützliche Wegleitung für den korrekten Umgang mit diesen Berichten. Auch den Versicherern bringt das abgestufte Vorgehen einen Gewinn, weil sie ausführliche Berichte nur ausnahmsweise verarbeiten müssen und keine überflüssigen Informationen erhalten.

---

17. Vollmacht für Datenbeschaffung

Keine unbestimmten Generalvollmachten

Art. 65 Abs. 1 der Invalidenversicherungsverordnung (IVV) lautet: «Wer auf Leistungen der Versicherung Anspruch erhebt, hat sich auf amtlichem Formular anzumelden und eine Ermächtigung zur Einholung weiterer Auskünfte zu erteilen.»
Die Antragstellenden erteilen damit eine Generalvollmacht zur Beschaffung sensibler personenbezogener Daten; andernfalls kann die IV-Stelle eine Nichteintretensverfügung erlassen.

Art. 65 Abs. 1 IVV bildet die Rechtsgrundlage für das Beschaffen von Personendaten bei Dritten. Es handelt sich um eine Ausnahme vom Grundsatz, dass Daten bei der betroffenen Person selbst zu beschaffen sind. Diese Ausnahme wird eingeschränkt durch die Bestimmung, dass die betroffene Person ihre Einwilligung zur Datenbeschaffung geben muss. Die IV-rechtliche Mitwirkungspflicht schliesslich verpflichtet die Antragstellenden, ihre Einwilligung zu erteilen.

Anstelle dieser umständlich erscheinenden Regelung hätte die IVV auch bestimmen können, dass die IV-Organe bei bestimmten, zu nennenden Personen, Institutionen und Amtsstellen Auskünfte einholen dürfen.
Die aktuelle Regelung schafft allerdings für die Betroffenen mehr Transparenz, weil nicht in allen Fällen bei den gleichen Stellen Daten beschafft werden müssen. Die Antragstellenden werden in den Prozess der Datenbeschaffung einbezogen, indem sie ihre Einwilligung erteilen. Aus der Einwilligung müsste jedoch hervorgehen, bei welchen Stellen welche Informationen zu welchem Zweck beschafft werden. Der Vollständigkeit halber müsste auch ein Hinweis auf die Mitwirkungspflicht und die Rechtsfolgen bei Verweigerung der Ermächtigung erfolgen.

In der Praxis verhält es sich häufig so, dass den betroffenen Personen eine Generalvollmacht zur Unterzeichnung vorgelegt wird, welche die IV-Organe ermächtigt, die «erforderlichen» Auskünfte bei «allen in Betracht fallenden Personen und Stellen» einzuholen.

- Vollmachten, die die IV-Organe generell berechtigen, Auskünfte über Antragstellende einzuholen, sind für diese zu wenig transparent. Anzustreben sind Vollmachten, aus denen konkret hervorgeht, wo und zu welchem Zweck Auskünfte eingeholt werden.

18. Überflüssige Daten an private Durchführungsstelle

Keine Übermittlung der vollständigen Verfügung

Eine invalide Person hatte durch einen Entscheid des Sozialversicherungsgerichts die leihweise Abgabe eines PCs als Hilfsmittel zugesprochen erhalten. Daraufhin schickte die Sozialversicherungsanstalt der Person eine Verfügung, in der ihr das Hilfsmittel mit einem expliziten Hinweis auf das Urteil des Sozialversicherungsgerichts zugesprochen wurde. Eine Kopie dieser Verfügung ging an das Computergeschäft (Durchführungsstelle), das den PC an die betroffene Person liefern sollte. Diese wollte von uns wissen, ob es zulässig sei, das Computergeschäft über die Existenz und das Datum des Urteils zu informieren.

Wir wiesen die Sozialversicherungsanstalt darauf hin, dass die Durchführungsstelle keine Angaben über die Grundlagen der Verfügung benötige. Die Sozialversicherungsanstalt rechtfertigte ihr Vorgehen damit, dass es in gewissen Fällen aus Gründen der Transparenz sinnvoll sei, der versicherten Person bekannt zu geben, auf welchen Grundlagen der Entscheid beruhe. Für die zugegebenermassen überflüssige Information an die private Durchführungsstelle entschuldigte sich die Sozialversicherungsanstalt bei der betroffenen Person.

- Werden privaten Durchführungsstellen Kopien von Verfügungen der Sozialversicherungsanstalt übermittelt, so sind alle Daten, die für die Durchführungsstelle ohne Belang sind, wegzulassen.

19. Versand von AHV-Kontoauszügen

Schwierige Sachverhaltsabklärungen

Ein geschiedener Mann wandte sich an den Datenschutzbeauftragten und beanstandete, dass seine Exfrau über einen detaillierten Auszug aus seinem individuellen AHV-Konto (IK-Auszug) verfüge. Der Mann vermutete, die Ausgleichskasse der Sozialversicherungsanstalt habe der Frau den IK-Auszug während des von ihr veranlassten Splitting-Verfahrens zugestellt. Um den Sachverhalt abklären zu können, stellten wir der Sozialversicherungsanstalt sowie einer weiteren involvierten Ausgleichskasse mehrere Fragen. Zudem nahmen wir anlässlich einer Besprechung bei der Sozialversicherungsanstalt Einsicht in das Dossier des Mannes und liessen uns die Abläufe beim Splitting-Verfahren erläutern.

In Bezug auf die generellen Verfahrensabläufe stellten wir keine Mängel fest. Warum es im konkreten Fall zur Datenbekanntgabe kam, konnten wir nicht eruieren. Weder die Antworten auf die gestellten Fragen noch die Einsicht ins Dossier ergaben Anhaltspunkte, dass die Ausgleichskasse den IK-Auszug der Exfrau überlassen hatte; allerdings konnte dies auch nicht mit Sicherheit ausgeschlossen werden. In rechtlicher Hinsicht hielten wir fest, dass der IK-Auszug an den geschiedenen Partner bzw. die geschiedene Partnerin nur mit Einwilligung der betroffenen Person weitergegeben werden darf.

Der Datenschutzbeauftragte hat keine Kompetenz für verbindliche Sachverhaltsabklärungen im Sinne von Zeugeneinvernahmen etc., er kann offene Fragen nicht immer eindeutig beantworten. Will die betroffene Person eine verbindliche Klärung des Sachverhalts, muss sie den Rechtsweg beschreiten (zum Beispiel mit einem Begehren auf Feststellung der widerrechtlichen Datenbearbeitung an die Verwaltungsbehörde oder ein Gericht). De lege ferenda ist zu prüfen, ob die Kompetenzen des Datenschutzbeauftragten zu erweitern sind.

- Auszüge aus dem individuellen AHV-Konto dürfen nur mit Einwilligung der betroffenen Person an den geschiedenen Partner oder die geschiedene Partnerin herausgegeben werden. Findet eine Herausgabe trotzdem statt und kann der Datenschutzbeauftragte nicht eruieren, wo der Fehler passierte, muss die betroffene Person den Rechtsweg beschreiten.

20. Einführung von standardisierten Austrittsinterviews

Keine Anonymität der beteiligten Personen

In der kantonalen Verwaltung sind Austrittsgespräche mit Personen, welche die Verwaltung oder Organisationseinheit verlassen, in der Vollzugsverordnung zum Personalgesetz vorgesehen. Es fehlen jedoch Hinweise zu Inhalt und Umfang der Gespräche bzw. deren Auswertung. Die geplante Erfassung mittels Fragebogen und die Auswertung an einer zentralen Stelle führen zu verschiedenen Fragen in Bezug auf den Schutz der Privatsphäre der beteiligten Personen. Da bereits die Rahmendaten wie Ein- und Austrittsdatum, Organisationseinheit etc. Rückschlüsse auf die Befragten ermöglichen, kann im Alltag deren Anonymität nicht gewährleistet werden. Die Fragen im Austrittsgespräch betreffen aber auch das Umfeld der austretenden Person, insbesondere deren Verhältnis zu Vorgesetzten und/oder Mitarbeitenden. Um einen Nutzen aus der Befragung ziehen zu können und Missverständnisse zu vermeiden, muss eindeutig sein, um welches Umfeld es sich handelt. Eine anonyme Erhebung erscheint deshalb nicht sinnvoll.
Der Schutz der befragten Person sowie aller anderen Beteiligten muss durch möglichst grosse Transparenz und eine klar definierte Zweckbestimmung gewährleistet sein. Der befragten Person muss bekannt sein, in welchem Zusammenhang ihre Angaben verwendet werden. Sie muss insbesondere auch das Recht haben, grundsätzlich keine Auskunft über das Verhältnis zu ihren Vorgesetzten/Mitarbeitenden zu geben. Andererseits sind auch die Ansprüche der betroffenen Drittpersonen zu wahren. Nicht mehr benötigte Personendaten sind zu vernichten (§ 14 DSG). Dies gilt auch für die Interviewbogen nach der erfolgten Auswertung.

- Durch Transparenz und klare Zweckbestimmung der Datenbearbeitung kann der Datenschutz beim Austrittsinterview gewährleistet werden. Die austretenden Personen dürfen nicht zu Auskünften verpflichtet werden.

