Nr. 3

Tätigkeits-Bericht

Datenschutzbeauftragter des Kantons Zürich

1997

Tätigkeitsbericht

Nr. 3
1997

Der Datenschutzbeauftragte erstattet dem Regierungsrat jährlich oder nach Bedarf einen Bericht über seine Tätigkeit (§ 23 Datenschutzgesetz). Der vorliegende Tätigkeitsbericht Nr. 3 deckt den Zeitraum vom 1. Januar 1997 bis 31. Dezember 1997 ab. Ein weiterer Bericht gemäss § 23 Datenschutzgesetz zur «Zulässigkeit der Bearbeitung einer bestimmten Datenkategorie (‹Vereinszugehörigkeit›) im Rahmen des Arbeitsverhältnisses» ist am 5. August 1997 erschienen.

Zürich, März 1998

Der Datenschutzbeauftragte
des Kantons Zürich
Dr. Bruno Baeriswyl

Inhaltsverzeichnis

Zunehmende Bedeutung der Datensicherheit

Die wachsenden Investitionen in neue Informationstechnologien sind eine Herausforderung für den Datenschutz und die Datensicherheit. Auf der Ebene der Informationssicherheit konnten neue Leitlinien geschaffen werden.

Der enge Zusammenhang zwischen Datenschutz und Technik zeigte sich auch im vergangenen Jahr. In allen Bereichen der Verwaltung hat der Einsatz von Informatikmitteln zugenommen. Damit sind die Fragen des Datenschutzes und der Datensicherheit aktueller denn je geworden.
Der Einsatz neuer Technologien bringt neue Datenschutz- und Datensicherheitsprobleme. Von den verantwortlichen Organen wird oft vernachlässigt, dass neue Technologien auch ihre Kehrseiten haben:

- Datensicherheitsprobleme haben mit der Vernetzung der Systeme und dem Zugang zu öffentlichen Netzen (Internet) stark zugenommen.
- Datenschutzfragen werden wichtiger, da immer mehr Daten über eine einzelne Person bearbeitet werden und diese Daten sich aus verschiedenen Systemen übernehmen und kombinieren lassen.
- Generell ist eine Zunahme des Umfangs der Datenbearbeitungen und der Menge der Daten festzustellen.

Die Verknüpfung von Datenschutz und Technik zeigt, dass das Datenschutzgesetz (DSG) als eigentliches Technikfolgenrecht zu bezeichnen ist. Es bietet die Rahmenbedingungen zum Schutz der von den neuen Technologien betroffenen Menschen. Damit wird es zum unabdingbaren Wegbegleiter in die Informationsgesellschaft.

Den kantonalen und kommunalen Verwaltungen kommt eine spezielle Rolle zu. Sie setzen nicht nur zunehmend moderne Informationstechnologie ein, sondern sie verfügen auch über eine wachsende Zahl von unterschiedlichsten Daten über die Bürgerinnen und Bürger. Die Datenschutzgesetzgebung bedeutet deshalb sowohl eine Herausforderung für eine verantwortungsbewusste, bürgerorientierte Verwaltungsführung als auch für eine datenschutzkonforme Technikgestaltung.
Dieser Ausgangslage konnte im vergangenen Jahr auf verschiedenen Ebenen begegnet werden.

Regierungsrat setzt Zeichen für Datenschutz

Der Regierungsrat hat am 17. Dezember 1997 die Informatiksicherheitsverordnung (ISV) verabschiedet. Diese Verordnung ist im Auftrag der Arbeitsgruppe Planung und Steuerung der Informatik und Kommunikation (AGIK) in enger Zusammenarbeit zwischen der Abteilung für Informatikplanung und dem Datenschutzbeauftragten sowie weiteren interessierten Stellen der Verwaltung entstanden. Sie verpflichtet die kantonalen Verwaltungsstellen und die Gemeinden, die mit diesen Daten austauschen, in bezug auf ihre Informatiksysteme und -anwendungen eine Risikoanalyse

durchzuführen. Die Systeme und Anwendungen sind in drei Sicherheitsstufen zu klassifizieren. Für jede dieser Sicherheitsstufen bestehen Mindestanforderungen für die zu treffenden Sicherheitsmassnahmen.
Die Informatiksicherheitsverordnung konkretisiert die Anliegen des Datenschutzgesetzes in bezug auf die Datensicherheit. Mit der konsequenten Umsetzung der Verordnung sollte ein angemessener, dem Stand der Technik entsprechender Sicherheitsstandard der Informatiksysteme und -anwendungen der Verwaltung erreicht werden können (siehe S. 36).

Eigendynamik der Technik

Die informationstechnische Entwicklung gab auch Anlass zu grundlegenden rechtlichen Fragestellungen. Die Technik hat in verschiedenen Bereichen eine Eigendynamik entwickelt, die datenschutzrechtliche Anliegen in den Hintergrund treten lässt. Der elektronische Datenaustausch im Gesundheitswesen ist hierfür beispielhaft. Für die Erstellung der Gesundheitsstatistiken auf nationaler Ebene sowie für statistische Erhebungen der Gesundheitsdirektion werden Diagnosen nach dem ICD-10-Code erfasst. Diese Codes beinhalten sehr detaillierte Diagnosen, wie sie für Forschung und Statistik notwendig sind. Eine Weitergabe solcher Diagnosen an andere Stellen, insbesondere Versicherer, würde aber eine Verletzung des Patientengeheimnisses bedeuten, da hierfür keine Rechtsgrundlagen bestehen. Die Versicherer sind aufgrund der Bestimmungen des Krankenversicherungsgesetzes (KVG) nur berechtigt, diejenigen Angaben von den Leistungserbringern zu erhalten, die ihnen ermöglichen, die Berechnung der Vergütung und die Wirtschaftlichkeit der Leistung zu überprüfen. Dies beinhaltet im Regelfall keine detaillierten Diagnosen. Dennoch versuchen Krankenversicherer mit den Leistungserbringern Verträge abzuschliessen, die die Krankenhäuser zum elektronischen Datenaustausch und zur Codierung der Diagnosen nach ICD-10 verpflichten. Damit würden regelmässig und automatisch hoch detaillierte Diagnosen den Krankenversicherern übermittelt, obwohl sie für die Überprüfung der Leistung und der Wirtschaftlichkeit der Behandlung einerseits zu ausführlich und andererseits oft ungeeignet sind.
Seit Jahren genügten den Versicherern rund sechzig verschiedene Positionen bei der Diagnoseangabe. Mit dem ICD-10-Diagnosecode wären dies über 10 000 verschiedene Krankheitspositionen. Hier zeigt sich deutlich, dass mit einem früheren konventionellen System Daten in einem solchen Detaillierungsgrad nur schwierig zu handhaben waren. Mit den neuen technischen Möglichkeiten sind so genaue Angaben über einzelne Personen ohne weiteres möglich geworden. Die Gesundheitsdirektion hat auf diese datenschutzrechtliche Herausforderung angemessen reagiert und mittels Weisung den öffentlich-rechtlichen Krankenhäusern vorläufig die Bekanntgabe von ICD-10-Diagnosecodes an die Versicherer untersagt (siehe S. 20).

Kantonale Verwaltung

Eine starke Zunahme der Anfragen von Verwaltungsstellen und betroffenen Personen beim Datenschutzbeauftragten zeigt eine wachsende Sensibilisierung für die Anliegen des Datenschutzes. Viele kantonale Verwaltungsstellen gelangen von sich aus an den Datenschutzbeauftragten, um einzelne Rechtsfragen oder EDV-Projekte datenschutzrechtlich abklären zu lassen. Sie sind bemüht, der wachsenden Bedeutung von Datenschutz und Datensicherheit nachzukommen. Zahlreiche, im vorliegenden Tätigkeitsbericht erwähnte Sachverhalte und Rechtsprobleme illustrieren den Umfang und die Tragweite des Datenschutzes in der Verwaltung. Dabei sind oftmals die verschiedenen Interessen zwischen der Öffentlichkeit von Personendaten oder sogar deren Kommerzialisierung (siehe S. 12) und der Persönlichkeitsrechte der betroffenen Personen abzuwägen. Erschwerend kommt für die Verwaltungsstellen hinzu, dass die Rechtsgrundlagen oft nicht genügend klar sind. Auf der formellgesetzlichen Ebene sind Rechtsanpassungen nur langsam zu verwirklichen, doch gibt die gerichtliche Praxis schon heute genügend Anhaltspunkte in bezug auf die Zulässigkeit von Datenbearbeitungen (siehe S. 13).

Privates muss privat bleiben

Die zunehmende Verbreitung der Informationstechnologie in der Verwaltung (aber auch in der Wirtschaft) stellt das Grundrecht auf Privatsphäre vor neue Herausforderungen. Die technischen Möglichkeiten führen sowohl zu einer Zunahme der Daten, die über eine einzelne Person bearbeitet werden, als auch zu neuen Möglichkeiten der Kombination dieser Daten.
Aufgrund ihrer Aufgaben und Funktionen bearbeitet die öffentliche Verwaltung Daten aus den unterschiedlichsten Lebensbereichen einer Person: allgemeine Angaben bei der Einwohnerkontrolle, Daten über die finanziellen Verhältnisse durch das Steueramt, sensible Gesundheitsdaten in den Krankenhäusern, in verschiedenen Bereichen der Verwaltung bei Anträgen und Gesuchen. Die Bürgerinnen und Bürger sind in den meisten Fällen gesetzlich verpflichtet, die Daten bekanntzugeben. Daten der Verwaltung sind deshalb einerseits aktuell, und andererseits werden sie oft sehr lange aufbewahrt. Sie lassen sich grundsätzlich beliebig mit anderen Daten kombinieren, und wenn Online-Zugriffe zwischen den Verwaltungsstellen bestehen, sind sie sofort verfügbar.
Auch wenn diese Möglichkeiten heute noch nicht alle genutzt werden, die technische Infrastruktur hierzu steht zur Verfügung. Die Versuchung und der Druck der verschiedenen Verwaltungsstellen (oder auch von privaten Organisationen), auf die vorhandenen Daten jederzeit – auch zu anderen Zwecken – zugreifen zu können, sind gross.
Wer aber garantiert, dass bei dieser Entwicklung Privates privat bleibt und die technische Entwicklung dort haltmacht, wo die Privatsphäre beginnt? Die datenschutzrechtlichen Bestimmungen müssen die Leitplanken bei dieser Entwicklung sein. Sie genügen aber nicht, wenn nicht in der Praxis deren Einhaltung effizient überwacht und kontrolliert werden kann. Diese Aufgabe weist das Datenschutzgesetz dem Datenschutzbeauftragten zu. Die Schere zwischen seinem gesetzlichen Auftrag und seinen tatsächlichen Möglichkeiten der Aufsicht und Kontrolle der Datenbearbeitungen – insbesondere der neuen Informationssysteme – wird aufgrund des Fehlens entsprechender Ressourcen immer grösser.
Die Informationstechnologie dient der Erfüllung der staatlichen Aufgaben. Ihr Einsatz muss aber datenschutzgerecht erfolgen. Privates wird nur privat bleiben, wenn diese Systeme auch datenschutzkonform eingesetzt und betrieben werden. Heute begegnen die Bürgerinnen und Bürger diesen neuen Datenbearbeitungen mit Skepsis. Die Systeme laufen überwiegend ohne eine unabhängige Kontrolle. Letztendlich kann nur die regelmässige Kontrolle dieser neuen Systeme und technischen Möglichkeiten Vertrauen in die staatlichen Datenbearbeitungen bringen.

Unverhältnismässige Datenbearbeitungen

In zahlreichen Beratungs- und Vermittlungsfällen zeigte sich, dass insbesondere bei Datenbekanntgaben und beim Datenaustausch zwischen den Verwaltungsstellen die Rechte der betroffenen Personen nur ungenügend gewahrt werden. Das Prinzip der Verhältnismässigkeit, das jede Datenbearbeitung auf die notwendigen und geeigneten Daten beschränkt, wird zu oft nicht beachtet. Bei der Überweisung von Akten werden Informationen an die anderen Stellen weitergegeben, die für diese nicht notwendig sind und für die betroffenen Personen einen unnötigen Eingriff in ihre Privatsphäre bedeuten.
Auffallend war, dass auch nach der Versicherung der Amtsstelle, sie würde ihre Praxis den datenschutzrechtlichen Erfordernissen anpassen, weiterhin Beschwerden beim Datenschutzbeauftragten eintrafen (siehe S. 10).
Auch Mitteilungen über strafbare Handlungen an die Aufsichtsbehörden von im Staatsdienst tätigen Personen sowie Studierenden haben sich nach den datenschutzrechtlichen Grundsätzen zu richten.
In einem Rechtsgutachten nahmen wir ausführlich zu dieser Problematik Stellung (siehe S. 11). Auch hier ist zu bemängeln, dass einzelne Amtsstellen – obwohl sie bereits vor diesem Gutachten auf ihre rechtswidrige Praxis aufmerksam gemacht wurden – ihre Praxis nicht anpassen und es weiterhin der betroffenen Person überlassen ist, sich mittels Klagen dagegen zu wehren.

Datenspuren in Kommunikationssystemen

In zwei Empfehlungen beschäftigten wir uns mit den sogenannten «Datenspuren», die in Telekommunikationseinrichtungen anfallen. In den modernen ISDN-Telefonanlagen werden automatisch Daten über die Telefonverbindung festgehalten. Ebenso halten EDV-Systeme wie Internetzugangsserver fest, wer wann welche Dienste und wie lange in Anspruch genommen hat.
Ohne weiteres lassen sich diese

Daten zu Profilen über das Verhalten der Benutzerinnen und Benutzer auswerten. In unseren Berichten hielten wir fest, dass solche Daten nicht zur Überwachung und Kontrolle der Mitarbeitenden ausgewertet werden dürfen (siehe S. 32).

Schwerpunkte bei den Gemeinden

Die Erstellung der Register der Datensammlungen, welche bis am 30. Juni 1997 abzuschliessen war, veranlasste viele Gemeindeverwaltungen, ihre Datenbearbeitungen zu überprüfen. Die Register zeigen auf, in welch unterschiedlichen Bereichen die Gemeinden Daten über ihre Einwohnerinnen und Einwohner bearbeiten. Verschiedene grundsätzliche Fragen konnten beantwortet werden, und in einigen wichtigen Bereichen – wie beispielsweise der Datenbekanntgabe durch die Einwohnerkontrollen – ist die Praxis in zahlreichen Einzelfällen den datenschutzrechtlichen Anforderungen angepasst worden.
Kommunale Verwaltungsstellen bemühen sich, den Anliegen des Datenschutzes nachzukommen, und einzelne Stellen haben Merkblätter und spezifische Anleitungen für den täglichen Umgang mit Personendaten verfasst.
Der Datenschutz stösst aber leider nicht bei allen kommunalen Verwaltungen auf die notwendige Beachtung, die die Bürgerinnen und Bürger aufgrund des klaren Mandats, das sie den Gemeinden durch das Datenschutzgesetz gegeben haben, erwarten dürfen.

Auskunftsrecht ist ein Kernelement

Schwierigkeiten mit dem Auskunftsrecht waren in zahlreichen Fällen Grund, dass der Datenschutzbeauftragte vermittelnd eingreifen musste (siehe S. 22). Im weiteren gaben Datenbekanntgaben immer wieder zu Beanstandungen Anlass (siehe S. 24). Der Datenaustausch zwischen den verschiedenen Amtsstellen war ein weiterer Punkt, wo wir mit klärenden Stellungnahmen beratend tätig waren (siehe S. 24). Insgesamt ist festzustellen, dass sich einzelne Gemeinden sehr bemühen, den Datenschutz im Rahmen einer bürgerorientierten Verwaltungsführung angemessen umzusetzen. Bei anderen Gemeinden und Verwaltungsstellen ist aber noch ein Handlungsbedarf festzustellen.

Anliegen der Bürgerinnen und Bürger

Die Anfragen von Bürgerinnen und Bürgern haben im vergangenen Jahr erneut stark zugenommen.
Es fällt auf, dass die betroffenen Personen sehr sensibel auf die zunehmenden Datenbearbeitungen in allen Lebensbereichen reagieren. Dabei kommt der staatlichen Datenbearbeitung eine besondere Beachtung zu. Viele Personen konnten wir beraten, und in zahlreichen Einzelfällen waren wir vermittelnd zwischen den betroffenen Personen und den jeweiligen Verwaltungsstellen tätig. Das Auskunftsrecht war neben Datenbekanntgaben ein Schwerpunkt der Anliegen, die von den betroffenen Personen direkt an den Datenschutzbeauftragten herangetragen wurden.

Zunahme der Anfragen

Der Datenschutzbeauftragte berät, vermittelt, informiert, und er beaufsichtigt und kontrolliert auch die Datenbearbeitungen der Verwaltung.
1997 hat eine weitere Zunahme der Anfragen sowohl von kantonalen und kommunalen Verwaltungsstellen als auch von betroffenen Personen gebracht. Die Anfragen werden so rasch wie möglich beantwortet. Da die finanziellen und personellen Mittel des Datenschutzbeauftragten unzureichend sind, müssen oft Antwortzeiten von mehreren Monaten in Kauf genommen werden. Das Fehlen datenschutzrechtlicher Abklärungen schafft dabei ein zunehmendes Konfliktpotential mit rechtlichen und finanziellen Risiken für die Verwaltung.
Im Rahmen der Informationsaufgaben versuchen wir deshalb, aktuelle Fragen des Datenschutzes soweit wie möglich zu publizieren und den interessierten Stellen zugänglich zu machen. Dieses Vorgehen soll es den Verwaltungsstellen ermöglichen, vermehrt ihre Eigenverantwortung für den Datenschutz wahrzunehmen.

Verhältnismässigkeit der Datenbearbeitungen

Datenbearbeitungen müssen verhältnismässig sein. Auch bei Datenbekanntgaben dürfen nur die Daten weitergegeben werden, die geeignet und erforderlich sind.

