Tätigkeits-Bericht

Nr. 1

Datenschutzbeauftragter des Kantons Zürich

1995

Der Datenschutzbeauftragte
erstattet dem Regierungsrat
jährlich oder nach Bedarf einen
Bericht über seine Tätigkeit
(§ 23 Datenschutzgesetz). Der
vorliegende Bericht deckt den
Zeitraum vom 1. Januar 1995
bis 31. Dezember 1995 ab.

Zürich, Februar 1996

Der Datenschutzbeauftragte
des Kantons Zürich
Dr. iur. Bruno Baeriswyl

Inhaltsverzeichnis

I. Bilanz	Ein Jahr Datenschutzgesetz im Kanton Zürich	4
II. Kanton	1. Datenschutz im Gesundheitswesen	10
	2. Vollzug des Krankenversicherungsgesetzes	10
	3. Datensperre für Motorfahrzeughalter	11
	4. Steuerausweise und Privatsphäre	12
	5. Personalanmeldebogen	13
	6. Personalgesetz 97	14
	7. Abgrenzung Akteneinsichts- und Auskunftsrecht	15
III. Themen	1. Zugriff auf Einwohnerkontrolldaten	16
	2. Zugriffe auf die Daten des Handelsregisteramts	17
IV. Gemeinden	1. Daten für wissenschaftliche Forschung	18
	2. Publikation von Neuzuzügern	18
	3. Verwandtschafts- und Untermietverhältnisse	19
	4. Gratulationen zu Jubiläen	20
	5. Daten für die Kirchgemeinden	20
	6. Fragebogen für Wochenaufenthalter	21
	7. Schulpsychologische Dienste	22
	8. Verwaltungsinterne Amtshilfe	23
	9. Personendaten auf Stimmrechtsausweis	25
	10. Fragebogen beim Spitaleintritt	26
	11. Überprüfung von Gemeindereglementen	26
V. Datensicherheit	1. Informatikstrategie und Datensicherheit	28
	2. Sicherheit in Datennetzen	28
	3. Datenverschlüsselung bei der Direktion der Justiz	28
	4. Anschluss des kant. Netzwerkes an das Internet	29
	5. Vernichtung elektronischer Daten	29
	6. Vernichtung von Akten mit Personendaten	30
	7. Datenaufzeichnungen in Telefonanlagen	31
VI. Information	1. «Fakten» – Zeitschrift für Datenschutz	32
	2. Seminare zum Datenschutz	33
	3. Referate zum Datenschutz	33
	4. Telefonische Beratungen	33
	5. Zusammenarbeit der Datenschutzbeauftragten	34

Ein Jahr Datenschutzgesetz im Kanton Zürich

Mit dem Datenschutzgesetz, welches am 1. Januar 1995 in Kraft getreten ist, haben die Bürgerinnen und Bürger des Kantons Zürich den öffentlichen Organen von Gemeinden und Kanton einen klaren Auftrag erteilt, die Persönlichkeitsrechte zu wahren.

Das Datenschutzgesetz (DSG) hält fest, dass für den Datenschutz dasjenige Organ verantwortlich ist, das die Personendaten zur Erfüllung seiner Aufgaben bearbeitet oder bearbeiten lässt (§ 6 DSG). Der Datenschutzbeauftragte hat die Aufgabe, die Anwendung der Vorschriften über den Datenschutz zu überwachen und die verantwortlichen Organe in allen Fragen des Datenschutzes und der Datensicherheit zu beraten. Des weiteren erteilt er den betroffenen Personen Auskunft über ihre Rechte und vermittelt zwischen ihnen und den Verwaltungsstellen bei Differenzen in bezug auf Datenbearbeitungen. Er orientiert ausserdem die verantwortlichen Organe über wesentliche Anliegen des Datenschutzes und erstattet dem Regierungsrat jährlich oder nach Bedarf Bericht (§ 23 DSG).
Die vorliegende Berichterstattung umfasst den Zeitraum von Januar bis Dezember 1995. Es handelt sich damit um die ersten zwölf Monate nach Inkrafttreten des Datenschutzgesetzes. In dieser Zeit haben sich die ersten Konturen des Gesetzes bei der Umsetzung in die Praxis gezeigt. Unsere Tätigkeiten in dieser Zeitspanne lassen einige generelle Feststellungen zu.

Bedürfnis nach Information

Es hat sich rasch gezeigt, dass das Bedürfnis nach praxisbezogener Information im Bereich der Persönlichkeitsrechte bei den Verwaltungsstellen sehr gross ist. Die Umsetzung der Anliegen des Persönlichkeitsschutzes, welche bereits vor Inkrafttreten des Datenschutzgesetzes vor allem durch die Rechtsprechung des Bundesgerichtes vorgezeichnet war, bereitete teilweise erhebliche Mühe. Es galt, die Interessen der betroffenen Personen, über welche Daten durch die Verwaltung bearbeitet werden, in die konkreten Entscheidungsabläufe bzw. Interessenabwägungen der einzelnen Verwaltungsstellen zu integrieren. Das Datenschutzgesetz bietet hierzu die Rahmenbedingungen. Dabei konnten in einzelnen Verwaltungsbereichen klare Richtlinien für die Umsetzung des Datenschutzgesetzes festgelegt werden (z.B. Datenbekanntgabe durch die Einwohnerkontrollen), während andere sensible Bereiche der Datenbearbeitung (z.B. Gesundheitsbereich) noch auf diese Umsetzung warten. Durch gezielte Informationen mittels Rundschreiben und Publikationen sowie dem Angebot von Referaten und Seminaren ist es gelungen, die kantonalen und kommunalen Verwaltungsstellen anzusprechen und zumindest einen Anstoss für die Anliegen des Datenschutzes zu geben.

Anfragen von Bürgerinnen und Bürgern

Praktisch täglich gehen mehrere telefonische oder schriftliche Anfragen von Bürgerinnen und Bürgern ein. In vielen Fällen lassen sich Anfragen, welche insbesondere

Auskünfte bezüglich der Voraussetzungen von Datenbearbeitungen oder individueller Rechte nach dem Datenschutzgesetz betreffen, unmittelbar beantworten. Es ist festzustellen, dass die wenigsten Bürgerinnen und Bürger dabei zwischen Datenbearbeitungen durch die öffentliche Verwaltung und durch private Organisationen oder Personen unterscheiden, d.h. den unterschiedlichen Geltungsbereich von Bundesgesetz und kantonalem Gesetz sowie die damit verbundene Kompetenzaufteilung zwischen dem eidgenössischen und dem kantonalen Datenschutzbeauftragten kennen oder verstehen. Durch die Aufklärung der betroffenen Personen versuchen wir dabei, Klarheit zu schaffen. In diesem Zusammenhang ist anzumerken, dass sich im Bereich der Europäischen Union (EU) eine Rechtsentwicklung in bezug auf eine Vereinheitlichung der Datenschutzkonzepte des öffentlich-rechtlichen und des privatrechtlichen Bereichs abzeichnet, welche auch entsprechende Auswirkungen auf die Konzeption der Aufsicht über den Datenschutz mitbeinhaltet.
In materieller Betrachtung zeigen sich bei den Auskunfts- und Vermittlungsbegehren der einzelnen Bürgerinnen und Bürger drei Schwerpunkte:

1. Auskunftsrecht

In zahlreichen Fällen wird bemängelt, dass von den Verwaltungsstellen keine oder eine unvollständige Auskunft über die Daten, welche die gesuchstellende Person betreffen, erteilt wird. Gemäss § 17 DSG kann jede Person vom verantwortlichen Organ Auskunft verlangen, welche Daten über sie in dessen Datensammlung bearbeitet werden. Einschränkungen dieser Auskunft sind im konkreten Einzelfall möglich, wenn eine gesetzliche Bestimmung, überwiegende öffentliche Interessen oder überwiegend schützenswerte Interessen Dritter dies verlangen (§ 18 DSG).
Wir stellten fest, dass zahlreiche Verwaltungsstellen ohne formell und materiell zutreffende Begründung diese Auskunft ablehnen. Die Respektierung dieses Individualrechts gehört indessen zu den Grundanliegen des Datenschutzes. Soweit wie möglich wirkten wir auf eine gesetzeskonforme Handhabung des Auskunftsrechts bei den betroffenen Verwaltungsstellen ein.

2. Recht auf Datensperrung

Im weiteren gab die Möglichkeit der Datensperre durch die betroffenen Personen zu Anfragen Anlass. Auf Gemeindeebene, insbesondere bei den Einwohnerkontrollen, konnte in einzelnen Kontakten das Recht auf Sperrung geklärt werden. Die Frage, wie bei Vorliegen einer Datensperre die Auskunft zu erteilen ist, wenn eine gesuchstellende Person oder Organisation glaubhaft macht, dass die Sperrung sie in der Verfolgung eigener Rechte gegenüber der betroffenen Person behindert, gab zudem zu Schwierigkeiten in der Praxis Anlass. Eingehende rechtliche Abklärungen verlangte die von Bürgerinnen und Bürgern gewünschte Datensperre bezüglich der Motorfahrzeughalterangaben und der Steuerausweise (siehe S. 11 und 12).

3. Aufbewahrung von Daten

Die Aufbewahrung resp. Vernichtung von Daten bildete einen weiteren Schwerpunkt der Anfragen. Dabei stellte sich heraus, dass gerade in sehr sensiblen Bereichen der Datenbearbeitung (z.B. im Gesundheitswesen) ein grosses Misstrauen in der Bevölkerung besteht, dass Daten in unbefugte Hände gelangen könnten. Insbesondere Krankengeschichten mit heiklen Diagnosen werden als Risiko für Persönlichkeitsrechtsverletzungen betrachtet. In einem Fall, der uns vorgelegt wurde, führte die Verwechslung von Patientennamen bei einer Rechnungsstellung mit Angaben der Diagnosen dazu, dass die Rechnung an einen falschen Patienten mit gleichem Namen gesandt wurde. Dabei zeigte sich, dass Daten über den falschen Rechnungsempfänger in diesem Spital vorhanden waren, obwohl er sich dort nie behandeln liess. Sie stammten von einer Laboruntersuchung, die der Hausarzt früher einmal bei diesem Spital in Auftrag gegeben hatte. Es ist verständlich, dass bei einem fehlenden Vertrauen die betroffenen Personen – wo möglich – die Herausgabe oder Vernichtung ihrer Daten verlangen. Der Datenschutzbeauftragte interveniert dabei einerseits im konkreten Einzelfall (siehe S. 22), und andererseits versucht er, die verantwortlichen Organe auf ihre Verpflichtungen in bezug auf den Datenschutz hinzuweisen.

Auf einen Blick

Die kantonalen und kommunalen Verwaltungsstellen hatten 1995 erstmals die neue Datenschutzgesetzgebung anzuwenden. Es zeigte sich, das ein grosses Bedürfnis nach Informationen zu Datenschutz und Datensicherheit bestand. Durch die Beratung und Unterstützung der Verwaltung gelang es, für die Bereiche des verwaltungsinternen Datenaustausches, der Datenbekanntgabe und der Datensicherheit generell und in konkreten Einzelfällen datenschutzkonforme Lösungen zu entwickeln.
Bürgerinnen und Bürger wandten sich in vielen Fällen direkt an den Datenschutzbeauftragten. Insbesondere das Auskunftsrecht, das Recht auf Datensperrung und die Aufbewahrung von Daten gaben zu Fragen Anlass. Der Datenschutzbeauftragte erteilte dabei den betroffenen Personen Auskunft über die Rechtslage und wirkte – wo notwendig – vermittelnd zwischen diesen Personen und den verantwortlichen Organen.
Die Sensibilisierung für die Anliegen des Datenschutzes stand 1995 im Vordergrund, wobei festzustellen war, dass zahlreiche Verwaltungsstellen den Herausforderungen des Datenschutzes und der Datensicherheit mit Offenheit begegneten. In vielen Bereichen wurde ein Handlungsbedarf erkannt.
Im vergangenen Jahr wurde offensichtlich, dass der Datenschutz für die Bevölkerung einen wesentlichen Faktor für das Vertrauen in die Tätigkeit der Verwaltung darstellt. Diesem Vertrauen ist mit der Respektierung der Datenschutzbestimmungen und dem Einsatz der verhältnismässigen Mittel entgegenzukommen.

Beratung und Unterstützung der Verwaltung

Die kantonalen und kommunalen Verwaltungsstellen haben sich in zahlreichen schriftlichen Eingaben an den Datenschutzbeauftragten gewandt. Vielfach handelte es sich um Grundsatzfragen, die einer ausführlichen rechtlichen Abklärung bedurften und entsprechend zeitaufwendig waren. Daneben gingen täglich telefonische Anfragen ein.

1. Verwaltungsinterner Datenaustausch

Immer wieder zu Fragen Anlass gab der Datenaustausch innerhalb der Verwaltung. Die gesetzlichen Rahmenbedingungen finden sich dabei in § 8 DSG. Der regelmässige Datenaustausch zwischen Verwaltungsstellen braucht generell eine entsprechende Rechtsgrundlage. Diese ist in vielen Gesetzen in Form von Mitteilungspflichten und -rechten statuiert. Im Rahmen der Amtshilfe ist im Einzelfall eine Datenbekanntgabe möglich, wenn die Daten für den Empfänger zur Erfüllung seiner öffentlichen Aufgabe notwendig sind. Des weiteren können Daten weitergegeben werden, wenn die betroffene Person eingewilligt hat oder ihre Einwilligung nach den Umständen vorausgesetzt werden darf. Innerhalb dieser Rahmenbestimmungen ist ein Datenaustausch möglich. In verschiedenen Fällen wurden wir ersucht, die genauen Voraussetzungen des Datenaustausches, insbesondere bei der Amtshilfe, zu definieren. Dabei zeigte sich die Tendenz, das Amtsgeheimnis, das nach ständiger Rechtsprechung auch zwischen verschiedenen Amtsstellen zu beachten ist, «aufzuweichen». Ein solches Vorgehen kann sehr schwerwiegende Eingriffe in die Persönlichkeitsrechte der betroffenen Personen haben, wenn besonders schützenswerte Personendaten aus dem Sozial- und Fürsorgebereich weitergegeben werden sollen.
Falls ein solcher Datenaustausch nicht ausgeschlossen ist, sind die generellen Prinzipien der Subsidiarität, der Verhältnismässigkeit und der Zweckbindung zu beachten, die den Umfang und die Verwendung der Daten einschränken (siehe S. 23).

2. Datenbekanntgabe

Die Datenbekanntgabe an Drittpersonen ausserhalb der Verwaltung bildete einen weiteren Schwerpunkt der Beratungstätigkeit. Das Datenschutzgesetz hält die Rahmenbestimmungen fest, die im jeweiligen Verwaltungsbereich durch spezifische gesetzliche Grundlagen konkretisiert werden. Viele dieser Bestimmungen sind indessen wenig präzis und lassen einen breiten Beurteilungsspielraum für die Verwaltungseinheiten offen. Es war in diesem Zusammenhang immer wieder darauf hinzuweisen, dass bei der Datenbekanntgabe auch die allgemeinen Grundsätze des Datenschutzes zu beachten sind, vor allem das

Prinzip der Verhältnismässigkeit und der Zweckbindung. Das Verhältnismässigkeitsprinzip besagt, dass die Daten geeignet und erforderlich sein müssen für die jeweilige Verwendung, während die Zweckbindung verlangt, dass die Daten nur zu dem Zweck verwendet werden dürfen, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist. Damit lässt sich der Umfang der Datenbekanntgaben auf den Grundsatz beschränken: *«So wenig wie möglich, so viel wie notwendig»*.
Für die Einwohnerkontrollen stellt das DSG spezifische Bekanntgaberegeln auf (§ 9). Aufgrund verschiedener Anfragen konnten wir die gesetzlichen Bestimmungen in der Praxis konkretisieren, wobei wir im Rahmen unserer Publikationen Checklisten für die Einwohnerkontrollen zur Verfügung stellten. Es zeigte sich aber, dass im Hinblick auf eine einheitliche Praxis der Gemeinden auch im Interesse der gesuchstellenden Personen oder Organisationen weitere Anweisungen notwendig sein werden.
Bei jeder Datenbekanntgabe hat auch eine Interessenabwägung mit allenfalls entgegenstehenden Interessen zu erfolgen. Insbesondere bei wesentlichen öffentlichen Interessen oder offensichtlich schützenswerten Interessen einer betroffenen Person ist eine Datenbekanntgabe abzulehnen, einzuschränken oder mit Auflagen zu verbinden. Diese Interessenabwägungen sind durch direkte «Online»-Zugriffsmöglichkeiten in Frage gestellt. Während das Bundesrecht klare Regelungen für die direkten Zugriffsmöglichkeiten enthält, fehlen solche Bestimmungen im zürcherischen Gesetz. Da diese Art der Datenbeschaffung durch die zunehmende Vernetzung in der Informatik an Bedeutung gewinnt, arbeiten wir in der Praxis auf klare Bestimmungen hin, welche die Persönlichkeitsrechte der betroffenen Personen respektieren (siehe S. 16).