21. Veröffentlichung von Bonuszahlungen

Mitbericht zu einer Anfrage im Kantonsrat

Im Zusammenhang mit Bonuszahlungen an das Bankpräsidium und den Bankrat der ZKB kam es zu einer Anfrage im Kantonsrat, zu dem wir aus datenschutzrechtlicher Sicht Stellung bezogen. Im Zentrum stand die Frage, ob ein öffentliches Organ – z.B. die ZKB, ihre Aufsichtskommission oder der Regierungsrat – berechtigt oder verpflichtet ist, Angaben über die Entschädigungen für die Ausübung eines öffentlichen Amtes zu veröffentlichen.
Das Datenschutzgesetz gibt die Rahmenbedingungen vor, unter denen öffentliche Organe Daten bearbeiten und damit in die Persönlichkeitsrechte Betroffener eingreifen dürfen. Im Einzelfall ist zu prüfen, ob die Daten zum beabsichtigten Zweck in der vorgesehenen Art und Weise bearbeitet (bzw. bekannt gegeben) werden dürfen oder müssen.

Personen, die ein politisches Amt wahrnehmen, in einem Führungsgremium oder in leitender amtlicher Funktion tätig sind, sind generell einer grösseren Transparenz ausgesetzt als etwa Staatsangestellte mit untergeordneten Funktionen. Bei der Bekanntgabe der Höhe von Entschädigungen für solche Personen ist zwischen funktions- und leistungsbezogenen

Komponenten zu unterscheiden. Angaben, die sich auf die Funktion beziehen, sind tendenziell öffentlich. Leistungsbezogene Komponenten können jedoch ein Persönlichkeitsprofil darstellen. Hier überwiegen in der Regel die schützenswerten privaten Interessen an der Geheimhaltung gegenüber den Interessen an der Offenbarung.

Einen Anspruch auf erhöhte Transparenz bzw. Information hat im Prinzip nur dasjenige Organ, welches Kontroll- und Steuerungsfunktionen im betreffenden Bereich wahrnimmt; im Sinne der Verhältnismässigkeit wären deshalb bestimmte Informationen beispielsweise dem Parlament zugänglich, während andere nur einer parlamentarischen Kommission zu offenbaren wären. Der betroffenen Person selbst steht es frei, gegenüber der Öffentlichkeit Informationen über ihre Entschädigungen für die Ausübung eines öffentlichen Amtes zu offenbaren oder zu verweigern.

- Bei der Bekanntgabe von Bonuszahlungen ist eine Differenzierung nach den rein funktionsbezogenen Komponenten und denjenigen, welche sich an tatsächlichen Leistungen und Qualifikationen bemessen, vorzunehmen. Es genügt, wenn die auf die Funktion bezogenen Entschädigungen veröffentlicht werden und nur gegenüber den Kontroll- und Steuerungsorganen allenfalls weitere Details bekannt gemacht werden.

SCHULEN

22. Administrativuntersuchung gegen Lehrperson

Einsicht in das Befragungsprotokoll einer Schülerin

Die Bildungsdirektion hatte auf Anzeige von Eltern gegen einen Primarschullehrer eine Administrativuntersuchung eingeleitet. Im Rahmen dieser Untersuchung wurde eine Schülerin befragt, deren Eltern anschliessend Einsicht in das Befragungsprotokoll wünschten.
Die Bildungsdirektion lehnte das Gesuch ab mit dem Hinweis auf ein überwiegendes öffentliches Interesse gemäss § 9 Verwaltungsrechtspflegegesetz.

Nach Abschluss eines Administrativverfahrens sind die Bestimmungen des Datenschutzgesetzes anwendbar. Der Datenschutzbeauftragte gelangte auf Wunsch der Eltern an die Bildungsdirektion und wiederholte das Gesuch um Einsicht in das Protokoll bzw. um eine begründete Verfügung. Die Bildungsdirektion schrieb den Eltern des Mädchens, sie wolle erst eine Verfügung erlassen, wenn ein die gleichen Fragen betreffender hängiger Rekurs gegen eine abschlägige Verfügung entschieden sei. Erst auf nochmalige Intervention des Datenschutzbeauftragten mit Hinweis auf die in der Regel zu wahrende Frist von 30 Tagen (vgl. dazu S. 15) erliess die Bildungsdirektion eine Verfügung, in der sie das Gesuch der Eltern formell ablehnte. Die Eltern beschlossen, den Rechtsweg zu beschreiten.

- Die Eltern eines befragten Kindes haben grundsätzlich Anspruch auf Einsicht in das Befragungsprotokoll. Will die zuständige Behörde das Einsichtsrecht nicht gewähren, hat sie eine begründete Verfügung zu erlassen, die auf dem Rechtsweg überprüft werden kann.

23. Berichte von Lehrpersonen

Konkretisierung des Rechts auf Auskunft

Die Mutter einer schulpflichtigen Tochter wandte sich an uns mit der Bitte um Vermittlung. Ihre Tochter war von zwei Mitschülern auf dem Schulweg körperlich angegriffen und verletzt worden. Im Rahmen der folgenden Untersuchung erstellten die beiden Lehrerinnen der drei Kinder zuhanden der Schulpflege einen Bericht über die Vorgeschichte des Übergriffs. Die Mutter des Mädchens wollte diesen Bericht einsehen. Dies wurde ihr von der Primarschulpflege mit dem Hinweis auf die Persönlichkeitsrechte der betroffenen Mitschüler zwar verweigert, doch enthielt die Stellungnahme der Primarschulpflege eine Zusammenfassung der von den Lehrerinnen geschilderten Ereignisse. Die Frau war mit dieser Teilinformation nicht einverstanden.

Nach Vermittlung durch den Datenschutzbeauftragten erklärte sich die Primarschulpflege schliesslich bereit, der Mutter im Schulsekretariat Einsicht in den Originalbericht zu geben. Nach einer weiteren Intervention unsererseits erhielt die Frau eine Kopie des Berichts zugestellt.

- Betroffene Personen haben Anspruch auf Einsicht in Originalberichte sowie auf Kopien der Unterlagen.

24. Einsichtsrecht in Prüfungsunterlagen

Anspruch auf Kopien

Zwei Studierende an der Universität wandten sich unabhängig voneinander an uns, weil ihnen die verlangte Einsicht in abgelegte Prüfungen nicht, bzw. erst mit grosser Verzögerung, gewährt wurde.

Ein Student verlangte Einsicht in die Unterlagen einer bestandenen Prüfung. Mündlich wurde ihm beschieden, aus logistischen Gründen könnten nur nicht bestandene Prüfungen eingesehen werden.
Das Auskunftsrecht kann bei Prüfungsdaten nicht davon abhängig gemacht werden, ob die Prüfung bestanden wurde oder nicht (vgl. auch Tätigkeitsbericht Nr. 6 [2000], S. 13).
Eine Studentin, die eine schriftliche Prüfung nicht bestanden hatte, erhielt erst nach mehr als sechs Monaten Einsicht. Zudem stellte sich die Fakultät auf den Standpunkt, die Prüfungsunterlagen seien in den Räumlichkeiten der Universität einzusehen und dürften nicht kopiert werden.
Fünfzehn Monate nach erfolgter Prüfung erhielt die Studentin Kopien aller Prüfungsunterlagen. Dann stellte sie fest, dass nur der erste Prüfungsteil (Essay-Fragen) Korrekturen enthielt, der zweite Prüfungsteil (Multiple Choice) enthielt keine Korrekturen oder Bemerkungen. Die Studentin argumentierte, das Auskunftsrecht werde auf diese Weise untergraben. Ohne Korrekturen sei es nicht möglich, die Prüfungsbewertung nachzuvollziehen.
Die Auskunft ist grundsätzlich schriftlich zu erteilen. Es besteht somit ein Anspruch auf Aushändigung von Prüfungskopien. Zu prüfen war zusätzlich, ob das Auskunftsrecht den Anspruch auf eine in nachvollziehbarer Weise korrigierte Prüfung beinhaltet. Diese Frage muss verneint werden: Mit der Zustellung der vorhandenen Unterlagen, das heisst einer Kopie der Prüfung, hat die Universität der betroffenen Person offenbart, welche Daten über sie bearbeitet werden. Einen darüber hinausgehenden Anspruch gewährt das Datenschutzgesetz nicht. Wie eine Prüfung zu korrigieren und zu bewerten ist, ergibt sich hingegen aus den einschlägigen Prüfungsreglementen.

- Das Auskunftsrecht bei Prüfungen – ob bestanden oder nicht – beinhaltet die Einsicht in alle Prüfungsunterlagen und die Aushändigung von Kopien.

25. Fotoordner über Schülerinnen und Schüler

Keine Datenbearbeitung auf Vorrat

In einer Oberstufenschulpflege wurde beantragt, es sei ein Fotoordner mit Passfotos aller Oberstufenschülerinnen und -schüler zu erstellen. Der Antrag war im Zusammenhang mit einer allgemeinen Diskussion zum Thema «Gewalt an Schulen» gestellt worden. Ein Mitglied der Oberstufenpflege fragte uns an, ob eine solche Fotodokumentation aus datenschutzrechtlicher Sicht zulässig sei.
Über den Zweck, den der Fotoordner erfüllen sollte, konnte der Fragesteller keine konkreten Angaben machen; man wolle einfach «eine Art Sicherheit für den Fall, dass etwas passiert…».
Wir wiesen darauf hin, dass die Erhebung von Daten «auf Vorrat», ohne konkrete Zweckbestimmung und ohne gesetzliche Grundlage nicht zulässig ist.

- Für das Erstellen eines Fotoordners mit Passfotos aller Schülerinnen und Schüler braucht es eine Rechtsgrundlage und eine klare Zweckbestimmung.