1. IV-Akten an die medizinische Begutachtungsstelle

Unverhältnismässige Datenbekanntgaben

Mehrere Anfragen betrafen die Weitergabe von Daten durch die IV-Stelle der Sozialversicherungsanstalt bei medizinischen Abklärungen. Im Zusammenhang mit der Prüfung von Gesuchen erteilt die IV-Stelle regelmässig Gutachteraufträge für solche Abklärungen. Dabei wurden mehrfach die gesamten Originalakten an die Gutachterstelle weitergeleitet.
Diese Akten umfassen nebst dem eigentlichen Auftrag auch frühere Arztberichte zuhanden der IV-Stelle, andere ärztliche Berichte, frühere Verfügungen der IV-Stelle und Korrespondenz, etwa über die Anfechtung einer Verfügung.
Weiter sind auch Auszüge aus dem individuellen AHV-Konto, ein IV-Fragebogen für Arbeitgeber mit Angaben zum Einkommen, das IV-Anmeldeformular sowie Steuererklärungen enthalten. Vom Umfang her und von der Art der Daten handelt es sich um besonders schützenswerte Daten und um Daten, welche die Erstellung eines Persönlichkeitsprofils erlauben.
Die Bekanntgabe dieser Daten ist auf diejenigen Angaben zu begrenzen, welche der Datenempfänger zur Erfüllung seiner Aufgabe tatsächlich benötigt (§ 4 Abs. 3 DSG). Bei medizinischen Gutachteraufträgen sind dies vor allem medizinische Daten, also frühere Arztberichte, allenfalls auch Arbeitgeberberichte. Die Notwendigkeit ist in jedem Einzelfall zu prüfen. In der Regel nicht erforderlich sind Angaben zur finanziellen oder verfahrensmässigen Situation der betroffenen Person wie Steuererklärungen, Auszüge aus dem AHV-Konto, Korrespondenz über die Anfechtung von Verfügungen usw.. Werden im Einzelfall solche Daten doch einmal benötigt, sind sie nur auf eine begründete Anfrage hin zuzustellen.
Die Weitergabe der Originalakten ist aus der Sicht der Datensicherheit bedenklich, weil ein Verlust zu erheblichen Nachteilen für die betroffene Person führen kann. Die Beweisbarkeit von Sachverhalten wird damit in Frage gestellt. Verhältnismässig ist die Zustellung von Kopien.
Die IV-Stelle erliess nach unserer ersten Intervention eine interne Weisung über Aktenherausgaben bei medizinischen Begutachtungen. Die Sachbearbeiterinnen und Sachbearbeiter wurden angewiesen, nur noch die erforderlichen Akten mitzuliefern. Bereits geregelt war, dass die Akten nur in Kopie weiterzugeben sind (Kreisschreiben über das Verfahren der Invalidenversicherung).
Trotz dieser Anweisungen kam es weiterhin zu unverhältnismässigen Bekanntgaben, welche uns von betroffenen Personen mitgeteilt wurden. Wir mussten die IV-Stelle deshalb erneut auffordern, für eine datenschutzkonforme Praxis zu sorgen.

2. Geheimhaltung der informierenden Personen?

Auskunftsrecht kontra Drittinteressen

Das Strassenverkehrsamt erhält regelmässig Meldungen von Privatpersonen, in denen auf die mangelnde Fahreignung eines Fahrzeuglenkers oder einer Fahrzeuglenkerin hingewiesen wird. Bei den meldenden Personen handelt es sich vielfach um Familienangehörige, die sich Sorgen um ein betagtes Familienmitglied machen, oder um Personen aus der Nachbarschaft, vereinzelt auch um andere Verkehrsteilnehmende, denen die Fahrweise negativ aufgefallen ist. Aufgrund der Meldungen werden die Betroffenen zu einer verkehrsmedizinischen Kontrolluntersuchung oder einer

Kontrollfahrt aufgeboten, wobei sich herausstellt, dass die Meldungen meist gerechtfertigt sind. Während die Betroffenen häufig Auskunft über die Identität der meldenden Person wünschen, möchten diese oft, dass die Meldung vertraulich behandelt wird.
Das Auskunftsrecht nach § 17 DSG berechtigt die betroffenen Personen, Auskunft über alle über sie in einer Datensammlung bearbeiteten Daten zu erhalten. Dies schliesst Korrespondenzen anderer Personen mit ein, sofern ein Bezug zur betroffenen Person besteht. Folglich gilt das Auskunftsrecht auch betreffend Meldungen von Informantinnen und Informanten.
Ein Anspruch auf Akteneinsicht besteht auch aufgrund der Art. 35 und 125 der Verordnung über die Zulassung von Personen und Fahrzeugen zum Strassenverkehr.
Das Recht auf Auskunft ist einzuschränken oder zu verweigern, wenn überwiegende schützenswerte Interessen Dritter es verlangen (§ 18 DSG). Für die Interessenabwägung im Zusammenhang mit Informantinnen und Informanten sind verschiedene Kriterien massgebend.

- Erfolgt die Information ausschliesslich aus uneigennützigen Motiven in echter Sorge um das Gemeinwohl oder das Wohl der betroffenen Person, so spricht dies stärker für eine Geheimhaltung, als wenn persönliche Beweggründe oder gemischte Motive vorliegen.
- Sind die Hinweise informantenneutral, d.h. könnten die Behörden unabhängig davon eigene Nachforschungen anstellen, rechtfertigt sich die Geheimhaltung eher.
- Verlangt eine Behörde Auskunft von Informantinnen und Informanten, ist deren Geheimhaltungsinteresse höher zu gewichten, als wenn diese sich unaufgefordert in ein Verfahren einmischen.
- Im Hinblick auf einen allfälligen Berichtigungsanspruch der betroffenen Person (§ 19 Abs. 2 DSG) besteht ein verstärktes Interesse an der Offenlegung, wenn der Wahrheitsgehalt der Information nur im Zusammenhang mit der meldenden Person überprüft werden kann.
- Je weiter der in Frage stehende Sachverhalt zeitlich zurückliegt, desto schwächer wird das Interesse an der Offenbarung.
- Bestehen ernsthafte Anhaltspunkte, dass die betroffene Person die Informantin oder den Informanten nach Preisgabe des Namens belästigen oder mit rechtswidrigen Mitteln gegen sie oder ihn vorgehen wird, spricht dies für eine Geheimhaltung. Die blosse Gefahr von Unannehmlichkeiten vermag den Quellenschutz allerdings nicht zu rechtfertigen.

Zurückhaltung ist bei der Zusicherung der vertraulichen Behandlung der Informationen geboten. Solche Zusicherungen sollten nur abgegeben werden, wenn unter Berücksichtigung aller Umstände eine Interessenabwägung bereits zugunsten der Geheimhaltung ausgefallen ist. Selbst in diesen Fällen kann in einem Rechtsmittelverfahren die obere Instanz zu einem anderen Ergebnis gelangen.
Wir empfahlen dem Strassenverkehrsamt, den betroffenen Personen grundsätzlich Auskunft bezüglich der Informantenmeldungen zu erteilen, im Einzelfall aber zu prüfen, ob der Auskunft überwiegende Geheimhaltungsinteressen der meldenden Personen entgegenstehen, und allenfalls die Auskunft einzuschränken.

3. Information der Aufsichtsbehörde über strafbare Handlungen

Der Grundsatz der Verhältnismässigkeit

Mit einer öffentlich-rechtlichen Anstellung sind besondere Rechte und Pflichten der im Staatsdienst tätigen Personen verbunden, ohne dass alle Einzelheiten ausdrücklich im einschlägigen Recht umschrieben sind. Aufgrund verschiedener Anfragen nahmen wir Stellung zur Frage, ob aus dem sogenannten Sonderstatusverhältnis eine Grundlage abgeleitet werden kann, um sämtliche strafbaren Handlungen an die Aufsichtsbehörde zu melden. Informationen über den Verdacht einer deliktischen Tätigkeit oder eine

diesbezügliche Verurteilung einer Person sind sensibel. Für deren Bearbeitung und Weitergabe bestehen gemäss § 5 DSG qualifizierte Anforderungen: Vorausgesetzt ist, dass eine klare gesetzliche Grundlage vorliegt, die Daten zur Aufgabenerfüllung unabdingbar sind oder die betroffene Person eingewilligt hat.
Eine einschlägige gesetzliche Grundlage in dem von § 5 lit. a DSG geforderten Präzisierungsgrad ist trotz diverser konkretisierender Regelungen der Amtspflicht und der Disziplinargewalt nicht vorhanden. Infolgedessen bestimmen sich die Anforderungen an eine Datenbekanntgabe der Ermittlungs- und Untersuchungsbehörden oder der Gerichte an die Aufsichtsbehörde aus der Natur des Sonderstatusverhältnisses unter Berücksichtigung des Prinzips der Verhältnismässigkeit im Einzelfall.
Eine Mitteilung ist zulässig, wenn ein konkretes Fehlverhalten einer Person für den Staat als Arbeitgeber unzumutbar ist. Entweder muss aufgrund der Schwere des deliktischen Verhaltens die weitere Beschäftigung der betroffenen Person in Frage gestellt sein, oder das öffentliche Ansehen des Staates und das Vertrauen der Öffentlichkeit in die Verwaltung muss dadurch effektiv geschmälert werden. Von Bedeutung ist dabei die tatsächlich bekleidete Stellung der delinquierenden Person. Ein Fehlverhalten einer Kaderperson schadet dem Ansehen des Staates weit mehr, als das bei einer in einer untergeordneten Funktion tätigen Person der Fall ist.
Gemäss § 4 Abs. 2 DSG, wonach nur richtige Daten bearbeitet und somit auch bekanntgegeben werden dürfen, sind Meldungen an die Aufsichtsbehörde grundsätzlich erst nach rechtskräftiger Erledigung des Strafverfahrens zulässig. Nur wenn wesentliche öffentliche Interessen betroffen sind, kann ausnahmsweise bereits bei der Eröffnung des Verfahrens oder bei noch gravierenderer Gefährdung staatlicher Interessen bereits beim ersten Deliktsverdacht eine Meldung erfolgen. In diesen Fällen muss in der Meldung klar zum Ausdruck gebracht werden, dass der vorgeworfene Sachverhalt noch nicht erstellt ist.
Verantwortlich für die Einhaltung der datenschutzrechtlichen Erfordernisse ist gemäss § 6 DSG stets das meldende Organ. Es kann seine Verantwortung nicht delegieren, indem es der Aufsichtsbehörde alle Vorfälle meldet, damit diese die relevanten Sachverhalte selber heraussuchen kann. Dies würde das Prinzip der Verhältnismässigkeit verletzen. Diese Vorgehensweise gilt grundsätzlich auch für das Lehrpersonal, da keine abweichenden Regelungen vorhanden sind.
Für eine Mitteilung von Delikten Studierender oder anderer in Ausbildung befindlicher Personen an ihre Aufsichtsbehörde bestehen weder ausreichende gesetzliche Grundlagen, noch wäre damit das Verhältnismässigkeitsprinzip gewahrt. Vielmehr fallen lediglich solche Handlungen unter die Disziplinargewalt der Aufsichtsbehörde, welche den Lehrbetrieb stören oder gar verunmöglichen und infolgedessen gar nicht von Dritten mitgeteilt zu werden brauchen.
Die Verwaltungskommission des Obergerichts hat ein Kreisschreiben betreffend die Mitteilung von Strafurteilen gegen Lehrer, Studenten und Mittelschüler, das unsere Erwägungen berücksichtigt, verfasst. Obwohl wir bereits im Tätigkeitsbericht Nr. 2 (1996), S. 12, auf einen gleichartigen Handlungsbedarf im Strafuntersuchungsbereich hingewiesen haben, sind die entsprechenden Weisungen der Staatsanwaltschaft noch nicht angepasst worden.

4. Kommerzialisierung von Personendaten

Die Verwendung von Handelsregisterdaten

Die Kommerzialisierung von Personendaten ist tendenziell in verschiedenen Verwaltungsbereichen zu beobachten. Im konkreten Fall hatten wir zu prüfen, wieweit das Handelsregisteramt Daten auch kommerziell zu anderen Zwecken weitergeben darf.
Der Umgang mit Daten des Handelsregisters wird abschliessend in der Bundesgesetzgebung geregelt (Obligationenrecht; Handelsregisterverordnung). Da es sich um ein öffentliches Register des Privatrechtsverkehrs handelt, ist das Datenschutzgesetz auf das eigentliche Register nicht anwendbar (Art. 2 Abs. 2 lit. d

eidgenössisches Datenschutzgesetz). Insoweit das Handelsregisteramt als kantonales Organ über diesen ursprünglichen Zweck hinaus Daten aus dem Register bearbeiten will, fällt es unter das kantonale Datenschutzgesetz.
Es stellte sich die Frage, ob der kantonale Gesetzgeber eine Rechtsgrundlage schaffen kann, die dem Handelsregisteramt über die bundesrechtlichen Bestimmungen hinaus das Bearbeiten von Registerdaten ermöglicht. Im konkreten Fall war zu prüfen, ob dem Handelsregisteramt die Möglichkeit offensteht, die Handelsregisterdaten auch kommerziell weiterzuvertreiben. Dabei wurde festgestellt, dass keine Rechtsgrundlage besteht, die eine Kommerzialisierung der Daten im vorgesehenen Sinne ermöglicht hätte. Insbesondere war aber festzuhalten, dass auch bei einer Datenbekanntgabe aus öffentlichen Registern das Zweckbindungsgebot zu beachten ist. Daten aus dem Handelsregister dürfen nicht zu Zwecken, die unvereinbar sind mit denjenigen, für die sie erhoben wurden, an Dritte weitergegeben werden. Das Handelsregister dient primär der Rechtssicherheit im Geschäftsverkehr, weshalb eine generelle Verwendung dieser Daten zum Abgleich mit anderen Datenbanken zu Marketingzwecken unvereinbar ist. Eine Kommerzialisierung von Personendaten verlangt deshalb eine klare gesetzliche Grundlage, die im öffentlichen Interesse ist und die Grundrechte der betroffenen Personen angemessen berücksichtigt. Das geprüfte Projekt wird vorläufig nicht mehr weiterverfolgt.

---

5. Daten über VPM-Mitgliedschaft
Bericht an den Regierungsrat

Mit Entscheid vom 28. November 1996 (BGE 122 I 360) hat das Bundesgericht die Erziehungsdirektion angewiesen, «die Datenblätter betreffend die VPM-Mitgliedschaft sowie die darauf bezugnehmende Korrespondenz aus den ordentlichen Personaldossiers der Beschwerdeführer zu entfernen».
Dieser Entscheid hat einerseits zu einer Überprüfung der betroffenen Personaldossiers und andererseits zu einer Beurteilung der Rechtslage in bezug auf die Bearbeitung von Daten über die Vereinszugehörigkeit im Rahmen des Arbeitsverhältnisses geführt.
Der Bundesgerichtsentscheid wurde durch die Erziehungsdirektion unter Beizug des Datenschutzbeauftragten vollzogen.
Die entsprechenden Daten wurden vernichtet respektive teilweise unter Auflagen dem Staatsarchiv übergeben. Über das Vorgehen und den Abschluss der Datenvernichtung ist ein entsprechendes Protokoll erstellt worden.
Wir haben sodann in einem Bericht vom 5. August 1997 an den Regierungsrat zur Zulässigkeit der Bearbeitung einer bestimmten Datenkategorie («Vereinszugehörigkeit») im Rahmen des Arbeitsverhältnisses Stellung bezogen. Die Frage nach der Vereinszugehörigkeit eines Stellenbewerbers oder einer Stellenbewerberin sowie das Führen dieser Angabe im Personaldossier berühren sowohl Aspekte des verfassungsmässigen Rechts der persönlichen Freiheit als auch das Grundrecht der Vereinsfreiheit.
Das Datenschutzgesetz entspricht einem verfassungsrechtlichen Anliegen und beinhaltet eine Konkretisierung der verfassungsrechtlichen Anforderungen in diesem Bereich.
Die Tatsache der Mitgliedschaft in einem Verein mit weltanschaulichen oder politischen Ausrichtungen gilt als ein besonders schützenswertes Personendatum. Solche Daten dürfen bearbeitet werden, wenn dies aus einer gesetzlichen Grundlage klar hervorgeht (Prinzip der Rechtmässigkeit) und wenn die Daten geeignet und erforderlich sind (Prinzip der Verhältnismässigkeit). Daten, die im Rahmen des Personalwesens erfasst werden, haben sich auf die Eignung einer Person zu beziehen oder müssen für die Durchführung des Arbeitsverhältnisses notwendig sein.
Die Rechtsgrundlage für das Bearbeiten von Personendaten in diesem Zusammenhang ergibt sich aus §§ 6 ff. und 53 ff. des Gesetzes

über die Organisation und die Geschäftsordnung des Regierungsrates und seiner Direktionen (OGRR). Die weiteren personalrechtlichen Erlasse konkretisieren diese Bestimmungen; sie äussern sich indessen nur teilweise über die Bearbeitung einzelner Datenkategorien.
In bezug auf die Vereinszugehörigkeit ist das Prinzip der Verhältnismässigkeit anzuwenden. Das Datum der «Vereinszugehörigkeit» ist dann geeignet und erforderlich, wenn es Angaben über die berufliche Eignung enthält oder für die Durchführung des Arbeitsverhältnisses notwendig ist.
Im allgemeinen ist die Angabe einer Vereinszugehörigkeit hierfür nicht geeignet, weshalb im Bewerbungsverfahren nicht nach einer solchen gefragt und ein entsprechender Eintrag im Personaldossier nicht geführt werden darf.
Nur bei einem Tendenzbetrieb, der eine bestimmte weltanschauliche oder politische Richtung verkörpert, oder in Funktionen, die von einem (höheren) Beamten oder Angestellten eine besondere Treuepflicht verlangen, kann im Einzelfall – und sofern hierfür geeignet – die Vereinszugehörigkeit thematisiert werden.
Für Lehrpersonen ist die Rechtslage grundsätzlich nicht anders. Im Bewerbungsverfahren ist die Eignung einer Person aufgrund allgemeiner Fragen abzuklären. Ergeben sich daraus Hinweise, dass eine mangelnde Eignung allenfalls auf eine bestimmte Vereinszugehörigkeit zurückzuführen ist, kann im Einzelfall nach dieser gefragt werden. Dieses Vorgehen gilt grundsätzlich auch bei der Durchführung des Arbeitsverhältnisses, wenn aufgrund bestimmter Vorkommnisse eine weitere Eignung in Frage gestellt wird. In bezug auf Lehrpersonen ist somit eine konkrete Frage nach der Zugehörigkeit zum VPM nur nach Hinweisen einer fehlenden (oder verlorenen) Eignung aufgrund vorgängiger allgemeiner Fragen im Einzelfall als zulässig zu betrachten.