3. Datensicherheit

Die Datensicherheit, welche ein Kernelement des Datenschutzes ist, verlangt, dass Personendaten durch angemessene organisatorische und technische Massnahmen gegen das unbefugte Bearbeiten geschützt werden. Das DSG sieht eine zweijährige Übergangsfrist vor, in der die notwendigen Datensicherheitsmassnahmen einzurichten sind.
Wir sind in verschiedenen Bereichen mit teils schwerwiegenden Sicherheitsmängeln konfrontiert worden, welche hohe Risiken für Persönlichkeitsverletzungen enthalten. In zahlreichen Fällen fehlte es an minimalen Sicherheitsvorkehrungen:
In unbesetzten, unverschlossenen Büros waren Personendaten frei zugänglich, PCs nicht mit einem Passwort geschützt und Sicherheitskopien aus EDV-Anlagen offen in einem Schrank zugänglich. Wir wirkten darauf hin, dass in der kantonalen Verwaltung ein Informationssicherheitskonzept erstellt wird (siehe S. 28), und versuchten, mit spezifischen Publikationen auf wesentliche Sicherheitsaspekte hinzuweisen. Des weiteren war die sichere Vernichtung von Daten und Akten Gegenstand verschiedener Anfragen. Auf unser Ersuchen informierte die Staatskanzlei sämtliche kantonalen Verwaltungsstellen über die datenschutzkonforme Vernichtung von Akten (siehe S. 30).
Die Entwicklungen im Informatikbereich bringen neue Risiken für die Vertraulichkeit, Integrität und Authentizität von Daten. Mit angemessenen organisatorischen und technischen Massnahmen ist es heute möglich, die Risiken neuer Informationstechnologien einzuschränken, zum Beispiel mittels Chiffrierung von Daten, die über Netzwerke übertragen werden. Wir haben deshalb in einem ersten Schritt versucht, die Verwaltungsstellen über diesen besonders sensiblen Bereich der Datenbearbeitung zu informieren. Die Publikation «Sicherheit in Datennetzen» stellte neben einer Beschreibung der Risiken auch Lösungsmöglichkeiten für die Praxis vor. Der Bereich der Informationssicherheit wird auch in Zukunft einen Schwerpunkt des Datenschutzes bilden müssen, damit die Informationstechnologie von den Verwaltungsstellen unter Wahrung des Datenschutzes effizient eingesetzt werden kann.

Ressourcen

Die Aktivitäten, welche sich 1995 aus den Aufgaben und Funktionen des Datenschutzbeauftragten ergaben, mussten mit minimalen Ressourcen durchgeführt werden.

Dem Datenschutzbeauftragten standen zur Erfüllung seiner Aufgaben ein juristischer Mitarbeiter in Teilzeit (50 %) sowie eine Sekretärin, ebenfalls in Teilzeit (50 %), zur Verfügung. Diese Ressourcen waren nicht ausreichend, um alle Prioritäten 1995 angehen zu können. Dabei mussten Mängel in der Beratung der Verwaltungsstellen in dem Sinne in Kauf genommen werden, dass eingehendere Beantwortungen von Anfragen (z.B. die Beurteilung von Gemeindereglementen) mehrere Monate in Anspruch nahmen. Publikationen und Seminare des Datenschutzbeauftragten sind auf ein sehr grosses und positives Echo gestossen. Die Nachfrage nach zusätzlichen Seminaren für einzelne Verwaltungseinheiten übersteigt dabei die zeitlichen Kapazitäten. Mittelfristig ist eine effiziente Bearbeitung der Beratungsfälle und die Erfüllung der gesetzlichen Aufgaben nur möglich, wenn auch die entsprechenden Mittel zur Verfügung gestellt werden. Um einen effizienten Schutz der Persönlichkeitsrechte der Bürgerinnen und Bürger im Sinne des gesetzlichen Auftrages verwirklichen zu können, müssen die für den Datenschutz eingesetzten Mittel in einem vernünftigen Verhältnis stehen zum Aufwand, der für die Datenbearbeitungen in der Verwaltung aufgewendet wird. Diese Aufwendungen stehen heute in einem Missverhältnis. Die effiziente und bürgernahe Verwaltung setzt zunehmend auf die rationelle Datenbearbeitung mit EDV, die – es liegt in der Sache – ein weit höheres Potential an Persönlichkeitsverletzungen beinhaltet. Das Vertrauen von Bürgerinnen und Bürgern in die Verwaltung hängt deshalb auch mit den Mitteln zusammen, die dem Datenschutzbeauftragten zur Erfüllung seiner Aufgaben und Funktionen zur Verfügung gestellt werden.

Entwicklungen

Das Datenschutzgesetz ist in einem Zeitpunkt in Kraft getreten, in welchem die Verwaltungsstellen sich mit einer grundlegenden Verwaltungsreform (Wirkungsorientierte Verwaltung [WIF!]) konfrontiert sehen. Dies ist zugleich eine Chance und eine Herausforderung für den Datenschutz. Das Ziel der Verwaltungsreform ist eine effiziente und effektive Verwaltungsführung, welche sich an den Bedürfnissen der Bürgerinnen und Bürger orientiert. Sie ist deshalb auf die Akzeptanz der Bevölkerung angewiesen. In der Umsetzung bedeutet dies, dass Verwaltungsabläufe überprüft und rationellere Hilfsmittel eingesetzt werden sollen. Datenbearbeitungen erfolgen zunehmend mittels Datenaustausch und mit modernen Informatikmitteln. Nur wenn dabei auch von Anfang an die Persönlichkeitsrechte der betroffenen Bürgerinnen und Bürger sowie der Mitarbeiterinnen und Mitarbeiter der Verwaltung gewahrt werden, können diese eine solche Neuorientierung positiv aufnehmen. Effizienz in diesem Zusammenhang bedeutet deshalb auch, die Anliegen des Persönlichkeitsschutzes umfassend zu berücksichtigen. Eine nachträgliche Berücksichtigung – zum Beispiel aufgrund von Vorkommnissen und Pannen – ist auf jeden Fall die aufwendigere Lösung und deshalb zu vermeiden. Die effiziente Umsetzung des Datenschutzes im Rahmen der Verwaltungsreform verstärkt damit auch das Vertrauen der Bürgerinnen und Bürger in die angestrebten Zielsetzungen.
Dieses Umfeld wird auch die Datenbearbeitungen in der Zukunft beeinflussen. Die Entwicklungen zeigen, dass immer mehr Daten über Personen bearbeitet werden, diese Daten mit den modernen Informatikmitteln schneller zur Verfügung stehen und in der Kombination auch sehr rasch zu Persönlichkeitsprofilen zusammengestellt werden können.
Der Datenaustausch gewinnt an Bedeutung, und das kommerzielle Interesse an Personendaten ist stark zunehmend. Die Einführung von elektronischen Ausweisen, z.B. die Möglichkeit der Speicherung von medizinischen Diagnosen auf Chipkarten, sind neue Herausforderungen für den Persönlichkeitsschutz. Der Verwaltung, welche Daten aus den verschiedensten Lebensbereichen von Bürgerinnen und Bürgern bearbeitet (als Steuersubjekt, als Patientin oder Patient eines öffentlichrechtlichen Spitals usw.), verbleibt eine Schlüsselrolle, auch wenn die Datenbearbeitungen im privatwirtschaftlichen Bereich ebenso ständig wachsen. Es wird deshalb in den kommenden Jahren oberste Priorität sein, alle Verwaltungsstellen für die Anliegen des Persönlichkeits-

schutzes zu sensibilisieren. Nur wenn die datenschutzrechtlichen Bestimmungen eingehalten werden, wird es gelingen, den Befürchtungen der Bevölkerung angesichts der informationstechnischen Entwicklungen zu begegnen. Die persönliche Freiheit, eines der Grundrechte unserer liberalen Rechts- und Staatsordnung, beinhaltet den Schutz der Privatsphäre. Dieses Grundrecht vor Auge zu behalten ist Aufgabe und Pflicht der staatlichen Stellen und Institutionen, insbesondere bei der Datenbearbeitung mit zunehmend moderneren Möglichkeiten.

Respektierung der verschiedenen Interessen

Im Rückblick auf das Jahr 1995 ist all denjenigen Personen und Verwaltungsstellen zu danken, die sich aktiv um den Datenschutz und die Datensicherheit bemüht haben. Sie haben uns oftmals Lösungen präsentiert, denen wir vorbehaltlos zustimmen konnten, und vielfach war es in Zusammenarbeit möglich, unter Berücksichtigung der verschiedenen Interessen, einen für alle Seiten akzeptablen Weg zu finden.
Weiter sind von Verwaltungsstellen sowie Bürgerinnen und Bürgern Probleme und Schwierigkeiten im Umgang mit Personendaten an uns herangetragen worden, die zusätzlicher intensiver Arbeit bedürfen, um sie befriedigend zu lösen. Hier werden wir auch auf diejenigen Personen und Verwaltungsstellen angewiesen sein, die heute noch abwartend dem Datenschutz gegenüberstehen. Dabei ist festzuhalten, dass wir in allen Fällen auf einen offenen Umgang gestossen sind, der geprägt war von der Respektierung der gegenseitigen Interessen. Dies wird auch in Zukunft notwendig sein, um gemeinsame Lösungen für die Verwaltung und die Bürgerinnen und Bürger finden zu können.

Umsetzung der Datenschutzgesetzgebung

Der Überblick ausgewählter Themen beinhaltet grundlegende Fragestellungen, die sich bei der Umsetzung der Datenschutzgesetzgebung in der Praxis gezeigt haben.

1. Datenschutz im Gesundheitswesen

Anwendbarkeit des Datenschutzgesetzes

Die Gesundheitsdirektion lehnte die Anwendbarkeit des Datenschutzgesetzes im Bereich der kantonalen Krankenhäuser ab. Mehrfache Interventionen des Datenschutzbeauftragten führten nach Monaten zu einer Anerkennung der Geltung des Datenschutzgesetzes. Offene Fragen in Einzelbereichen verbleiben.
Am 31. Januar 1995 erliess die Gesundheitsdirektion eine Mitteilung an die kantonalen Krankenhäuser, in der festgehalten wurde, dass das kantonale Datenschutzgesetz wie auch das eidgenössische Datenschutzgesetz im Bereich der kantonalen Krankenhäuser nicht anwendbar seien. Lediglich die Verordnung über den Datenschutz in den kantonalen Krankenhäusern vom 9. September 1981 sowie Art. 321 Strafgesetzbuch (StGB) (Verletzung des Berufsgeheimnisses) und Art. 321bis StGB (Berufsgeheimnis in der medizinischen Forschung) seien zu beachten. Diese Mitteilung erfolgte ohne Rücksprache mit dem Datenschutzbeauftragten und hat bei einzelnen Spitälern, welche bereits grosse Bemühungen im Bereich des Datenschutzes unternommen haben (z.B. Universitätsspital), zu einer starken Verunsicherung geführt.
Da auch die Anwendbarkeit des eidgenössischen Datenschutzgesetzes in Frage gestellt wurde, haben wir nach Rücksprache mit dem Eidgenössischen Datenschutzbeauftragten im April 1995 der Gesundheitsdirektion unseren Rechtsstandpunkt mitgeteilt: Grundsätzlich ist für die öffentlich-rechtlichen Spitäler des Kantons Zürich das kantonale Datenschutzgesetz anwendbar. Lediglich in Fällen, wo beispielsweise ein Patient aufgrund eines privatrechtlichen Auftragsverhältnisses von seinem Arzt (z.B. Belegarzt) in einem öffentlich-rechtlichen Spital behandelt wird, basiert dieses Verhältnis auf dem Obligationenrecht. In diesem Teilbereich gilt Privatrecht und somit das Bundesgesetz über den Datenschutz.
Die Gesundheitsdirektion hat trotz mehrfacher Interventionen weder zu unserer Rechtsauffassung Stellung bezogen, noch ihre Mitteilung an die kantonalen Spitäler berichtigt. Erstmals in der Beantwortung einer Anfrage im Kantonsrat (Datenschutz in öffentlichen Heilanstalten; KR-Nr. 215/1995, 13. Dezember 1995) wurde die grundsätzliche Anwendbarkeit des kantonalen Datenschutzgesetzes bejaht.
Aufgrund dieser Situation sind aus der Sicht des Datenschutzes zahlreiche persönlichkeitsrechtlich relevante Fragen im Bereich des Gesundheitswesens in diesem Jahr offen geblieben. Insbesondere sind der Anwendungsbereich des Datenschutzgesetzes auf die vom Staat unterstützten Krankenhäuser, die Anpassungen bestehender Verordnungen sowie die Klärung wichtiger Fragen in bezug auf die individuellen Rechte der betroffenen Personen (Einsicht in die Krankengeschichte, Aufbewahrung und Herausgabe der Krankengeschichte, Weitergabe von Daten an Dritte) keiner Klärung zugeführt worden.

2. Vollzug des Krankenversicherungsgesetzes

Datenbearbeitungen durch Abgleichverfahren

Der Vollzug des Bundesgesetzes über die Krankenversicherung (KVG) vom 18. März 1994, welches auf den 1. Januar 1996 in Kraft gesetzt wurde, bringt ein enormes Volumen von Datenbearbeitungen mit sich. Im Kanton Zürich sind beim Vollzug die Gesundheitsdirektion, die Sozialversicherungsanstalt, die Gemeinden sowie die Krankenversicherer involviert. In der Arbeitsgruppe, welche die Vollzugsverordnung erarbeitete, konnten wir die datenschutzrechtlichen Aspekte einbringen.

Grundsätzlich ist beim Vollzug des Krankenversicherungsgesetzes von der Anwendbarkeit des kantonalen Datenschutzgesetzes auszugehen, da das KVG in Art. 84 auf das Bundesgesetz über den Datenschutz verweist, welches gemäss Art. 37 nur zur Anwendung gelangt, wenn keine kantonalen Gesetzgebungen bestehen. Die Datenbearbeitungen im Rahmen des Vollzuges des KVG erscheinen als sehr sensibel, einerseits aufgrund der Anzahl der betroffenen Personen und andererseits, weil sich unter den bearbeiteten Daten auch besonders schützenswerte Personendaten befinden.
Wir wirkten bei der Verordnung darauf hin, dass eine klare Abgrenzung des Verfahrens in bezug auf das Versicherungsobligatorium und desjenigen in bezug auf die Prämienverbilligung vorgesehen wird. In dieser Hinsicht begrüssten wir es, dass die verantwortlichen Stellen, welche die Daten zur Erfüllung ihrer Aufgabe erheben, in beiden Verfahren klar bestimmt wurden, damit auch die datenschutzrechtliche Verantwortung eindeutig feststeht. Ebenso wurde für beide Verfahren bestimmbar, welche Daten zu bearbeiten sind und welche Daten von einer Stelle der anderen zur Verfügung gestellt werden dürfen.
Allerdings erschien uns im Verfahren in bezug auf die Prämienverbilligung der Abgleich der Daten *aller* Versicherten, welche von den Krankenversicherern der Sozialversicherungsanstalt zur Verfügung gestellt werden, nicht unproblematisch. Von einer Prämienverbilligung sind nämlich nur rund *20 Prozent* der Versicherten betroffen. Wir wiesen darauf hin, dass der Datenfluss nach dem Verhältnismässigkeitsprinzip auf die für die Aufgabenerfüllung geeigneten und erforderlichen Daten zu beschränken ist und dass deshalb das Bearbeiten von Daten über Personen, welche von diesem Verfahren nicht betroffen sind, eine Ausnahme wäre, welche entsprechend abzusichern ist.
Beim Vollzug der Verordnung ist auch darauf zu achten, dass die notwendigen Datensicherheitsmassnahmen getroffen werden.
Eine abschliessende Beurteilung des Vollzugs des KVG aus datenschutzrechtlicher Sicht wird deshalb erst möglich, wenn auch diese konkreten Ausgestaltungen uns vorliegen (Informatikkonzept, Datenflüsse, Sicherheitskonzept). Zum gegebenen Zeitpunkt soll uns deshalb das Projekt zu einer eingehenderen Gesamtbeurteilung aus datenschutzrechtlicher Sicht vorgelegt werden.