FORSCHUNG UND STATISTIK

26. Lärmstudie

Bekanntgabe von Adressmaterial zu Forschungszwecken

Eine Forschungsstelle der ETH Zürich verlangte von zahlreichen Gemeinden im Umkreis des Flughafens aus deren Einwohnerregistern Namen, Adressen und Telefonnummern sowie Alter und Geschlecht sämtlicher mündiger Personen, die seit mindestens einem Jahr in der Gemeinde wohnten. Zur Begründung gab die Forschungsstelle an, sie benötige die Daten für eine wissenschaftliche Untersuchung über die Auswirkungen von Fluglärm auf die Flughafenanwohner und -anwohnerinnen. Verschiedene Gemeinden fragten uns, ob sie die gewünschten Daten herausgeben dürften.

Nach zusätzlichen Abklärungen über die Modalitäten der Untersuchung kamen wir zum Schluss, dass die Bekanntgabe der Namen und Adressen sämtlicher mündiger Personen unverhältnismässig sei, weil die Forschungsstelle aus dem Adressmaterial eine Zufallsauswahl treffen wollte, also nur einen Bruchteil der verlangten Daten tatsächlich benötigen würde. Als Alternative empfahlen wir, die Gemeinden sollten die Zufallsauswahl selbst vornehmen und nur die Daten der ermittelten Personen an die Forschungsstelle weitergeben. Zudem stellten wir fest, dass keine Telefonnummern herauszugeben seien, da eine schriftliche Befragung geplant war.
Die Forschungsstelle befolgte unsere Empfehlungen und erfragte in der Folge bei den jeweiligen Gemeinden Postadresse, Jahrgang und Geschlecht von ungefähr 60 nach dem Zufallsprinzip ausgewählten Personen.

- Auch bei der Bekanntgabe von Listen mit Personendaten für Forschungszwecke ist zu prüfen, ob die Datenbekanntgabe verhältnismässig ist. Es sind nur die geeigneten und erforderlichen Daten bekannt zu geben.

27. Schweizerische Sozialhilfestatistik

Erhebungen bei den Gemeinden

Die Gemeinden sind gemäss Bundesstatistikgesetz verpflichtet, dem Bundesamt für Statistik Personendaten bekannt zu geben, die sie bei der Bearbeitung von Sozialhilfefällen erhoben haben. Verschiedene Gemeinden wandten sich im Zusammenhang mit der Durchführung der Erhebungen an uns.

Da es sich um besonders schützenswerte Personendaten handelt, ist die Bekanntgabe dieser Daten sensibel. Das Bundesamt für Statistik hat sich den Gemeinden gegenüber zur Einhaltung von Sicherheitsvorschriften verpflichtet. Die bekannt zu gebenden Personendaten werden dem Bundesamt für Statistik verschlüsselt übermittelt. Dieses verwendet sie nach der Entschlüsselung in anonymisierter Form für die Sozialhilfestatistik.

Wir haben für die Gemeinden «Empfehlungen für die Bekanntgabe von Personendaten im Zusammenhang mit der Schweizerischen Sozialhilfestatistik» verfasst. Sie enthalten Anweisungen, worauf bei der Erfassung und Übermittlung der Daten zu achten ist.

Einige Anfragen betrafen den Umfang der bekannt zu gebenden Personendaten. Dazu haben wir wiederholt festgehalten, dass nur bereits erhobene Daten unter die erleichterten Voraussetzungen von § 12 DSG fallen. Für die Erhebung von zusätzlichen Personendaten allein zu Statistikzwecken wäre eine entsprechende Rechtsgrundlage erforderlich, welche im Fall der Sozialhilfestatistik nicht vorliegt. Das Fehlen von Angaben ist auf ein Vollzugsproblem in der Sozialhilfe zurückzuführen: Die Gemeinden haben zu wenig konkrete Vorgaben über die Daten, die bei der Fallbearbeitung zu erheben sind.

- Die Gemeinden sind verpflichtet, dem Bundesamt für Statistik die für die Sozialhilfestatistik benötigten Personendaten bekannt zu geben, dies betrifft jedoch nur die bereits erhobenen Daten. Die Gemeinden sind weder berechtigt noch verpflichtet, zusätzliche Daten einzig für Statistikzwecke zu erheben.

INFORMATIONSSICHERHEIT

28. Instrumente des Datenselbstschutzes

Neue Browser-Diagnose

Der Datenselbstschutz nimmt an Bedeutung zu. Wo die Technologie oder das Recht den Schutz der Privatsphäre nicht mehr ausreichend gewähren können, sind ergänzende Instrumente des Datenselbstschutzes notwendig.

Für die Benutzenden von Informationstechnologie bedeutet das Internet den Gewinn neuer Souveränitäten, für den Schutz der Privatsphäre hingegen bewirkt die neue Technologie einen Verlust der Souveränität über die eigenen Daten.

Drei Kernsouveränitäten stehen im Vordergrund:

- Die Ortssouveränität: Die Benutzerinnen und Benutzer können die Services, wie sie im Internet angeboten werden weltweit irgendwo nutzen.
- Die Zeitsouveränität: Die Benutzerinnen und Benutzer können die Services, wie sie im Internet angeboten werden, wann immer es ihnen beliebt, benutzen.
- Die Inhaltssouveränität: Die Benutzerinnen und Benutzer können die Services, wie sie das Internet anbietet, mit aus ihrer Sicht beliebigen Inhalten füllen.

Auf Grund dieser Ausgangslage erstaunt es nicht, dass das Internet sich schnell wachsender Beliebtheit erfreut.
Die Kehrseite ist

- der Verlust der Datensouveränität: Durch die Benutzung des Internets geht eine klassische Souveränität, die Souveränität über die eigenen Daten, verloren.

Die «Browser-Diagnose» ist ein

neues Instrument, das wir in Zusammenarbeit mit der Hochschule Rapperswil entwickelt haben und den Internetnutzenden unter «www.datenschutz.ch» zur Verfügung stellen. Dieser Test ergänzt Angebote von anderen unabhängigen Datenschutzbehörden und bietet den Benutzenden eine vertrauenswürdige Möglichkeit, die Sicherheitseinstellungen ihres PCs beim Surfen zu überprüfen.

Die Browser-Diagnose zeigt in vier Stufen die Datenschutzrisiken bei der Nutzung des Internets auf:

- Die Stufe «Fragwürdige Transparenz» gibt Auskunft über die Spuren, die jede Internetnutzung hinterlässt.
- Unter «Bedenkliche Offenheit» werden insbesondere die Einstellungen betreffend Java, Javascript und Cookies geprüft.
- Die «Gefährliche Manipulierbarkeit» untersucht ActiveX.
- In der Stufe «Unnötiges Risiko» wird geprüft, ob freigegebene Ressourcen auf dem PC bestehen.

Jede Stufe wird in Bezug auf das Datenschutzrisiko erklärt und bewertet. Die Benutzenden erhalten somit die Möglichkeit, ihre Sicherheitseinstellungen anzupassen. Datenselbstschutz ist aber nicht Selbstzweck, sondern nur sinnvoll, wenn er zusammen mit datenschutzfreundlichen Technologien und neuen rechtlichen Instrumenten, die deren Einsatz fördern, angewandt wird.

- Die neue Browser-Diagnose ist ein Instrument des Datenselbstschutzes, das Bürgerinnen und Bürger und die Verwaltung für einen sicheren Umgang mit dem Internet sensibilisiert.

29. Umsetzung der Informatiksicherheitsverordnung

Keine Informatik-Sicherheitsstrategie in der Verwaltung

Die Informatiksicherheitsverordnung (ISV) bildet die Grundlage für die Qualifikation der Datenbearbeitungen nach Sicherheitsstufen. Je nach Sicherheitsstufe sind unterschiedliche Massnahmen notwendig.
In der Praxis werden diese Sicherheitsmassnahmen unterschiedlich umgesetzt. Gründe hierfür sind fehlendes Know-how und mangelnde Ressourcen, fehlende Nachkontrollen (Bereich IT-Audit) und mangelnde interne Schutzmassnahmen (in Form eines IT-Sicherheitscontrollings). Zudem besteht keine direktionsübergreifende IT-Sicherheitsorganisation.

Diese Mängel wurden im Forum der Informatik-Verantwortlichen der Direktionen besprochen. Zur Behandlung der festgestellten Probleme wurde eine Arbeitsgruppe gebildet, bestehend aus Mitarbeitenden der Abteilung für Informatikplanung (AIP) und des Datenschutzbeauftragten.

Die Arbeitsgruppe war beauftragt, einen Antrag an das oberste Strategiegremium, die Kommission für strategische Informatikführung (KOSIF), auszuarbeiten. Konsequenterweise lautete der Antrag an die KOSIF, es sei eine Informatiksicherheitsstrategie auszuarbeiten, da die erwähnten Mängel erst nach der Verabschiedung einer direktionsübergreifenden Zielsetzung angegangen werden können und die Informatiksicherheitsverordnung (ISV) als bereits vorhandene Leitlinie zu konkretisieren ist.

Die KOSIF lehnte den Antrag ab mit dem Hinweis, dass mehr Datenschutzreviews und zusätzliche Sensibilisierungsmassnahmen notwendig seien, obwohl im Rahmen der bestehenden Ressourcen der Datenschutzbeauftragte seinen Anteil an Datenschutzreviews kaum verstärken und die Sensibilisierungsmassnahmen kaum ausweiten kann.

- Der unterschiedlichen Umsetzung der Sicherheitsmassnahmen gemäss Informatiksicherheitsverordnung müsste mit einer umfassenden Informatiksicherheitsstrategie begegnet werden.