6. Datenbearbeitungen der Aufsichtsbehörden

Datenbekanntgaben und Auskunftsrecht

Die Frage, welche Daten der Aufsichtsbehörde zur Verfügung gestellt werden müssen oder durch diese den unterstellten Behörden weitergegeben werden dürfen und ob die betroffene Person auch bei der Aufsichtsbehörde ein Auskunftsrecht geltend machen kann, wurde in verschiedenen Zusammenhängen abgeklärt.
Das Offenlegen von Unterlagen mit Personendaten gegenüber einer Aufsichtsbehörde stellt datenschutzrechtlich eine Bekanntgabe dar, für die eine gesetzliche Grundlage erforderlich ist.
Die Bestimmungen, die die Aufsicht regeln, stellen auch Rechtsgrundlagen für Datentransfers zwischen der Aufsichtsbehörde und der unterstellten Behörde dar. Von zentraler Bedeutung sind die Prinzipien der Verhältnismässigkeit und der Zweckbindung:
Die Datenbekanntgaben sind umfangmässig auf das für die Aufsichtstätigkeit Erforderliche zu beschränken, und Daten dürfen nur im Rahmen des gesetzlich umschriebenen Aufsichtsbereichs offenbart werden.
Eine Anfrage betraf das Einsichtsrecht der Bezirksschulpflegen in die Protokolle der einzelnen Schulpflegen. Zwar können deren Mitglieder im Rahmen ihrer Aufsichtsbefugnis grundsätzlich die Unterlagen der beaufsichtigten Behörde einsehen. Jedoch besteht das Einsichtsrecht nicht generell und absolut, sondern ist auf die Daten zu beschränken, die zur Erfüllung der Aufsichts- und Kontrollaufgaben erforderlich und geeignet sind. Die Bezirksschulpflege hat deshalb gegenüber der Schulpflege im Einzelfall einzugrenzen, was sie genau überprüfen will. Daraus geht hervor, welche Teile der Schulpflegeprotokolle sie daher einsehen muss.
Abzuklären war auch der Datenfluss von der Aufsichtsbehörde zur unterstellten Behörde. Die Frage, wer in die Protokolle der Bezirksjugendkommissionen Einblick nehmen darf respektive wem diese automatisch zuzustellen sind, war insbesondere unter dem Aspekt zu betrachten, ob die Gemeinden,

welche finanzielle Unterstützungen leisten und infolgedessen über die Verwendung ihrer Gelder informiert sein wollen, Kopien der Protokolle erhalten dürfen oder sogar zwangsläufig damit bedient werden müssen.
Eine finanzielle Beteiligung an einer Organisation wie der Jugendkommission begründet kein umfassendes Einsichtsrecht. Nach dem Prinzip der Verhältnismässigkeit genügt es, wenn den Gemeinden ein Protokollauszug ausgehändigt wird, welcher über die Beschlüsse mit finanzieller Relevanz Auskunft gibt.
Aufgrund der in § 7 des Jugendhilfegesetzes (LS 852.1) umschriebenen Aufgaben der Bezirksjugendkommission, die Bezirksjugendsekretariate zu beaufsichtigen und deren Aufgaben festzulegen, ergibt sich dagegen, dass ihre knapp gehaltenen Entschlussprotokolle den Bezirksjugendsekretariaten im Sinne einer Orientierung und Aufgabenumschreibung zugestellt werden können. Jedoch muss das Einsichtsrecht eingeschränkt, aufgeschoben oder verweigert werden, wenn und soweit aufgrund einer Interessenabwägung gemäss § 10 DSG anderweitige Interessen vorgehen.
Besorgt die Gemeinde im Sinne von § 17 des Jugendhilfegesetzes die Aufgaben des Bezirksjugendsekretariats, ist sie im selben Masse einsichtsberechtigt wie letzteres. Nehmen lediglich einzelne Behördenmitglieder in der Jugendkommission Einsitz, dürfen diese Personen, wie alle anderen Kommissionsmitglieder, eine vollständige Kopie des Protokolls erhalten. In beiden Fällen ist jedoch der Grundsatz der Zweckbindung zu beachten, indem die den Vertreterinnen und Vertretern der Jugendkommission bekanntgewordenen Informationen nicht zuhanden der Gemeinde weiterverwendet werden dürfen.
Des weiteren stellt sich die Frage, ob betroffene Personen ihr Auskunftsrecht auch gegenüber einer Aufsichtsbehörde geltend machen können. Wir prüften, ob Lehrpersonen die Schulbesuchsprotokolle der Bezirksschulpflege einsehen dürfen.
Die Unterlagen einer Aufsichtsbehörde unterstehen wie alle anderen Datensammlungen § 17 DSG. Daher kann jede Lehrperson grundsätzlich Auskunft über die sie betreffenden Stellen im Schulbesuchsprotokoll verlangen und sich Kopien davon anfertigen lassen. Dabei ist irrelevant, ob die Ausführungen im Schulbesuchsprotokoll unmittelbare Auswirkungen auf das Anstellungsverhältnis haben, da für eine Auskunft kein begründetes Interesse vorzuliegen braucht. Ebenfalls bedeutungslos ist, ob die Lehrperson bereits anschliessend an den Schulbesuch mündlich über die gemachten Feststellungen und Eindrücke orientiert wurde, da ein Auskunftsrecht auch gegenüber bereits bekannten Daten besteht.
Protokolle sind deshalb entsprechend sorgfältig und gewissenhaft zu formulieren, und subjektive Werturteile sind klar als solche und nicht als Tatsachen zu deklarieren.

7. Zeitgeschichtliche Interessen und Persönlichkeitsrechte

Einsicht in archivierte Dokumente

Verschiedene Medienleute stellten Gesuche um Einsicht in archivierte Dokumente. Wir haben die angefragten Behörden in bezug auf die vorzunehmende Interessenabwägung beraten. Da das kantonale Archivgesetz vom 24. September 1995 noch nicht in Kraft ist, beurteilt sich die Rechtslage weiterhin nach der Verordnung über das Staatsarchiv vom 10. April 1974 (ArchivVo) (vgl. dazu ausführlich Tätigkeitsbericht Nr. 2 [1996], S. 18 f.). Archivierte Akten sind während einer Schutzfrist von 35 Jahren vom Zeitpunkt der Anlage – allenfalls längere Frist gemäss Beschluss der Behörde – der Öffentlichkeit nicht zugänglich (§ 7 ArchivVo). Anschliessend stehen sie allgemein zur Verfügung, wobei die Einsicht einzuschränken ist, wenn wesentliche öffentliche Interessen oder offensichtlich schützenswerte Interessen einer betroffenen Person es verlangen (§ 10 lit. a DSG). Vor Ablauf der Schutzfristen stehen die Akten nur ausnahmsweise offen, soweit sie ebenfalls zu im Archivzweck liegenden Gründen benötigt

werden. Auch in diesem Fall hat eine Interessenabwägung nach § 10 DSG stattzufinden. Konkret ging es um Einsicht in fremdenpolizeiliche Akten und Regierungsratsbeschlüsse über Familienangehörige eines nationalsozialistischen Kriegsverbrechers, die sich im Kanton Zürich aufhielten. Die archivrechtlichen Schutzfristen dieser Akten waren erst teilweise abgelaufen. Das zeitgeschichtliche Interesse an der Aufarbeitung der Schweizer Geschichte im Zusammenhang mit den Ereignissen des Zweiten Weltkrieges und der Bewältigung der Folgen ist jedoch erheblich und liess eine Ausnahmebewilligung zu, sofern eine wissenschaftliche Aufarbeitung gewährleistet war. Schützenswerte Interessen von Drittpersonen erforderten jedoch unter Umständen Einschränkungen der Einsicht, etwa durch Abdeckung der sie betreffenden Passagen eines Textes. Insbesondere bestanden schützenswerte Interessen in bezug auf nicht direkt involvierte Personen, so die Hauseigentümer und Mieter an der fraglichen Adresse, den Namen eines Institutes, wo ein Familienangehöriger sich aufhielt, sowie die Adresse des Rechtsvertreters, da sich dort heute zwei nicht involvierte Anwaltskanzleien befinden. Die Einsicht in die Akten konnte deshalb mit der Auflage gewährt werden, diese Drittinteressen zu berücksichtigen, die Auswertung des Dossiers vor der Publikation vorzulegen sowie die Informationen nicht zu einem anderen als dem im Gesuch angeführten Zweck zu verwenden.

Eine weitere Anfrage an ein öffentliches Organ betraf die Rolle des (verstorbenen) Vorfahren eines heutigen Bundespolitikers während des Zweiten Weltkrieges; diese Person stand damals in einem arbeitsrechtlichen Verhältnis zum angefragten Organ. Konkret wurde Einsicht in diejenigen Aktenstücke des betreffenden Personaldossiers verlangt, welche die Haltung und die praktizierten Verhaltensweisen zu politischen Fragen der damaligen Zeit zum Ausdruck bringen. Auch bei diesem Gesuch waren die Interessen abzuwägen. In Betracht zu ziehen waren nebst dem Offenlegungsinteresse des Journalisten einerseits die Interessen der Hinterbliebenen an einem ungestörten Andenken und an der Wahrung ihrer Anonymität. Andererseits waren auch die Interessen der verstorbenen Person selbst an ihrer Ehre und dem ungetrübten Andenken zu berücksichtigen.

Der Inhalt eines Personaldossiers umfasst in der Regel mehr Daten über eine Person, als im konkreten Fall relevant sind. Es rechtfertigt sich deshalb nicht, das gesamte personalrechtliche Verhältnis zu offenbaren, sondern vielmehr nur die relevanten Aktenstücke, was aber nicht auf eine Vorzensur hinauslaufen darf, indem nur die «genehmen» Daten präsentiert werden. Diese Interessenabwägung ist vom verantwortlichen Organ vorzunehmen.

8. Telefonüberwachung, Anwaltsgesetz, Krankenversicherungsgesetz

Mitberichte in Vernehmlassungsverfahren

Der Entwurf zu einem Bundesgesetz über die Überwachung des Post- und Fernmeldeverkehrs sowie den Einsatz technischer Überwachungsgeräte (Post- und Fernmeldeverkehrsüberwachungsgesetz) hat aus datenschutzrechtlicher Sicht zu verschiedenen Bemerkungen Anlass gegeben. Überwachungsmassnahmen bedeuten immer einen schweren Eingriff in die Grundrechte, weshalb sie nur aufgrund klarer und bestimmter Rechtsgrundlagen erfolgen dürfen. Diese haben nach dem Prinzip der Verhältnismässigkeit auch die rechtlichen und technischen Grenzen der Überwachungsmöglichkeiten zu regeln. In bezug auf den Einsatz solcher Mittel, die Verwendung der Erkenntnisse sowie die Überwachung von Berufsgeheimnisträgern, die nicht selbst verdächtigt werden, weist der Entwurf unverhältnismässige Bestimmungen auf. Über den sachlichen Zweck dieses Gesetzes hinaus wird der Koordinationsstelle für die Überwachungsmass-

nahmen die Schaffung einer zentralen Datenbank über die Fernmeldeanschlüsse übertragen. Die Anbieter von Fernmeldediensten sind verpflichtet, dieser Stelle im Abrufverfahren Zugriff auf die Angaben über sämtliche Fernmeldeanschlüsse zu geben. Diese präventive Datenbank zu polizeilichen Zwecken ist unverhältnismässig, da für die Anordnung einzelner Überwachungsmassnahmen ein Zugriff auf die jeweiligen Daten genügen würde.
Der Entwurf für ein Bundesgesetz über die Freizügigkeit der Anwältinnen und Anwälte (Anwaltsgesetz) sieht die Schaffung eines einheitlichen Anwaltsregisters, das durch die entsprechende kantonale Behörde geführt wird, vor. Im Entwurf fehlen insbesondere klare Bestimmungen über die Einsicht in das Register, die Ausstellung von Registerauszügen, die Veröffentlichung von Listen sowie die Aufbewahrungsdauer der Daten. Im Interesse einer gesamtschweizerisch einheitlichen Lösung wäre eine diesbezügliche Regelung im Anwaltsgesetz vorzusehen.
In der Vernehmlassung zum Einführungsgesetz zur Bundesgesetzgebung über die Krankenversicherung (EG KVG) haben wir darauf hingewiesen, dass beim Vollzug des Krankenversicherungsgesetzes die Datenflüsse auf die notwendigen und geeigneten Daten zu beschränken sind. Daten, die dem Patientengeheimnis unterstehen, sind von einer Stelle zu bearbeiten, die ebenfalls dem Berufsgeheimnis untersteht. Insbesondere fehlen im Entwurf auch Bestimmungen über die Führung des EDV-Systems in bezug auf die Regelung der Abrufverfahren und die zu treffenden organisatorischen und technischen Massnahmen der Datensicherheit.

9. Handhabung der Akten bei Amtsauflösungen

Weitergabe, Aufbewahrung oder Vernichtung

Im Rahmen von Reorganisationen oder Rechtsänderungen kommt es gelegentlich zur Auflösung einer Amtsstelle oder Behörde. Die Totalrevision des Gastgewerbegesetzes hatte eine Liberalisierung sowie die Übertragung der übriggebliebenen Aufsichtsaufgaben vom Kanton auf die Gemeinden zur Folge. Der Kanton übt nur noch die Oberaufsicht aus; die Abteilung Wirtschaftswesen der Finanzdirektion war daher aufzulösen. Ebenfalls aufzuheben ist das Börsenkommissariat. Das neue Bundesgesetz über die Börsen und den Effektenhandel übertrug die Aufsichtskompetenzen in diesen Bereichen auf die Eidgenössische Bankenkommission. Wir berieten beide Amtsstellen hinsichtlich der Frage, was mit ihren Akten zu geschehen habe.

Daten sind zu vernichten, wenn sie nicht mehr benötigt werden und sofern sie nicht zu archivieren sind (§ 14 DSG). Dies bedeutet aber nicht, dass bei der Auflösung einer Amtsstelle die Daten unverzüglich zu vernichten oder zu archivieren sind. Geht die Aufgabe auf eine andere Behörde über, bleibt die Rechtsgrundlage und damit die Berechtigung zur Datenbearbeitung grundsätzlich erhalten. Die neu zuständige Behörde ist als Rechtsnachfolgerin zu betrachten. Soweit die Daten von dieser Behörde weiterhin benötigt werden, sind ihr die entsprechenden Akten zu übergeben.

Umfangmässig richtet sich die Weitergabe nach dem Prinzip der Verhältnismässigkeit, d.h., es sind diejenigen Akten zu übergeben, welche für die Erfüllung der Aufgaben geeignet und erforderlich sind (§ 4 Abs. 3 DSG). Dies ist insbesondere dann relevant, wenn die Aufgabe nur teilweise übergeht, im übrigen aber aufgehoben wird.

Soweit eine Aufgabe aufgehoben wird, entfällt die Rechtsgrundlage für die Bearbeitung. Die Daten werden nicht mehr für die Erfüllung einer Aufgabe benötigt; sie sind zu vernichten oder zu archivieren. Eine Rechtsänderung entfaltet ihre Wirkungen in der Regel bezüglich zukünftiger Datenbearbeitungen. Für die Gegenwart kommt meist eine übergangsrechtliche Regelung zur Anwendung, insbesondere für

Verfahren, welche im Moment der Inkraftsetzung des neuen Rechts noch nicht abgeschlossen sind. Im weiteren laufen oft noch Fristen, z.B. für Rechtsmittel. Bedeutsam sind in diesem Zusammenhang auch die Verjährungsfristen für einen allfälligen Staatshaftungsprozess oder für die Rückforderung einer grundlos erbrachten Leistung. Soweit Akten zu archivieren sind, bestimmt § 6 der Verordnung über das Staatsarchiv, dass sie frühestens nach 10 Jahren dem Staatsarchiv abzuliefern sind.

Daher sind Akten, die nach neuem Recht für keine Aufgaben mehr benötigt werden, aus Beweis- und Sicherungsgründen während 10 Jahren nach Abschluss des Verfahrens aufzubewahren. Besondere Bestimmungen können kürzere oder längere Fristen vorsehen. Nach Ablauf dieser Aufbewahrungsfristen ist über die Archivierung zu befinden. Akten, für welche die zehnjährige Frist bereits abgelaufen ist, können archiviert werden. Über die Archivierung ist nach archivrechtlichen Grundsätzen zu entscheiden. Mit der Archivierung geht eine Zweckänderung der Daten einher (§ 4 Abs. 4 DSG); die Daten dienen nicht mehr zur Erfüllung der ursprünglichen Aufgaben, sondern zu Zwecken einer dauerhaften dokumentarischen Überlieferung (vgl. dazu ausführlich Tätigkeitsbericht Nr. 2 [1996], S. 18 f.). Da die aufzulösende Stelle für diese Aufbewahrung nicht mehr zur Verfügung steht, kommt als Aufbewahrungsort z.B. die bis anhin zuständige Direktion in Frage. Nach der aktuellen Rechtslage können die Akten auch beim Staatsarchiv zwischengelagert werden. Das neue Archivgesetz, das noch nicht in Kraft steht, bietet diese Möglichkeit hingegen nicht mehr.

Die Abteilung Wirtschaftswesen und das Börsenkommissariat hatten zu prüfen, welche Akten den neu zuständigen Behörden zu übergeben waren, und sie hatten für die Aufbewahrung der übrigen Daten bis zum Zeitpunkt des Entscheides der Vernichtung oder Archivierung zu sorgen.

10. Publikation und Weitergabe von Gerichtsentscheiden

Anonymisierung unumgänglich

Das Sozialversicherungsgericht beabsichtigte, richtungsweisende Entscheide in der Fachpresse zu veröffentlichen sowie auf Gesuch hin Entscheide an Universitätsprofessoren, die sich mit der Materie der Sozialversicherung befassen, und an kantonale Behörden, denen Aufgaben in diesem Bereich übertragen sind, weiterzugeben. Die Publikation von Entscheiden ist als eine zu den allgemeinen Aufgaben gehörende Tätigkeit des Gerichts zu betrachten und daher auch ohne ausdrückliche gesetzliche Verpflichtung zulässig. Für die Leserschaft der Fachpresse ist jedoch die Kenntnis der Personendaten, die ein Gerichtsentscheid enthält, in der Regel nicht erforderlich, weshalb nur eine Publikation in anonymisierter Form verhältnismässig ist. Ausnahmsweise ist die Nennung von Personendaten zulässig, wenn dies zum Verständnis unentbehrlich ist (z.B. bei Marken- oder Firmenrechtsstreitigkeiten). Werden die Entscheide nicht durch das Gericht selbst, sondern durch einen Fachverlag veröffentlicht, sind zusätzlich die Vorschriften über das Bearbeiten im Auftrag zu beachten (§ 13 DSG). Dem Fachverlag können die Entscheide in nichtanonymisierter Form ausgehändigt werden, wenn durch eine vertragliche Verpflichtung sichergestellt ist, dass der Datenschutz eingehalten wird, die Entscheide nur anonymisiert veröffentlicht werden und der beauftragte Fachverlag angemessene organisatorische und technische Datensicherheitsmassnahmen trifft.
Die Weitergabe von Entscheiden an Universitäten bzw. Professoren und an kantonale Fachbehörden gehört nicht mehr zu den Kernaufgaben eines Gerichts. § 8 der Verordnung über die Akteneinsicht durch Gerichtsberichterstatter und andere Dritte (LS 211.15) erlaubt Dritten die Einsicht in Entscheide, wenn ein wissenschaftliches Interesse es rechtfertigt und nach

Ansicht des Gerichtspräsidenten keine berechtigten Interessen verletzt werden. Das Prinzip der Verhältnismässigkeit verlangt in diesen Fällen eine Anonymisierung, weil die Kenntnis der Personendaten für den Empfänger nicht erforderlich ist. Auch eine Interessenabwägung mit den offensichtlich schützenswerten Interessen der betroffenen Personen (§ 10 lit. a DSG) würde zum gleichen Ergebnis führen.
Für die Bekanntgabe der Entscheide an kantonale Fachbehörden fehlt es an einer Rechtsgrundlage. Die Kenntnis der Gerichtspraxis stellt lediglich eine Aufgabenerleichterung dar; für die Aufgabenerfüllung ist sie jedoch nicht zwingend erforderlich.
Aus diesen Gründen darf in diesen Fällen nur eine Weitergabe von anonymisierten Entscheiden erfolgen. Selbstverständlich hat die Fachbehörde Anspruch auf einen vollständigen Entscheid, wenn sie selbst Partei im Verfahren vor Sozialversicherungsgericht ist.