3. Datensperre für Motorfahrzeughalter

Sperrecht ohne Interessennachweis

Jede Person kann die Bekanntgabe ihrer Daten an private Personen und Organisationen sperren lassen (§ 11 DSG).
Diese Bestimmung ist auch beim Vollzug von Bundesrecht anwendbar, was in bezug auf die Datensperre für Motorfahrzeughalter im Kanton Zürich zu einer Praxisänderung des Strassenverkehrsamtes führte, indem nun diesbezügliche Datensperren ohne Interessennachweis akzeptiert werden.

Aufgrund einer Vereinbarung der Vereinigung der Strassenverkehrsämter mit der Telecom PTT, der auch der Kanton Zürich beigetreten ist, werden Name und Adresse von Motorfahrzeughalterinnen und -halter auch über Telefonnummer 111 und Videotex bekanntgegeben. Es zeigte sich, dass diese Art der Datenbekanntgabe sehr viel stärker in die Persönlichkeitsrechte betroffener Personen eingreift als beispielsweise die Publikation eines Halterindexes. Viele Personen verlangten deshalb beim Strassenverkehrsamt eine Sperre ihrer Daten. Diese Sperrgesuche wurden vom Strassenverkehrsamt nur akzeptiert, wenn der betreffende Halter nachweisen oder zumindest glaubhaft machen konnte, dass er aufgrund seiner beruflichen, politischen oder familiären Situation gefährdet oder bedroht ist.
Nachdem das Strassenverkehrsamt auch nach Inkrafttreten des kantonalen Datenschutzgesetzes, welches ein Sperrecht ohne Interessennachweis vorsieht, an seiner bisherigen Praxis festhielt, wandten sich

zahlreiche Bürgerinnen und Bürger an den Datenschutzbeauftragten. Wir setzten uns in der Folge mit dem Strassenverkehrsamt in Verbindung mit dem rechtlichen Hinweis, dass die entsprechenden Bestimmungen des Strassenverkehrsrechts (Art. 104 Abs. 5 SVG; Art. 126 VZV) keine Verpflichtung zur Veröffentlichung dieser Daten enthalten, weshalb § 11 DSG die Sperre dieser Daten ohne Interessennachweis ermöglicht.
Nach Gesprächen mit der Polizeidirektion konnte die Angelegenheit in einem für die betroffenen Personen befriedigenden Sinne gelöst werden: Das Strassenverkehrsamt akzeptiert nunmehr Datensperren von Motorfahrzeughalterinnen und -haltern ohne Interessennachweis (Praxisänderung). Des weiteren hat die Polizeidirektion die eingangs erwähnte Vereinbarung auf den nächstmöglichen Termin, den 1. November 1998, gekündigt. Im Kündigungsschreiben hält die Polizeidirektion fest, dass «sehr viele Gesuchsteller von der Möglichkeit der Datensperre Gebrauch machen, weil sie vor allem die Auskunftserteilung durch Telefon 111 und Videotex ablehnen».

4. Steuerausweise und Privatsphäre

Persönlichkeitsschutz und private Informationsinteressen

Zahlreiche Bürgerinnen und Bürger sind an den Datenschutzbeauftragten mit der Frage gelangt, ob sie die Bekanntgabe ihrer Steuerdaten an private Personen und Organisationen (Steuerausweise gemäss § 83 Steuergesetz) sperren lassen könnten.
Wir haben zu dieser Problematik in zwei Teilbereichen Stellung bezogen: Einerseits im Rahmen der Revision des Steuergesetzes, welche auf den 1. Januar 1999 in Kraft treten soll, und andererseits in bezug auf die Rechtslage bis zu einer allfälligen Steuergesetzrevision.
Der Entwurf zu einem neuen (harmonisierten) Steuergesetz sieht die ersatzlose Streichung von § 83 Steuergesetz (StG) vor, welcher die Möglichkeit der Ausstellung von Steuerausweisen (Einkommen und Vermögen oder Ertrag und Kapital gemäss letzter rechtskräftiger Einschätzung oder aufgrund der letzten Steuererklärung) an jede gesuchstellende Person zulässt.
Der Antrag des Regierungsrates, welcher aus Gründen des Persönlichkeitsschutzes die Streichung von § 83 StG vorschlägt, ist indessen nicht unumstritten.
In einer Stellungnahme haben wir festgehalten, dass den Anliegen des Persönlichkeitsschutzes in einem revidierten Steuergesetz Rechnung getragen werden müsse. Falls die vorgesehene Streichung von § 83 StG nicht berücksichtigt wird, sollten die Persönlichkeitsrechte der betroffenen Personen mindestens wie folgt geschützt werden:
a) Die Datenbekanntgabe ist an den Nachweis eines schutzwürdigen Interesses der auskunftsersuchenden Person zu binden. Ein schutzwürdiges Interesse kann dabei sowohl rechtlicher wie tatsächlicher Natur sein. Mit einer solchen Bestimmung würden die reine Neugier sowie die zweckwidrige Verwendung dieser Daten ausgeschlossen.
b) Die Möglichkeit der Datensperre gemäss Datenschutzgesetz ist der betroffenen Person offenzuhalten. Dabei kann die Datensperre durchbrochen werden, wenn eine gesuchstellende Person glaubhaft macht, dass die Sperre sie in der Verfolgung eigener Rechte gegenüber der betroffenen Person behindert.

Da das revidierte Steuergesetz erst auf den 1. Januar 1999 in Kraft treten soll, haben wir mit dem kantonalen Steueramt Kontakt aufgenommen, um die aktuelle Rechtslage zu klären. Dabei vertreten wir den Standpunkt, dass § 83 StG keine gesetzliche Grundlage im Sinne von § 8 des Datenschutzgesetzes ist, welche die Weitergabe von Steuerdaten in der Form von Steuerausweisen gestatten würde. Eine Auslegung von § 8 Abs. 1 DSG zeigt, dass unter «gesetzlicher Grundlage» allein eine Regelung zu verstehen ist, in der bereits eine Abwägung zwischen den sich entgegenstehenden Interessen der betroffenen Person und dem Interesse an der Bekanntgabe der Daten getroffen wurde.
In diesem Sinne ist § 83 als spezialgesetzliche Regelung nicht daten-

schutzkonform, und mit dem Inkrafttreten des Datenschutzgesetzes ist eine vorbehaltlose Weitergabe von Steuerinformationen nicht mehr möglich. Wir gehen auch davon aus, dass § 83 StG keine verpflichtende Norm für das Steueramt zur Datenbekanntgabe darstellt, sondern lediglich eine Ermächtigung, weshalb einer Datensperre im Sinne von § 11 des Datenschutzgesetzes nichts im Wege steht. Weiter stellt sich die Frage, ob § 83 StG mit Art. 8 der Europäischen Menschenrechtskonvention (EMRK) in Einklang steht. Als Rechtfertigungsgründe für den Eingriff in die Privatsphäre gelten öffentliche Interessen oder der Schutz der Rechte und Freiheiten anderer (Art. 8 Abs. 2 EMRK). § 83 StG dient dagegen in erster Linie der Befriedigung privater Informationsinteressen.

---

5. Personalanmeldebogen

Zu umfassende Daten bei Stellenbewerberinnen und -bewerbern

Im Zusammenhang mit der Prüfung von Fragebogen für Stellenbewerberinnen und -bewerber haben wir festgestellt, dass Arbeitgeber sehr weit in die Persönlichkeitsrechte auch nur potentieller Arbeitnehmer eingreifen. So werden etwa bereits im Stadium einer allgemeinen Erfassung von Interessenten für eine offene Stelle detaillierte Fragen zu den Personalien der Familienangehörigen, zum Beruf und Arbeitgeber des Ehepartners und zu dessen Arbeitszeiten gestellt und Angaben über Anzahl und Alter der Kinder (sowie ob ehelich, ausserehelich oder Adoptiv- oder Pflegekinder) sowie zur Haushaltführung (eigener oder gemeinsamer Haushalt) verlangt. Ferner Details zur Kranken- und Pensionskasse und zum Salärkonto (Nummer und bei welcher Bank).
Die Grundlage für das Bearbeiten von Personaldaten besteht in der Regel in den Erlassen, welche die Begründung und Aufrechterhaltung der öffentlichen Dienstverhältnisse regeln. Weist das öffentliche Recht Lücken auf, werden die obligationenrechtlichen Bestimmungen, im vorliegenden Fall Bestimmungen des Arbeitsvertragsrechts, ersatzweise angewendet. Im öffentlichen Recht fehlen meistens genauere Vorschriften über den Umfang der Daten, die bearbeitet werden dürfen. Im Arbeitsrecht wurden hingegen im Rahmen der Rechtsprechung zum Persönlichkeitsschutz und insbesondere in jüngster Zeit unter dem Datenschutzrecht sowohl Vorschriften erlassen (Art. 328b OR) als auch eine Lehre und Praxis entwickelt, die für das Stellenbewerbungsverfahren verschiedene Stadien der Datenerhebung vorsehen.
Art. 328b OR lautet wie folgt: «Der Arbeitgeber darf Daten über den Arbeitnehmer nur bearbeiten, soweit sie dessen Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrages erforderlich sind. Im übrigen gelten die Bestimmungen des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz.» Gestützt auf diese Bestimmung sowie die erwähnte Lehre und Praxis darf ein Arbeitgeber heute von einem Stellenbewerber beim ersten Kontakt nur diejenigen Angaben verlangen, die er zur Abklärung einer Eignung für das Arbeits- bzw. Dienstverhältnis benötigt. Das bedeutet, dass ein dem Bewerber oder der Bewerberin unterbreiteter allgemeiner Fragebogen nur Fragen enthalten darf, die eine engere Auswahl der für die Arbeitsstelle in Frage kommenden Personen erlauben, gleichzeitig aber nicht übermässig in das Recht der Betroffenen eingreifen, selbst über die Bekanntgabe persönlicher Daten bestimmen zu können. Wo eine bestimmte Eigenschaft Voraussetzung für die Stellenbesetzung ist, soll diese Bedingung möglichst als solche deklariert werden und nicht indirekt als Auswahlkriterium durch die Beurteilung von Antworten erhoben werden. Falls dies dennoch notwendig sein sollte, ist der betroffenen Person durch einen Hinweis darauf, in welchem Zusammenhang die verlangten Angaben eine Rolle spielen, zu ermöglichen, über die Preisgabe der Daten selber zu entscheiden.
In zwei Fällen haben wir im Sinne dieser Erwägungen den Arbeitgebern (einem Spital und einem

Altersheim) empfohlen, ihre ersten Fragebogen für Stellenbewerber so zu ändern, dass die erfassten Personalien nur Name, Vorname, Geschlecht, Adresse, Telefon, Geburtsdatum, Zivilstand umfassen und nur Fragen zu Schulen, beruflicher Ausbildung und bisheriger Tätigkeit, besonderen Kenntnissen sowie Referenzen gestellt werden. Zudem empfahlen wir, Bedingungen für den Stellenantritt, wie zum Beispiel das Schweizerbürgerrecht oder eine bestimmte Konfession, soweit wie möglich zu erwähnen (statt über indirekte Fragen ihre Erfüllung bzw. Nichterfüllung festzustellen). Spezielle Fragen, die weiter in die Persönlichkeitsrechte eingreifen, sollten nach getroffener Auswahl nur noch den in Frage kommenden Bewerberinnen und Bewerbern gestellt werden.

6. Personalgesetz 97

Datenschutzrechtliche Bestimmungen für das Personalwesen

Im Rahmen der Projektarbeiten zum Entwurf Personalgesetz 97 wurden wir durch die Projektgruppe eingeladen, die durch das Inkrafttreten des Datenschutzgesetzes (DSG) notwendig gewordenen speziellen Bestimmungen zum Datenschutz im Personalwesen vorzuschlagen. Der bis dahin ausgearbeitete Entwurf sah nur ein Einsichtsrecht der Staatsangestellten in ihre Personalakten vor. Wir erachteten es als sinnvoll, im datenschutzrechtlich sensiblen Bereich der Personaldatenbearbeitung die entsprechenden Vorschriften im Spezialgesetz zu regeln und nicht nur auf die allgemeinen Bestimmungen des Datenschutzgesetzes zu verweisen, welches als Rahmengesetzgebung zu betrachten ist. Bei den von uns zusätzlich vorgeschlagenen Bestimmungen handelt es sich einerseits um eine Umsetzung des im öffentlich-rechtlichen Arbeitsverhältnis analog anwendbaren, mit dem eidgenössischen Datenschutzgesetz in Kraft getretenen Art. 328b OR, welcher die Personaldatenbearbeitung des Arbeitgebers im Privatrecht regelt, und andererseits um grundsätzliche Datenschutzregeln, wie sie sich aus den §§ 4, 8 und 17ff. DSG ergeben. Unser Vorschlag umfasste fünf Paragraphen, die in einem Abschnitt «Datenschutz» zusammengefasst werden sollen.
Sie regeln im einzelnen:
– die Rechte und Pflichten des Staats als Arbeitgeber bei der Erhebung und Bearbeitung von Personendaten der Angestellten sowie der Stellenbewerberinnen und -bewerber;
– die Bedingungen, unter denen der Arbeitgeber Personendaten seiner Angestellten während und nach dem Arbeitsverhältnis bekanntgeben darf;
– die Aufbewahrung von Personalakten nach dem Ende des Arbeitsverhältnisses;
– die Rechte der Angestellten in bezug auf Einsicht in ihre Personalakten und in die über sie bearbeiteten Personendaten, auf Korrekturmassnahmen bei unrichtigen Personendaten und auf Sperrung der Bekanntgabe ihrer Daten an private Personen und Organisationen;
– die Voraussetzungen, unter denen das Einsichtsrecht eingeschränkt werden kann.
Auf Verordnungsstufe werden weitere datenschutzrechtliche Ausführungsbestimmungen, wie zum Beispiel die Festsetzung der Aufbewahrungsdauer des Personaldossiers, zu regeln sein.

7. Abgrenzung Akteneinsichts- und Auskunftsrecht

Konkurrierende Geltung beider Ansprüche

In einem Fall sind wir vermittelnd tätig geworden, in welchem die betreffende Verwaltungsstelle die Akteneinsicht aufgrund einer Weisung verweigert hatte und die betroffene Person gleichzeitig ein Auskunftsrecht nach § 17 DSG geltend machte. Wir nahmen grundsätzlich zur Abgrenzung zwischen Akteneinsichts- und Auskunftsrecht Stellung.

Soweit das Akteneinsichtsrecht nach der ständigen Rechtsprechung des Bundesgerichts ausserhalb eines hängigen Verwaltungsrechtspflegeverfahrens gewährleistet ist, steht es in Konkurrenz zum Auskunftsrecht, wobei die betroffene Person sich auf beide Ansprüche gleichzeitig stützen kann. Das Auskunftsrecht ist somit unabhängig von einem bestehenden Akteneinsichtsrecht zu betrachten. In Form und Inhalt unterscheidet sich das Auskunftsrecht aber vom Akteneinsichtsrecht.

Das datenschutzrechtliche Auskunftsrecht nimmt Bezug auf das verfassungsmässige Recht der persönlichen Freiheit. Es steht der betroffenen Person als Rechtsbehelf zur Verfügung, um mögliche Eingriffe in ihre persönliche Freiheit überprüfen zu können, mithin um Rechtsverletzungen geltend machen zu können. Da das Auskunftsrecht zum Ziel hat, der betroffenen Person die über sie bearbeiteten Daten offenzulegen, deckt es sich in seinem Resultat in weiten Bereichen mit dem Akteneinsichtsrecht, welches, gestützt auf Art. 4 der Bundesverfassung, überwiegend der Gewährung des rechtlichen Gehörs dient.