30. Informatikprojekte an Spitälern

Mangelhafter Einbezug des Datenschutzbeauftragten

Im Berichtsjahr gelangten zwei Projektleitungen an uns, die sich mit der Einführung von digitalen Bildbewirtschaftungssystemen an Spitälern (sog. «PACS») befassten. Die Gesundheitsdirektion hatte beide Projekte zur Ausschreibung freigegeben, unter anderem mit der Auflage, den Datenschutzbeauftragten über das Projekt zu informieren.
Zu diesem Zeitpunkt ist das – in der Regel umfangreiche – Pflichtenheft bereits fertig erstellt und die Rahmenbedingungen des Datenschutzgesetzes und der Informatiksicherheitsverordnung können kaum mehr rechtzeitig und konzeptionell sinnvoll eingepasst werden. Es ist daher denkbar ungeeignet, den Datenschutzbeauftragten so spät in ein Informatikprojekt einzubeziehen. Der Einbezug sollte bereits während der Erarbeitung der Ausschreibungsunterlagen stattfinden.
Ausserdem erhielten wir in beiden Projekten die Projektinformation nur zur Kenntnisnahme. Wir informierten die Projektleitungen, dass wir ohne entsprechenden Auftrag davon ausgingen, auf eine Beratung werde vorerst verzichtet. Eine genaue Prüfung der Unterlagen bzw. eine datenschutzrechtliche Beurteilung machten wir davon abhängig, dass klare Fragen formuliert und alle relevanten Unterlagen eingereicht werden. Beide Projekte – notabene aus Bereichen mit sehr sensiblen Datenbearbeitungen – werden nun offenbar ohne weiteren Einbezug des Datenschutzbeauftragten weitergeführt.

- Der Datenschutzbeauftragte ist in Informatikprojekte möglichst früh und in aktiver Form einzubeziehen. Die blosse Information nach der Freigabe zur Ausschreibung macht wenig Sinn.

DATENSCHUTZREVIEW

31. IT-Grundschutzmassnahmen mangelhaft

Datenschutzreviews weitergeführt

Wir haben wieder bei ausgewählten Amtsstellen und Gemeinden Datenschutzreviews durchgeführt. Ziel der Reviews ist, die geprüften Stellen innert möglichst kurzer Zeit für bestimmte Aspekte des Datenschutzes und der Informationssicherheit zu sensibilisieren. Die Amtsstellen sollen auf Grund der Empfehlungen des Datenschutzbeauftragten ihre Datenbearbeitungen an die rechtlichen Rahmenbedingungen anpassen und Verbesserungen im organisatorischen und technischen Bereich vornehmen.

Um die Ergebnisse der geprüften Stellen über einen längeren Zeitraum miteinander vergleichen zu können, wurde die Review inhaltlich nicht verändert. Gleichzeitig profitierten die geprüften Stellen von den Erfahrungen der Prüfenden und die Prüfungen konnten schneller abgewickelt werden.

Bei den Prüfungen während des Berichtsjahres mussten wir mehrheitlich die bereits früher (siehe Tätigkeitsbericht Nr. 6 [2000], S. 32 f.) aufgezeigten Mängel beanstanden:

- Die Zugriffsbestimmungen im Bereich der LAN-Server sind zu generell definiert. Meistens sind die eher älteren Anwendungen (wie Host-Applikation von Lösungsanbietern in Rechenzentren) im Bereich Zugriffsschutz gut bis sehr gut administriert und dokumentiert, im Bereich der File-Server (für Office-Dokumente usw.) ist meistens das Need-to-know-Prinzip schlechter eingehalten. Der Datenschutzbeauftragte hat Hilfen und Checklisten für den Aufbau eines Konzepts erarbeitet und bietet auch Unterstützung bei der Implementierung an. Wie für jede organisatorische Massnahme ist ein Initialaufwand zu leisten, der sich aber auszahlt – intern mit einer

gestrafften Organisation und gegen aussen mit gesteigertem Vertrauen in die Abläufe und Einhaltung der rechtlichen Rahmenbedingungen.

- Bei allen Stellen war immer eine verantwortliche Person für den gesamten IT-Bereich bestimmt, die Verantwortlichkeit für IT-Sicherheit wurde jedoch nicht zugewiesen. Damit entfallen auch die konkreten Zielsetzungen für dringende und wichtige Punkte wie die Umsetzung der Informatiksicherheitsverordnung (ISV) und die notwendige Schulung der Mitarbeitenden für IT-Sicherheit.
- Immer häufiger kaufen Amtsstellen Dienstleistungen bei externen Dritten ein. Die datenschutzkonforme Bearbeitung von Personendaten muss in diesen Fällen durch den Abschluss von Verträgen mit den externen Partnern sichergestellt werden. In der Praxis erweisen sich die Vertragswerke oftmals als mangelhaft.

Es ist unerlässlich, den Zweck und den Umfang der Datenbearbeitungen durch die externen Partner klar zu umschreiben. Vereinbarungen über die Geheimhaltung, den Datenschutz und die Daten- und Informationssicherheit sind ebenfalls notwendig. Die Verantwortlichkeiten auf beiden Seiten müssen genau festgehalten werden. Schliesslich sind die Anforderungen an die Sicherheit für beide Vertragsparteien durch eine aktuelle Vereinbarung im Sinne einer Sicherheits-Policy verbindlich zu regeln (siehe auch S. 36).

Die nach der Datenschutzreview abgegebenen Empfehlungen beinhalten konkrete Verbesserungsvorschläge für den betrieblichen Alltag. Das oft angetroffene Ressourcen- und Know-how-Problem ist mit der Zuteilung der Verantwortlichkeiten zu lösen.

- Die Datenschutzreviews sind ein wichtiger Beitrag zur Informationssicherheit. Die festgestellten Mängel in den Bereichen Zugriffskonzept, Verantwortlichkeit für IT-Sicherheit und externe Dienstleister zeigen, dass weiterhin grosser Handlungsbedarf besteht.

Konzept für ein Informations- und Datenschutzgesetz

Neue Bedürfnisse nach Informationszugang und die technologische Entwicklung sind Ausgangspunkt für ein wegweisendes Gesetzgebungskonzept, das den Zugang zu Informationen und den Schutz der Privatheit umfassend regeln soll.

Das Datenschutzgesetz des Kantons Zürich trat 1995 in Kraft; es beruht auf einem Konzept aus den 1970er-Jahren. Seit dieser Zeit hat sich die Technologie grundlegend verändert, ohne dass das Recht mit dieser Entwicklung Schritt gehalten hätte. Betrachtet man das Datenschutzgesetz im Hinblick auf seine Wirkungen sowie das Umfeld der gesellschaftlichen und technischen Entwicklungen, besteht Handlungsbedarf: Das DSG ist revisionsbedürftig. Welche Bereiche eine Revision umfassen müsste, haben wir bereits im Tätigkeitsbericht Nr. 6 [2000], S. 28 f. dargestellt.

Nebst dem Revisionsbedarf besteht eine allgemeine Tendenz für mehr Transparenz in der Verwaltung. So verlangt eine parlamentarische Motion (KR-Nr. 328/1998) vom Regierungsrat die Einführung des Öffentlichkeitsprinzips im Kanton Zürich. Das Öffentlichkeitsprinzip beinhaltet einen Paradigmawechsel zu einer transparenten Verwaltung: Alle Informationen, die nicht auf Grund eines besonderen Beschlusses (Gesetz oder Interessenabwägung) vertraulich oder geheim sind, sollen frei zugänglich sein. Informationszugang und Öffentlichkeit von Daten und Akten einerseits sowie Geheimhaltungspflicht und Schutz der Privatsphäre andererseits stellen die beiden Seiten der gleichen Medaille dar und sind deshalb konzeptionell einheitlich zu regeln. Es drängte sich deshalb auf, bei der Umsetzung der Motion nicht nur die Aspekte des Informationszugangs, sondern auch den Schutz der Privatsphäre (d.h. den Datenschutz) einzubeziehen.

Der Regierungsrat hat entschieden, ein Informations- und Datenschutzgesetz zu schaffen, das beide Aspekte konzeptionell einheitlich regelt und auch die einleitend erwähnte Revisionsbedürftigkeit des Datenschutzgesetzes angeht. Unter der Leitung der Direktion der Justiz und des Innern, welche mit der Umsetzung der Motion beauftragt ist, erarbeitete eine Arbeitsgruppe ein entsprechendes

Revision des Datenschutzgesetzes des Bundes

Während der Kanton Zürich der Revisionsbedürftigkeit des Datenschutzgesetzes mit einem wegweisenden konzeptionellen Ansatz begegnet, begnügt man sich auf Bundesebene mit «Garantiearbeiten». Die Teilrevision des Bundesgesetzes über den Datenschutz soll vor allem die Transparenz der Datenbearbeitungen verbessern. Nachteilig ist dabei, dass nach wie vor betroffenen Personen zugemutet wird, gegen unrechtmässige Datenbearbeitungen vorzugehen. Insbesondere im Privatrechtsbereich ist auf Grund des Prozessrisikos, der wenig ausgeprägten Sanktionen und der einseitigen Beweislastverteilung ein solches Vorgehen zum Vornherein illusorisch. Die (einseitige) Abschaffung der Meldepflicht von Datensammlungen bzw. der Bekanntgabe von Datensammlungen ins Ausland für private Datenbearbeiter beweist, dass keine konzeptionellen Arbeiten gemacht wurden, sondern nur vor einem Vollzugsnotstand kapituliert wird.

Der Regierungsrat des Kantons Zürich kritisierte in seiner Vernehmlassung, dass die Revision keine konzeptionellen Ansätze enthält, um die strukturellen und instrumentellen Defizite der heutigen Gesetzgebung zu lösen. Er zeigte dem Bund die wesentlichen Problembereiche auf, die im Kanton Zürich erkannt und angegangen werden, und nahm auch kritisch Stellung zu einzelnen Revisionspunkten.