11. Keine Aufbewahrung nicht mehr relevanter Gesuchsunterlagen

Rückgabe auf Begehren oder Vernichtung

Mangels Zuständigkeit (fehlender stipendienrechtlicher Wohnsitz im Kanton Zürich) lehnte die Abteilung Stipendien der Erziehungsdirektion das Stipendiengesuch einer betroffenen Person ab. Diese verlangte daraufhin die Rückgabe aller für den Ablehnungsentscheid nicht relevanten Unterlagen.
Die Abteilung Stipendien erklärte, dass die Dossiers nach der letzten unbenutzt verstrichenen Rechtsmittelfrist geschlossen würden und in der Registratur aufbewahrt blieben, bis die Finanzkontrolle die Revision durchgeführt hätte. Anschliessend gingen die Akten für fünf Jahre in eine Zwischenarchivierung, bevor sie dem Staatsarchiv zur endgültigen Archivierung oder Vernichtung übergeben würden.
Personendaten, die nicht mehr benötigt werden, müssen vernichtet werden, soweit sie nicht zu archivieren sind (§ 14 DSG). Dieser Grundsatz ergibt sich aus dem Prinzip der Verhältnismässigkeit, wonach Personendaten nur bearbeitet werden dürfen, soweit sie für die Aufgabenerfüllung geeignet und erforderlich sind. Zur Kontrolle des Geschäftsganges bzw. zur Rechenschaftsablage werden die Angaben benötigt, aus welchen sich der Grund für die Ablehnung ergibt, das heisst im konkreten Fall diejenigen Akten, aus denen sich ergibt, dass ein stipendienrechtlicher Wohnsitz im Kanton Zürich fehlt. Alle übrigen Unterlagen werden nach Eintritt der Rechtskraft, dem unbenutzten Ablauf der Rechtsmittelfrist, nicht mehr benötigt und sind unmittelbar danach zurückzugeben oder zu vernichten. Im konkreten Fall schien es zulässig, die Akten nicht einzeln nach Ablauf der Rechtsmittelfrist, sondern in einem (mindestens) alljährlichen Turnus zu bereinigen, bevor sie in die Zwischenarchivierung gelangen. Dieser Spielraum besteht allerdings nicht, wenn eine betroffene Person vorher ausdrücklich die nicht mehr benötigten Unterlagen zurückfordert. Opportunitätsgründe müssen in diesem Fall gegenüber dem Vernichtungs- bzw. Herausgabeanspruch zurücktreten.
Von selbst versteht sich, dass in Fällen, in denen die betroffene Person die Herausgabe ausdrücklich fordert, die Akten nicht vernichtet werden dürfen. Ein solches Vorgehen wäre rechtsmissbräuchlich. Ebenso wäre die Praxis unzulässig, die Originale herauszugeben, aber Kopien davon zu behalten. Die nicht mehr relevanten Unterlagen waren deshalb der betroffenen Person zurückzugeben.

Heikler Datenfluss im Gesundheitswesen

Der Datenaustausch im Gesundheitswesen ist sensibel. Auf dem Spiel steht das Patientengeheimnis.

Gesundheitsdaten sind besonders schützenswerte Personendaten und durch das Patientengeheimnis auch strafrechtlich geschützt (Art. 321 StGB). Sie dürfen nur weitergegeben werden, wenn die betroffene Person eingewilligt hat oder wenn eine klare gesetzliche Grundlage hierzu ermächtigt.

Zunehmender Datenaustausch

Die Umstrukturierungen im Gesundheitswesen haben zur Folge, dass zu Zwecken des Controllings, der Statistik und der Leistungsüberprüfung immer mehr Daten bearbeitet werden. Auch wenn diese Daten im Verlaufe dieser Prozesse anonymisiert werden können, die Basis dieser Daten bilden immer sensible, patientenbezogene Gesundheitsdaten.
Die Gesundheitsdirektion erstellt umfangreiche Statistiken über das Gesundheitswesen im Kanton. Die Krankenhäuser sind verpflichtet, hierfür die notwendigen Angaben zu liefern. Diese Daten werden nicht nur kantonsintern benötigt, sondern auch für die Erstellung der gesamtschweizerischen Spitalstatistiken aufbereitet. Zu diesem Zweck werden die Daten nach den Vorgaben des Bundesamts für Statistik anonymisiert und verschlüsselt übermittelt. Damit wird im Rahmen der Erstellung der Gesundheitsstatistiken gewährleistet, dass das Patientengeheimnis gewahrt bleibt.

Daten für Versicherer

Für die Erstellung der Gesundheitsstatistiken werden die einzelnen Diagnosedaten mittels des sogenannten ICD-10-Codes (Internationale statistische Klassifikation der Krankheiten und verwandter Gesundheitsprobleme, 10. Revision) festgehalten. ICD-9-CM/3 (schweizerische Ausgabe der amerikanischen Operationsklassifikation) wird für die operativen Eingriffe verwendet. Somit wird für alle Patientinnen und Patienten in den Krankenhäusern eine Diagnose mittels des ICD-10-Codes erfasst. Der ICD-10- Code weist über 10 000 detaillierte Diagnosecodes auf. Klarerweise werden diese Informationen zu statistischen Zwecken benötigt und deshalb auch im Verfahren der Erstellung der Statistiken anonymisiert, so dass die einzelne Diagnose nicht einer bestimmten Person, sondern im Rahmen der «Fallkostenstatistik» nur mehr einem bestimmten Krankheitsfall zugeordnet werden kann.
Die Versicherer verlangten nun, dass diese ICD-10-Diagnosecodes mit der Rechnungsstellung auch an sie, in nichtanonymisierter Form, weitergeleitet werden. Bisher wurden den Versicherern mit der Rechnungsstellung sogenannte Rahmendiagnosen mitgeteilt, um die Behandlungskosten entsprechend überprüfen zu können. Diese Rahmendiagnosen umfassen zirka sechzig Positionen und bedeuten einen verhältnismässigen Eingriff in die Persönlichkeitsrechte der betroffenen Personen. Das Begehren der Versicherer ist im Rahmen einer allgemein feststellbaren Tendenz zu sehen, immer mehr Informationen über den Gesundheitszustand ihrer Versicherten zu bearbeiten. Dabei nimmt die Transparenz für die betroffenen Personen laufend ab, da keine Informationen darüber bestehen, was mit diesen Daten geschieht und wie lange sie aufbewahrt bleiben. Die Folgen solcher Datenbearbeitungen für die versicherten Personen sind nicht absehbar.

Technische Möglichkeiten

Um diese Datenbearbeitungen zu ermöglichen, stellen die Versicherer technische Möglichkeiten zur Verfügung, die im standardisierten Verfahren den Austausch der Daten zwischen Leistungserbringern und Versicherern zulassen. ICD-10-Diagnosecodes werden dabei selbstverständlich mit eingeschlossen. Der elektronische Datenaustausch wird vertraglich vereinbart.
Die nationale Konferenz der Datenschutzbeauftragten hat in einer Resolution auf diese Situation aufmerksam gemacht und festgehalten, dass die Weitergabe von ICD-10-Diagnosecodes an Versicherer das Patientengeheimnis verletzt (siehe Kasten).
Die Gesundheitsdirektion hat die Rechtslage aufgrund dieser Resolution überprüft und eine Weisung an die öffentlichen und mit einer öffentlichen Aufgabe betrauten Krankenhäuser erlassen.

Darin werden die Spitäler angewiesen, auf die Bekanntgabe von ICD-10-Diagnosecodes mit der Rechnungsstellung an die Versicherer zu verzichten. Als Übergangslösung bis zum Vorliegen einer gesamtschweizerisch einheitlichen Regelung soll höchstens eine Diagnose bekanntgegeben werden, die einer Rahmendiagnose entspricht und keine detaillierte Diagnose darstellt.
In diesem sensiblen Bereich der Datenbearbeitungen konnte damit eine schwerwiegende Verletzung der datenschutzrechtlichen Bestimmungen verhindert werden.

Weitere Entwicklungen

Das Gesundheitswesen wird angesichts neuer technischer Möglichkeiten des Datenaustausches (Telemedizin; Chipkarten usw.) auch in Zukunft ein sensibler Bereich der Datenbearbeitungen bleiben. Dabei steht die wohl älteste Datenschutzbestimmung der Welt – das Patientengeheimnis – auf dem Spiel. Es sind deshalb klare gesetzliche Grundlagen zu schaffen, die den Datenaustausch regeln und die datenschutzrechtlichen Bestimmungen respektieren.
Die Fragen um den ICD-10-Code zeigen, dass nicht einseitig auf die Forderungen der Versicherer abzustellen ist, sondern dass unter allen Beteiligten im Gesundheitswesen ein Interessenausgleich stattzufinden hat. Dabei dürfen die datenschutzrechtlichen Anliegen und das Patientengeheimnis nicht unberücksichtigt bleiben.

Resolution der Datenschutzbeauftragten

Die nationale Konferenz der Datenschutzbeauftragten teilt die Besorgnis von Spitälern, Ärzten und Patientinnen und Patienten, dass ein zunehmender Datenfluss zu den Versicherungen das Patientengeheimnis in Frage stellt. Dieser Datenfluss führt nicht nur zu einem kostenverursachenden Mehraufwand, sondern widerspricht auch dem Grundgedanken des Krankenversicherungsgesetzes (KVG).
Immer häufiger läuft eine grosse Masse von Informationen automatisch und oft ohne Wissen der Betroffenen vom Spital zum Versicherer. Dabei verlangen die Versicherer, dass die Diagnoseinformationen in jedem Fall und voraussetzungslos in Form des detaillierten, über 10 000 Positionen umfassenden ICD-10-Diagnosecodes geliefert werden. Zwar gibt das KVG den Versicherern das Recht, im Einzelfall detaillierte Angaben zu verlangen. Eine automatische Mitteilung solcher Informationsmengen ist jedoch vom KVG nicht gedeckt. Damit würde das Patientengeheimnis umgangen, da der Vertrauensarzt die Datenmenge nicht mehr bearbeiten kann und die sensiblen Gesundheitsdaten direkt in die Administration der Versicherer fliessen.
Der kritisierte Datenfluss ist im übrigen aus folgenden Gründen exzessiv sowie langfristig auch gefährlich:

Der ICD-10-Code ist eine von der Weltgesundheitsorganisation weiterentwickelte Klassifikation, welche globalen Statistik- und Forschungszwecken dient und deshalb auch viele Codierungsziffern aufweist, die nicht Diagnosen von Krankheiten betreffen, sondern vielmehr bestimmte Verhaltensweisen («antisoziale Persönlichkeit», «oppositionelles Verhalten» des jugendlichen Patienten, «Erziehungsfehler der Eltern», «gesteigertes sexuelles Verlangen» oder «Konflikte mit Vorgesetzten») beschreibt. Aber auch sonst sind die Codes in vielerlei Hinsicht für die Überprüfung von Rechnungen ungeeignet. So kann etwa die Berechtigung der teuren Computertomographie nicht mittels des erst im nachhinein bekannten Diagnosecodes geprüft werden, und die Spitalbedürftigkeit eines Patienten hängt oft stärker von seinem sozialen Umfeld ab als von einer Diagnose.
Weiter erhöht die Codierung der Informationen die Gefahr, dass Verdachts- oder Ausschlussdiagnosen nach ihrer Übermittlung als bestätigte Diagnosen gewertet oder gerade in ihrer Bedeutung umgekehrt werden. Zudem wären kostspielige Einrichtungen zu schaffen, um den Patientinnen und Patienten die Codierung transparent zu machen.
Ausserdem sind bis heute die Aufbewahrungsdauer und der Verwendungszweck der Daten beim Versicherer nicht transparent, weshalb die Gefahr besteht, dass die Daten für andere Versicherungszweige missbraucht werden.
Die nationale Konferenz der Datenschutzbeauftragten fordert daher, dass der Datenfluss auf die notwendigen und geeigneten Daten beschränkt wird, dass die geplante Einführung des ICD-10-Codes für die Rechnungsprüfung gestoppt wird.
Damit das Patientengeheimnis gewahrt werden kann, sind die Kosten- und Wirtschaftlichkeitsprüfung nicht versicherten-, sondern fallbezogen durchzuführen. Mit einem solchen Vorgehen wird weder die Administration durch unnötigen Datentransfer aufgebläht noch das Patientengeheimnis in Frage gestellt. Damit könnte gar ein aktiver Beitrag zur Kostenbegrenzung verwirklicht werden.

(Resolution verabschiedet von der IV. Nationalen Konferenz der Datenschutzbeauftragten am 3. November 1997 in Bellinzona.)

Datenbearbeitungen in sensiblen Bereichen

Die Gemeinden bearbeiten Personendaten zu den unterschiedlichsten Zwecken. Vielfach standen deshalb grundlegende Fragen zur Diskussion.

1. Schwieriger Umgang mit dem Auskunftsrecht

Voraussetzungsloser Anspruch der betroffenen Personen

Das Auskunftsrecht ist eines der zentralen Rechte des Datenschutzgesetzes. Dennoch bekunden zahlreiche Stellen noch immer erhebliche Mühe mit der korrekten Gewährung dieses Rechts. In verschiedenen Fällen wurde der Datenschutzbeauftragte um Vermittlung ersucht.

Zwei betroffene Personen hatten vergeblich bei mehreren Kirchgemeinden sowie Spitälern, wo sie angestellt waren, ihr Auskunftsrecht geltend gemacht. Wir wiesen die beteiligten kirchlichen Institutionen darauf hin, dass das DSG auch für die staatlich anerkannten Kirchen gilt. Dementsprechend haben die betroffenen Personen ein Anrecht, eigene Daten ausnahmslos auch bei kirchlichen Institutionen einzusehen. Lediglich gegenüber dem Generalvikariat für den Kanton Zürich sowie dem Bischöflichen Ordinariat Chur konnten wir mangels eigener Zuständigkeit keine Stellungnahme abgeben, da es sich nicht um Organe der öffentlich-rechtlich anerkannten kirchlichen Körperschaft des Kantons Zürich handelt. Diesbezüglich überwiesen wir die Anfrage an den Eidgenössischen Datenschutzbeauftragten. Er stellte in seiner Antwort fest, dass in diesen Fällen das Auskunftsrecht gemäss Art. 8 des Bundesgesetzes über den Datenschutz zu gewähren sei.
Im weiteren war zu beurteilen, ob die Auskunft gratis erteilt werden müsse oder ob für die Aufbereitung der im betreffenden Fall relativ umfangreich gewordenen Unterlagen ein bestimmter Betrag verrechnet werden könne. Das DSG äussert sich zur Kostenpflichtigkeit einer Auskunft nicht.
Klar ist, dass nicht durch exzessiv hohe Kosten von der Geltendmachung dieses Rechts abgehalten werden darf. Demgegenüber sieht das Bundesgesetz über den Datenschutz in Art. 8 Abs. 5 im Normalfall ausdrücklich eine kostenlose Auskunft vor. Nur in den von Art. 2 der Datenschutzverordnung umschriebenen Ausnahmefällen kann eine Beteiligung an den Kosten der Auskunft, maximal Fr. 300.–, verlangt werden. In Analogie zur bundesrechtlichen Regelung wurde für die Vorbereitung der auskunftspflichtigen Dossiers (beispielsweise sind Angaben über Drittpersonen vorher auszusondern) je ein Betrag von Fr. 300.– festgesetzt.

In einem anderen Fall war vom zuständigen Bezirksrat die Auskunft verweigert worden mit der Begründung, das verlangte Anhörungsprotokoll aus dem damaligen Adoptionsverfahren sei mehr als zwanzig Jahre alt, weshalb die gesuchstellende Person kein schützenswertes Interesse für eine Akteneinsicht mehr habe. Ausserdem beurteile sich die Zulässigkeit der Akteneinsicht als Vorbereitung für ein allfälliges Revisionsgesuch des Adoptionsverfahrens ausschliesslich nach Art. 4 der Bundesverfassung, weshalb das Datenschutzgesetz gar nicht zur Anwendung gelange.
Wir wiesen den Bezirksrat darauf hin, dass die Rechte der betroffenen Person nach § 17 DSG voraussetzungslos bestehen, weshalb ein Interessennachweis nicht erbracht werden muss und von der zuständigen Verwaltungsbehörde auch nicht verlangt werden kann. Von der Behörde ist lediglich das Vorhandensein allfälliger entgegenstehender Interessen gemäss § 18 DSG zu prüfen. Bei abgeschlossenen Verfahren besteht das Auskunftsrecht allenfalls neben dem Akteneinsichtsrecht, weshalb eine betroffene Person beide Ansprüche gleichzeitig geltend machen kann (siehe dazu ausführlich Tätigkeitsbericht Nr. 1 [1995], S. 15).
Der betroffenen Person wurde letztendlich eine Kopie des verlangten Adoptionsprotokolls ausgehändigt.

Bei der Vormundschaftsbehörde wollte eine Person die vorhandenen Daten über gewisse Vorfälle in ihrer Jugend einsehen. Sie wurde wiederholt abgewiesen, insbesondere mit dem Hinweis, dass sie die entsprechenden Informationen

psychisch allenfalls nicht verkraften oder damit ungeschickt umgehen werde. Das Auskunftsrecht kann ausschliesslich bei überwiegenden Interessen privater Dritter oder der Öffentlichkeit eingeschränkt oder verweigert werden. Dagegen ist die voraussichtliche Reaktion der betroffenen Person selber bei der Interessenabwägung nicht mit einzubeziehen. Allenfalls kann der betroffenen Person empfohlen werden, das Auskunftsrecht über eine Vertrauensperson wahrzunehmen, um einen allfälligen «Aufklärungsschaden» zu vermeiden.

Gleichzeitig wiesen wir darauf hin, dass jedes datenbearbeitende Organ verpflichtet ist, die Aufbewahrungsdauer seiner Unterlagen zu limitieren. Nach Ablauf dieser Frist sind die betreffenden Aktenstücke entweder zu vernichten oder zu archivieren. Mit der Archivierung tritt eine Zweckänderung ein, indem die Daten künftig nur noch gemäss den Bestimmungen des Archivrechts genutzt werden können. Für die abliefernde Behörde hat die Archivierung dieselbe Wirkung wie die Vernichtung: Sie darf nicht mehr darauf zugreifen, weshalb sie auch keine Daten mehr an andere Stellen weiterleiten kann.