Jede Person, die sich ausgewiesen hat, kann vom verantwortlichen Organ Auskunft verlangen, welche Daten über sie in dessen Datensammlung bearbeitet werden (§ 17 DSG). Das Auskunftsbegehren ist schriftlich an das verantwortliche Organ zu richten (§ 10 DSV). Einschränkungen des Auskunftsrechts können sich ergeben, wenn eine gesetzliche Bestimmung, überwiegende öffentliche Interessen oder überwiegende schützenswerte Interessen Dritter dies verlangen (§ 18 Abs. 1 DSG).

Das Auskunftsrecht beinhaltet die Mitteilung der auskunftsgebenden Stelle an die betroffene Person bezüglich aller über sie in der Datensammlung vorhandenen Daten, die Rechtsgrundlage und den Zweck des Bearbeitens, die an der Datensammlung beteiligten Stellen und die regelmässigen Datenempfänger (§ 10 Abs. 1 lit. a und b DSV). Im Regelfall wird diese Auskunft schriftlich erteilt (Ausdrucke, Kopien); sie kann auf Verlangen der betroffenen Person auch nur mündlich erteilt werden (§ 10 Abs. 2 DSV). Soweit es Mittel und Verfahren des Bearbeitens zulassen, kann die Auskunft durch Einsichtnahme erfolgen (§ 10 Abs. 2 DSV).

Das Auskunftsrecht erstreckt sich auf die Daten, welche die eigene Person betreffen. Je nach Datensammlung oder Akten kann sich das Auskunftsrecht deshalb auch nur auf einen Teil des Akteninhaltes beziehen. Der Informationsgehalt des Auskunftsrechts und des Akteneinsichtsrechts muss sich daher nicht zwingend decken. Auskunftsrecht wie Akteneinsichtsrecht können aber je nach Informationsinteresse der betroffenen Person zum gleichen Ergebnis führen.

Bei der Entgegennahme des Auskunftsbegehrens hat das Verwaltungsorgan im Einzelfall zu prüfen, ob aufgrund einer gesetzlichen Bestimmung, überwiegenden öffentlichen Interessen oder schützenswerten Interessen Dritter die Auskunft aufzuschieben, einzuschränken oder zu verweigern ist.

Im vorliegenden Fall hielten wir insbesondere fest, dass in Weisungen oder Kreisschreiben enthaltene Anweisungen in bezug auf das Akteneinsichtsrecht nicht geeignet sind, das Auskunftsrecht einzuschränken.

Online-Abfragemöglichkeiten von Datenbanken

Die Möglichkeit automatisierter Datenbankzugriffe, sogenannter Abrufverfahren oder Online-Zugriffe, hat zu verschiedenen Anfragen geführt. Bei diesen Verfahren gilt es, besondere datenschutzrechtliche Voraussetzungen zu beachten.

1. Zugriff auf Einwohnerkontrolldaten

Die notwendigen Rahmenbedingungen

Die Justizdirektion ersuchte um Stellungnahme zu einem Projekt, wonach der Bezirksanwaltschaft Zürich und der Staatsanwaltschaft Zugriff auf die in der elektronischen Datenbank der Einwohnerkontrolle der Stadt Zürich enthaltenen Personendaten gewährt werden sollte. Dadurch sollte der Aufwand für schriftliche Anfragen bei der Einwohnerkontrolle betreffend die korrekten Personalien von Angeschuldigten, Zeugen und Auskunftspersonen reduziert werden.
Das Datenschutzgesetz ist gemäss § 3 lit. b nicht anwendbar, wenn Daten im Rahmen hängiger Strafverfolgungsverfahren erhoben werden. Soweit es sich im vorliegenden Fall um hängige Strafverfahren handelt, sind indessen die allgemeinen Grundsätze des Datenschutzes zu beachten. Für nicht im Verfahren beteiligte Parteien – vorliegendenfalls die Einwohnerkontrolle – gilt das Datenschutzgesetz uneingeschränkt.
§ 8 Abs. 1 DSG setzt für die Bekanntgabe von Personendaten durch öffentliche Organe voraus, dass dafür gesetzliche Grundlagen bestehen oder die Daten für den Empfänger im Einzelfall zur Erfüllung seiner öffentlichen Aufgabe notwendig sind, die betroffene Person im Einzelfall eingewilligt hat, ihre Einwilligung vorausgesetzt werden darf oder dass sie ihre Daten allgemein zugänglich gemacht hat.
Eine ausdrückliche gesetzliche Grundlage für eine generelle Bekanntgabepflicht der Einwohnerkontrolle besteht nicht. § 8 Abs. 1 lit. a DSG beschränkt die Bekanntgabe auf den Einzelfall.
Eine Datenbekanntgabe im Einzelfall kann für die in § 9 Abs. 1 und 2 DSG (Bekanntgabe an private Personen und Organisationen) genannten Daten der Einwohnerkontrolle (Name, Vorname, Adresse, Datum von Zu- und Wegzug, Beruf, Zu- und Wegzugsort, Geburtsdatum, Geschlecht, Zivilstand, Heimatort) auch von einem öffentlichen Organ verlangt werden. Es besteht kein Anlass, in diesem Fall Privatpersonen und öffentliche Organe unterschiedlich zu behandeln.
Ein Einzelfall ist indessen nicht gegeben, wenn eine generelle Abfragemöglichkeit im Abrufverfahren (Online-Zugriff) eingerichtet wird. Des weiteren ist dadurch die im Einzelfall zu treffende Güterabwägung bei der Datenbekanntgabe mit allenfalls entgegenstehenden Geheimhaltungsinteressen nicht möglich. Bei Abrufverfahren stehen die vorhandenen Daten zudem in ihrer Gesamtheit (hier die Daten aller Einwohnerinnen und Einwohner der Stadt Zürich) zur Verfügung. Damit werden auch Personendaten der abrufenden Stelle bekannt, die im Rahmen des Selektionsverfahrens normalerweise anfallen (z.B. Personen mit gleichen Namen und Vornamen), aber für die Anfrage nicht von Belang sind.
Das Datenschutzgesetz des Bundes fordert in Art. 19 Abs. 3 aus diesem Grund für Abrufverfahren eine ausdrückliche gesetzliche Grundlage, bei besonders schützenswerten Personendaten ein formelles Gesetz. Eine solche Regelung fehlt im zürcherischen Datenschutzgesetz, jedoch ist aufgrund allgemeiner Überlegungen davon auszugehen, dass das Abrufverfahren nur dort ermöglicht werden soll, wo keine oder möglichst geringe Interessen betroffener Personen entgegenstehen können. Das wäre der Fall, wenn es nur um den Zugriff auf Namen und Adressen geht, nicht jedoch, wenn der ganze Datenstamm einer Einwohnerkontrolle frei verfügbar sein soll.
Die gesetzliche Beschränkung auf den Einzelfall der Bekanntgabe im Sinne von § 8 Abs. 1 lit. a DSG ist erfüllt, wenn eine Rechtsgrundlage beim Datenempfänger sicherstellt, dass kein wahlloser Zugriff erfolgt. Solche Bestimmungen könnten im vorliegenden Fall beispielsweise sein, dass ein hängiges Strafverfahren vorausgesetzt wird, die

abfragbaren Datenfelder definiert werden, die Zugriffsberechtigungen auf die mit der Aufgabe betrauten Personen beschränkt werden und der Einwohnerkontrolle als verantwortlichem Organ für die Datenbekanntgabe eine Überprüfung der begründeten Einsichtsanträge ermöglicht wird. Zusätzlich müsste auf Nichtweiterverbreitung der Daten durch Übernahme in andere Verfahren oder Bekanntgabe an unbeteiligte Dritte geachtet werden (Zweckbindung der Daten). Diese Rechtsgrundlage muss im übrigen nur dem materiellen Gesetzesbegriff genügen (es sei denn, es würden besonders schützenswerte Personendaten verlangt). Mit entsprechenden organisatorischen und technischen Datensicherheitsmassnahmen ist das unbefugte Bearbeiten zu verhindern.

2. Zugriffe auf die Daten des Handelsregisteramts

Voraussetzungen für Private und Verwaltungsstellen

Aufgrund verschiedener Anfragen beschäftigten wir uns mit geplanten direkten Zugriffsmöglichkeiten auf die Datenbank des kantonalen Handelsregisteramts. Solche Zugriffsmöglichkeiten sollen sowohl privaten Personen und Organisationen wie auch Verwaltungsstellen ermöglicht werden.
Soweit das Handelsregisteramt die ihm vom Bundesrecht übertragenen Aufgaben eines öffentlichen Registers des Privatrechtsverkehrs erfüllt, unterliegt es, obwohl an sich ein kantonales öffentliches Organ im Sinne von § 2 lit. c DSG, weder dem kantonalen noch dem eidgenössischen Datenschutzgesetz (Art. 2 Abs. 2 lit. d Bundesgesetz über den Datenschutz). Der Ausschluss ist dadurch gerechtfertigt, dass diese Datenbearbeitungen sehr detaillierten und formellen Vorschriften (Handelsregisterverordnung) unterstehen, die aus Gründen der Rechtssicherheit nicht durch allgemeine Datenschutzvorschriften abgeändert werden sollen. Die Grundsätze für die Bearbeitung von Personendaten und insbesondere diejenigen für die Bekanntgabe dürfen jedoch, da sie eine Konkretisierung der Lehre und Praxis zum Persönlichkeitsschutz darstellen, als analog geltendes Recht herangezogen werden, wo keine speziellen Regeln bestehen. Ein Zugriff privater Personen und Organisationen auf die Datenbank des Handelsregisters erfordert eine gesetzliche Grundlage, welche im materiellen Handelsregisterrecht nicht gegeben ist. Das Handelsregisterrecht regelt die Bestimmungen betreffend die Öffentlichkeit des Registers abschliessend. Gemäss Art. 119 Abs. 3 der Handelsregisterverordnung führt das Eidgenössische Amt für das Handelsregister ein Zentralregister, das im Fall der Bedürfnisse erweitert werden kann. Nur wenn man davon ausgehen könnte, dass das Bundesrecht keine abschliessende Regelung aufweisen würde, wäre allenfalls eine eigenständige Tätigkeit des kantonalen Handelsregisteramtes möglich, falls eine entsprechende Rechtsgrundlage geschaffen würde oder eine erweiterte Verwendung der Daten mit dem Einverständnis der betroffenen Personen erfolgen würde.
In bezug auf direkte Zugriffsmöglichkeiten anderer Verwaltungsstellen haben wir im Sinne eines generellen Hinweises darauf aufmerksam gemacht, dass im Zusammenhang mit der Übernahme von Daten anderer Organe und speziell bei einer Übernahme mittels Abrufverfahren eine Regelung der Verantwortlichkeiten für den Datenschutz und die Massnahmen zur Datensicherheit besonders wichtig ist. Auszugehen ist von der Verantwortlichkeit jedes Organs für den Umgang mit den von ihm in Erfüllung seiner Aufgabe bearbeiteten Daten (§ 6 Abs. 1 DSG).
Wenn einer Amtsstelle erlaubt werden soll, nach Belieben auf Handelsregisterdaten zuzugreifen, muss damit eine Übernahme der Verantwortung für die weitere Datenbearbeitung einhergehen. Dabei wären insbesondere der Kreis der zugriffsberechtigten Personen mindestens nach Funktionen und/oder bearbeiteten Rechtsgeschäften zu bezeichnen und allenfalls im Rahmen eines Datenbearbeitungsreglements weitere Massnahmen zu treffen (z.B. Datensicherheitsmassnahmen).

Datenbekanntgaben im Mittelpunkt

Die Bekanntgabe von Personendaten durch kommunale Verwaltungsstellen – insbesondere die Einwohnerkontrollen – bildete Gegenstand spezifischer Anfragen in bezug auf den Verwendungszweck und den Umfang der bekanntzugebenden Daten.

1. Daten für wissenschaftliche Forschung

Voraussetzungen der Datenbekanntgabe

Ein Hochschulinstitut ersuchte zum Zweck einer wissenschaftlichen Studie über die Wahl des Verkehrsmittels um Bekanntgabe der Adressen einer repräsentativen Auswahl von Einwohnerinnen und Einwohnern verschiedener Gemeinden, die mittels Fragebogen befragt werden sollten. Die Fragebogen waren anonym auszufüllen, und die Daten sollten ausschliesslich für wissenschaftliche Zwecke verwendet und nicht an Dritte weitergegeben werden.
§ 12 DSG erlaubt die Bearbeitung von Personendaten für nicht personenbezogene Zwecke wie Forschung, Planung und Statistik, wenn die Daten anonymisiert werden, sobald es der Zweck der Bearbeitung erlaubt und die Ergebnisse so veröffentlicht werden, dass die betroffenen Personen nicht bestimmbar sind. Zu solchen Zwecken darf eine Gemeinde die Adressen von Einwohnern bekanntgeben, wenn keine Geheimhaltungspflicht oder eine andere Bestimmung entgegensteht und Rückschlüsse auf die betroffenen Personen möglichst erschwert sind. Bei privaten Bearbeitern muss überdies gewährleistet sein, dass die Bearbeitungsvoraussetzungen bezüglich Anonymisierung und Veröffentlichung eingehalten und die Daten nur mit Zustimmung des Datenlieferanten weitergegeben werden.
Da im vorliegenden Fall die Bearbeitungsvoraussetzungen erfüllt waren, bestanden aus datenschutzrechtlichen Überlegungen keine Bedenken für eine Bekanntgabe. Den Gemeinden wurde empfohlen, die Daten unter der Auflage einer Bearbeitung gemäss den Voraussetzungen von § 12 DSG weiterzugeben und sich dies bestätigen zu lassen.
Ein ausserkantonales Hochschulinstitut ersuchte bei verschiedenen Gemeinden um die Bekanntgabe, ob und in welchem Umfang eine stichprobenweise ausgewählte Anzahl Einwohnerinnen und Einwohner fürsorgerische Unterstützungsleistungen bezogen hatten. Diese Daten sollten für eine wissenschaftliche Studie über die Armut in der Schweiz verwendet werden.
Die vom Institut vorgelegten Unterlagen des Projekts liessen die Bekanntgabe im Sinne von § 12 DSG zu, weil sichergestellt war, dass alle personenbezogenen Daten nach Validierung unter notarieller Aufsicht vernichtet werden, die beteiligten Personen eine Datenschutzverpflichtung unterzeichnet hatten, unter den Bestimmungen eines anderen kantonalen Datenschutzgesetzes arbeiteten und zudem eine sichere Aufbewahrung personenbezogener Daten garantiert wurde.
Der Gemeinde wurde empfohlen, bei der Datenübermittlung Vorsichtsmassnahmen zu treffen, weil es sich um besonders schützenswerte Personendaten im Sinne von § 2 lit. d Ziff. 3 DSG handelt. Vorgeschlagen wurde eine separate Übermittlung von anonymisierten, mit einem Schlüssel versehenen Sachdaten und den zum Schlüssel gehörenden Personendaten.
Überdies war das Institut auf die Einhaltung der Datenschutzvorschriften aufmerksam zu machen.

2. Publikation von Neuzuzügern

Zustimmung der betroffenen Personen

Die Publikation der Daten von Neuzuzügern in einem gemeindeeigenen, d.h. von der Gemeindeverwaltung herausgegebenen Informationsorgan (z.B. Gemeindekurier) setzt eine gesetzliche Grundlage oder die Einwilligung der betroffenen Person voraus. Allenfalls darf die Bekanntgabe erfolgen, wenn die Einwilligung der betroffenen Personen nach den Umständen vorausgesetzt werden

darf. Mit dieser Vermutung ist allerdings Zurückhaltung geboten, und die persönliche Einwilligung ist vorzuziehen. Zulässig wäre eine Bekanntgabe auch, wenn eine betroffene Person ihre Daten allgemein zugänglich gemacht hat, was ebenfalls nur ausnahmsweise anzunehmen ist.
Eine gesetzliche Grundlage für Veröffentlichungen der Daten von Neuzuzügerinnen und Neuzuzügern besteht nicht. Die betroffenen Personen geben die notwendigen Angaben beim Neuzuzug in Erfüllung einer gesetzlichen Pflicht (Anmeldung bei der Gemeinde). Damit machen diese Personen ihre Daten aber nicht allgemein zugänglich, wenn sie nicht selbst die Initiative zur Verbreitung ergriffen haben. Demnach verbleibt für die Publikation nur die Zustimmung der betroffenen Personen als Rechtsgrundlage. Sie könnte bei Neuzuzügern im Rahmen des Anmeldeverfahrens eingeholt werden. In diesem Zusammenhang wäre ein Hinweis auf die Freiwilligkeit der Zustimmung zu empfehlen.
Eine Publikationspflicht besteht dagegen beispielsweise bei Todesfällen, für welche die Verordnung über die Bestattungen eine Bekanntmachung der Bestattungen durch die Gemeinde vorschreibt.