Öffentlichkeitsprinzip in der Schweiz und international

Das Öffentlichkeitsprinzip in der Verwaltung wurde erstmals bereits vor über 200 Jahren in Schweden eingeführt. Auch Kanada gilt als Vorreiter für ein «right of access to information». Neuste Beispiele für die Einführung des Öffentlichkeitsprinzips sind die Organe der Europäischen Union sowie die deutschen Bundesländer Brandenburg, Berlin und Schleswig-Holstein.

In der Schweiz führte der Kanton Bern als Pionier 1995 das Öffentlichkeitsprinzip ein. Dabei machte er mehrheitlich positive Erfahrungen. Zu Schwierigkeiten führt jedoch, dass zwei Erlasse – ein Informationsgesetz und ein Datenschutzgesetz – nebeneinander bestehen, die inhaltlich nicht aufeinander abgestimmt sind.

Seit 2002 verfügt der Kanton Solothurn über ein Informations- und Datenschutzgesetz. Wegweisend ist der Ansatz, Informationszugang und Schutz der Privatsphäre in einem einzigen Erlass zu regeln.
Der Kanton Zürich steht mit seinen Bestrebungen mitten in einem Feld von mehreren weiteren Kantonen, die derzeit Verfassungsänderungen und/oder Gesetze zur Einführung des Öffentlichkeitsprinzips erarbeiten. Auf Bundesebene wurde – wie beim Datenschutzgesetz – auch beim Entwurf eines Öffentlichkeitsgesetzes verpasst, ein konsequentes Konzept zu erarbeiten; der Gesetzesentwurf weist einige Mängel auf (siehe Tätigkeitsbericht Nr. 6 [2000], S. 15 f.).

Konzept, das vom Regierungsrat im März 2002 verabschiedet wurde. In dieser Arbeitsgruppe wirken Vertreterinnen und Vertreter des Datenschutzbeauftragten, der Kommunikationsabteilung des Regierungsrates, des Staatsarchivs, der Gerichte und der Gemeinden mit.

Das neue Informations- und Datenschutzgesetz wird den Zugang und den Nicht-Zugang zu Informationen einheitlich regeln. Dabei geht es zum Beispiel um die Öffentlichkeit oder Nicht-Öffentlichkeit von Sitzungen (Regierung, Kommissionen, Parlament, Gerichtsverhandlungen, Gemeindebehörden etc.), oder es ist zu regeln, wie weit eine Informationspflicht der Behörden geht.

Das Öffentlichkeitsprinzip geht auch von einem grundsätzlichen Akteneinsichtsrecht aller Personen aus; dieses geht weiter als das Auskunftsrecht über die eigenen Daten (§ 17 DSG) oder das Akteneinsichtsrecht im Verfahren bei einem schutzwürdigen Interesse (§ 8 Verwaltungsrechtspflegegesetz; VRG). In allen Fällen stellen sich sodann Fragen des Geheimnisschutzes bei überwiegenden öffentlichen oder privaten Geheimhaltungsinteressen. Der Gesetzgeber hat eine Interessenabwägung über den Umfang des Informationszugangs bzw. der Geheimhaltung vorzunehmen. Er kann auch eine Regelung treffen, wonach die Pflicht zur Interessenabwägung mit einem gewissen Ermessensspielraum der rechtsanwendenden Behörde bzw. dem Richter übertragen wird.

Das neue Informations- und Datenschutzgesetz wird auch den Schutz der Privatsphäre (Datenschutz) regeln. Die bestehenden Bestimmungen können jedoch nicht einfach übernommen werden, da – wie erwähnt – Revisionsbedarf besteht. Die Regelungen über die Datenbekanntgabe sind im Rahmen des Informations(nicht)-zugangs zu behandeln. Die Revision geht jedoch darüber hinaus und betrifft insbesondere Fragen im Zusammenhang mit der Technologie.
Das DSG ist eigentlich Technikfolgenrecht und hat deshalb wünschbare und unerwünschte Folgen der Technik zu regulieren.

So sind für den Einsatz neuer Technologien (z.B. Videoüberwachung), neuer Datenbearbeitungsmethoden (z.B. sog. «Data Warehousing» und «Data Mining») und neuer Datenbearbeitungen der Verwaltung (z.B. Outsourcing) auf Grund einer Abwägung von Chancen und Risiken Schranken aufzustellen und entsprechende Rahmenbedingungen zu schaffen.
Die Technik ist jedoch nicht nur als Bedrohung der Privatsphäre wahrzunehmen, sondern bietet auch Möglichkeiten zu deren Schutz. Datenschutzfreundliche Technologien können die Wirksamkeit des Datenschutzrechts erhöhen und nachträgliche aufwändige Einzelfallkontrollen ersetzen. Der Einsatz solcher Technologien (z.B. Verschlüsselung) ist deshalb zu fördern und in sensiblen Bereichen vorzuschreiben.

Die Komplexität und Vernetzung von Informatiksystemen und -anwendungen erfordert, dass Systeme in Zukunft mehrheitlich mit einer Auditierung auf ihre rechtliche und technische Vereinbarkeit mit den Prinzipien des Datenschutzes und der datenschutzgerechten Systemgestaltung überprüft werden. Damit ist eine Zertifizierung im Sinne eines Qualitäts- und Gütesiegels verbunden. Das System der Auditierung und Zertifizierung wird beispielsweise im Umweltbereich schon seit längerem eingesetzt und hat sich dort bewährt. Auditierung und Zertifizierung verhindern nicht die (Weiter-)Entwicklung der Informationstechnologien, sondern sie tragen bei zu einer datenschutzfreundlichen Systemgestaltung im Sinne einer grösstmöglichen Stärkung des Grundrechts auf Schutz der Privatsphäre der betroffenen Personen.

Der Entwurf des neuen Informations- und Datenschutzgesetzes soll voraussichtlich bis Mitte 2003 vorliegen und in der zweiten Jahreshälfte 2003 ins Parlament gelangen.

- Das Konzept für ein Informations- und Datenschutzgesetz geht in die richtige Richtung. Auf Grund der umfassenden Betrachtung von Informationszugang und Schutz der Privatheit ist ein konzeptionell schlüssiger Gesetzesentwurf zu erwarten. Zugleich kann die nötige Revision des DSG stattfinden, so dass die Wirksamkeit des Datenschutzes erhöht und der Grundrechtsschutz optimiert werden kann.

Verwaltungsweite Sicherheitsinfrastruktur als Ziel

Im Projekt SOPRANO konnten weitere Grundlagen für die Einführung einer verwaltungsweiten Sicherheitsinfrastruktur geschaffen werden.

Für eine verwaltungsweite Sicherheitsinfrastrukur, die unterschiedlichste Bedürfnisse befriedigen kann, wird eine Public-Key-Infrastruktur (PKI) die Grundlage bilden. Der Kanton Zürich legt im Projekt SOPRANO mit diversen Pilotprojekten die Grundlagen für die Einführung der Sicherheitsinfrastruktur (vgl. Tätigkeitsbericht Nr. 5 [1999], S. 22 f. und Tätigkeitsbericht Nr. 6 [2000], S. 30 f.).

Im Frühjahr 2001 wurde die Strategie verabschiedet und definiert, für welche Einsatzzwecke eine PKI aufgebaut werden soll. Auf der Basis einer eigenen Certification Authority (CA) wurden die Ausführungsbestimmungen (Certification Policy und Certification Pratice Statement) nach eigenen Anforderungen definiert. Das Know-how bezüglich PKI wird mit einer Koordinationsstelle intern aufgebaut und verbleibt im Kanton. Damit wird die Kontrolle über die Funktionalität (Verwendungs- und Einsatzzweck) und den Sicherheitsstandard der Infrastruktur, die der kantonalen Verwaltung und den Gemeinden zur Verfügung steht, gewahrt.

Mit Pilotprojekten wurden erste Erfahrungen im Betrieb einer Public-Key-Infrastruktur gesammelt. Neben dem technischen Aspekt war vor allem die organisatorische Integration einer PKI in der Verwaltung eine Herausforderung. Im Hinblick auf die verwaltungsweite Verbreitung der Zertifikatsnutzung galt es sicherzustellen, dass der Ausbau der Sicherheitsinfrastruktur koordiniert und dass die Erkenntnisse aus den Pilotprojekten berücksichtigt wurden.

Auf der Grundlage einer provisorischen Infrastruktur wurde eine CA (Certification Authority) mit einer Sub-CA und mehreren dezentralen RAs (Registration Authority) aufgebaut. Im August 2001 wurde die PKI technisch erfolgreich in Betrieb genommen.

Für den Pilotbetrieb werden zwei Zertifikatsklassen, «Hoch» und «Tief», verwendet. Die Zertifikatsklasse «Hoch» besteht aus zwei Zertifikaten, welche auf einer Smartcard ausgestellt und nur gegen persönliche Vorstellung des Antragstellers an der RA-Stelle ausgegeben werden. Die beiden Zertifikate werden für die digitale Signatur und die Verschlüsselung benötigt.
Die Zertifikatsklasse «Tief» besteht aus einem Zertifikat, welches elektronisch beantragt werden kann und nur für die Verschlüsselung eingesetzt werden soll. Die beiden Zertifikatsklassen werden aus Kostengründen von einer Sub-CA verwaltet, wobei die Zertifikatsklassen durch entsprechende Regeln des PKI-Systems erzeugt werden. In der definitiven Infrastruktur soll pro Klasse jeweils eine eigene Sub-CA betrieben werden. Beim Datenschutzbeauftragten und im Universitätsspital wurden zwei dezentrale RA-Stellen installiert und in Betrieb genommen. Es folgten eine RA bei der zentralen Informatik der Direktion der Justiz und des Innern und bei der Kantonspolizei. Damit sollen einerseits die technischen Möglichkeiten und die betrieblichen Prozesse verifiziert werden, andererseits entsprechende Erfahrungen in den Anforderungskatalog für die Beschaffung der definitiven Infrastruktur einfliessen.