Seine Grenzen hat das Auskunftsrecht dort, wo es sich nicht mehr um eigene Daten handelt. Dies hatten wir auf eine konkrete Anfrage hin zu bestätigen: Eine Person hatte sich an das zuständige Jugendsekretariat gewandt mit dem Begehren, ihr die Gesamtsumme der von ihrem Ex-Ehepartner geleisteten Alimentenleistungen an dessen Kinder aus einer früheren Ehe bekanntzugeben, mit der Begründung, dass sie während der Zeit ihrer eigenen Ehe mit ihm diese Gelder faktisch zu einem Teil mitfinanziert habe. Hier hat das angegangene Jugendsekretariat zu Recht eine Auskunft verweigert, da ein Auskunftsrecht nur in Bezug auf Daten über die eigene Person besteht.
Im vorliegenden Fall betreffen die Daten aber den Ex-Ehepartner einerseits und die Kinder als Gläubiger der Alimentenleistungen andererseits.

2. Einsicht in Personalakten

Wahrung der Rechte der betroffenen Personen

Mehrere Anfragen betrafen die von kommunalen Stellen geführten Personalakten. Einerseits wurde uns geschildert, dass entweder die Einsichtnahme in die eigene Personalakte grundsätzlich verweigert oder dass zumindest das Erstellen von Kopien sämtlicher Unterlagen nicht zugelassen worden sei. Andererseits wurde dargelegt, dass Personalakten teilweise überflüssiges Material, beispielsweise Unterlagen zu früheren negativ beantworteten Bewerbungen, enthielten. Ein dritter Bereich betraf interne Bewerbungen, wo ohne Wissen der betroffenen Person deren vorgesetzte Person um eine Stellungnahme zu Leistung und Persönlichkeit ersucht worden war.
§ 17 DSG garantiert ein umfassendes Einsichtsrecht in die eigene Personalakte, welches nur bei Vorliegen der in § 18 DSG genannten Gründe durch eine begründete und bei der oberen Instanz anfechtbare Verfügung aufgeschoben, eingeschränkt oder verweigert werden kann. Die Auskunft erfolgt gemäss § 10 Abs. 2 DSV in der Regel schriftlich, das heisst durch Abgabe von Fotokopien. Ein Personaldossier darf nur solche Daten enthalten, welche zur Abwicklung des konkreten Arbeitsverhältnisses geeignet und erforderlich sind. Abgewiesene Bewerbungen fallen nicht darunter. Die Auskunftserteilung einer vorgesetzten Person im Rahmen eines internen oder anderen Bewerbungsverfahrens stellt eine Datenbekanntgabe dar, die nur mit Einwilligung der sich bewerbenden Person erfolgen darf.

3. Bekanntgabe von Kündigungsgründen

Verhältnismässigkeit ist zu beachten

Eine Stadtverwaltung versandte Kündigungsbestätigungen an die zuständigen Amtsstellen, wobei auf der Rückseite das Kündigungsschreiben in vollem Wortlaut abgedruckt war. Eine Weiterleitung der eingereichten Kündigung stellt eine Datenbekanntgabe dar, die sich insbesondere nach dem Grundsatz der Verhältnismässigkeit zu richten hat. Zwar sind diverse Stellen innerhalb einer Verwaltung von einer erfolgten Kündigung eines Arbeitsverhältnisses zu informieren, wie die politischen und administrativen Vorgesetzten, die Lohnbuchhaltung sowie das Versicherungswesen. Wenn eine Mitteilung über die Tatsache der Kündigung ausreicht, sind weitere Daten nicht bekanntzugeben. Insbesondere fehlen die Voraussetzungen, um in der Kündigung enthaltene besonders schützenswerte Angaben aus dem persönlichen oder gesundheitlichen Geheimbereich weiterzuverbreiten. Einblick in den Originalwortlaut der Kündigung wird in der Regel lediglich für personalverantwortliche oder vorgesetzte Stellen zur Aufgabenerfüllung geeignet und erforderlich sein. Aufgrund dieser Erwägungen wurde die Praxis entsprechend angepasst.

Eine weitere Anfrage hatte zum Inhalt, ob eine Arbeitslosenkasse vom ehemaligen Arbeitgebenden Auskunft über die Kündigungsgründe verlangen dürfe. Auszugehen ist von den geltenden Bestimmungen des Arbeitslosenversicherungsrechts, wonach eine Person aus verschiedenen Gründen, beispielsweise bei selbstverschuldeter Arbeitslosigkeit, in der Anspruchsberechtigung eingestellt werden kann. Dies ermächtigt die zuständige Arbeitslosenkasse, entsprechende Informationen über die Gründe, welche zur Auflösung des Arbeitsverhältnisses geführt haben, einzuholen. Jedoch darf nach dem Prinzip der Verhältnismässigkeit nicht über das geeignete und erforderliche Mass an Detaillierung hinausgegangen werden. Nur Angaben, welche unmittelbar zur Beurteilung des Anspruchs der arbeitslosen Person notwendig sind, dürfen erfragt und somit bekanntgegeben werden. Daher reicht es aus, wenn mitgeteilt wird, dass wegen der Verletzung arbeitsvertraglicher Pflichten (allenfalls mit Hinweisen auf Schwere und Häufigkeit) gekündigt worden ist. Angaben zu Abmahnungen sind ebenfalls erforderlich, um die Schwere des Verschuldens abschätzen zu können. Nur in begründeten Ausnahmefällen kann es sich allenfalls rechtfertigen, zusätzliche Daten mitzuteilen.

4. Amtshilfe für polizeiliche Zustellung

Kein Schutz des Rechtsmissbrauchs

Die Polizei ist häufig beauftragt, amtliche Sendungen zuzustellen, wobei die absendenden Ämter selber oft nicht über eine aktuelle Adresse dieser Personen verfügen. Wir wurden deshalb angefragt, ob die Polizei in solchen Fällen die aktuelle Adresse von möglicherweise arbeitslosen Personen beim Arbeitsamt, welches in der Regel in dauerndem Kontakt mit diesen Personen steht, einholen dürfe. Im Bereich der Arbeitslosenversicherung statuiert Art. 97 Abs. 1 des Arbeitslosenversicherungsgesetzes eine besondere Schweigepflicht, welche nur in den ausdrücklich aufgeführten Fällen von Art. 125 der Arbeitslosenversicherungsverordnung durchbrochen werden kann. In allen anderen Fällen dürfen Angaben nur mit der Einwilligung der betroffenen Person herausgegeben werden. Grundsätzlich sind die Behörden jedoch zur Amtshilfe verpflichtet. Da im vorliegenden Fall keine gesetzliche Ermächtigung zur Datenbekanntgabe besteht, muss das zuständige Arbeitsamt daher versuchen, bei der betroffenen Person eine Einwilligung zur Bekanntgabe der neuen Adresse zu erhalten. Mit der Einwilligung kann die Auskunft ohne weiteres gegeben werden. Wird die

Zustimmung verweigert, hat das Arbeitsamt abzuklären, ob die Verweigerung der Zustimmung rechtsmissbräuchlich ist. Der Schutz des Sozialversicherungsrechts darf nicht missbraucht werden, um die Durchsetzung von Rechtsansprüchen oder die Wahrung anderer schutzwürdiger Interessen zu vereiteln. Beim Vorliegen eines Rechtsmissbrauchs ist das Arbeitsamt nicht mehr an das Sozialversicherungsgeheimnis gebunden und darf die Auskunft erteilen.

Zur Erteilung von Adressauskünften ist jedoch grundsätzlich die Einwohnerkontrolle zuständig. Die Polizei hat sich deshalb an sie zu halten. Ist dort die aktuelle Adresse nicht bekannt, weil die betroffene Person ihrer Meldepflicht nicht nachgekommen ist, muss die Einwohnerkontrolle auf dem Amtshilfeweg nach der richtigen Adresse forschen und sich beispielsweise an das Arbeitsamt wenden. Dieses kann die neue Adresse bekanntgeben, da eine Verweigerung der Einwilligung durch die betroffene Person in diesem Fall rechtsmissbräuchlich wäre. Infolgedessen kommt die Polizei regelmässig über die Einwohnerkontrolle zu den für ihre Arbeit notwendigen Adressangaben.

5. Auskunftserteilung an die Betreibungsämter

Daten über arbeitslose und verbeiständete Personen

Am 1. Januar 1997 ist die Revision des Schuldbetreibungs- und Konkursgesetzes (SchKG) in Kraft getreten. Verschiedene Neuerungen führten zu Unsicherheiten über die Rechtslage in bezug auf Datenbekanntgaben an die Betreibungsämter.

Die Arbeitsämter bzw. Regionalen Arbeitsvermittlungszentren erteilten Betreibungsämtern bis anhin nur dann Auskünfte über arbeitslose Personen, wenn diese ihre Einwilligung dazu erteilten. Dies erfordert die Schweigepflicht nach Art. 97 des Arbeitslosenversicherungsgesetzes (AVIG). Ausnahmen von der Schweigepflicht sind nur vorgesehen für Auskünfte an Stellen anderer Sozialversicherungen oder an Fürsorgebehörden sowie unter bestimmten Umständen an Zivil- und Strafgerichte (Art. 125 Arbeitslosenversicherungsverordnung [AVIV]). Für alle weiteren Auskünfte bedarf es der schriftlichen Einwilligung der betroffenen Person (vgl. ausführlich Tätigkeitsbericht Nr. 2 [1996], S. 24).

Im betreibungsrechtlichen Pfändungsverfahren trifft die Schuldner eine vollumfängliche Auskunftspflicht über ihre Vermögenswerte. Diese Auskunftspflicht gilt neu auch für Behörden (Art. 91 Abs. 5 SchKG). Diese Bestimmung stellt eine gesetzliche Grundlage im Sinne von § 8 DSG dar, damit öffentliche Organe den Betreibungsämtern Daten bekanntgeben dürfen. Eine Datenbekanntgabe ist jedoch einzuschränken, mit Auflagen zu verbinden oder zu verweigern, wenn gesetzliche Geheimhaltungspflichten oder besondere Datenschutzvorschriften es verlangen (§ 10 lit. b DSG).

Im Bereich der Arbeitslosenversicherung steht einer Bekanntgabe die Schweigepflicht nach Art. 97 AVIG entgegen. Die Bestimmung von Art. 91 Abs. 5 SchKG stellt keine weitere Ausnahme von der arbeitslosenversicherungsrechtlichen Schweigepflicht dar, sondern nur eine gesetzliche Grundlage, damit Datenweitergaben irgendwelcher Behörden an die Betreibungsämter überhaupt zulässig sind. Hätte der Gesetzgeber gewollt, dass Organe der Arbeitslosenversicherung auskunftspflichtig sind, hätte er auch Art. 125 AVIV entsprechend ändern müssen. Diese Auffassung wird in einem (noch) nicht publizierten Entscheid des Bundesgerichts in bezug auf das Sozialversicherungsgeheimnis nicht geteilt. Das Bundesgericht geht davon aus, dass sich in den Materialien zur Revision des SchKG genügend Hinweise finden, die auf die Durchbrechung der gesetzlichen Schweigepflicht hinweisen. Der in der Begründung nicht überzeugende Entscheid ist indessen sachgerecht und bedeutet für die betroffenen Amtsstellen, dass sie den Betreibungsämtern Auskunft zu erteilen haben.

Die Beistandschaft ist eine Massnahme des Vormundschaftsrechts mit dem geringsten Eingriff in die Rechtsstellung der betroffenen Person. Die verbeiständete Person bleibt grundsätzlich handlungsfähig und damit auch betreibungsfähig. Der Sozialdienst eines Bezirks erkundigte sich, weshalb es dennoch vorkomme, dass Beistandschaften den Betreibungsämtern gemeldet werden und weshalb im Betreibungsverfahren gegen verbeiständete Schuldner die Betreibungsurkunden auch dem Beistand zugestellt werden. In beiden Fällen handelt es sich um Datenbekanntgaben, welche entsprechende Rechtsgrundlagen erfordern (§ 8 Abs. 1 DSG).
Der neue Art. 68d SchKG sieht vor, dass bei Betreibungen gegen die verbeiständete Person die Betreibungsurkunden auch dem Beistand zugestellt werden. Damit das Betreibungsamt überhaupt Kenntnis einer Verbeiständung hat, regelt Art. 397 Abs. 3 Zivilgesetzbuch (ZGB), der ebenfalls durch die SchKG-Revision eingeführt wurde, dass Beistandschaften, die nicht veröffentlicht werden, dem Betreibungsamt mitgeteilt werden, «sofern dies nicht als unzweckmässig erscheint». Mitgeteilt werden auch Wohnsitzwechsel oder die Aufhebung der Beistandschaft (Art. 440 Abs. 2 ZGB).
Beide Bestimmungen stellen Rechtsgrundlagen im Sinne von § 8 DSG dar, um Daten bekanntzugeben.
Bei jeder Datenbekanntgabe hat eine Interessenabwägung zu erfolgen (§ 10 DSG). Der Beistand vertritt ein öffentliches Interesse, das darin besteht, dass er Kenntnis der Betreibung gegen die verbeiständete Person erhält, um allenfalls korrigierend eingreifen zu können. Dem stehen Geheimhaltungsinteressen der betroffenen Person gegenüber. Diese Interessen sind gegeneinander abzuwägen. Dies impliziert auch die Formulierung von Art. 397 Abs. 3 ZGB («sofern dies nicht als unzweckmässig erscheint»).
Das Betreibungsamt ist im Rahmen der Zustellung der Betreibungsurkunden nicht in der Lage, diese Interessenabwägung durchzuführen, da es keine Informationen darüber hat, inwieweit die verbeiständeten Schuldner ihre Interessen selber wahrzunehmen imstande sind. Die Interessenabwägung muss deshalb bereits vorher, bei der Mitteilung der Verbeiständung an das Betreibungsamt, stattfinden und um so sorgfältiger vorgenommen werden.
Ist die Beistandschaft einmal dem Betreibungsamt mitgeteilt (oder veröffentlicht), so sind die Betreibungsurkunden auch dem Beistand zuzustellen.
Die Zuständigkeit für solche Mitteilungen (bzw. Veröffentlichungen) liegt bei der Vormundschaftsbehörde am Wohnsitz der verbeiständeten Person (§ 88 Einführungsgesetz zum ZGB in Verbindung mit Art. 375 Abs. 1 und Art. 397 Abs. 1 ZGB).
Sie bearbeitet die Vormundschaftsdaten zur Erfüllung ihrer Aufgaben und ist auch das für den Datenschutz verantwortliche Organ (§ 6 Abs. 1 DSG).
Eine entsprechende Mitteilung durch eine andere Behörde an das Betreibungsamt – etwa durch die Einwohnerkontrolle – ist unzulässig.

6. Listen mit gesuchten Fahrgästen

Datenaustausch zwischen Verkehrsbetrieben und Polizei

In verschiedenen Medienberichten wurde eine Liste der Verkehrsbetriebe Zürich (VBZ) mit dem Titel «Gesuchte Fahrgäste» zitiert respektive abgedruckt. Die Liste wurde ebenfalls dem Datenschutzbeauftragten zugestellt. Sie enthält Namen und Vornamen, Geburtsdatum und Bemerkungen zu offensichtlich «gesuchten» Fahrgästen. Nachdem die VBZ zu diesen Datenbearbeitungen Stellung bezogen hatte, liess sich der Datenschutzbeauftragte die Datenbearbeitung im System «Taxzu» der VBZ vorführen. In diesem System sind ca. 40 000 Personen mit Adressen und weiteren Angaben verzeichnet. Grundsätzlich stellte sich die

Frage, ob das Führen einer Datensammlung über die ohne gültigen Fahrausweis angetroffenen Personen und speziell das Führen einer darauf basierenden Liste mit gesuchten oder neu «speziellen Fahrgästen» durch eine genügende Rechtsgrundlage abgedeckt wird.
Rechtsgrundlage für die Fahrausweiskontrollen im Verkehrsverbund des Kantons Zürich ist § 17 Abs. 4 des Gesetzes über den öffentlichen Personenverkehr. Der Verkehrsverbund erlässt Richtlinien über den Fahrausweisverkauf und die Fahrausweiskontrolle. Deren Durchführung obliegt den Transportunternehmungen. Mit dieser Gesetzesgrundlage werden die Kontrollen und die Bearbeitung von Daten über Personen, die bei diesen Kontrollen ohne Fahrausweis angetroffen werden, abgedeckt.
In bezug auf die Verhältnismässigkeit der Datenbearbeitung ist indessen anzumerken, dass die Daten dieser Personengruppen nicht unterschiedlich lang aufzubewahren sind. Da insbesondere derjenige, der die Fahrtaxe bar bezahlt, nicht registriert wird, sind diejenigen Personen, welche die Taxe erst nachträglich bezahlen, auch nicht länger als notwendig mit ihren Personalien und dem entsprechenden Vorfall zu registrieren. Anders verhält es sich bei Personen, welche die Fahrtaxe und den Zuschlag nicht entrichten. Art. 150 StGB und Art. 51 Abs. 1 lit. b des Transportgesetzes stellen das Fahren ohne gültigen Fahrausweis auf Antrag unter Strafe. Während die Strafandrohung von Art. 150 StGB Gefängnis oder Busse ist, ist die Strafandrohung in Art. 51 Transportgesetz Busse. Personen, welche die Fahrtaxe nicht bezahlen, können somit durch die VBZ verzeigt werden. Solange ein solches Verfahren läuft und die Zahlung nicht eingegangen ist, sind entsprechende Angaben als geeignet und erforderlich zu betrachten. Sobald indessen eine Bezahlung erfolgt, die Antragsfrist (Art. 29 StGB) abgelaufen oder die Verfolgungsverjährung (Art. 70 StGB) eingetreten ist, sind nach dem Prinzip der Verhältnismässigkeit diese Angaben nicht mehr geeignet und notwendig.
Es ist nicht Aufgabe des Kontrolldienstes, Personen, die ihre Schulden den VBZ gegenüber nicht bezahlt haben oder in einem Strafverfahren wegen Fahrens ohne gültigen Fahrausweis stehen, anzuhalten. Wäre dies auch Aufgabe des Kontrolldienstes, wäre eine Identitätskontrolle sowohl bei Fahrgästen, die sofort bar bezahlen resp. die VBZ mit einem gültigen Fahrausweis benutzen, zumindest stichprobenweise als Teil der Tätigkeit gesetzlich zu verankern. Die Strafverfolgung ist indessen Sache der Strafverfolgungsbehörden, die über die entsprechenden Mittel verfügen. Das Führen einer Spezialliste ist deshalb zu beschränken auf Angaben zu Personen, die zweckdienlich sind, um eine Strafverfolgung einleiten zu können. Dies sind beispielsweise Fälle, bei denen Personen eine falsche Identität angegeben haben. Sofern solche Daten geeignet und erforderlich sind, müssen sie nach dem Prinzip der Integrität auch richtig sein. Die anlässlich des Augenscheins gemachten stichprobenweisen Überprüfungen gaben uns diesbezüglich zu Bedenken Anlass. Die uns vorgelegten Listen wiesen sowohl Angaben auf, die dem Prinzip der Verhältnismässigkeit als auch dem Prinzip der Integrität widersprachen.
Datenbekanntgaben erfolgen von den VBZ zu den Strafverfolgungsbehörden im Rahmen der gegen Schwarzfahrer angestrengten Verfahren. Hierzu bestehen ausreichende gesetzliche Grundlagen in Art. 51 Transportgesetz und Art. 150 StGB. Als Anzeigeerstatter werden die VBZ von den Strafbehörden auch über den Ausgang des Verfahrens informiert. Dies erfolgt aufgrund der einschlägigen Verfahrensgesetze. Im weiteren teilt die Polizei den VBZ die Personalien von Schwarzfahrern, die dieser zugeführt worden sind, mit. Art. 7 Abs. 2 des Bahnpolizeigesetzes ist hierzu ausreichende Rechtsgrundlage, wobei festzuhalten ist, dass die VBZ lediglich als Anzeigeerstatter im oben erwähnten Sinne zu betrachten sind.
Weitergehende Rechtsgrundlagen für eine Datenbekanntgabe der Stadtpolizei an die VBZ bestehen

nicht. Es sind keine Rechtsgrundlagen vorhanden, welche den Mitarbeiterinnen und Mitarbeitern des Kontrolldienstes weitere Kompetenzen in bezug auf die Verfolgung der zur Anzeige gebrachten Delikte oder weiterer Delikte einräumen würden. Insbesondere ist auch kein Raum für eine generelle Amtshilfe in diesem Bereich gegeben, da entsprechende gesetzliche Grundlagen, Mitteilungsrechte oder -pflichten, fehlen.
Aus den unterschiedlichen Angaben in den uns vorgelegten Listen mussten wir schliessen, dass ein regelmässiger Datenaustausch zwischen der Stadtpolizei und den VBZ zumindest stattfand.
Aufgrund dieser Feststellungen empfahlen wir, die Datenbearbeitungen über Fahrgäste ohne gültigen Fahrausweis an die datenschutzrechtlichen Bestimmungen anzupassen, insbesondere nur Daten zu bearbeiten, die geeignet und erforderlich sind, die Daten regelmässig auf ihre Richtigkeit zu überprüfen, nicht mehr benötigte Daten zu vernichten und keine über den Zweck der Kontrolle der Personen ohne gültigen Fahrausweis hinausgehenden Daten zu bearbeiten, vor allem keine polizeilichen Angaben für die polizeiliche Ermittlung und die Strafverfolgung zu führen und zu verwenden. Sowohl die VBZ wie die Stadtpolizei erklärten, ihre Datenbearbeitungen in diesem Bereich den datenschutzrechtlichen Bestimmungen anzupassen.