3. Verwandtschafts- und Untermietverhältnisse

Keine Angaben von den Einwohnerkontrollen

Ein Rechtsanwalt verlangte zuhanden seiner Klientschaft bei der Einwohnerkontrolle Daten über den geschiedenen Partner und seiner allfälligen Wohnpartner für die Verwendung in einer gerichtlichen Anfechtung des Scheidungsurteils.
Die Bekanntgabe von Personendaten der Einwohnerkontrolle an private Personen und Organisationen wird in § 9 DSG geregelt. Gemäss § 9 Abs. 1 DSG gibt die Einwohnerkontrolle im Einzelfall auf Gesuch ohne Einschränkung (d.h. ohne die Glaubhaftmachung oder den Nachweis eines Interesses prüfen zu müssen) Name, Vorname, Adresse, Datum von Zu- und Wegzug sowie Beruf einer Person bekannt.
Bei Glaubhaftmachung eines berechtigten Interesses sind zudem Zu- und Wegzugsort, Geburtsdatum, Geschlecht, Zivilstand und Heimatort eines Einwohners oder einer Einwohnerin bekanntzugeben. Die Bekanntgabe der Daten kann gegenüber einem mit Vollmacht ausgewiesenen Rechtsvertreter erfolgen, der anstelle und im Namen seines Mandanten als Privatperson im Sinne von § 9 DSG handelt.
An die Glaubhaftmachung eines berechtigten Interesses werden keine hohen Anforderungen gestellt. Es sollen hierbei die rechtsmissbräuchliche Datenbeschaffung (durch Umgehung oder Verletzung einer Vorschrift) und Anfragen aus blosser Neugier ausgeschlossen werden. Hingegen ist ein Rechtsanspruch wie im vorliegenden Fall der Anspruch auf Änderung eines Scheidungsurteils ein genügender Ausweis, wenn glaubhaft dargetan wird, dass die Anfrage der Durchsetzung dieses Anspruchs dient.
Eine Bekanntgabe im Sinne von § 9 unterliegt den Einschränkungen von § 10 und § 11 DSG. In bezug auf § 10 DSG war im vorliegenden Fall nach unserer Beurteilung lediglich zu prüfen, ob offensichtlich schützenswerte Interessen der betroffenen Personen entgegenstanden. Falls eine betroffene Person ihre Daten im Sinne von § 11 DSG sperren liess, muss die Bekanntgabe ihrer Daten unterbleiben, es sei denn, dass ein Gesuchsteller (im vorliegenden Fall die klagende Partei) glaubhaft macht, dass er dadurch in der Verfolgung eigener Rechte behindert wird.
Eine solche Glaubhaftmachung dürfte durch Vorlegung des Scheidungsurteils für die Daten (gemäss § 9 Abs. 1 und 2 DSG) des geschiedenen Partners gelingen.
Die Daten von Mitbewohnerinnen und Mitbewohnern sowie volljährigen Verwandten, soweit sie mit der Urteilsänderung nichts zu tun haben, fallen indessen nicht darunter. Es ist festzuhalten, dass zu den gemäss § 9 DSG bekanntzugebenden Daten nicht die Rechtsbeziehungen von Personen untereinander, die am gleichen Ort wohnen, gehören. Angaben über Verwandtschaft oder Miet- bzw. Untermietverhältnisse sind deshalb ausgeschlossen.

4. Gratulationen zu Jubiläen

Abgabe von Adresslisten mit Geburts- und Hochzeitsdaten

Die Bekanntgabe von Einwohnerdaten an eine Zeitung mit dem Zweck, zu besonderen Jubiläen wie runden Geburtstagen und speziellen Hochzeitsdaten zu gratulieren, ist ein Anwendungsfall von § 9 DSG. Nach § 9 Abs. 3 DSG kann die Einwohnerkontrolle einer privaten Person oder Organisation in Form von Listen, d.h. nach bestimmten Gesichtspunkten geordnet, Name, Vorname, Adresse, Datum von Zu- und Wegzug, Beruf, Geburtsdatum, Geschlecht, Zivilstand und Heimatort einer Person bekanntgeben, wenn der Empfänger diese Daten für schützenswerte ideelle Zwecke verwendet und sie nicht an Dritte weitergibt. Es handelt sich hierbei nicht um eine Bekanntgabeverpflichtung, sondern um eine freiwillige Leistung.
Schützenswerte ideelle Zwecke sind solche, die der Förderung des Gemeinschaftslebens, der politischen Meinungsbildung oder der Kultur auf lokaler Ebene dienen oder die Verfolgung von gemeinnützigen Zielen beinhalten.
Die Gemeinde hat einen eigenen Beurteilungsspielraum bei der Frage, ob eine Aktivität unter diese Definition fällt.
Für eine Bekanntgabe von Namen, Adressen und Geburtstagen braucht es die grundsätzliche Entscheidung der Gemeinde, dass die Veröffentlichung solcher Daten in einer Lokalzeitung als schützenswerter ideeller Zweck anerkannt wird. Bei dieser Entscheidung ist im Interesse einer nicht zu weiten Auslegung von § 9 Abs. 3 DSG darauf zu achten, dass die Veröffentlichung auf das Gemeindegebiet beschränkt bleibt (Lokalzeitung wird in diesem Sinn als Gemeindeblatt verstanden). Diese Zurückhaltung ist mit der Überlegung zu begründen, dass eine Zeitung, die eine Region (mehrere Gemeinden) abdeckt, nicht mehr nur die Funktion hat, dem örtlichen Gemeinschaftsleben zu dienen, sondern an einen weit darüber hinausgehenden Personenkreis gelangt. Die Daten werden damit freier verfügbar für Dritte, die sie (vor allem kommerziell) weiterverwenden können. Das widerspricht dem Ziel von § 9 Abs. 3 DSG. Eine allfällige Bekanntgabe ist denn auch aus diesem Grund mit der Auflage zu verbinden, dass ein Empfänger die Daten (als Listen) nicht an Dritte weitergibt.
Hochzeitsdaten fallen nicht unter § 9 Abs. 1–3 DSG. Das Interesse der betroffenen Personen an der Wahrung ihrer Privatsphäre verlangt hier das Einholen der Zustimmung zur Publikation.

5. Daten für die Kirchgemeinden

Welche Daten dürfen den Kirchen weitergegeben werden?

Die staatlich anerkannten Kirchen benötigen zur Erfassung ihrer Mitglieder und zur Erfüllung ihrer Aufgaben Daten von der Einwohnerkontrolle. Die gesetzlichen Grundlagen für diese Bekanntgabe sind nicht eindeutig.
Wir wurden sowohl von Einwohnerkontrollen als auch von Kirchgemeinden angefragt, welche Daten im Rahmen der Datenschutzgesetzgebung von der politischen Gemeinde den Kirchgemeinden zur Verfügung gestellt werden dürfen. Das Datenschutzgesetz gilt auch für die Datenbearbeitung der öffentlich-rechtlich anerkannten kirchlichen Körperschaften und deren Einrichtungen, soweit der Regierungsrat dafür keine Ausnahmen vorsieht, was bisher nicht der Fall war.
Eine gesetzliche Grundlage für die Bekanntgabe gewisser Daten findet sich in § 39a Gemeindegesetz. Danach erhalten staatlich anerkannte Kirchen aus dem Einwohnerregister der Niederlassungsgemeinde die Mitteilungen, deren sie zur Erfassung ihrer Mitglieder bedürfen. Aus einzelnen Bestimmungen in den spezifischen Rechtsgrundlagen der jeweiligen Kirchen, wie z.B. dem Auftrag zum Erteilen kirchlichen Unterrichts, ergeben sich im weiteren Personendaten, welche zur Erfüllung kirchlicher Aufgaben benötigt werden. Wir haben aufgrund einer Beurteilung

bestehender kirchlicher Erlasse für die evangelisch-reformierte und die römisch-katholische Kirche die folgenden aus dem Einwohnerregister zu übermittelnden Personendaten eruiert: Name und Vorname der Kirchenmitglieder und Haus- bzw. Wohnungsgenossen gleicher Konfession (beim Vorhandensein anderer Konfessionen oder bei Konfessionslosigkeit nur diese Angabe und die Anzahl betroffener Personen ohne Namen); Adresse (Strasse, Nummer, PLZ, Ort); Geschlecht; Geburtsdatum; Zivilstand; Heimatort, Heimatstaat bzw. Nationalität bei Ausländern; Niederlassungsstatus im Gebiet der Kirchgemeinde, Zuzugs- und Wegzugsdatum. Diese Daten sind notwendig für die Führung der Mitgliedschaft, die Ausübung des Stimm- und Wahlrechts, die Seelsorge sowie für die Durchführung des kirchlichen Unterrichts. Dabei handelt es sich um Mindestangaben, welche durch die gesetzlichen Bestimmungen abgedeckt sind und für die Erfassung der Kirchenmitglieder genügen. Es besteht jedoch von kirchlicher Seite ein Interesse an weiteren Personendaten für spezifische kirchliche Aufgaben. Solche Daten sollten gemäss geltendem Gesetz (§ 7 DSG) direkt von den Mitgliedern erhoben werden.
Wir haben die Landeskirchen zu einer Vernehmlassung zur Frage der für die Erfüllung ihrer Aufgaben notwendigen Daten und zur Frage der Notwendigkeit einer speziellen Datenschutzregelung im Kirchenwesen eingeladen. Es hat sich als sinnvoll erwiesen, diese Fragen im Rahmen einer Arbeitsgruppe zu bearbeiten. Die kirchlichen Behörden haben diesem Vorgehen zugestimmt, und eine Arbeitsgruppe, welcher Mitglieder aus den verschiedenen kirchlichen Kreisen und der Einwohnerkontrollen angehören, wurde gebildet. Die Arbeitsgruppe, in der auch der Datenschutzbeauftragte vertreten ist, soll zudem nach Bedarf als Beratungsorgan für die Bearbeitung auftretender Probleme sowie zur gegenseitigen Information und Klärung bei neuen Fragen einberufen werden können.

6. Fragebogen für Wochenaufenthalter

Zu starke Eingriffe in die Privatsphäre

Aufgrund verschiedener Anfragen von betroffenen Personen und Gemeinden nahmen wir Stellung zu Fragebogen, die von Personen ausgefüllt werden müssen, welche sich als Wochenaufenthalter anmelden. In diesen Formularen werden teilweise sehr weit in die persönlichen Verhältnisse greifende Fragen gestellt. Neben Fragen nach den Gründen des Aufenthalts und der Art des Domizils (Wohnung oder Zimmer, möbliert oder unmöbliert, Zimmerzahl, Hotel oder Pension), werden Angaben verlangt über die Art des Zusammenlebens mit einer anderen Person (Konkubinat; Name und Geburtsdatum dieser Person), nach dem Wohnort und den Personalien der Familienangehörigen, dem Aufenthaltsort an freien Tagen, zu Vereinsmitgliedschaften sowie zu Stellung im Beruf und zum Arbeitgeber.
Für die Beurteilung der Zulässigkeit solcher Fragen ist vom verfassungsmässigen Recht auf Niederlassungsfreiheit auszugehen. Dies gewährleistet die Möglichkeit, in jeder beliebigen Gemeinde über kürzere oder längere Dauer zu verweilen.
Die Steuergesetzgebung erlaubt die Erhebung von Personendaten, welche für die vollständige und gerechte Besteuerung der Steuerpflichtigen notwendig sind. Handelt es sich dabei um Wochenaufenthalter, so können die näheren Umstände des Aufenthalts festgestellt werden, da nicht nur der Wohnsitz, sondern auch der Aufenthalt im Kanton und in einer Gemeinde Steuerpflichten begründet (§ 3 Steuergesetz). Es ist davon auszugehen, dass ein Wochenaufenthalter in einer anderen Gemeinde Wohnsitz hat. Zum Nachweis dieser Tatsache ist er auf Verlangen verpflichtet (§ 35 Abs. 2 Gemeindegesetz). Fragen der Steuerpflicht, die sich aus dem Aufenthalt ergeben, sind unter den betroffenen Gemeinden zu regeln. Persönliche Angaben des Bürgers zum (steuerrechtlich wichtigen) Mittelpunkt der Lebensbeziehun-

gen sind nur in jenen Fällen notwendig, in denen in guten Treuen unterschiedliche Auffassungen vertreten werden.
Nach dem Prinzip der Verhältnismässigkeit erachten wir in einer allgemeinen, d.h. alle Wochenaufenthalter betreffenden Erhebung nur Fragen als zulässig, die mit der grundsätzlichen Beurteilung zusammenhängen, ob ein Wochenaufenthalter als Steuerpflichtiger in Frage kommt oder nicht. Der uns vorgelegte Fragebogen verlangt von jeder Person die Beantwortung aller Fragen. Dabei werden auch in einfachen Fällen klaren Wochenaufenthalts viele sehr persönliche Daten erhoben, die in dieser Menge nicht erforderlich sind; es findet gleichsam ein übermässiges Datensammeln auf Vorrat statt. Es könnte sogar durchaus von der Erstellung eines Persönlichkeitsprofils gesprochen werden (§ 2 lit. e DSG), deren Zulässigkeit sich aus einer klaren gesetzlichen Grundlage ergeben müsste (§ 5 DSG). Daher sind in diesem Zusammenhang nur Fragen erlaubt nach der Wohnsitzgemeinde (nicht aber nach den Wohnverhältnissen oder nach Steuerveranlagungsdaten, da der Zweck der Bearbeitung nicht die Steuereinschätzung ist), nach der Aufenthaltsdauer (kürzer oder länger als drei Monate) und nach der Art des Aufenthalts (jedoch nur so formuliert, ob ein steuerrechtlich relevanter Aufenthalt im Sinne von § 3 Abs. 3 Steuergesetz, nämlich in einer Heil-, Pflege-, Erziehungs-, Verwahrungs- oder Strafanstalt, der Besuch einer Lehranstalt oder das Absolvieren einer Berufslehre vorliegt oder nicht). Es kann sich aus der Beantwortung dieser grundsätzlichen Fragen die Notwendigkeit näherer Abklärungen ergeben. Diese wären von der Gemeinde wieder unter möglichster Schonung der Privatsphäre zu treffen, d.h. es wäre z.B. primär danach zu fragen, ob die Lebensbeziehungen innerhalb oder ausserhalb der Gemeinde liegen, jedoch nicht nach persönlichen Details der Freizeitgestaltung oder der partnerschaftlichen Beziehung.
Sowohl unter dem Aspekt der Verhältnismässigkeit als auch unter demjenigen der Zweckbindung der Datenbearbeitung war in den zu beurteilenden Fällen festzuhalten, dass aus den Fragebogen nicht klar ersichtlich war, wer die Daten erhebt. Ob die Daten vom Steueramt oder beispielsweise von der Einwohnerkontrolle erhoben werden, ist von der unterschiedlichen Aufgabe dieser Organe her jedoch relevant. Auf den Formularen muss deshalb angegeben werden, von wem die Daten erhoben werden.