Das Universitätsspital (USZ) arbeitete bis Ende 2001 mit Swisskey-Zertifikaten auf Smartcards. Für die Fernabfrage von E-Mails erfolgt die Authentifikation der Benützenden über einen SSL-Proxy, welcher die Anfragen an den Webserver für Outlook-Webaccess weiterleitet. Mit dieser Infrastruktur wird die sichere Abfrage der Mailboxen für USZ-Mitarbeitende möglich. Noch vor der Betriebseinstellung von Swisskey wurden bereits diverse SOPRANO-Zertifikate der Klasse «Hoch» ausgestellt, die noch heute verwendet werden. Weitere Benützende werden laufend mit SOPRANO-Zertifikaten ausgerüstet. Die SOPRANO-Smartcards und -Zertifikate konnten problemlos mit der bereits bestehenden Infrastruktur (Smartcard-Leser) verwendet werden.

Diverse Stellen wurden mit Secure Mail für MS Outlook und Lotus Notes ausgerüstet. Der Pilot wird neben den Mitarbeitenden des Datenschutzbeauftragten auch weitere Verwaltungsstellen und – als Spezialfall – den Kanton Luzern umfassen. Interoperabilitätstests mit dem Bund verliefen erfolgreich. Auch die Direktion für Justiz und Inneres testet SOPRANO-Zertifikate (für den Einsatz mit Secure E-Mail). In dieser Direktion wird bisher schon eine Sicherheitslösung mit über 1200 Benützenden eingesetzt. Das Ziel, die vorhandene Lösung so umzurüsten, dass die vorhandenen Smartcard-Leser mit neuen Smartcards auch SOPRANO-Zertifikate speichern können, wurde im Test erfolgreich erreicht. Speziell beachtet wird in allen Tests die benutzerfreundliche Handhabung.

Für das Personalinformationssystem PALAS, das auf einem Hostrechner bei einem kantonsnahen IT-Betreiber läuft, soll die sichere Verbindung und Authentifikation der Benützenden mittels einer VPN-Lösung (Virtual Private Network) erreicht werden. Als Zwischenlösung wird eine geschützte und verschlüsselte Verbindung zwischen Client und Rechenzentrumsumgebung aufgebaut. Die Benutzer-Authentifikation erfolgt via Smartcard. Anschliessend wird die VPN-Verbindung aufgebaut. Die definitive Lösung soll später in Verwendung mit der definitiven Infrastruktur auf weitere Host-Anwendungen übertragen werden können.

Für das Projekt der Bildungsstatistik wurden Authentisierungsanforderungen der Web-Clients erarbeitet. Eine erste Gruppe von Testpersonen wird im Juli 2002 die Applikation vor dem Rollout im Jahr 2003 benützen können.

Im Projekt E-Workpermits soll der Einsatz von SOPRANO-Zertifikaten für Authentisierungszwecke der Systemadministratoren überprüft werden. Nach der erfolgten Ausschreibung können die Zertifikate in der gewählten Lösung verwendet werden.

Im Teilprojekt E-Procurement geht es im Wesentlichen um elektronische Formulare jeglicher Art. Diese sollen bei der Benutzung im Internet mit SOPRANO-Zertifikaten digital signiert werden können. Der Einsatzzweck der SOPRANO-Zertifikate bleibt vorerst auf die öffentlichen Stellen beschränkt.

Der Erfahrungsaustausch mit anderen Anwendern von PKI, insbesondere mit dem Bundesamt für Informatik und Telekommunikation (BIT), erfolgte regelmässig und brachte wichtige Erkenntnisse für die Ausschreibungsunterlagen.

Neben den Pilotprojekten wurde parallel ein detailliertes Pflichtenheft für eine Submission erstellt. Die Publikation der Submissionsanzeige erfolgte im Frühjahr 2002.

- Im Verlaufe des vergangenen Jahres konnten weitere Grundlagen für den Aufbau einer verwaltungsweiten Sicherheitsinfrastruktur geschaffen werden. Die gewonnenen Erfahrungen werden die Einführung einer definitiven Lösung erleichtern.

Schaffung von Rechtsgrundlagen notwendig

Während im Bereich der Informatik klare rechtliche Rahmenbedingungen geschaffen werden konnten, bleiben andere Gesetzgebungsarbeiten unbefriedigend.

1. Neue «AGB Sicherheit»

Neben AGB auch Checklisten für Outsourcing-Verträge

Weil die Informatik des Kantons Zürich ausgelagert und ein entsprechendes Gesetz bereits erlassen worden war (Gesetz über die Auslagerung von Informatikdienstleistungen, LS 172.71), setzte die Kommission für strategische Informatikführung (KOSIF) eine Arbeitsgruppe ein, die Lösungen für die notwendigen Vertragsgrundlagen zu entwerfen hatte (vgl. Tätigkeitsbericht Nr. 5 [1999], S. 16). Der Datenschutzbeauftragte wirkte in dieser Arbeitsgruppe mit und erarbeitete «Allgemeine Geschäftsbedingungen über die Geheimhaltung, den Datenschutz und die Daten- und Informationssicherheit bei der Erbringung von Informatikdienstleistungen» («AGB Sicherheit»). Die «AGB Sicherheit» wurden interessierten Kreisen zur Stellungnahme unterbreitet. Die KOSIF verabschiedete die «AGB Sicherheit» im September 2001 und erklärte sie verwaltungsweit verbindlich.
Der Datenschutzbeauftragte empfahl allen öffentlichen Organen – insbesondere auch den Gemeinden, den Organen der Rechtspflege und den selbstständigen öffentlichen Anstalten – die «AGB Sicherheit» in die Verträge mit externen Informatikdienstleistern zu integrieren. Parallel dazu erarbeitete der Datenschutzbeauftragte «Checklisten für Outsourcing-Verträge». Diese Checklisten ermöglichen es den verantwortlichen Organen, mit ihren Outsourcing-Partnern umfassende und vollständige Regelungen im Bereich Datenschutz und Informationssicherheit zu treffen.

- Die «AGB Sicherheit» und die Checklisten für Outsourcing-Verträge bieten den verantwortlichen Organen umfassende und vollständige Hilfestellungen speziell für das Informatik-Outsourcing und vervollständigen die Bestimmungen des Auslagerungsgesetzes.

2. (Kein) Gesetz zur Bewirtschaftung raumbezogener Daten?

Fehlender Handlungswille der Verantwortlichen

Anfang 2001 hatte der Regierungsrat die Baudirektion mit der Erarbeitung der notwendigen gesetzlichen Grundlagen für die Datenbearbeitungen im Bereich der Bewirtschaftung raumbezogener Daten beauftragt (vgl. Tätigkeitsbericht Nr. 6 [2000], S. 35). Bereits vor fünf Jahren hatten wir auf die Notwendigkeit von Rechtsgrundlagen in diesem Bereich hingewiesen (vgl. Tätigkeitsbericht Nr. 2 [1996], S. 16 f.) und angesichts der technologischen und tatsächlichen Entwicklungen ein formelles Gesetz verlangt (vgl. Tätigkeitsbericht Nr. 5 [1999], S. 19 ff.).
Die Baudirektion versäumte es jedoch, das Projekt zu organisieren. Vielmehr begann eine Art «Ad-hoc-Arbeitsgruppe», in welche der Datenschutzbeauftragte und der Gesetzgebungsdienst einbezogen wurden, erste Entwürfe zu formulieren. Da jedoch ein Gesamtkonzept fehlte, sahen wir uns schliesslich veranlasst, mit erheblichem Aufwand ein Konzept für die Bearbeitung raumbezogener Daten zu erarbeiten und einzelne Bestimmungen ansatzweise zu formulieren. Fragen, welche über die datenschutzrechtlichen Aspekte hinausgehen (z.B. Urheberrecht, Gebühren, Rechtsschutz etc.), mussten dabei offen bleiben.
Im vierten Quartal 2001 wurden die Gesetzgebungsarbeiten offensichtlich sistiert. Der Regierungsrat bewilligte weitere Ausbauten der Systeme in diesem Bereich, obwohl die Baudirektion verpflichtet gewesen wäre, bis Mitte 2001 Antrag bezüglich Rechtsgrundlagen zu stellen.
Mittlerweile stellt sich die Baudirektion auf den Standpunkt, dass die notwendigen gesetzlichen Grundlagen im Rahmen des neuen

Informations- und Datenschutzgesetzes (siehe S. 31 ff.) zu schaffen seien. Dabei verkennt sie, dass auch ein zukünftiges Informations- und Datenschutzgesetz vorwiegend ein Rahmengesetz sein wird und konkrete Rechtsgrundlagen über Datenbearbeitungen in den bereichsspezifischen Erlassen nicht ersetzen kann.

Die Notwendigkeit der Rechtsetzung im Bereich der Bewirtschaftung raumbezogener Daten zeigte sich einmal mehr bei einer konkreten Anfrage einer grösseren Zürcher Gemeinde. Wir konnten zu den vorwiegend technischen Fragen bezüglich Sicherheitsmassnahmen nicht Stellung nehmen, da weiterhin unklar bleibt, ob die vorgesehenen Zugriffe aus rechtlicher Sicht überhaupt zulässig sind.