7. Wahrnehmung des Besuchsrechts

Durchbrechung einer Datensperre

Eine Jugend- und Familienberatungsstelle (eine Abteilung des Jugendsekretariats) verlangte bei einer Einwohnerkontrolle im Namen einer Privatperson eine Adressauskunft. Konkret wurde nach der Wegzugsadresse des Sohnes dieser Person gefragt. Dieser lebt nach der Scheidung der Eltern bei der Mutter und steht unter ihrer elterlichen Gewalt. Begründet wurde die Anfrage damit, dass der Vater das ihm zugesprochene Besuchsrecht wahrnehmen wolle. Die Mutter, die mit ihrem Sohn inzwischen ins Ausland weggezogen war, hatte eine Datensperre errichtet. Die Datensperre gilt nicht bei Anfragen von öffentlichen Organen. Da die Jugend- und Familienberatungsstelle jedoch im Namen und im Auftrag einer Privatperson handelte, war die Sperre grundsätzlich wirksam. Hingegen war zu prüfen, ob sie zu durchbrechen war. Die Bekanntgabe ist trotz Sperrung zulässig, wenn die gesuchstellende Person glaubhaft macht, dass die Sperre sie in der Verfolgung eigener Rechte gegenüber der betroffenen Person behindert (§ 11 Abs. 2 lit. b DSG). Ein durch gerichtlichen Entscheid eingeräumtes Besuchsrecht nach Art. 156 Abs. 2 in Verbindung mit Art. 273 ff. ZGB stellt ein «eigenes Recht» dar. Dieses Recht kann insbesondere durch Einreichen einer Kopie des Urteilsdispositivs bei der Einwohnerkontrolle glaubhaft gemacht werden. Fraglich war jedoch, ob die Einwohnerkontrolle eine im vorliegenden Fall erfolgte Begründung für die Errichtung der Datensperre in ihre Entscheidung mit einbeziehen musste.
Liegt ein rechtskräftiger Entscheid eines Gerichts vor, ist die Verwaltungsbehörde aufgrund der Gewaltentrennung daran gebunden. Dies ergibt sich aus dem Grundsatz, dass Justiz- und Verwaltungsbehörden gegenseitig die Entscheidungen der anderen Gewalt innerhalb deren Kompetenzbereich anerkennen. Will die betroffene Person die Ausübung des Besuchsrechts am Wohnort des Kindes verhindern, muss sie beim zuständigen Zivilgericht eine Abänderung des Scheidungsurteils erwirken. Die Verwaltungsbehörde darf nicht durch einen Entscheid oder ein faktisches Verhalten in den Urteilsspruch des Gerichts eingreifen. Aus diesem Grunde war der Wegzugsort des Sohnes bekanntzugeben.

8. Verdacht auf Kindsmisshandlung

Datenbekanntgabe aus Kinderhorten und -krippen

Die Frage, ob die verantwortlichen Personen einer kommunalen Kinderkrippe oder eines Horts bei Verdacht auf Kindsmissbrauch oder -misshandlung ihre Beobachtungen allenfalls einem Arzt mitteilen dürften, war differenziert zu beantworten. Massgeblich für die Bekanntgabe von Personendaten ist § 8 DSG, wonach entweder eine gesetzliche Grundlage, die Voraussetzungen der Amtshilfe oder eine Einwilligung der betroffenen Person vorliegen muss. Relevant sind im vorliegenden Fall § 60 des Einführungsgesetzes zum ZGB sowie § 20 der Strafprozessordnung, welche im Verdachtsfalle eine Benachrichtigung der Vormundschaftsbehörde respektive eine Anzeige bei den Organen der Strafverfolgungsbehörden vorsehen. Diese Aufzählung ist abschliessend, weshalb eine Mitteilung beispielsweise an einen Arzt oder Seelsorger oder der Beizug eines Jugendsekretariats nur dann statthaft wäre, wenn die betroffenen Personen respektive bei unmündigen Kindern die gesetzlichen Vertreter eingewilligt hätten. Angesichts der heiklen Situation (in der Regel liegt nicht mehr als ein blosser Verdacht vor) würden viele Krippen- und Hortverantwortliche einen weniger formellen Weg als denjenigen über die Vormundschaftsbehörde respektive die Strafverfolgungsorgane begrüssen. Hierfür bestehen jedoch keine Rechtsgrundlagen. Ausserdem wäre fraglich, ob jeder beliebig ausgewählte Arzt in bezug auf die besondere Thematik von Kindsmissbrauch und -misshandlung eine umfassende Beratung bieten könnte. Als Ausweg kann einem Arzt oder einer anderen geeigneten Person der Fall mit den relevanten Besonderheiten anonymisiert geschildert werden, da für die Erteilung von Ratschlägen und Hilfestellungen die Kenntnis des Namens des betroffenen Kindes nicht erforderlich ist.
Etwas anderes gilt nur, wo ein Arzt zum Team des Hortes oder der Krippe gehört. Denn hier ist einerseits für die gesetzlichen Vertreter von Anfang an transparent, wer im Bedarfsfalle beigezogen und infolgedessen nähere Kenntnis vom Kind und von seinen Lebensumständen erhalten wird. Andererseits kann ein Teammitglied in den Informationsfluss einbezogen werden, wenn und soweit es für seine spezifische Tätigkeit erforderlich ist.

9. Kommunales Behördenverzeichnis

Anforderungen an Erstellung und Verteilung

Eine Gemeinde, die periodisch ein Behördenverzeichnis herausgibt, erkundigte sich nach den Rahmenbedingungen aus datenschutzrechtlicher Sicht. Das Behördenverzeichnis enthält Namen, Adressen und Telefonnummern von Behördenmitgliedern, Funktionären, kommunalen Angestellten sowie von Kontaktpersonen von Vereinen, Parteien und weiteren Institutionen und Organisationen. Es wird an alle Angestellten der Gemeindeverwaltung sowie an private Dritte abgegeben.
Das Behördenverzeichnis stellt eine Bearbeitung von Personendaten dar und bedarf einer gesetzlichen Grundlage (§ 4 Abs. 1 DSG). Ein gewisses öffentliches Interesse an einem solchen Verzeichnis rechtfertigt die Bearbeitung selbst nicht, weshalb eine Rechtsgrundlage dafür zu schaffen ist. Soll das Behördenverzeichnis zudem nach extern abgegeben werden, hat sich die gesetzliche Grundlage auch über diese Datenbekanntgabe auszusprechen (§ 8 Abs. 1 DSG). Die Herausgabe von Adressbüchern und ähnlichen Nachschlagewerken unterliegt überdies detaillierten Sondervorschriften der Datenschutzverordnung (DSV), die insbesondere gelten, wenn Daten an einen Verleger oder eine Verlegerin zwecks Herausgabe eines solchen Verzeichnisses weitergegeben werden, aber auch zu

beachten sind, wenn das öffentliche Organ das Verzeichnis selbst herausgibt.
Gemäss § 5 Abs. 2 lit. c DSV dürfen in Staatskalendern, Behördenverzeichnissen und ähnlichen Nachschlagewerken Name, Vorname, Beruf, Titel, Grad, Jahrgang, Wohnort, Funktion, Eintritt in die Funktion sowie die Amtsadresse der Behördenmitglieder, Beamten und Angestellten aufgenommen werden. Die Aufnahme weiterer Daten wie genaue Privatadresse, private Telefonnummer usw. ist nur mit der ausdrücklichen Einwilligung der betroffenen Person zulässig. In Einzelfällen kann sich aus dem Dienstverhältnis eine Verpflichtung zur Aufnahme solcher Daten ins Behördenverzeichnis ergeben, z.B. bei einer Funktion, die eine dauernde Erreichbarkeit erfordert.
Die Aufnahme von Daten privater Dritter in das Verzeichnis richtet sich nach § 5 Abs. 2 lit. a DSV. Diese Bestimmung lässt für Adressbücher und ähnliche Nachschlagewerke Daten über Name, Vorname, Firma, Adresse, Beruf und Titel von natürlichen und juristischen Personen zu. Die betroffenen Personen und Organisationen haben ein uneingeschränktes Sperrecht und können verlangen, dass ihre Daten nicht in das Verzeichnis aufgenommen werden.
Das Behördenverzeichnis ist nach diesen Grundsätzen zu erstellen, und soweit notwendig sind entsprechende kommunale Rechtsgrundlagen zu schaffen.

10. Daten für Adressbücher

Nur vereinbarungsgemässe Nutzung

Datenbekanntgaben für Adressbücher dürfen nur von Amtsstellen erfolgen, die zur Bekanntgabe der Daten grundsätzlich ermächtigt sind. Der Verlag darf die Daten ausschliesslich zum Zwecke der Herausgabe des Adressverzeichnisses verwenden.
Die Datenbekanntgabe an Adressbuchverlage ist besonders geregelt in den §§ 5 und 6 Datenschutzverordnung (DSV). Daneben gelten die allgemeinen Grundsätze des DSG. Insbesondere ist das Gebot der Zweckbindung einzuhalten: Der Verlag darf die Adressauskünfte nur zum Bearbeitungszweck verwenden, das heisst konkret zur Herausgabe des betreffenden Adressverzeichnisses. Anschliessend muss er die Daten vernichten. Er darf sie also weder in seine Kundenkartei einspeisen noch anderen interessierten Personen weitergeben. Dem Verlag dürfen auch keine gesperrten Daten geliefert werden.
§ 5 Abs. 2 DSV bestimmt, welche Daten für Adressbücher und ähnliche Nachschlagewerke bekanntgegeben werden dürfen. Grundsätzlich können auch die Namen von Hauseigentümerinnen und -eigentümern zur Erstellung eines Häuserverzeichnisses herausgegeben werden.
Als datenliefernde Stelle kommt jedoch nur in Betracht, wer gemäss § 8 DSG durch eine Rechtsgrundlage oder die Einwilligung der betroffenen Personen ermächtigt ist. Ämter, welche einem Spezialgeheimnis unterstehen, dürfen keine Datenlieferungen vornehmen (§ 10 lit. b DSG). So dürfen insbesondere die Steuerämter keine diesbezüglichen Angaben weitergeben. Gemäss § 82 des Steuergesetzes gilt das Steuergeheimnis auch für Angaben über den Grundbesitz, welche das Steueramt im Rahmen seiner Aufgabenerfüllung bearbeitet. Es ist daher nicht befugt, an Verlage Auskünfte über die Eigentumsverhältnisse an Liegenschaften zu erteilen.
§ 6 DSV nennt die Punkte, welche in einer Vereinbarung zwischen der datengebenden Stelle und dem Verlag zwingend zu regeln sind. Als Grundlage für konkrete Vereinbarungen besteht ein Muster, das den Gemeinden vom Datenschutzbeauftragten zur Verfügung gestellt worden ist.
Die Frage der Entgeltlichkeit und die Höhe der Gebühren richten sich nach den einschlägigen Bestimmungen des Gebührenrechts. Dies sind die Verordnung über die Gebühren der Gemeindebehörden vom 8. Dezember 1966 sowie allfällige weitere kantonale und kommunale Erlasse.

11. Privilegierte Datenbekanntgabe zu Forschungszwecken

Daten über Arbeitslose und Ausländer

Mehrere Anfragen betrafen die Frage, unter welchen Rahmenbedingungen Personendaten für Forschungsvorhaben weitergegeben werden dürfen. Das DSG sieht erleichterte Voraussetzungen für Datenbearbeitungen vor, die zu nichtpersonenbezogenen Zwecken wie Forschung, Planung oder Statistik erfolgen (§ 12 DSG).

Ein öffentliches Organ darf Personendaten für Forschungszwecke bekanntgeben, sofern keine Geheimhaltungspflicht oder eine andere Bestimmung dies ausschliesst und Rückschlüsse auf die betroffenen Personen möglichst erschwert sind (§ 12 Abs. 2 lit. a und b DSG). Die Projektleitung muss Gewähr für die Einhaltung des Datenschutzes bieten und darf die Daten nur mit Zustimmung des verantwortlichen Organs weitergeben (§ 12 Abs. 2 lit. c DSG). Das verantwortliche Organ muss sich der Seriosität des Forschungsvorhabens vergewissern und bei Zweifeln überprüfen, ob die gemachten Angaben stimmen. Es erlässt eine Verfügung mit Auflagen oder schliesst eine Vereinbarung, womit die Projektleitung des Forschungsvorhabens verpflichtet wird, die Daten zu anonymisieren, sobald es der Zweck des Bearbeitens erlaubt (§ 12 Abs. 1 lit. a DSG), die Ergebnisse so zu veröffentlichen, dass die betroffenen Personen nicht bestimmbar sind (§ 12 Abs. 1 lit. b DSG), und angemessene Datensicherheitsmassnahmen zu treffen, insbesondere die Aufbewahrung und den Zugriff zu den Daten zu regeln (§ 4 Abs. 5 DSG; §§ 1 und 2 DSV). Eine Absicherung erfolgt durch die Vereinbarung einer Konventionalstrafe in angemessener Höhe. Die Auflage oder Vereinbarung sollte auch eine Verpflichtung enthalten, dass jede an der Forschung beteiligte Person einen Datenschutz-Revers unterzeichnet, mit dem sie sich zur Einhaltung der datenschutzrechtlichen Vorschriften verpflichtet.

Im konkreten Fall betraf eine Anfrage ein Forschungsprojekt mit Daten der Arbeitsvermittlung. Dabei sollten die Dossiers der Regionalen Arbeitsvermittlungszentren offengelegt werden. Das Arbeitsvermittlungsgesetz des Bundes enthält jedoch eine strenge Schweigepflicht mit wenigen Ausnahmen. Für nichtpersonenbezogene Zwecke dürfen Daten nur mit dem Einverständnis der betroffenen Personen oder in anonymisierter Form bekanntgegeben werden (Art. 57 Abs. 4 Arbeitsvermittlungsverordnung). Diese bundesrechtliche Bestimmung geht der kantonalrechtlichen Regelung in § 12 DSG vor. Der Rechtslage nicht zu genügen vermochte deshalb die vorgesehene Methode, dass die Forschenden die Dossiers vor Ort sichteten und Daten in anonymisierter Form erfassten. Dies wäre nur möglich, wenn die betroffenen Personen vorgängig ihre Einwilligung erteilt hätten, was jedoch nicht der Fall war.

Ein anderes Forschungsprojekt sah vor, aus den Einwohnerregistern verschiedener Gemeinden die Adressdaten von jugendlichen ausländischen Einwohnerinnen und Einwohnern (sog. «Zweit- bzw. Drittgeneration-Ausländer/-innen») zu ziehen, um mit ihnen Interviews durchzuführen. Die Personen sollten durch ein spezialisiertes Institut interviewt werden. Bei solchen Projekten kann naturgemäss keine anonymisierte Datenbekanntgabe erfolgen. Dies ist durch § 12 Abs. 2 lit. b DSG auch nicht zwingend vorgeschrieben. Hingegen muss die für die Forschung verantwortliche Person einen besonders sorgfältigen Umgang mit den Daten garantieren und insbesondere für eine sofortige Vernichtung der Personendaten nach der Durchführung der Befragungen besorgt sein. Bei der Befragung ist überdies ausdrücklich darauf hinzuweisen, dass die Teilnahme freiwillig ist und dass auch einzelne Antworten verweigert werden können. Durch den Beizug eines externen Instituts galt es zusätzlich, die Vorschriften über das Bearbeiten im Auftrag (§ 13 DSG) zu beachten.
Die Projektleitung des Forschungsvorhabens musste mit dem Institut eine Vereinbarung abschliessen, die den Zweck des Auftrags bestimmte und das Institut auf den Datenschutz verpflichtete.

Neue Herausforderungen für die Informatik

Der Betrieb von EDV-Systemen stellt zunehmend höhere Anforderungen an die Datensicherheit.

1. Datenspuren in EDV-Systemen

Personendaten in Internetzugangsservern

Der Betrieb von EDV-Systemen erfordert das Führen von Betriebsdaten. Soweit sich diese Daten einer bestimmten oder bestimmbaren Person zuordnen lassen, handelt es sich um Personendaten. Für das Bearbeiten dieser Daten sind deshalb die Voraussetzungen des Datenschutzgesetzes zu beachten (§ 4 ff. DSG). Die Tatsache, dass solche Daten immer wieder zur Überwachung und Kontrolle von Mitarbeiterinnen und Mitarbeitern ausgewertet wurden, führte zu einer generellen Empfehlung für diese Art der Datenbearbeitungen.