7. Schulpsychologische Dienste

Umgang mit schulpsychologischen Berichten

Die umstrittene Weitergabe eines schulpsychologischen Berichtes in einem Fall zeigte auf, dass im Bereich der schulpsychologischen Dienste sehr sensible Personendaten bearbeitet werden. Der Umgang mit diesen Daten ist gesetzlich nicht ausreichend geregelt.
Den Anlass für ausführliche Abklärungen in diesem Bereich bildete die Anfrage von betroffenen Eltern. Sie wandten sich aus eigener Initiative an den Schulpsychologischen Dienst (kommunaler Zweckverband), um eine Schulreifeabklärung ihrer sechsjährigen Tochter vornehmen zu lassen. Nach einer anschliessenden Besprechung der ersten Abklärung lehnten die Eltern weitere Beratungsgespräche des Schulpsychologen ab. Der zuständige Mitarbeiter des Schulpsychologischen Dienstes verfasste im nachhinein einen Untersuchungsbericht und leitete ihn an die Schulpflege weiter. Die Eltern verlangten zuerst eine Kopie und nachher die Herausgabe oder Vernichtung des Untersuchungsberichtes sowie gleichzeitig eine Vernichtung der gegen ihren Willen an die Schulpflege weitergeleiteten Kopie des Berichtes. Die Angelegenheit konnte im Einverständnis mit allen beteiligten Stellen gelöst werden.
In bezug auf die Herausgabe einer Kopie des Berichtes verweist das Auskunftsrecht gemäss dem Datenschutzgesetz (§ 17 DSG) auf einen grundsätzlichen Herausgabeanspruch der Daten in schriftlicher Form (§ 10 Abs. 2 DSV). Diese Bestimmungen gehen einer revisionsbedürftigen Empfehlung für schulpsychologische Dienste des

Erziehungsrates vom 26. Februar 1985 vor, welche festhält, dass die Eltern in der Regel keinen schriftlichen Bericht erhalten.
Die Weitergabe von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen (schulpsychologischer Bericht) erfordert eine klare gesetzliche Grundlage. Des weiteren ist die Bekanntgabe möglich, wenn sie für den Empfänger im Einzelfall zur Erfüllung einer öffentlichen Aufgabe notwendig ist, wenn die betroffene Person im Einzelfall eingewilligt hat oder die Einwilligung nach den Umständen vorausgesetzt werden darf (§ 8 i.V. mit § 5 DSG). Eine qualifizierte Rechtsgrundlage lag in diesem Fall nicht vor, und die Schulpflege hat nie geltend gemacht, dass sie diesen Bericht benötige. Vielmehr haben die betroffenen Eltern von sich aus den Auftrag zur Schulreifeabklärung gegeben. Auch wenn sie im Zeitpunkt des Auftrages stillschweigend ihr Einverständnis zur Information der Schulpflege gegeben hätten, was umstritten war, konnte zumindest nach dem Widerruf des Auftrages nicht mehr von dieser Zustimmung ausgegangen werden. Damit erwies sich die zwei Monate nach dem Widerruf erfolgte Information der Schulpflege als gesetzeswidrig.
Auch die Aufbewahrung von Personendaten ist eine Datenbearbeitung nach dem DSG und erfordert deshalb eine gesetzliche Grundlage. Eine ausdrückliche gesetzliche Grundlage für das Aufbewahren schulpsychologischer Berichte besteht nicht. Voraussetzung für die Aufbewahrung schulpsychologischer Berichte ist demnach die (auch stillschweigende) Zustimmung der betroffenen Person im Sinne von § 5 lit. c DSG. Das Bundesgericht hat wiederholt festgehalten, dass auch das Aufbewahren persönlicher Daten eine Verletzung der persönlichen Freiheit bedeuten kann, selbst wenn diese Daten nicht öffentlich zugänglich sind (BGE 113 Ia 263f.; 120 Ia 147 f.). Im vorliegenden Fall war auch kein überwiegendes öffentliches Interesse an der Aufbewahrung gegeben. Der schulpsychologische Bericht war deshalb in diesem Fall – unter Vorbehalt archivrechtlicher Bestimmungen – zu vernichten oder der betroffenen Person herauszugeben.
Anlässlich einer Weiterbildungsveranstaltung des Schulärztlichen und Schulpsychologischen Dienstes der Stadt Zürich konnten wir in einem Referat auf verschiedene datenschutzrechtliche Aspekte der Arbeit der Schulpsychologinnen und Schulpsychologen eintreten. Es zeigte sich einerseits, dass die gesetzlichen Grundlagen im Kanton Zürich den schulpsychologischen Bereich nur ungenügend regeln und deshalb auch in bezug auf persönlichkeitsrechtlich relevante Sachverhalte sich heute keine spezifischen Antworten in der Gesetzgebung finden; andererseits steht der Schulpsychologe nur unter dem Amtsgeheimnis nach § 71 des Gemeindegesetzes und nicht auch unter dem Berufsgeheimnis nach Art. 321 StGB, was durch eine Revision des Strafgesetzbuches geändert werden müsste.
Des weiteren ist der Verband der Schulpsychologinnen und Schulpsychologen an uns herangetreten und hat uns ein Merkblatt zur Beurteilung vorgelegt. In diesem Merkblatt, das den Verbandsmitgliedern abgegeben werden soll, werden die wichtigsten datenschutzrechtlichen Fragen aus der Praxis im Sinne einer Handlungsanleitung zusammengestellt.

---

8. Verwaltungsinterne Amtshilfe
Daten des Sozialamtes an andere Amtsstellen

Das Sozialamt einer Gemeinde ersuchte um Stellungnahme zur Frage, ob und allenfalls unter welchen Bedingungen Daten der sozialen Fürsorge anderen Verwaltungsabteilungen, insbesondere dem Steueramt und der Einwohnerkontrolle, mitgeteilt werden dürfen. Die Schweigepflicht verlangt, dass die Beamten und Angestellten einer Gemeinde in Amts- und Dienstsachen Verschwiegenheit bewahren, soweit es sich um Tatsachen und Verhältnisse handelt, welche im Interesse der Gemeinde oder beteiligter Privater geheimzuhalten sind (§ 71 Gemeindegesetz). In der heutigen Lehre und Praxis besteht

weitgehend Einigkeit darüber, dass Amtsgeheimnisse auch zwischen verschiedenen Verwaltungseinheiten gewahrt bleiben müssen, soweit nicht gesetzliche Auskunfts-, Amtshilfe- oder Rechtshilfepflichten bestehen. Solche Pflichten zur Datenbekanntgabe stellen eine gesetzliche Grundlage im Sinne von § 8 Abs. 1 DSG dar und verursachen in der Regel keine Probleme. Schwierigkeiten ergeben sich bei der Beantwortung der Frage, in welchen Fällen Daten für die Erfüllung einer öffentlichen Aufgabe dem Empfänger im Einzelfall zur Verfügung zu stellen sind (§ 8 Abs. 1 lit. a DSG). Nicht in jedem Fall ist eine eindeutige gesetzliche Grundlage für die Datenbearbeitung beim Empfänger gegeben.

Der Entscheid im Einzelfall hat die folgenden Kriterien zu beachten: Die Amtshilfe darf nur geleistet werden, wenn eine gesetzliche Aufgabe vom Empfänger nicht auf andere Weise erfüllt werden kann (Prinzip der Subsidiarität). Die Daten müssen für die Erfüllung der Aufgabe des Empfängers geeignet sein (Prinzip der Verhältnismässigkeit). Des weiteren ist das Prinzip der Zweckidentität zu beachten, das heisst die um Amtshilfe ersuchende Verwaltungsstelle darf die Daten nur für einen Zweck gebrauchen, welcher mit dem ursprünglichen Verwendungszweck der Daten vereinbar ist, indem damit eine gleichartige Aufgabe erfüllt wird. Es gilt zu beurteilen, ob die betroffene Person damit rechnet oder rechnen muss, dass ihre Daten, obwohl zu einem anderen Zweck erhoben, für den vorgesehenen Zweck bearbeitet werden. Eine Amtshilfe darf nicht erfolgen, wenn ihr eine besondere gesetzliche Schweigepflicht entgegensteht.

Ein erheblicher Teil der vom Sozialamt bearbeiteten Personendaten, vor allem jene, die im Zusammenhang mit Massnahmen der sozialen Hilfe stehen, sind besonders schützenswerte Personendaten. Die verwaltungsinterne Bekanntgabe im Sinne der Amtshilfe hat die oben erwähnten Kriterien zu erfüllen.
In bezug auf die Bekanntgabe von einzelnen Daten des Sozialamtes an das Steueramt konnte deshalb folgendes festgehalten werden: Wenn vormundschaftliche Massnahmen angeordnet worden sind und der entsprechende Vertreter die Steuerangelegenheiten besorgt, dürfen die betroffenen Personen und deren Vertretung der Steuerbehörde bekanntgegeben werden. Die Tatsache, dass gewisse Personen, die Sozialhilfe beziehen oder anderweitig Klienten des Sozialamtes sind, ihre Steuerpflichten, wie z.B. das Einreichen der Steuererklärung, nicht erfüllen, berechtigt das Sozialamt hingegen nicht ohne weiteres zur Bekanntgabe ihres Namens oder gar finanzieller Daten an das Steueramt. Hier ist zu prüfen, ob das Steueramt die notwendigen Daten nicht auf eine andere, weniger weit in die Persönlichkeitsrechte eingreifende Weise (als durch Nachfrage beim Sozialamt, das sich mit sensiblen Daten befasst) beschaffen könnte. Ein Steuerpflichtiger, der sich allerdings seiner Zahlungspflicht entzieht, verdient diesbezüglich keinen Schutz. Die Bestimmungen über den Steuerbezug sind hier eine genügende gesetzliche Grundlage für die Bekanntgabe der für eine Eintreibung der Steuerforderung notwendigen Personendaten.
Eine Bekanntgabe der Personalien von Klienten, die nicht in der Lage sind, selber eine Steuererklärung auszufüllen, an das Steueramt zur Weitergabe an private Steuerberater zwecks Übernahme dieser Aufgabe ist ausgeschlossen. Dies wäre nur mit Einwilligung der betroffenen Person möglich (§ 8 Abs. l lit. b DSG).

Die Einwohnerkontrolle benötigt für ihre normale Auskunftstätigkeit gegenüber privaten Personen und Organisationen keine Daten des Sozialamtes. Ihre Auskunftskompetenzen sind in § 9 DSG festgelegt. Besonders schützenswerte Personendaten wie vormundschaftliche Massnahmen fallen nicht darunter, es sei denn, es werde ein besonders schützenswertes Interesse dafür nachgewiesen. Im übrigen fehlt es an einer klaren gesetzlichen Grundlage für eine solche Bekanntgabe.

9. Personendaten auf Stimmrechtsausweis
Nur Adressangaben auf Stimmkuvert

Auf Anfrage haben wir zuhanden der Direktion des Innern eine Stellungnahme zu der von verschiedenen Gemeinden geübten Praxis abgegeben, den Stimmrechtsausweis mit den darauf vorhandenen Personendaten offen mit der Post zu versenden.
Bei Wahlen und Abstimmungen weisen sich die Stimmberechtigten durch ihren Stimmrechtsausweis aus, der gemäss § 10 Wahlgesetz «die unerlässlichen Personalangaben» aufweist. § 7 der Wahlverordnung schreibt in den Ziffern 1 und 2 vor, dass der Stimmrechtsausweis u.a. das Geburtsdatum und die Zugehörigkeit zu einer staatlich anerkannten Kirche, allenfalls die AHV-Nummer sowie die Kennzeichnung für eine besondere Stellvertretung (längerdauernde Verhinderung eines Vertretenen aus medizinischen Gründen) enthält. Der Stimmrechtsausweis kann nach § 8 Wahlverordnung auf dem Kuvert gedruckt sein, das die Abstimmungszettel enthält.
§ 8 Wahlverordnung ist eine gesetzliche Grundlage für die Erhebung des Geburtsdatums sowie der Kirchenzugehörigkeit. Er ist dagegen keine genügende Grundlage für die in vielen Gemeinden geübte Praxis der offenen Postzustellung der Stimmrechtsausweise. § 8 schreibt diese Art der Zustellung nicht vor.
Nach heutiger Rechtsauffassung zum Persönlichkeitsschutz besteht ein gerechtfertigtes und durch das Datenschutzgesetz konkretisiertes Interesse betroffener Personen daran, dass gewisse Personendaten, die der Stimmrechtsausweis enthält, nicht zur Kenntnis von unbestimmten Dritten gelangen. Es handelt sich um das Geburtsdatum, die Zugehörigkeit zu einer staatlich anerkannten Kirche (auch aus dem fallweisen Fehlen dieser Angabe können für betroffene Personen unliebsame Schlüsse gezogen werden), die besondere Stellvertretung (die eventuell Rückschlüsse auf den Gesundheitszustand von Vertretenen erlaubt) und die AHV-Nummer. Im Sinne von § 4 Abs. 3 DSG (Verhältnismässigkeit) ist die Bearbeitung dieser Daten durch offenen Postversand, welcher die Kenntnisnahme durch einen unbestimmbaren Kreis von Personen ohne entsprechende öffentliche Aufgabe ermöglicht, weder geeignet noch erforderlich für die Feststellung der Stimmberechtigung an der Urne, um die es allein geht. Ein solcher Umgang mit Personendaten entspricht auch nicht dem Prinzip der Zweckgebundenheit der Datenbearbeitung (§ 4 Abs. 4 DSG), muss doch der Bürger, wenn er sich bei der Gemeinde anmeldet, nicht damit rechnen, dass die erwähnten Daten in dieser Form unbeteiligten Dritten zugänglich gemacht werden. Bei der Kirchenzugehörigkeit ist zusätzlich festzuhalten, dass diese Angabe geeignet ist, je nach ihrer Verwendung als besonders schützenswertes Personendatum qualifiziert zu werden. Als solches unterliegt es den speziellen Bearbeitungsvoraussetzungen von § 5 DSG, d.h. die Zulässigkeit dieser Bearbeitung (offener Postversand) müsste sich aus einer gesetzlichen Grundlage klar ergeben oder sie müsste zur Erfüllung einer gesetzlich klar umschriebenen Aufgabe unentbehrlich sein. Wahlgesetz und Wahlverordnung genügen diesen Anforderungen nicht.

Wir empfahlen aufgrund dieser Erwägungen, den Gemeinden eine Zustellung des Stimmrechtsausweises in einem Kuvert vorzuschreiben, das ausser Namen und Adresse sowie allenfalls für die spezielle Identifizierung unbedingt notwendige weitere Angaben keine zusätzlichen Personendaten erkennen lässt.
Überdies empfahlen wir eine Änderung der entsprechenden Bestimmungen des Wahlgesetzes und der Wahlverordnung.

10. Fragebogen beim Spitaleintritt

Zulässigkeit der Fragen

Ein Bezirksspital ersuchte um Stellungnahme zum Anmeldeformular, das den Patienten bei oder vor dem Spitaleintritt vorgelegt wird. Das Formular enthält neben betrieblichen Angaben (die vom Spitalpersonal gemacht werden) wie Einweisungsgrund oder Behandlungsart u.a. Fragen an die Patienten nach ihrem Zivilstand, ihrer Konfession, dem Namen und der Adresse sowie der Telefonnummer ihres Arbeitgebers und desjenigen ihrer (zu benachrichtigenden) Angehörigen, dem Bezug einer Hilflosenentschädigung.
Es wird sowohl für stationäre als auch für ambulante Behandlungen verwendet.
Bei Daten, die im Rahmen einer Spitalbehandlung erfasst werden, handelt es sich um besonders schützenswerte Personendaten im Sinne von § 5 DSG. Eine gesetzliche Grundlage für die Erhebung von Patientendaten stellt § 8 Patientenrechtverordnung dar, wonach der Patient auf Verlangen die für die Untersuchung und Behandlung notwendigen oder nützlichen Angaben über seine Person, seine Familie und seine Umgebung erteilen muss. Diese Bestimmung ist abgestützt auf § 42a Gesundheitsgesetz, d.h. eine formellgesetzliche Delegationsnorm, und genügt somit § 5 DSG. Wo es sich nur um die Erhebung nützlicher Daten handelt, die nicht notwendig sind im Sinne von gesetzlich vorgeschriebener Erfassung (etwa Daten, die bloss einer Erleichterung des Betriebs dienen), kann eine Zustimmung der betroffenen Person im Einzelfall genügen.
Wir haben darauf hingewiesen, dass im Sinne der Verhältnismässigkeit bei einer ersten Erfassung der Daten sowenig wie möglich in die persönlichen Verhältnisse der Befragten eingegriffen werden sollte und Details, falls notwendig, in einer weiteren Befragung zu erheben sind. Wir empfahlen, die Notwendigkeit der Erfassung jeder Patientenangabe und die Verwendung eines einheitlichen Formulars sowohl für stationäre als auch für ambulante Behandlung zu überprüfen. Es ist anzunehmen, dass für ambulante Behandlungen wesentlich weniger persönliche Angaben nötig sind, weshalb unterschiedliche Formulare dem Persönlichkeitsschutz mehr Nachachtung verschaffen würden.
Sodann empfahlen wir, die Erhebung der besonders schützenswerten Personendaten «Bezug einer Hilflosenentschädigung» und «Geburtsgebrechen» zu überprüfen, da aufgrund der Ausstattung des Fragebogens mit betrieblichen Daten (Art der Spitalbenutzung, Kostenverrechnung) davon auszugehen war, dass er nicht nur dem unmittelbar zuständigen Pflegepersonal zugänglich ist.
Auf dem Formular waren die Rechtsgrundlagen und der Zweck der Bearbeitung zu ergänzen (§ 7 Abs. 2 DSG). Diese Angaben erlauben der betroffenen Person im Sinne der informationellen Selbstbestimmung, die Tragweite ihrer Bekanntgabe besser abschätzen zu können und die Notwendigkeit eventuell in Frage zu stellen. In diesem Sinn ist es auch angebracht, bei Fragen, die aus betrieblichen Gründen nur nützlich, aber nicht unbedingt im Sinne gesetzlicher Vorschriften nötig sind, klar darauf hinzuweisen, dass ihre Beantwortung freiwillig ist.