- Ohne ausreichende Rechtsgrundlagen lässt sich der weitere Ausbau der geografischen Informationssysteme und der Gebäudedatenbanken nicht rechtfertigen.

---

3. Entwurf eines Patientenrechtsgesetzes

Nachbesserungen vorgenommen

Der Entwurf eines Patientenrechtsgesetzes hatte aus datenschutzrechtlicher Sicht verschiedene Mängel (siehe Tätigkeitsbericht Nr. 6 [2000], S. 10). Die Gesundheitsdirektion überarbeitete den Entwurf in einzelnen Punkten und unterbreitete ihn uns zu einer Stellungnahme. Der überarbeiteten Fassung konnten wir mehrheitlich zustimmen.

Die Unterscheidung zwischen Informationen über den Gesundheitszustand und Informationen aus der Krankengeschichte wurde zwar beibehalten, die Widersprüche wurden jedoch beseitigt. Da das Konzept offenbar auf den tatsächlichen Gegebenheiten in der Praxis beruht, ist zu hoffen, dass die betroffenen Medizinalpersonen die Regelungen in der Praxis auch umsetzen können.

In Bezug auf die Aufbewahrung sieht der Entwurf nun klare Regelungen vor. Begrüssenswert ist der Grundsatz, wonach Krankengeschichten so zu führen sind, dass sie auf einfache Weise anonymisiert werden können. Ist die Krankengeschichte einmal anonymisiert, stellen sich aus datenschutzrechtlicher Sicht keine weiteren Fragen zur Aufbewahrung.

Beim Auskunftsrecht gilt der Grundsatz, dass die betroffene Person Anspruch auf Kopien hat (§ 10 Abs. 2 Datenschutzverordnung). Der Entwurf des Patientenrechtsgesetzes bestätigt diesen Grundsatz, sieht jedoch ohne weitere Konkretisierung die Möglichkeit der Kostenauflage vor. Es besteht die Gefahr, dass die Kostenauflage zur Regel wird. Müssen betroffene Personen für Auskünfte über die eigenen Daten bezahlen, wird der Grundrechtsgehalt des Datenschutzes faktisch ausgehöhlt. Wünschenswert wäre die analoge Anwendung der bundesrechtlichen Regelung, die vom Grundsatz der Kostenlosigkeit ausgeht und die Ausnahmen eng begrenzt. Der Entwurf sollte in dieser Hinsicht konkretisiert werden.

- Die Mängel am Entwurf des Patientenrechtsgesetzes wurden teilweise behoben. Problematisch bleibt die Bestimmung, dass für die Erteilung von Auskünften Kosten erhoben werden dürfen.

Erweitertes Informationsangebot

Das neue Informationskonzept wurde schrittweise umgesetzt. Die Homepage soll die Grundlage für den Informationspool der Zukunft bilden.

1. Aktualisierte Homepage
www.datenschutz.ch

Im vergangenen Jahr wurde die Homepage des Datenschutzbeauftragten neu konzipiert. Unter «www.datenschutz.ch» sind nun sämtliche Publikationen des Datenschutzbeauftragten zu finden (Tätigkeitsberichte, Zeitschrift «Fakten», Broschüren). Die Rubrik «Beratung» enthält aktuelle Fragen und Antworten aus der Beratungspraxis des Datenschutzbeauftragten und Informationen zu bestimmten Themen; sie wird laufend ausgebaut.
Grundlegende Gerichtsentscheide zu Datenschutz und Informationssicherheit sind in der Rubrik «Rechtsprechung» zusammengefasst und kommentiert. Zur Sensibilisierung der Internet-Benutzenden gibt die Rubrik «Sicher surfen» wichtige Sicherheitstipps im Umgang mit dem Internet.
Neu ist die Möglichkeit, mittels Selektion einer Zielgruppe einzusteigen: das Informationsangebot ist dann auf die Bedürfnisse der jeweiligen Zielgruppe ausgerichtet.

Das neue Webangebot enthält auch einen Passwort-Check, der an der Hochschule Rapperswil entwickelt wurde. Benutzer und Benutzerinnen können die Qualität eines Passwortes bzw. eines Passwort-Typus online überprüfen; die Daten werden in verschlüsselter Form übermittelt. Der Passwort-Check erläutert Fachbegriffe und enthält Empfehlungen für gute Passwörter. Mit der «Browser-Diagnose» (siehe S. 27 f.) und dem «Passwort-Check» stehen der Verwaltung und der Bevölkerung damit vertrauenswürdige Tools zur Verfügung, die zu einer erhöhten Sensibilisierung und einem verbesserten Risikobewusstsein beitragen.

- Die Homepage des Datenschutzbeauftragten wurde neu konzipiert und gestaltet. «www.datenschutz.ch» ermöglicht den raschen Zugang zu zielgruppenspezifischen Informationen und bietet alle bestehenden Publikationen in elektronischer Form an.

Web:
www.datenschutz.ch
E-Mail:
datenschutz@dsb.zh.ch

2. Symposium on Privacy and Security

Schlüsselthemen der Informationsgesellschaft

Nach den Erfolgen der jeweils eintägigen Symposien für Datenschutz und Informationssicherheit in den letzten Jahren fand das – neu von der Stiftung für Datenschutz und Informationssicherheit veranstaltete – Symposium on Privacy and Security erstmals an zwei Tagen im November 2001 statt. Neben vier Plenumsveranstaltungen wurden zusätzlich acht Tracks angeboten. Den Veranstaltern gelang es, namhafte Fachleute aus dem In- und Ausland zu verpflichten.

Die Plenumsveranstaltungen deckten folgende Themenkreise ab:

- «Die Rolle des Datenschutzes beim E-Commerce (B2C)»: John Dryden, Head of the Information Computer and Communications Policy Division bei der OECD, präsentierte deren Rahmenbedingungen für erfolgreichen E-Commerce. Diesen vorwiegend theoretischen Ansatz übertrug Peter Quadri, Vorsitzender der Geschäftsleitung IBM Schweiz, in die Praxis. Er betonte die Wichtigkeit eines glaubwürdigen und transparenten Datenschutzes für den E-Commerce und erläuterte anhand von Beispielen, wie die IBM Datenschutz im Unternehmen eingeführt und umgesetzt hat.
- «Sicherheitsinfrastrukturen und -lösungen»: Prof. Dr. Ueli Maurer, Professor für Theoretische Informatik und führender Kryptologe, referierte über die Frage, ob und wie die digitale Welt real fassbar gemacht werden kann. Howard A. Schmidt, Chief Security Officer bei Microsoft, äusserte sich zu den wichtigsten Herausforderungen im Bereich Sicherheitsstrategien für die Zukunft.
- «Konfliktfelder zwischen E-Future und Privatspäre»: David Petraitis, Direktor Global Risk Management Solutions bei PricewaterhouseCoopers AG, veranschaulichte anhand einer von seiner Gesellschaft durchgeführten Untersuchung die Sicherheitsprobleme, die für einen erfolgreichen E-Commerce der Zukunft gelöst werden müssen. Xavier Comtesse, Stellvertretender Direktor der Stiftung «Avenir Suisse» und Leiter der «Antenne Romande», plädierte für den totalen Schutz der Privatsphäre im virtuellen Raum. Dr. David Brin, Philosoph und Autor des Buches «The Transparent Society – Will Technology Force Us to Choose Between Privacy and Freedom?», beleuchtete aus philosophischer Sicht das Spannungsfeld zwischen dem technologisch Machbaren und dem Bedürfnis nach Schutz der Privatsphäre.
- «Überwachung»: Ein MTW-Fernsehreport leitete das brisante Thema ein. Anhand anschaulicher Beispiele zeigte anschliessend Professor David Hogg, Pro-Vice-Chancellor and Professor of Artificial Intelligence, die Möglichkeiten automatischer visueller Überwachung auf. Dann sprach Dr. Bruno Baeriswyl über das Grundrecht auf Privacy und die oft mangelhaften bzw. mangelnden gesetzlichen Grundlagen für die Überwachung von unbestimmt vielen Personen.
  Eine abschliessende Podiumsdiskussion unter der Leitung von Helen Issler, Redaktionsleiterin MTW bei SF DRS, leuchtete die unterschiedlichen Standpunkte zum Thema Überwachung aus: Während sich Dr. David Brin provokativ für uneingeschränkte Überwachung (alle gegen alle) aussprach, wollten die übrigen Teilnehmeden nicht an die selbstzerstörerische Kraft ungebremster Überwachung glauben und sprachen sich – aus unterschiedlichen Perspektiven – klar gegen die Tendenz zu vermehrter Überwachung aus.

Die Tracks wurden jeweils von einem Moderator und zwei bis drei Fachleuten geführt. Zur Auswahl standen die folgenden Diskussionsthemen:

- «Risk Management Through Content Analysis – Opportunities and Limits»: Vertrauenswürdige Datenverwaltung als Schlüsselthema für Unternehmen, Verwaltungen und Private.
- «Datenschutz als Wettbewerbsvorteil»: Grundrechtsschutz ist unabdingbare Voraussetzung für das Vertrauen der Konsumentinnen und Konsumenten in den E-Commerce.
- «Online-Beratung im Internet»: Im Bereich E-Health werden

besonders sensible Personendaten bearbeitet – der Schutz der Betroffenen lässt sich nur mit Anonymisierung und Authentifizierung gewährleisten.
- «E-Government und Sicherheit»: Public-Key-Infrastruktur (PKI) als Voraussetzung für den Aufbau eines sicheren E-Government.
- «Consumer Privacy and Technology»: Das virtuelle Warenhaus funktioniert nur, wenn den Kunden und Kundinnen IT-Sicherheit garantiert wird.
- «Sicherheit beim Webauftritt»: Praktische Anleitungen für grosse Sicherheit bei mittleren und kleinen Unternehmen oder Gemeinden.
- «PKI Architecture: Trend – Problems – Solutions»: PKI heute und in der Zukunft – welches sind die Erfolgsfaktoren?
- «Secure E-Business – A Well Secured Way from Vision to Reality»: So lässt sich ein E-Business-Projekt erfolgreich durchführen – eine Anleitung.