Grundsätzlich können drei datenschutzrechtlich relevante Kategorien von Daten unterschieden werden:

a) Daten zur Erfassung eines Benutzers (Authentifizierung, Autorisierung etc.): *Identifikationsdaten*.

b) Daten, die aus betrieblichen Gründen, beispielsweise unter dem Aspekt der Sicherheit, bearbeitet werden (Protokollierung, Log-Dateien etc.): *Sicherheitsdaten*.

c) Daten, die zur Abrechnung von EDV-Dienstleistungen benötigt werden (IT-Accounting): *Accountingdaten*.

Identifikationsdaten sind für die Erfüllung der Aufgabe des Betreibers eines EDV-Systems als notwendig zu betrachten und somit von der Rechtsgrundlage, welche die Aufgabe des EDV-Betreibers beschreibt, umfasst. Zu beachten gilt insbesondere das Prinzip der Zweckbindung, welches die Verwendung dieser Daten zu anderen Zwecken als für den Betrieb untersagt.

Gemäss § 4 Abs. 5 DSG in Verbindung mit §§ 1 und 2 Datenschutzverordnung (DSV) sind angemessene organisatorische und technische Sicherheitsmassnahmen zu treffen. Das Führen von Loggingdateien (Sicherheitsdaten) kann deshalb beim Betrieb von Internetzugangsservern als angemessene Massnahme bezeichnet werden. Nach dem Prinzip der Verhältnismässigkeit haben sich Loggingdateien auf die geeigneten und erforderlichen Daten zu beschränken. Eine Auswertung und Analyse dieser Daten (Audit) darf nur aus Gründen der Informatiksicherheit erfolgen. Nach dem Prinzip der Zweckbindung ist eine Auswertung nach Personen («Wer hat welche Ressourcen und Informationen benutzt?») grundsätzlich ausgeschlossen. Nur im Einzelfall können solche personenbezogenen Auswertungen vorgenommen werden, wenn sich ein sicherheitsrelevanter Vorfall ereignet hat oder wenn konkrete Anhaltspunkte für einen bevorstehenden Vorfall vorhanden sind und sie hierfür als geeignet erscheinen.

Die betroffenen Personen sind über solche Auswertungen zu informieren.

Die Aufzeichnung von Personendaten zur Gebührenverrechnung (Accountingdaten) muss in einer entsprechenden Rechtsgrundlage vorgesehen sein (Verordnung, evtl. Weisung). Für die kantonale Verwaltung besteht keine solche Rechtsgrundlage. Auf kommunaler Ebene ist die Rechtslage im Einzelfall abzuklären.

Dies bedeutet, dass ein IT-Accounting keine personenbezogenen Daten beinhalten darf. Dabei ist davon auszugehen, dass zwar an der Basis personenbezogene Daten entstehen können, je nachdem ob Accountingzahlen pro Anschluss oder pro Benutzer festgehalten werden, dass hingegen eine Auswertung nur anonym erfolgen darf. Da der Schuldner solcher IT-Leistungen nicht eine einzelne Person ist, sondern eine Abteilung oder Amtsstelle, welche im Regelfall keine Rechtspersönlichkeit besitzt, ist lediglich ein Total der IT-Leistungen pro Amtsstelle auszuweisen, ohne Details in bezug auf die Benutzung durch einzelne Personen. Eine andere Auswertung der Accountingdaten würde dem Prinzip der Zweckbindung widersprechen.

Die private Benutzung von Internetdienstleistungen (insbesondere E-Mail; WWW) ist grundsätzlich analog der Behandlung der privaten Telefongespräche zu betrachten. Auf kantonaler Ebene sind diese in einem bestimmten Umfang erlaubt, wobei in bezug auf die Gebührenverrechnung das Prinzip der

Selbstdeklaration gilt (§ 86 Vb BVO). Bei der privaten Benutzung von Telekommunikationseinrichtungen sind – solange das Prinzip der Selbstdeklaration der Gebühren gilt – keine Daten aufzuzeichnen. Da die private Benutzung von Internetdienstleistungen indessen nicht von der geschäftlichen zu unterscheiden ist, ergibt sich daraus auch die grundsätzliche Unzulässigkeit der personenbezogenen Auswertung von Accountingdaten.
Bei Missbrauch von Internetdienstleistungen bleiben Disziplinar- oder Strafverfahren vorbehalten. In disziplinarrechtlich relevanten Fällen (z.B. Verdacht auf übermässige Benutzung des Internets) ist der betroffene Mitarbeiter oder die betroffene Mitarbeiterin vorgängig über die Kontrolle zu informieren, was auch bedeutet, dass die Kontrolle nur für die Zukunft, nicht aber für die Vergangenheit angeordnet werden kann. Eine solche Kontrolle im Einzelfall könnte sich über eine Zeitdauer von einem bis drei Monaten erstrecken. Die Kontrolle hat sich grundsätzlich auf die Adresse der abgerufenen Seiten und E-Mails sowie auf die Verbindungsdauer bzw. Datenmenge zu beschränken.
Eine weitergehende Kontrolle oder eine Kontrolle ohne vorgängige Information der betroffenen Person ist nur unter Beachtung der strafprozessualen Anforderungen (insbesondere §§ 104 ff. StPO) zulässig. Dies kann in einem strafrechtlich relevanten Verhalten liegen (z.B. Verdacht auf Amtsgeheimnisverletzung). Dabei sind die verfahrensrechtlichen Bestimmungen der Strafprozessordnung massgebend.

2. Umgang mit Telefonverbindungsdaten

Anforderungen bei der Auswertung der Daten zur Gebührenverrechnung

Aufgrund eines Beschlusses des Regierungsrates werden die Telefongebühren den Amtsstellen weiterverrechnet (RRB 733/1997, Ziff. 3.4.8.). In diesem Zusammenhang war zu prüfen, wie die Aufzeichnung und die Auswertung von Daten der Telefonanlage unter den Aspekten des DSG zu erfolgen haben.
Die Telefonanlage der Zentralverwaltung ist mit der modernen ISDN-Technologie (ISDN = «Integrated Services Digital Network») ausgestattet. In einer solchen Anlage fallen verschiedene Daten an, insbesondere über die zustande gekommenen Verbindungen im Hinblick auf die Gebührenverrechnung. Erfasst werden Teilnehmernummer, Kostenstelle, Datum und Uhrzeit des Gesprächs, Gesprächsdauer (in Sek.), Netzknoten, angerufene Zielnummer, Impulse sowie Betrag (Kosten des Gesprächs). Diese Daten werden im System gespeichert und sind beliebig auswertbar.
Hierbei handelt es sich um Personendaten, da mittels Teilnehmernummern in der Regel eine Zuordnung zu den Personen möglich ist, die das Gespräch geführt haben. Die Auswertung von Daten über einen gewissen Zeitraum ermöglicht unter Umständen gar die Erstellung eigentlicher Kommunikationsprofile, welche als Persönlichkeitsprofile (§ 2 lit. e DSG) besonders zu schützen sind. Die Bearbeitung solcher Daten bedarf einer klaren Rechtsgrundlage (§ 5 lit. a DSG).
Der erwähnte Regierungsratsbeschluss stellt keine Rechtsgrundlage dar, der eine Bearbeitung von Personendaten erlaubt. Dies ist offensichtlich auch nicht gewünscht; vielmehr geht es um die Regelung der generellen Weiterbelastung der Telefonkosten an die Amtsstellen. In bezug auf die privaten Telefongespräche am Arbeitsplatz gilt § 86 der Vollziehungsbestimmungen zur Beamtenverordnung. Dieser legt fest, dass die private Benutzung von Telefon und Telefax, die einen angemessenen Umfang übersteigt, sowie Auslandsgespräche bzw. -faxe vergütungspflichtig sind. Der geschuldete Betrag wird periodisch von den Amtsstellen auf der Basis der Angaben der Mitarbeitenden eingezogen. Aufgrund des Prinzips der Selbstdeklaration ist keine

Aufzeichnung von Daten erforderlich.
Diese Rechtslage hat zur Folge, dass die Auswertungen nur in anonymisierter Form erfolgen und an die Amtsstellen weitergeleitet werden dürfen. Eine Erfassung nichtanonymisierter Grunddaten in der Telefonanlage ist erforderlich, um die Auswertungen überhaupt vornehmen und die Kosten weiterbelasten zu können. Für die Gebührenverrechnung darf indessen nur eine Auswertung in der Form erfolgen, dass pro Amtsstelle ein Total der Gebühren ausgewiesen wird. Ein darüber hinausgehender Detaillierungsgrad schafft einen Personenbezug und ist nur mit der Einwilligung der betroffenen Personen und im Einzelfall möglich.
Die in Frage stehenden Daten dienen zum Zweck der Gebührenverrechnung. Sie dürfen insbesondere nicht zur Überwachung des Arbeitsverhaltens der Mitarbeiterinnen und Mitarbeiter verwendet werden (Prinzip der Zweckbindung; § 4 Abs. 4 DSG). Vorbehalten bleiben Disziplinar- oder Strafverfahren, wenn das Verfahren einen Zusammenhang mit dem Telefonierverhalten aufweist. Kontrollen dürfen jedoch nur nach Information der betroffenen Person und für die Zukunft angeordnet werden und haben sich auf einen verhältnismässigen Zeitraum (einen bis drei Monate) zu beschränken. Darüber hinausgehende Kontrollen oder solche ohne vorherige Information sind nur zulässig, wenn die strafprozessualen Voraussetzungen für eine Telefonüberwachung erfüllt sind (§§ 104 ff. StPO).
Die in der Telefonanlage aufgezeichneten Daten sind zudem technisch und organisatorisch angemessen zu sichern und nicht länger als für den Zweck der Abrechnung notwendig aufzubewahren.
Für den Fall, dass die bestehende Rechtslage als unbefriedigend empfunden wird, empfahlen wir, eine entsprechende Rechtsgrundlage zu schaffen, welche die Art der aufgezeichneten Daten, den Zweck der Aufzeichnung, die Art der Daten einer Detailauswertung, die Voraussetzungen für die Weitergabe einer Detailauswertung sowie die Aufbewahrungsdauer der Daten regelt. Aus Gründen der Verhältnismässigkeit empfiehlt sich die Unterscheidung von Dienst- und Privatgesprächen durch Festlegung verschiedener Ausgänge (z.B. 0 für Dienst-, 9 für Privatgespräche). In diesem Fall wäre bei Dienstgesprächen eine Auswertung als Amtstotale und pro Anschluss (nur als Totale, nicht aber nach einzelnen Gesprächen) und deren Weitergabe an den Amtschef bzw. die Amtschefin zulässig. Daten über die Privatgespräche dürfen hingegen nur der betroffenen Person weitergegeben werden.
Zu berücksichtigen sind überdies die Besonderheiten bei Personen, die einem Berufsgeheimnis unterstehen.

3. Sicherheits-Check ausgewählter Netzwerkkomponenten

Überprüfung der Datensicherheit

In Zusammenarbeit mit der Finanzkontrolle und der internen Revision des Amts für Informatikdienste unterzogen wir ausgewählte Komponenten des kantonalen Netzwerkes (KZH-Netz) einer Sicherheitsüberprüfung. Dabei wurde ein neues Vorgehen im Rahmen der Aufsichtstätigkeit gewählt, das sich an aktuelle Bedrohungsszenarien selber anlehnt. Insbesondere ging es darum, neue Risiken und Schwachstellen rasch zu identifizieren.
Es wurden deshalb – mit einem bewusst limitierten finanziellen, personellen und zeitlichen Aufwand – Systeme mit sensiblen Daten kontrolliert attackiert, um Risiken und Schwachstellen aufzudecken. Mit der Beiziehung externer Spezialisten, die ein praxisbezogenes Know-how im Bereich der Bedrohungsrisiken aufweisen, liessen sich die Zielsetzungen dieser Vorgehensweise am besten erreichen.
Bei der «kontrollierten Netzwerk-Attacke» geht es neben der

Kontrolle einzelner sensibler Bereiche auch darum, das Sicherheitsbewusstsein in bezug auf den Schutz von Personendaten zu verbessern, indem man allfällige Sicherheitslücken möglichst prägnant aufzeigt. Die Reaktionen bei Angriffen bzw. die Frage, ob Angriffe überhaupt bemerkt und allenfalls eskaliert werden, sollten abgeklärt werden. Die Tätigkeiten erstreckten sich über etwa drei Monate.

Es waren drei Phasen geplant:
a) Angriffe über Daten- und Telefonnetze von aussen (ohne Insiderinformationen);
b) Angriffe über Datennetze von innen (mit Insiderinformationen);
c) Angriffe auf Rechner mit sensitiven Daten.

Die Angriffe über Daten- und Telefonnetze von aussen (Phase a) entsprechen der typischen Situation, wie sie sich irgendeinem Angreifer im globalen Netz stellt. Beispiele von Aktionen aus diesem Bereich sind:

- «Data Mining»: Welche Informationen zur Verwaltung sind über öffentliche Web-Server, Mailing-Listen, Newsgroups verfügbar? Das elektronische Profil der Verwaltung wird durch extensive Nutzung von Suchmaschinen erfasst.
- Zugriff auf die internen Netze: Gibt es Zugriffswege, welche nicht über die Firewalls führen? Gibt es Zugriffsmöglichkeiten über Modems bei internen Stellen?
- Verleitung zu Reaktionen auf E-Mails mit falschen Absenderadressen: Geben Leute Informationen preis, wenn sie mit E-Mail mit falschen Absenderadressen angesprochen werden?

Die Angriffe über die internen Datennetze (Phase b) entsprechen der Situation, wie sie Angestellte der Organisation antreffen. Hierzu sind folgende Möglichkeiten zu zählen:

- Studium der internen Netzstruktur (mit Insiderinformationen, Netzplänen) zur Identifikation neuralgischer Punkte.
- Messungen am internen Netz mit Netzwerkanalysatoren: Hier wurde direkt an den Netzen gemessen. Auf das vorerst geplante Plazieren von «Sniffer-Wanzen» wurde verzichtet, um den Aufwand zu minimieren.

Auf die Angriffe auf Rechner mit den in Phase b gefundenen Passwörtern (Phase c) wurde verzichtet, da sich das Schwergewicht der Untersuchung auf die Netze richtete und aus diesem Bereich für die Zielsetzung «Bewusstseinsbildung» schon genügend signifikante Ergebnisse vorlagen.

Bei allen diesen (beispielhaft) aufgeführten Punkten konnten aufgrund der Angriffe in bestimmten Bereichen Lücken festgestellt und Verbesserungen der Sicherheitskonzepte empfohlen werden. Signifikante Resultate gab es vor allem in den folgenden Bereichen:
1. Bei einer systematischen Suche nach Modems (Modem-Check von ausserhalb der Organisation) wurden Computer mit angeschlossenen Modems identifiziert, welche in keinem Inventar verzeichnet waren und zudem eine Login-Möglichkeit anboten.
2. Bei verschiedenen Systemen wurden im Hinblick auf die Detektion von Attacken Einwahlversuche vorgenommen, die – obwohl mehrere hundert Versuche erfolgten – lediglich im Einzelfall zu einer Reaktion seitens der Systemadministratoren führten.
3. Zufällig ausgewählte Mail-Benutzerinnen und -Benutzer erhielten Mails mit einem gefälschten Absender. Zirka ein Drittel der Benutzer antwortete innerhalb von 24 Stunden. Die Fälschung der E-Mails wurde von niemandem gemeldet (oder entdeckt?).
4. Bei Messungen am internen Netz (Sniffing) konnten innerhalb von zwei Stunden Mails von Entscheidungsträgern gelesen und Passwörter für Host-Systeme beschafft werden.

Generell konnte indessen festgehalten werden, dass die bisher getroffenen Sicherheitsmassnahmen einen guten Stand erreicht haben. Es drängen sich einzelne sicherheitstechnische Massnahmen auf, insbesondere ist aber die Bewusstseinsbildung für Sicherheitsrisiken zu verbessern.
Die Kontrolle unter Beiziehung

externer Spezialisten mittels der Methode der «kontrollierten Attacke» ersetzt nicht die kontinuierliche Überwachung und Kontrolle der Systeme und Datenbearbeitungen. Sie ergänzt die konventionelle Aufsichtstätigkeit des Datenschutzbeauftragten und ist einerseits als «Stichprobenmittel» zur Aufdeckung von Sicherheitslücken zu verstehen. Dabei ist klar festzuhalten, dass die Aussagen nicht umfassend sein können in bezug auf das Bestehen von Sicherheitslücken. Andererseits kann die «kontrollierte Attacke» durch externe Spezialisten hinsichtlich der Verbesserung des Sicherheitsbewusstseins sehr effizient sein, da sie den Beteiligten allfällige Schwachstellen realistisch vor Augen führt. Auch in Umgebungen, welche eine relativ hohe Sicherheit aufweisen, hat diese Prüfung mit verhältnismässig geringem Aufwand Resultate erbracht, welche viel zu dieser Bewusstseinsbildung beigetragen haben.
Interessanterweise deckten sich die Vorschläge, die sich aus den aufgedeckten Sicherheitslücken ergaben, mehrfach mit ohnehin geplanten oder sich in der Umsetzung befindenden Massnahmen.

4. Informatiksicherheitsverordnung setzt Rahmenbedingungen

Umsetzung von Sicherheitsmassnahmen

Die Informatiksicherheitsverordnung vom 17. Dezember 1997 setzt Richtlinien für die Umsetzung von Datensicherheitsmassnahmen in der kantonalen Verwaltung. Sie ist auch für Gemeinden verbindlich, sofern sie mit der kantonalen Verwaltung Daten austauschen.
Die Direktionen haben die Sicherheitsmassnahmen festzulegen und deren Umsetzung zu kontrollieren. Dabei ist jede Amtsstelle verpflichtet, eine Risikoanalyse ihrer Informatiksysteme vorzunehmen. Die Daten sind in drei Sicherheitsstufen einzuteilen, wobei jeweilen die konkreten Schutzziele zu ermitteln sind.
Die Sicherheitsstufen ergeben sich aufgrund der Sensibilität der bearbeiteten Daten respektive aufgrund der möglichen Negativfolgen. Die Risikobeurteilung der Informatiksysteme und -anwendungen ist hierfür die Basis. Neben datenschutzrechtlichen Kriterien werden auch weitere rechtliche und betriebswirtschaftliche Faktoren berücksichtigt.
Eine Einteilung der Daten in die jeweiligen Schutzstufen hat entsprechende Sicherheitsmassnahmen zur Folge. Dabei haben die Amtsstellen einen Plan vorzulegen, mit welchen organisatorischen und technischen Massnahmen die Schutzziele pro Sicherheitsstufe erreicht werden.
Die Arbeitsgruppe für Planung und Steuerung der Informatik (AGIK) erlässt Richtlinien über die Konkretisierung der Schutzziele. Sie legt aber auch Mindestanforderungen an die Sicherheitsmassnahmen pro Sicherheitsstufe fest. Die Sicherheitsmassnahmen haben dem Stand der Technik zu entsprechen und müssen in bezug auf die definierten Schutzziele verhältnismässig sein.
Mit der Informatiksicherheitsverordnung, welche für die elektronische Bearbeitung sämtlicher Daten der Verwaltung gilt, werden auch die datenschutzrechtlichen Anforderungen an die Sicherheit der Datenbearbeitungen konkretisiert. Neben den weiteren Fachstellen der Verwaltung unterstützt auch der Datenschutzbeauftragte die Amtsstellen bei der Umsetzung der neuen Richtlinien.
Ein wesentlicher Punkt der Informatiksicherheitsverordnung ist auch die Verpflichtung der Direktionen und Amtsstellen, die Umsetzung und Einhaltung der Sicherheitsmassnahmen regelmässig durch unabhängige Stellen überprüfen zu lassen. Die Finanzkontrolle und der Datenschutzbeauftragte können in diese Berichte Einsicht nehmen.