11. Überprüfung von Gemeindereglementen

Konkretisierung des Datenschutzgesetzes

Das Datenschutzgesetz und die Datenschutzverordnung verpflichten die Gemeinden und öffentlichen Einrichtungen nicht zum Erlass von speziellen Datenschutzbestimmungen. Solche Regelungen können aber sehr wertvoll sein, beispielsweise als Konkretisierung kantonaler Vorschriften auf Gemeindeebene, als Auslegungshilfen bei unbestimmten Rechtsbegriffen oder als interne Organisationsrichtlinie. Dabei steht es der Gemeinde frei, ob sie sich auf die Regelung einer bestimmten Aufgabe, wie z.B. den Umgang mit Einwohnerkontrolldaten, beschränken oder eine eigentliche

Datenschutzverordnung für die gesamte Verwaltungstätigkeit erlassen will.
Gemeindedatenschutzreglemente sollten aber keine blossen Ausschmückungen und Wiederholungen des Datenschutzgesetzes enthalten. Sie haben die organisatorischen Bestimmungen zu regeln, die für die Organisation des Datenschutzes auf der Ebene der Gemeindeverwaltung notwendig sind, wie beispielsweise die Bezeichnung der verantwortlichen Organe, die Regeln für die Zusammenarbeit zwischen den verantwortlichen Organen, die Bestimmungen für die Führung des zentralen Registers.
Bereits bestehende Datenschutzregelungen auf Gemeindeebene, seien dies Verordnungen, Richtlinien, Reglemente oder interne Weisungen, sind innert zwei Jahren nach Inkrafttreten des Datenschutzgesetzes, d.h. bis zum 31. Dezember 1996, aufzuheben oder an das Gesetz anzupassen. Sie sind somit nicht automatisch am 1. Januar 1995 ausser Kraft getreten, sondern gelten weiterhin; allerdings nur dort, wo sie dem Gesetz und der Verordnung nicht widersprechen. Sind also z.B. die Bekanntgabevoraussetzungen für Einwohnerkontrolldaten in einem Gemeindeerlass einschränkender formuliert als im Gesetz, so geht in diesem Punkt das Gesetz vor.
Die Schwergewichtspunkte bei unseren Stellungnahmen zu den eingereichten Gemeindereglementen lagen bei den Definitionen von Personendaten, den Bekanntgaberegeln und den Bestimmungen über die Datenschutzkontrolle.
Einige Reglemente wiesen Begriffsdefinitionen von Personendaten auf, die sich nicht mit jenen des Datenschutzgesetzes deckten.
Manche enthielten eine nach heutigem Gesetz nicht mehr zulässige Kategorisierung der Personendaten wie «freie Personendaten», «allgemeine Personendaten», «vertrauliche Personendaten» oder «geheime Personendaten» (das DSG unterscheidet nur zwischen Personendaten und besonders schützenswerten Personendaten).
Bei den Bekanntgaberegeln mussten wir auf die unterschiedlichen Bestimmungen für die Verwaltung generell und die Einwohnerkontrolle im speziellen (§§ 8 und 9 DSG) hinweisen. Bei der Datenschutzkontrolle hielten wir fest, dass ein eigentliches Kontrollorgan im Sinne von § 23 DSG, d.h. eine mit Zustimmung des Regierungsrats bestellte Aufsichtsstelle, weitestgehend von der Verwaltung unabhängig sein muss. In seiner Überwachungsfunktion zur Anwendung der Datenschutzvorschriften hat es nämlich weitreichende Auskunfts- und Einsichtskompetenzen, und zudem ermöglicht ihm seine Befugnis, sich Datenbearbeitungsabläufe vorführen zu lassen, eine Einflussnahme auf die Verwaltungsorganisation, weshalb die Gefahr von Interessen- und Kompetenzkonflikten in diesem Bereich von Anfang an auszuschliessen ist.
Den Wunsch nach einem Musterreglement für die Gemeinden, der wiederholt an uns herangetragen wurde, haben wir zusammen mit den interessierten Verbänden aufgenommen. Eine Arbeitsgruppe soll ein solches Musterreglement vorlegen.

Informationssicherheit – Anstrengungen notwendig

Ein Kernelement des Datenschutzes ist die Datensicherheit. Personendaten sind durch angemessene organisatorische und technische Massnahmen gegen das unbefugte Bearbeiten zu schützen (§ 4 Abs. 5 DSG).

1. Informatikstrategie und Datensicherheit

Kantonale Verwaltung

Die kantonale Informatik- und Kommunikationsstrategie für die administrative Verwaltung von 1993 sieht in ihrer Realisierungsstrategie das Erstellen von Richtlinien für Programm- und Datensicherheit (Sicherheitsdispositiv) vor. Bisher sind aber keine diesbezüglichen Aktivitäten entwickelt worden. Das Fehlen eines solchen Sicherheitskonzepts führt dazu, dass keine Beurteilung der Gesamtrisikosituation vorliegt und dass Einzelprojekte in bezug auf die Datensicherheit nur schwer beurteilbar sind. Wir haben bei verschiedener Gelegenheit auf diese unbefriedigende Situation hingewiesen. Datensicherheit muss ein integraler Bestandteil jedes EDV-Projektes sein. In Projekten und Arbeitsgruppen, in denen wir beigezogen wurden, gaben wir Hinweise, wie die Datensicherheit nach den Anforderungen des Datenschutzgesetzes zu realisieren ist. Wir stellten aber auch fest, dass der Datensicherheit oftmals nicht der notwendige Stellenwert eingeräumt wird und Personendaten deshalb vermeidbaren Risiken ausgesetzt sind.

2. Sicherheit in Datennetzen

Eine Studie des Datenschutzbeauftragten

Mit der von uns vorgelegten Studie von Prof. Dr. Ueli Mauer, ETH Zürich, «Sicherheit in Datennetzen», haben wir versucht, Risiken und Lösungsmöglichkeiten in einem besonders sensiblen Bereich der modernen Datenbearbeitung aufzuzeigen. Die Vernetzung von EDV-Arbeitsplätzen, verteilte und offene Systeme beinhalten hohe Risiken vor allem in bezug auf die Vertraulichkeit, Integrität und Authentizität von Personendaten. Um diese Risiken vermeiden zu können, sind angemessene technische und organisatorische Massnahmen notwendig. Die Studie vermittelt den verantwortlichen Datenbearbeitern die Grundlagen, um die nach dem Datenschutzgesetz verlangten Massnahmen treffen zu können. Sie wurde allen interessierten kantonalen und kommunalen Verwaltungsstellen zur Verfügung gestellt und hat ein sehr positives Echo ausgelöst.

3. Datenverschlüsselung bei der Direktion der Justiz

Sensible Daten über Netzwerke

Die Datenbearbeitung der Justizdirektion ist stark geprägt vom Datenaustausch über Netzwerke. Auf zentralen Rechnern sind die Daten gespeichert, wobei über lokale Netze und das kantonale Netz der Zugriff durch die Benutzerinnen und Benutzer erfolgt (z.B. Bezirksanwaltschaften). Bei einem grossen Teil der bearbeiteten Daten handelt es sich um besonders schützenswerte Personendaten nach dem Datenschutzgesetz (z.B. Daten über strafrechtliche Verfolgungen und Sanktionen). Die Justizdirektion legte uns ein Projekt zur Beurteilung vor, welches die Verschlüsselung des gesamten Datenverkehrs auf dem Netzwerk, die Chiffrierung abgespeicherter Daten sowie eine Sicherung der einzelnen PC-Arbeitsplätze vorsieht. Aus datenschutzrechtlicher Sicht konnte in bezug auf die vorgeschlagenen Massnahmen festgestellt werden, dass sie dem Stand der Technik und dem Grundsatz der Verhältnismässigkeit entsprechen und die Anforderungen des Datenschutzgesetzes erfüllen können.

4. Anschluss des kantonalen Netzwerkes an das Internet

Organisatorische und technische Massnahmen notwendig

Aus datenschutzrechtlicher Sicht haben wir zum Anschluss des kantonalen Netzwerkes (KZH-Netz) an das Internet differenziert Stellung bezogen.
Für die angemessenen Datensicherheitsmassnahmen ist grundsätzlich dasjenige Organ verantwortlich, welches die Daten zur Erfüllung seiner Aufgabe bearbeitet oder bearbeiten lässt (§ 6 Abs. 1 DSG). Das Fehlen einer kantonsweiten Informationssicherheitsstrategie führt dazu, dass das verantwortliche Organ Auswirkungen einzelner Projekte, wie zum Beispiel den Anschluss des KZH-Netzes an das Internet, nicht beurteilen kann, da die Auswirkungen solcher Massnahmen in bezug auf die Sicherheitssituation nicht transparent sind.
Das einzelne Organ hat deshalb davon auszugehen, dass Daten in einem Netz nicht sicher sind und dass nur eventuell aufgrund einer Risikoanalyse gewisse Teile eines Netzes als sicher betrachtet werden könnten. Es hat eigenständig die nach dem Stand der Technik und dem Prinzip der Verhältnismässigkeit notwendigen Sicherheitsmassnahmen zu treffen. Dies kann konkret beinhalten, dass sensible Daten nur verschlüsselt über das KZH-Netz zu übertragen sind und eigene Netze eventuell wieder gegenüber dem KZH-Netz abzusichern sind, um die Vertraulichkeit, Verfügbarkeit und Integrität der Daten gewährleisten zu können.
Aus diesen Gründen ist es notwendig, dass das Konzept und die Lösung des Anschlusses des KZH-Netzes an das Internet für alle beteiligten Stellen – darunter fallen auch solche, die diesen Anschluss nicht benutzen werden – klar kommuniziert wird.

Die vorgeschlagene Lösung des Anschlusses («Firewall») kann heutigen technischen Anforderungen an einen abgesicherten Zugang zum Internet entsprechen. Gerade in diesem Bereich ist die Entwicklung aber äusserst dynamisch und verlangt eine ständige Überprüfung der einmal getroffenen Massnahmen. Auch sind neben informationstechnischen Massnahmen organisatorische Massnahmen zu treffen. Für deren Einhaltung ist eine entsprechende Kontrolle vorzusehen. Das Konzept der Implementation des «Firewalls» ist transparent zu gestalten. Der Betrieb des Servers ist durch kompetente Personen zu gewährleisten und permanent zu überwachen. Alle relevanten Vorgänge sind festzuhalten und umfassend auszuwerten. Klare Kompetenzregelungen und eine regelmässige externe Kontrolle sind vorzusehen.
Da die Sicherheitssituation sich dauernd ändern kann, ist laufend über die Entwicklungen und die getroffenen Massnahmen zu orientieren. Der Datenschutzbeauftragte verlangte, dass er über das Konzept der Implementation, den Betrieb und dessen Überwachung sowie die laufenden «Alarms» und Massnahmen ständig informiert wird.
Damit kann die notwendige Transparenz in bezug auf die Sicherheit der Daten geschaffen werden.

5. Vernichtung elektronischer Daten

Benutzung von CD-WORM zur Datenspeicherung

Eine Anfrage des Amts für Administrativmassnahmen im Strassenverkehr führte dazu, dass wir uns eingehender mit der Speicherung von Personendaten auf neuen Medien (CD-WORM), insbesondere in bezug auf die Vernichtung solcher Daten beschäftigten.
Gemäss § 14 Abs. 1 Datenschutzgesetz (DSG) sind nicht mehr benötigte Personendaten zu vernichten (unter Vorbehalt der Bestimmungen über die Archivierung). Das für die Bearbeitung der Daten verantwortliche Organ legt für jede Datensammlung fest, wann die Personendaten zu vernichten sind (§ 14 Abs. 2 DSG). Es ist dabei an die in seinem Bereich geltenden gesetzlichen Grundlagen gebunden.
Mit dem Begriff der «Vernichtung» ist grundsätzlich die physische Vernichtung der Daten gemeint. Solange solche Daten auf Papier

festgehalten sind, lässt sich diese Vernichtung durch entsprechende Aktenvernichtungsanlagen einfach bewerkstelligen. Die mit neuen Technologien (EDV) gespeicherten Daten sind heute nicht mehr ohne weiteres zu vernichten. Was im Sinne einer beweissicheren Aufbewahrung notwendig ist, bereitet in bezug auf die datenschutzrechtliche Anforderung der Vernichtung besondere Schwierigkeiten.
Insbesondere die neuen Datenträger auf opto-elektronischer Basis (CD-WORM), welche die Speicherung von sehr grossen Datenmengen auf einer physischen Einheit erlauben, werden heute zunehmend eingesetzt. Dabei gelangen überwiegend einmal beschreibbare Platten zum Einsatz, was bedeutet, dass die zu speichernde Information einmalig abgespeichert werden kann und nachher nur noch im Lesezugriff steht (sog. WORM-Technologie: «Write Once Read Many»).
Es können insbesondere drei Möglichkeiten der Datenvernichtung von solchen Datenträgern in Erwägung gezogen werden:
Die physische Vernichtung des Datenträgers (z.B. durch Shreddern) erfüllt die Anforderungen des Gesetzes auf Vernichtung der Daten vollumfänglich. Bei der Weitergabe an Dritte zur Entsorgung ist durch entsprechende Absicherung zu gewährleisten, dass die Platte tatsächlich vernichtet wird. (Daten auf opto-elektronischen Platten lassen sich nur durch chemische Methoden eindeutig löschen.)
Die logische Löschung meint die Vernichtung des Zugriffsschlüssels (Index) auf die Daten. Der Index wird bei diesen Datenträgern als Datei auf einem übergeordneten Datenverwaltungssystem geführt, welches mit wieder beschreibbaren Speichermedien arbeitet. Für die Vernichtung des Zugriffsschlüssels kommt deshalb insbesondere das technische Überschreiben (mehrfaches Überschreiben mit zufälligen Zeichenfolgen) in Frage.
Mit dem «organisatorischen Löschen» ist gemeint, dass die Organisationsabläufe der Datenspeicherung so gestaltet werden, dass der Datenträger möglichst umgehend nach dem Eintritt der gesetzlichen Vernichtungspflicht physisch vernichtet werden kann. Dies bedeutet, dass Daten mit einer etwa gleich langen Aufbewahrungsfrist auf den gleichen Datenträger geschrieben werden, was nach Ablauf der Frist die gesamthafte Vernichtung des Datenträgers ermöglicht.
Bei einem Restbestand von noch wenigen aufzubewahrenden Daten können diese auf einen neuen Datenträger übertragen werden, so dass der alte Datenträger zur Vernichtung freigegeben werden kann.
Wir empfahlen den Einsatz der WORM-Technologie unter Berücksichtigung der notwendigen organisatorischen und technischen Massnahmen. Diese beinhalten insbesondere die Festlegung der maximalen Aufbewahrungsdauer eines Datenträgers und dessen Vernichtung nach Ablauf dieser Frist, das Speichern von Daten mit einer gleichen Aufbewahrungsdauer auf den gleichen Datenträger, das Führen der Index-Datenbank auf dem EDV-System mit den notwendigen Datensicherheitsmassnahmen sowie organisatorische Richtlinien für den Umgang mit logisch gelöschten Daten.