● Das Symposium on Privacy and Security hat sich zu einer wichtigen – auch international beachteten – Veranstaltung entwickelt. Als Plattform für Teilnehmende aus Wissenschaft, Wirtschaft und Verwaltung trägt es dazu bei, dass die Themen «Privacy» und «Security» als Schlüsselthemen der Informationsgesellschaft wahrgenommen und diskutiert werden.

3. Perspektive Datenschutz

Grundlagenwerk für einen zeitgemässen Datenschutz

Auf Grund der zahlreichen Kontakte, die wir im Rahmen des Symposiums für Datenschutz und Informationssicherheit und bei verschiedenen anderen Gelegenheiten knüpfen konnten, gelang es uns, eine Anzahl namhafter Autoren zu gewinnen, die bereit waren, einen Artikel zur Perspektive des Datenschutzes zu verfassen. In diesem Sammelband (Perspektive Datenschutz. Praxis und Entwicklungen in Recht und Technik, Hrsg. Bruno Baeriswyl / Beat Rudin, Zürich 2002, ISBN 3 7255 4329 1) beschäftigen sich die Autoren mit der Entwicklung des Daten(schutz)-rechts und der Technologie und diskutieren Ansätze für einen effektiven Datenschutz. Sie zeigen damit Wege für eine wirksame Umsetzung des Datenschutzes in der Praxis auf und weisen zugleich auf die notwendige konzeptionelle Weiterentwicklung der Gesetzgebung hin. Themenschwerpunkte sind die Grundlagen der Datenschutzkonzepte, Datenschutz in der Informationsgesellschaft und als Teil einer umfassenden Informationsordnung, Datenschutz durch Technik sowie Strukturen und Instrumente der Umsetzung des Datenschutzes. Erste Reaktionen nach Erscheinen dieser Publikation zeigen, dass die vielen Hinweise für einen praxisbezogenen und wirksamen Datenschutz, der die Grundrechte der betroffenen Personen auch angesichts der rasanten technologischen Entwicklung respektiert, auf ein breites Echo stossen.

● Die Publikation «Perspektive Datenschutz» beinhaltet viele Hinweise für einen praxisbezogenen und effizienten Datenschutz.

4. Vertiefte Hintergrundinformationen

Breites Themenspektrum von «digma»

«digma» – die Zeitschrift für Datenrecht und Informationssicherheit – hat die hohen Erwartungen erfüllt und ist zu einem wichtigen Teil des Informationskonzepts des Datenschutzbeauftragten geworden. In «digma» ist es möglich, aktuelle Themen umfassend darzustellen und die Aspekte von Recht und Technik abzudecken. Die aktive Mitarbeit an der Zeitschrift erlaubt es, wichtige Fragestellungen aufzugreifen und notwendige Hilfeleistungen für die Umsetzung des Datenschutzes und der Informationssicherheit in der Praxis zu erbringen. Der erste Jahrgang von «digma» beschäftigte sich schwerpunktmässig mit den Themen «Internet am Arbeitsplatz» (2001.1), «Public Key Infrastructure» (2001.2), «Kundentransparenz» (2001.3) und «IT-Outsourcing» (2001.4). Ergänzt werden die Schwerpunktthemen durch Berichte aus der Praxis und Kommentierung der einschlägigen Rechtsprechung im Bereich des Datenschutzes und der Informationssicherheit.

- Im Informationskonzept des Datenschutzbeauftragten bildet «digma» die Plattform für die umfassende Darstellung von Themen im Bereich des Datenschutzes und der Informationssicherheit.

5. Zusammenarbeit der Datenschutzbeauftragten

DSB+CPD.CH und kommunale Datenschutzbeauftragte

Auf kantonaler Ebene finden vierteljährlich Sitzungen der kommunalen Datenschutzbeauftragten statt, an denen auch der kantonale Datenschutzbeauftragte teilnimmt. Folgende Themen waren im Berichtsjahr aktuell: Datenbanken der Polizeiorgane, Datenschutz im Bereich der Landeskirchen, optische Überwachung, geografische Informationssysteme, das geplante Informations- und Datenschutzgesetz, die Sozialhilfestatistik des Bundes sowie Einzelfragen aus dem Bereich der Einwohnerkontrollen.

Auf nationaler Ebene nahm die Vereinigung der Schweizerischen Datenschutzbeauftragten (DSB+CPD.CH) in verschiedenen Vernehmlassungsverfahren Stellung. Zudem befassten sich die Mitglieder der Vereinigung in mehreren Arbeitsgruppen mit folgenden Hauptthemen: Einsatz biometrischer Verfahren, Aufbau von PKI (Arbeitsgruppe Informatiktechnologien), Merkblatt Austritts- und Operationsberichte (Arbeitsgruppe Gesundheit), Musterstatistikgesetz für Kantone, Sozialhilfestatistik des Bundes (Arbeitsgruppe Register), Konsequenzen von «Schengen» für Kantone, Rechtsgrundlagen für Videoaufnahmen auf Nationalstrassen (Arbeitsgruppe Innere Sicherheit) sowie Broschüre für PC-Benutzende zur Informatiksicherheit (Arbeitsgruppe Broschüre).

Im November fand die 8. Schweizerische Konferenz der Datenschutzbeauftragten in Bern statt. Thema der Konferenz war die Rolle der Datenschutzbeauftragten bei Informatikprojekten. In mehreren Vorträgen beschrieben ausgewiesene Fachleute die derzeit aktuellen Problemstellungen bei Informatikprojekten und zeigten mögliche Lösungsansätze auf. Aus aktuellem Anlass wurde zudem das Thema Terrorismusbekämpfung und Datenschutz behandelt.

- Die Zusammenarbeit mit anderen Datenschutzbeauftragten ermöglicht, Themen von allgemeiner und grundlegender Bedeutung effizient und wirkungsvoll zu bearbeiten.

6. Seminare, Referate und Tagungen

Bedürfnis nach spezifischer Aus- und Weiterbildung

Die bewährten, im Jahre 1999 neu konzipierten Seminare im Rahmen der kantonalen Aus- und Weiterbildung führten wir auch im Berichtsjahr weiter. Daneben hielten wir auf Anfrage verschiedene Referate und Seminare.
Der modulare Aufbau der Seminare und Referate ermöglichte es, diese nach Bedarf zielgruppen- und bedürfnisgerecht auszugestalten. So führten wir Kurse durch für angehende Sekundarlehrer, für den Weiterbildungslehrgang «Multimedia-Koordinatoren» an der Allgemeinen Berufsschule, für den Verein Zürcher Gemeindeschreiber und Verwaltungsfachleute (VZGV) und für die Aus- und Weiterbildung von Gefängnis-Mitarbeitenden.

Besonders zu erwähnen sind die Tagungen des Schweizerischen Gemeindeverbandes, an welchen die Verantwortlichen der Gemeinden in das Projekt «Guichet virtuel» eingeführt wurden. Wir konnten an diesen Tagungen Fragen zu Datenschutz und Informationssicherheit beim «Guichet virtuel» bzw. beim E-Government im Allgemeinen aufzeigen und die Vertreter und Vertreterinnen der Gemeinden für diese Fragen sensibilisieren.
Der Datenschutzbeauftragte referierte überdies auf Einladung des Verbandes des Staats- und Gemeindepersonals im Rahmen der jährlichen «Kandersteger Tage», die als Schwerpunkt «Datenschutz und Informationssicherheit» zum Thema hatten.
Nach wie vor besteht ein grosses Bedürfnis nach spezifischer Aus- und Weiterbildung im Bereich Datenschutz und Informationssicherheit. In Zukunft wollen wir dieses Bedürfnis mit neuen Angeboten bezüglich Zielgruppen, Inhalten und Lernformen befriedigen.

- Die Seminare, Referate und Tagungen sprechen ein breites Publikum an und ermöglichen, die Verantwortlichen für die Belange von Datenschutz und Informationssicherheit zu sensibilisieren.

Datenschutzbeauftragter
Kanton Zürich
Postfach
8090 Zürich
Tel.: 043 259 39 99
Fax: 043 259 51 38
E-Mail: datenschutz@dsb.zh.ch
Web: www.datenschutz.ch

Datenschutzbeauftragter:
Dr. iur. Bruno Baeriswyl

Stellvertreter:
lic. iur. Marco Fey

Juristisches Sekretariat:
lic. iur. Barbara Egli
lic. iur. Joëlle Kupfer-Matey (bis 30.6.2002)
lic. iur. Barbara Mathis

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

Projektleitung SOPRANO:
Hans-Peter Leibacher (ab 1.4.2002)

Sekretariat:
Tanja Blass

Tätigkeitsbericht Nr. 7 (2001)
ISSN 1422-5816

Konzeption und Produktion:
Fabian Elsener für Frontpage AG, Zürich

Druck:
KDMZ
Gedruckt auf Recyclingpapier

Bezug:
Datenschutzbeauftragter
des Kantons Zürich
Postfach
8090 Zürich
Tel.: 043 259 39 99
Fax: 043 259 51 38
E-Mail: datenschutz@dsb.zh.ch
Web: www.datenschutz.ch