5. «Espresso» – kein kalter Kaffee

«Sourcing-Projekt» der kantonalen Verwaltung

Der Regierungsrat hatte Ende 1996 beschlossen, die Verwaltungsinformatik einer generellen Strukturüberprüfung zu unterziehen. Im Vordergrund standen dabei die Fragen der Zentralisierung respektive Dezentralisierung der Informatik sowie der Zusammenarbeit mit externen privaten Unternehmen oder anderen öffentlichen Verwaltungen. Das Projekt «Espresso» wurde mit einer Machbarkeitsstudie abgeschlossen. Aus datenschutzrechtlicher Sicht von Interesse waren vor allem Fragen der Auslagerung der Informatik und der Kooperation mit anderen Verwaltungsstellen. Diese Formen sind als Datenbearbeitung im Auftrag zu qualifizieren, wofür § 13 DSG Rahmenbedingungen aufstellt. Sofern die Datenbearbeitung durch Dritte nicht durch gesetzliche Schranken ausgeschlossen ist, ist sie datenschutzrechtlich grundsätzlich zulässig. Dabei ist der Datenschutz durch Auflagen, Vereinbarungen oder auf andere Weise zu garantieren, wie wenn das verantwortliche Organ diese Daten selber bearbeiten würde. Spezielle Bedeutung erlangen bei diesen Konstellationen die Datensicherheitsmassnahmen. Bei einer Auslagerung der Datenbearbeitung ist hierfür tendenziell von einem grösseren Aufwand auszugehen, um das unbefugte Bearbeiten (Kenntnisnahme durch unbefugte Dritte, Veränderungen der Daten etc.) verhindern zu können. Eine abschliessende Beurteilung von Auslagerungen oder Kooperationen ist nur im Einzelfall möglich, unter Kenntnis der Art und Weise der Datenbearbeitung und der geplanten rechtlichen, technischen und organisatorischen Massnahmen. Der Regierungsrat hat entschieden, das Projekt weiter zu detaillieren.

Ausweitung des Informationsangebots

Die Umsetzung der Anliegen des Datenschutzes und der Datensicherheit wird unterstützt mit aktuellen themenspezifischen Informationen.

1. Aktuelle Informationen im Internet
Homepage des Datenschutzbeauftragten

Mit dem Aufbau eines Informations- und Beratungsangebots im Internet konnte einem wachsenden Bedürfnis nach aktuellen Informationen begegnet werden. Gemeindebehörden, kantonale Verwaltungsstellen, Privatpersonen und weitere interessierte Kreise können sich auf der Homepage über Fragen des Datenschutzes informieren und erhalten eingehende Berichte zu ausgewählten Themen. Des weiteren bietet die Homepage Hinweise auf themenspezifische Informationsquellen zu Datenschutz und Informationssicherheit. Zusätzlich ist es möglich, sich via Internet direkt an den Datenschutzbeauftragten zu wenden, um Fragen und Anliegen vorzubringen. Bereits in den ersten Monaten hat sich gezeigt, dass die wachsende Zahl der Internet-Benutzerinnen und -Benutzer diese Dienstleistungen zunehmend in Anspruch nimmt. Eine (anonyme) Auswertung der Zugriffe zeigt, dass die aktuellen Meldungen und Publikationen oft angewählt werden. Des weiteren benutzen sowohl private Personen als auch Verwaltungsstellen die Möglichkeit, sich per E-Mail an den Datenschutzbeauftragten zu wenden.

Homepage:
http://www.ktzh.ch/dsb

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

2. Konzepte und Technologien für einen wirksamen Datenschutz

Zweites Symposium für Datenschutz und Informationssicherheit

Zum zweiten Mal haben der Datenschutzbeauftragte und das Departement Informatik der Eidgenössischen Technischen Hochschule (ETH) das Symposium für Datenschutz und Informationssicherheit veranstaltet. Am 11. September 1997 trafen sich erneut rund 250 Teilnehmerinnen und Teilnehmer, um sich über «Konzepte und Technologien für einen wirksamen Datenschutz» zu informieren. Die Verlagerung der Kommunikation auf elektronische Mittel, insbesondere das Internet, stellt Herausforderungen an die Sicherstellung der Authentizität und Geheimhaltung von Informationen. Das Symposium widmete die thematischen Schwerpunkte den technischen und rechtlichen Aspekten der digitalen Signatur und der Verschlüsselung, den neuen Herausforderungen an die Datenschutzkonzepte sowie der Frage der Verantwortung für den Datenschutz und die Datensicherheit. Nebst den Veranstaltern referierten Vertreter von Datenschutzbehörden, Wirtschaft und Wissenschaft aus dem In- und Ausland. Als besonderer Gast konnte der weltbekannte Kryptologie-Spezialist Phil Zimmermann aus den USA gewonnen werden, der als erster ein von ihm entwickeltes Verschlüsselungsprogramm (PGP) unentgeltlich im Internet verfügbar machte. Die grosse Teilnehmerzahl am Symposium widerspiegelt die zunehmende Bedeutung von Datenschutz und Informationssicherheit in unserer Gesellschaft und entspricht einem grossen Bedürfnis nach Informationen in diesem Bereich. Das 3. Symposium wird am 29. Oktober 1998 wiederum an der ETH stattfinden.

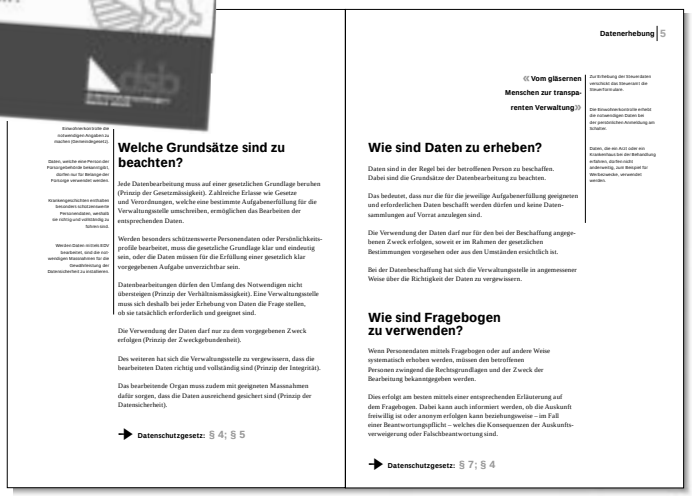
3. Zusammenarbeit der Datenschutzbeauftragten

Kantonale und kommunale Arbeitsgruppen

Die Zusammenarbeit mit kantonalen und kommunalen sowie dem eidgenössischen Datenschutzbeauftragten konnte weiter verstärkt werden. Erstmals trafen sich kommunale Datenschutzbeauftragte mit dem kantonalen Datenschutzbeauftragten im Rahmen einer Arbeitsgruppe. Dabei konnten Themen von aktuellem Interesse für die Gemeinden behandelt werden. Der Nutzen dieses Informationsaustausches war offensichtlich, und es wurde deshalb beschlossen, diese Sitzungen zu institutionalisieren. Sie stehen grundsätzlich allen kommunalen Datenschutzbeauftragten und Datenschutzberaterinnen und -beratern offen.
Die Zusammenarbeit auf nationaler Ebene war fokussiert auf Fragen des Datenschutzes im Gesundheitswesen. Die IV. Nationale Konferenz der Datenschutzbeauftragten, welche vom Kanton Tessin in Bellinzona organisiert wurde, verabschiedete hierzu eine Resolution (siehe S. 21). Weiter wurde beschlossen, themenspezifische Arbeitsgruppen einzusetzen. Dabei liegen die Schwerpunkte zurzeit bei Fragen der Auswertung von Datenspuren im Bereich der Telekommunikation, der systematischen Weitergabe von Personendaten sowie der Strukturierung der Aufsichts- und Kontrolltätigkeit der Datenschutzbeauftragten im Rahmen von Datenschutzreviews.

4. «In punkto Datenschutz» – die neue Informationsbroschüre
Publikationen des Datenschutzbeauftragten

Auch 1997 konnten wieder vier Nummern unserer Zeitschrift «Fakten» herausgegeben werden. «Fakten» 4/1997 beinhaltet die Informationsbroschüre «In punkto Datenschutz». Die Broschüre richtet sich sowohl an interessierte Personen als auch an Behörden und Verwaltungsstellen und gibt Antworten auf Fragen zum Datenschutz. Mit Beispielen und Illustrationen soll sie jedermann einen schnellen und leicht verständlichen Zugang zur Thematik des Datenschutzes und zu seiner rechtlichen Ausgestaltung im Kanton Zürich ermöglichen. Eine weitere Sondernummer («Fakten» 3/1997) enthält «Beiträge '97 zum Datenschutz». Die Autoren beschäftigen sich mit der Verantwortung im Datenschutz, neuen Herausforderungen für das bestehende Datenschutzkonzept, der datenschutzrechtlichen Aufsicht, dem deutschen Gesetz zur digitalen Signatur und der Kryptographie. «Fakten» 1/1997 thematisiert die Auftragsdatenbearbeitung durch Dritte. Schwerpunkt von «Fakten» 2/1997 bilden Controlling, Haushalts- und Geschäftsprüfung in der Gemeindeverwaltung. Dem wachsenden Bedürfnis nach praxisbezogener Information soll «Fakten» in Zukunft weiter entsprechen.



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

Ausarbeitung datenschutzkonformer Lösungen

Themen und Sachverhalte, die bereits in früheren Tätigkeitsberichten aufgegriffen wurden, haben sich weiterentwickelt.

1. Sperrecht im Steuerwesen

Neue Bestimmungen des Steuergesetzes

Am 1. Januar 1999 tritt das neue Steuergesetz in Kraft. Damit wird das voraussetzungslose Sperrecht der Steuerpflichtigen formellgesetzlich anerkannt. Die im Tätigkeitsbericht Nr. 2 [1996], S. 41, aufgezeigte Problematik besteht nicht mehr, da einerseits die Steuerämter aufgrund eines am Bundesgericht noch hängigen Verfahrens 1997 ihre Praxis geändert haben und Datensperren (vorläufig) entgegennehmen und andererseits mit dem neuen Steuergesetz eine klare Rechtslage geschaffen wurde.
In bezug auf die Modalitäten der Datensperre nach neuem Recht, die in einer Weisung der Finanzdirektion festgehalten werden sollen, haben wir Stellung bezogen. Insbesondere betonten wir, dass ein Sperrecht auf schriftliches Begehren der betroffenen Person voraussetzungslos zu gewähren ist und nicht von irgendwelchen Bedingungen abhängig gemacht werden kann.
Eine Durchbrechung der Sperre ist nur möglich, wenn eine auskunftsersuchende Person glaubhaft macht, dass die Sperrung sie in der Verfolgung eigener Rechte behindert (§ 11 Abs. 2 lit. b DSG). Voraussetzung sind somit das Bestehen eigener Rechte sowie eine Behinderung in deren Geltendmachung durch die Datensperre. Mit anderen Worten darf die Sperre nur durchbrochen werden, wenn die anfragende Person ohne Auskunft des Steueramtes nicht oder nur mit unverhältnismässigem Aufwand zu ihrem Recht kommen könnte. Deshalb sind beim Vorliegen einer Datensperre keine Steuerausweise auszustellen, wenn jemand mit dem Steuerpflichtigen lediglich in wirtschaftlichem Kontakt steht respektive solchen aufnehmen will. Sowohl Gläubiger wie Inkassobüros können unabhängig von der Auskunft des Steueramtes betreibungsrechtlich vorgehen. Kreditinstitute können einen Steuerausweis ohne weiteres bei den Steuerpflichtigen selber erhalten. Des weiteren ist darauf hinzuweisen, dass auch nicht gesperrte Steuerdaten nicht ohne jegliche Abklärungen herauszugeben sind. Vielmehr ist aufgrund von § 10 DSG vor jeder Datenbekanntgabe vom verantwortlichen Organ das Entgegenstehen öffentlicher oder offensichtlich schützenswerter Privatinteressen zu prüfen.

2. Detaillierte Regelungen im Personalrecht

Entwurf der Vollzugsverordnung zum Personalgesetz

Die Gesetzgebungsarbeiten für das neue Personalrecht des Kantons Zürich sind weiter vorangeschritten. Wir hatten bereits früher in einer Arbeitsgruppe zum Personalgesetz mitgewirkt (siehe Tätigkeitsbericht Nr. 1 [1995], S. 14). Detaillierte Bestimmungen über den Umgang mit Personendaten wurden nun auch in den Entwurf der Verordnung über den Vollzug des Personalgesetzes aufgenommen. Insbesondere konnten der Umfang und der Umgang mit den Personaldossiers sowie die Beschaffung und Bekanntgabe von Personaldaten von beziehungsweise an Dritte geregelt werden. In bezug auf die Aufbewahrung der Personalakten nach Austritt einer Person wurde festgehalten, dass nur mehr die notwendigen und geeigneten Daten aufzubewahren sind und diese nach Ablauf einer Aufbewahrungsfrist von zehn Jahren entweder zu vernichten oder dem Staatsarchiv zu übergeben sind. Weiter wurden Bestimmungen über die EDV-geführten Personalinformationssysteme aufgenommen und die Datenbearbeitung bei der Benutzung technischer Einrichtungen wie Telefon oder EDV-System geregelt. Insgesamt ergibt das Kapitel «Datenschutz» im Entwurf der Vollzugsverordnung eine sachgerechte und angemessene Antwort auf die diesbezüglichen Fragen im Arbeitsbereich.

3. Angepasster Bedarfsplan für Spitex-Basisdienste

Beschränkung auf die geeigneten und erforderlichen Angaben

Der Bedarfsplan für Spitex-Basisdienste, der uns bereits früher beschäftigte (siehe Tätigkeitsbericht Nr. 2 [1996], S. 33), konnte in Zusammenarbeit mit der Gesundheitsdirektion jetzt in eine Fassung gebracht werden, die einerseits unter den gegebenen Verhältnissen umgehend realisierbar war und andererseits die datenschutzrechtlichen Erfordernisse wie auch die pflegerischen Bedürfnisse berücksichtigte. Gleichzeitig wurden wir informiert, dass Bestrebungen im Gange sind, für die ganze Schweiz ein einheitliches Formular zur Erfassung der im Einzelfall erforderlichen Spitex-Pflege- und -Betreuungsleistungen zu kreieren. Wir wandten uns daher an den Spitex Verband Schweiz mit dem Hinweis, dass die Spitex-Organe im Kanton Zürich in allen ihren Datenbearbeitungen den Grundsätzen des kantonalen Datenschutzgesetzes unterstünden. Ebenfalls stellten wir klar, dass bei einer grundlegenden Neufassung der entsprechenden Spitex-Unterlagen die Anforderungen des Datenschutzes in vollem Umfang berücksichtigt werden müssten.

4. Datenbearbeitungen im kirchlichen Bereich

Erste Ergebnisse der Arbeitsgruppe

Anfang 1997 konnte der Entwurf für ein kirchliches Datenschutzreglement als Resultat diverser Arbeitssitzungen (vgl. Tätigkeitsbericht Nr. 1 [1995], S. 20 f., und Nr. 2 [1996], S. 32 f.) in eine von allen beteiligten Stellen akzeptierte Fassung gebracht werden.

Es zeigte sich jedoch, dass bei gewissen Formulierungen, insbesondere bezüglich der Bekanntgabe von Daten über Angehörige eines Kirchenmitgliedes, das einer anderen oder keiner Konfession angehört, sowie bezüglich des zwischenkirchlichen Datenaustausches offene Fragen bestanden. Sie betreffen die Auslegung der gesetzlichen Grundlagen und die Tragweite der kirchlichen Autonomie. Die beiden beteiligten Kirchen gaben deshalb ein Gutachten in bezug auf die für die Kirchen offenen Gestaltungsspielräume in Auftrag.

Das Gutachten ergab einen Handlungsbedarf in bezug auf die beiden Kirchenordnungen. Daher sollen so bald als möglich in einem neuen Datenschutzartikel die Grundlagen für das geplante kirchliche Datenschutzreglement geschaffen werden. Ebenfalls durch das Gutachten wurde bewirkt, dass der Entwurf zu einem Datenschutzreglement vorerst der Direktion des Innern als der für die Aufsicht über die Kirchen zuständigen Instanz zur Stellungnahme unterbreitet werden soll.

In bezug auf die zwischen Schule und Kirche auszutauschenden Daten setzte im Juli 1997 ein Schreiben der Erziehungsdirektion Richtlinien: Es stellte fest, dass Klassenlisten mit den Namen der konfessionsangehörigen Schülerinnen und Schüler an die Kirchenpflegen abgegeben werden könnten. Ebenfalls sei zulässig, den Eltern bei Abmeldung eines Kindes vom gemischtkonfessionellen Religionsunterricht («Kokuru») ein von den Kirchen vorbereitetes Schreiben zuzustellen, worin über die allfälligen kirchenrechtlichen Konsequenzen dieses Schrittes informiert werde. Als eindeutig nicht datenschutzkonform wurde dagegen die Abgabe von vollständigen Klassenlisten an die Kirchenpflegen sowie die Bekanntgabe der Namen der vom «Kokuru» abgemeldeten Kinder an die Kirchen bezeichnet. Damit sind die von uns empfohlenen Grundsätze den Schul- und Kirchenpflegen gegenüber kommuniziert worden.

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

Datenschutzbeauftragter:
Dr. iur. Bruno Baeriswyl

Juristische Sekretärin:
Dr. iur. Esther Knellwolf

Auditor:
lic. iur. Marco Fey

Sekretariat:
Regula Rüeger

Tätigkeitsbericht Nr. 3 (1997)
ISSN 1422-5816

Konzeption und Produktion:
Frontpage AG, Zürich

Druck:
KDMZ
Gedruckt auf Recyclingpapier

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