6. Vernichtung von Akten mit Personendaten

Sichere Papierentsorgung

Wir sind vom Universitätsspital beigezogen und von der Polizeidirektion angefragt worden bezüglich Richtlinien für eine datenschutzkonforme Entsorgung von Papieren und Akten mit Personendaten. Im Universitätsspital fallen jährlich etwa 160 Tonnen Papier mit Personendaten zur Vernichtung an. Um die Datensicherheit bei dieser Menge gewährleisten zu können, wurde entschieden, eine hauseigene Shredderanlage einzusetzen und ein entsprechendes Konzept für das Einsammeln und Entsorgen der Papiere zu erstellen.
In bezug auf die Vernichtung vertraulicher Akten in der kantonalen Verwaltung erliess die Staatskanzlei am 4. Dezember 1995 auf

unseren Vorschlag eine Weisung, worin die Entsorgung von Papieren über die kantonale Drucksachen- und Materialzentrale (KDMZ) geregelt wird. Die KDMZ besitzt eine Shredderanlage, und für den Transport vertraulicher Akten zur Vernichtung werden entsprechende Säcke zur Verfügung gestellt. Ebenso ist es möglich, den Transport und die Vernichtung der Akten von eigenem Personal begleiten zu lassen. Durch dieses Vorgehen können die datenschutzrechtlichen Anforderungen an die Datensicherheit erfüllt werden. Das einzelne Organ kann aufgrund der Sensibilität der Daten das verhältnismässige Vorgehen in bezug auf die Vernichtung wählen.

7. Datenaufzeichnungen in Telefonanlagen

Absicherung durch technische und organisatorische Massnahmen

In einem Gutachten nahmen wir Stellung zu den Aufzeichnungsmöglichkeiten einer neuen Telefonanlage für eine Verwaltungsabteilung. Dabei stellten wir fest, dass diese Teilnehmervermittlungsanlage (TVA) grundsätzlich die Aufzeichnung von Daten über Verbindungen und das Aufzeichnen von Gesprächen zulässt. Die im Rahmen des Rechtsgutachtens festgehaltenen Bedingungen für eine Aufzeichnung solcher Daten sind deshalb in der Einführung der TVA durch entsprechende technische und organisatorische Massnahmen abzusichern.
Die im Gutachten zu beantwortenden Fragen bezogen sich auf die Aufzeichnung des Inhalts sämtlicher Gespräche, die von einem Telefonapparat aus geführt werden, eventuell nur der externen Gespräche und auf die Protokollierung der Verbindungsdaten (Zeitpunkt und Dauer des Gespräches, vollständige Rufnummern).
Der Zugang zu diesen Daten sollte im Bedarfsfall bestimmten verwaltungsinternen Personen vorbehalten sein.
Nach der Rechtsprechung gehören Telefongespräche zur Privatsphäre. Das Telefon- und Telegrafengeheimnis ist auch in Art. 36 Abs. 4 der Bundesverfassung geschützt. Das Aufzeichnen von Gesprächen mit Drittpersonen hat sich insbesondere nach den Prinzipien des öffentlichen Interesses, der Verhältnismässigkeit und des Grundsatzes von Treu und Glauben zu richten. Im Rahmen der allgemeinen Verwaltungstätigkeit besteht keine gesetzliche Grundlage, welche die Aufnahme von Telefongesprächen generell erlauben würde. Eine Gesprächsaufzeichnung wäre deshalb nur möglich, wenn sowohl die verwaltungsinterne Person als auch die verwaltungsexterne Person im Einzelfall zustimmen würden. Es müsste hierzu jedoch ein überwiegendes öffentliches Interesse der Verwaltungsstelle für ein solches Vorgehen im Einzelfall bestehen.
In bezug auf die Protokollierung von Verbindungsdaten hielten wir fest, dass das Aufzeichnen solcher Daten im dienstlichen Verkehr erlaubt sein kann, wenn es beispielsweise darum geht, dem Angerufenen die Kosten des Gespräches zu belasten. Eine entsprechende Rechtsgrundlage müsste dies vorsehen. Die Protokollierung hat sich auf die für den Zweck notwendigen Angaben zu beschränken. Private Gespräche von Verwaltungsangestellten sind differenziert zu betrachten, und die Aufzeichnungsmöglichkeiten von Daten sind davon abhängig, ob grundsätzlich solche Gespräche erlaubt sind oder nicht und ob eventuell eine direkte Verrechnung des einzelnen Gespräches erfolgt.
Bei Telefonanlagen mit der Möglichkeit der Gesprächsaufzeichnung und der Protokollierung von Verbindungsdaten empfiehlt es sich deshalb auch, in einem Betriebsreglement die Kompetenzen und Verantwortlichkeiten in bezug auf den Einsatz der Anlage festzuhalten.

Sensibilisierung für Anliegen des Datenschutzes

Die Information über wesentliche Anliegen des Datenschutzes gehört zu den Kernaufgaben des Datenschutzbeauftragten (§ 23 lit. e DSG). In der Einführungsphase des Datenschutzgesetzes kommt ihr eine wesentliche Bedeutung zu.

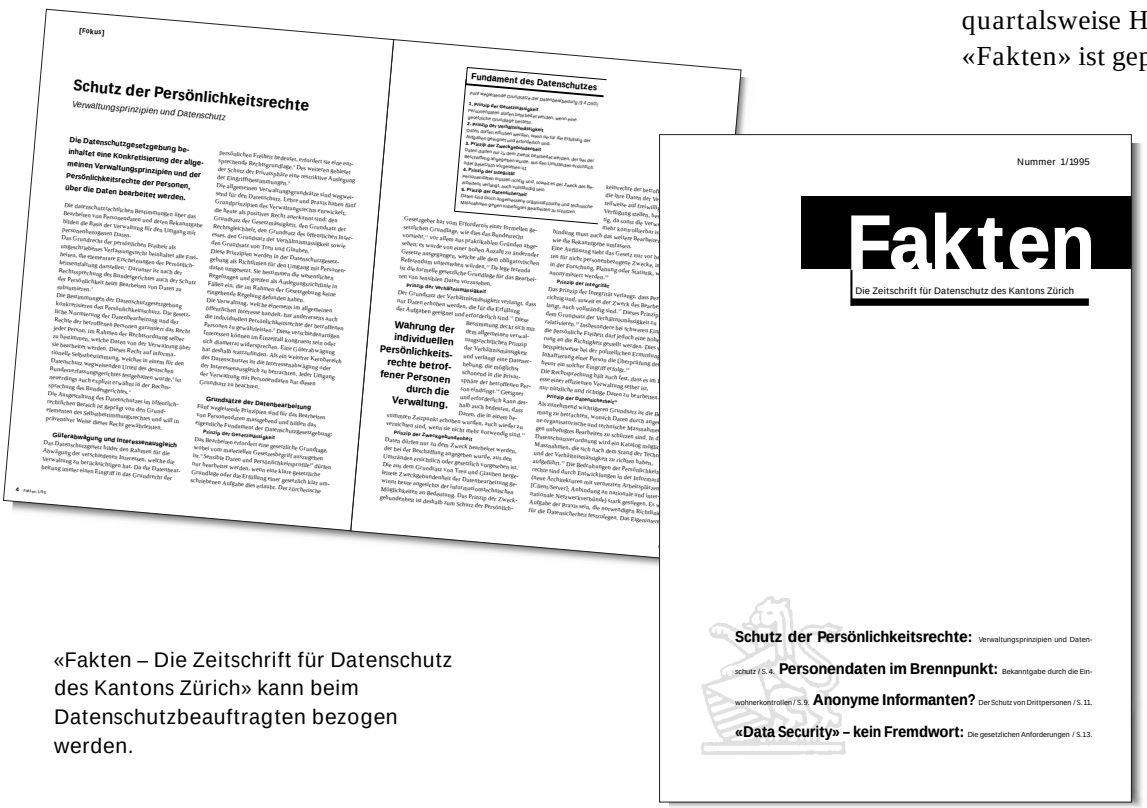
1. «Fakten»

Die Zeitschrift für Datenschutz des Kantons Zürich

Ein sehr positives Echo bei den Leserinnen und Lesern haben die ersten beiden Nummern von «Fakten – Die Zeitschrift für Datenschutz des Kantons Zürich», welche wir 1995 herausgegeben haben, ausgelöst. Wir haben Fakten als Informationsmedium geschaffen, um über die aktuellen Fragen des Datenschutzes und der Datensicherheit im Kanton Zürich zu informieren und die Verwaltungsstellen bei der Anwendung der datenschutzrechtlichen Bestimmungen in ihrem Arbeitsgebiet zu unterstützen. In «Fakten» werden grundsätzliche Fragen des Persönlichkeitsschutzes und der Datensicherheit aufgenommen und konkrete Fälle und Anliegen aus der Praxis der Verwaltung, welche auch für die anderen Amtsstellen und Behörden von Bedeutung sind, dargestellt.

Als Themenschwerpunkt hat die Nummer 1 von «Fakten» die Problematik der Datenbekanntgaben und des Amtsgeheimnisses aufgegriffen. «Fakten» Nr. 2/1995 befasste sich mit der Transparenz der Datenbearbeitung, welche mit dem Register der Datensammlungen gewährleistet wird. Eine Sondernummer zum Thema Sicherheit in Datennetzen wurde Ende Dezember herausgegeben (siehe S. 28).

«Fakten» wird nach Bedarf den kantonalen und kommunalen Verwaltungsstellen zur Verfügung gestellt. Die Nachfrage nach Informationen über Datenschutz und Datensicherheit in dieser Form war sehr gross. Die Auflage der Nummer 1 von «Fakten» war sehr rasch vergriffen, weshalb ein Nachdruck notwendig wurde. Für die Nummer 2 musste die Auflage verdoppelt werden. «Fakten» soll von den Verwaltungsstellen aufbewahrt werden und mit der Zeit ein Nachschlagewerk für die Praxis des Datenschutzes im Kanton Zürich bilden. Die regelmässige, quartalsweise Herausgabe von «Fakten» ist geplant.



«Fakten – Die Zeitschrift für Datenschutz des Kantons Zürich» kann beim Datenschutzbeauftragten bezogen werden.

2. Seminare zum Datenschutz

Vermittlung von Datenschutzgrundlagen

Im zweiten Halbjahr 1995 führten wir in Zusammenarbeit mit der kantonalen Aus- und Weiterbildung (Finanzdirektion) halbtägige Seminare zum Datenschutz durch. Ziel dieser Seminare war es, die datenschutzrechtlichen Grundsätze zu vermitteln, damit die Verwaltungsstellen ihre Verantwortung im Bereich des Datenschutzes und der Datensicherheit wahrnehmen können. Neben den grundsätzlichen Ausführungen wurden auch Fallbeispiele aus der Praxis besprochen und die Fragen der Teilnehmerinnen und Teilnehmer beantwortet. Diese Seminare richteten sich an Führungskräfte, Kaderleute, Vorgesetzte und Stabsmitarbeiterinnen und -mitarbeiter. Es waren Teilnehmerinnen und Teilnehmer fast sämtlicher Direktionen der kantonalen Verwaltung vertreten. Die Tatsache, dass sämtliche Seminare innert kurzer Frist ausgebucht waren, zeigt das grosse Bedürfnis nach praxisbezogener Information in diesem Bereich. Das Seminar wurde von den Teilnehmerinnen und Teilnehmern in bezug auf Form und Inhalt überwiegend mit sehr gut beurteilt. Weitere, ganztägige Seminare werden 1996 durchgeführt werden. Dem vielfach geäusserten Wunsch nach bereichsspezifischen Seminaren oder Seminaren für bestimmte Berufsgruppen (Juristinnen und Juristen, Informatikerinnen und Informatiker etc.) konnte aus Kapazitätsgründen nicht immer entsprochen werden und soll deshalb möglichst in kommenden Jahren Rechnung getragen werden.

3. Referate zum Datenschutz

Informationen zu bereichsspezifischen Fragen

In zahlreichen Referaten haben wir Grundlagen des Datenschutzes vermittelt und zu bereichsspezifischen Datenschutzfragen Stellung bezogen.
In der kantonalen Verwaltung hatten wir Gelegenheit, bei der Generalsekretärkonferenz, bei Direktionsrapporten der Direktion des Innern und der Militärdirektion zu referieren, und wir wurden für Vorträge eingeladen von der Direktion der Justiz (Opferhilfe-Beratungsstellen), der Finanzdirektion (Rapport der Personalverantwortlichen) sowie zahlreichen weiteren Amtsstellen.
Des weiteren hielten wir Referate anlässlich einer Tagung des Europa-Institutes der Universität Zürich, beim Verband der Zürcher Einwohnerkontrollen, beim Schweizerischen Verband der Einwohner- und Fremdenkontrollchefs, an einer Tagung der Bezirksratsschreiber, beim Gemeindeschreiberverband des Bezirkes Pfäffikon, beim Schulärztlichen und Schulpsychologischen Dienst der Stadt Zürich, um hier nur einige zu nennen.

4. Telefonische Beratungen

Beantwortung von Rechtsfragen

Fast täglich gehen mehrere telefonische Anfragen von Verwaltungsstellen sowie Bürgerinnen und Bürgern ein, welche Rechtsauskünfte in bezug auf den Datenschutz verlangen. Bei dieser Gelegenheit informieren wir die anrufenden Personen über die Rechtslage nach dem Datenschutzgesetz und nehmen komplexere Sachverhalte zur weiteren Abklärung entgegen. Viele dieser Anfragen erhalten wir auch von kommunalen Amtsstellen und Behörden, die nicht über juristische Mitarbeiterinnen oder Mitarbeiter verfügen, sich jedoch täglich zum Teil mit sensiblen Datenbearbeitungen beschäftigen (Einwohnerkontrollen, Sozialämter, Schulpflegen usw.). Bürgerinnen und Bürger stellen uns

Fragen zu den unterschiedlichsten Sachverhalten, welche den Verkehr mit der Verwaltung und die diesbezüglichen Datenbearbeitungen betreffen. Dabei geht es – um einige Beispiele zu nennen – um die Geltendmachung des Auskunftsrechts, die Sperrmöglichkeit von Daten, die Herausgabe von Daten, die Verwendung der AHV-Nummer in der Adresse, Videoaufnahmen durch die Polizei. Wir stellten fest, dass vielfach keine Unterscheidung zwischen Datenbearbeitungen durch private Personen oder Organisationen und Verwaltungsstellen gemacht wird. Wir leisten hierbei die notwendige Informationsarbeit.

5. Zusammenarbeit der Datenschutzbeauftragten

Informationsaustausch

Dem Aufbau einer Zusammenarbeit mit anderen Datenschutzbeauftragten wurde 1995 grosses Gewicht beigemessen. Ein regelmässiger Informations- und Meinungsaustausch in diesem Bereich ist notwendig, um einen effizienten und praxisbezogenen Datenschutz verwirklichen zu können. Der Kanton Zürich kann dabei von Erfahrungen in anderen Kantonen, im Bund und in Nachbarländern profitieren, die teilweise schon seit Jahren über eine Datenschutzgesetzgebung verfügen. Ausserdem zeigt sich, dass die Entwicklungen im Bereich der Persönlichkeitsrechte wie auch im Gebiet der Technik in bezug auf die Datensicherheit vermehrt gemeinsame Bemühungen erfordern, um adäquate Lösungen für die Verwaltung erarbeiten zu können.

Die Zusammenarbeit mit den Kantonen Bern, Baselland, Freiburg und Luzern, welche sich zu einer informellen Arbeitsgruppe zusammengeschlossen haben, stand dabei im Vordergrund. Weitere Kontakte bestehen punktuell zu anderen kantonalen und kommunalen Datenschutzbeauftragten.

Der Eidgenössische Datenschutzbeauftragte hat im Oktober 1995 die Zweite Nationale Konferenz der Datenschutzbeauftragten in Bern durchgeführt. Diese Konferenz bot einen Informationsaustausch über aktuelle Fragen des Datenschutzes in der Schweiz.
Im übrigen bestehen Kontakte mit dem Eidgenössischen Datenschutzbeauftragten insbesondere bei Fragen des Vollzugs von Bundesrecht durch den Kanton.

Die XVII. Internationale Konferenz der Datenschutzbeauftragten fand im September 1995 in Kopenhagen statt. Diese Konferenz vereinigt die Datenschutzbeauftragten von nationalen, regionalen und kommunalen Verwaltungen aus den verschiedenen europäischen Ländern sowie von aussereuropäischen Staaten. Schwerpunkte der diesjährigen Konferenz waren die Entwicklungen des Datenschutzrechts im europäischen Rechtsgebiet und ihre Bedeutung für die einzelnen Länder sowie die technologischen Entwicklungen und ihre Auswirkungen auf den Datenschutz und die Datensicherheit.

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

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