Nummer 11

Tätigkeitsbericht 2005

SYSTEM CERTIFICATION ISO 9001:2000 SGS

Datenschutz
mit Qualität

dsb

datenschutzbeauftragter
kanton zürich

Nummer 11
Tätigkeitsbericht 2005

Der Datenschutzbeauftragte erstattet dem Regierungsrat jährlich oder nach Bedarf einen Bericht über seine Tätigkeit (§ 23 Datenschutzgesetz). Der vorliegende Tätigkeitsbericht Nr. 11 [2005] deckt den Zeitraum vom 1. Januar 2005 bis 31. Dezember 2005 ab.

Der Bericht ist auch auf der Website **www.datenschutz.ch** veröffentlicht.

Zürich, Juni 2006

Der Datenschutzbeauftragte des Kantons Zürich
Dr. Bruno Baeriswyl

Datenschutzbeauftragter des Kantons Zürich
Postfach, 8090 Zürich
Tel.: 043 259 39 99
Fax: 043 259 51 38
datenschutz@dsb.zh.ch
www.datenschutz.ch

Inhaltsverzeichnis

VI. INFORMATION

VII. ENTWICKLUNGEN

ANHANG

Erneuerung des Datenschutzes

Gleich zwei Ereignisse – die Einführung des Öffentlichkeitsprinzips und die Assoziierung der Schweiz an Schengen und Dublin – bringen eine Erneuerung des Datenschutzes auf gesetzlicher Ebene.

Bereits bevor die neue Verfassung im Kanton Zürich das Prinzip der Öffentlichkeit der Verwaltung zum Grundsatz erklärte, waren aufgrund einer kantonsrätlichen Motion Vorbereitungen im Gange zur Einführung des Öffentlichkeitsprinzips. Der Zugang zu Informationen ist sehr stark mit dem Schutz der Informationen – dem Datenschutz – verknüpft: Beide Materien sind die Kehrseite derselben Medaille. Ein Entscheid über den Schutz der Privatheit der Bürgerinnen und Bürger, sei es auf Gesetzesebene oder in einer konkreten Interessenabwägung, ist gleichzeitig auch immer ein Entscheid über den Zugang oder den Nichtzugang zu Informationen. Da aufgrund der technischen Möglichkeiten der Grossteil der Informationen sich mit Leichtigkeit einer bestimmten oder bestimmbaren Person zuordnen lässt, ist auch immer der Datenschutz involviert.

Konsequente Verzahnung

Von Anfang an wurden deshalb im Kanton Zürich die beiden Materien als Einheit betrachtet, und der Entwurf eines Informations- und Datenschutzgesetzes (IDG) enthält eine konsequente Verzahnung von Informationszugang und Datenschutz. Im vergangenen Jahr wurde eine breite Vernehmlassung zu diesem Gesetzesentwurf abgeschlossen, und im November 2005 hat der Regierungsrat die Vorlage zuhanden des Kantonsrats verabschiedet.

Die Betrachtung von Informationen – von ihrer Entstehung bis zu ihrer Archivierung oder Vernichtung – in einem Prozess ermöglicht es, für die verschiedenen Stadien die Rahmenbedingungen festzulegen. Dabei ist Information der Oberbegriff und der Umgang mit personenbezogener Information – Personendaten oder besondere Personendaten – braucht nur noch da eine spezifische Regelung, wo die Privatheit der Bürgerinnen und Bürger betroffen ist. Dies ist insbesondere der Fall bei der Erhebung der Information und bei deren Weitergabe. Beim Recht auf Zugang zu Informationen sind die Interessen der betroffenen Person so weit abgedeckt, dass sie beim Zugang zu Personendaten angehört wird und der Zugang zu besonderen Personendaten nur mit ihrer Zustimmung erfolgen kann.

Sicherheit mit Qualitätssiegel

Die Betrachtung des Informationsprozesses in seiner Gesamtheit ermöglicht auch eine konsequente Abbildung im informationstechnischen Prozess. Das Gesetz setzt dabei nicht nur Rahmenbedingungen in Bezug auf Datenvermeidung und Datensparsamkeit, sondern übernimmt auch die bewährten Prinzipi-

en in Bezug auf die Datensicherheit. Weiter soll es möglich werden, mit einem Qualitätssiegel die Umsetzung der Vorgaben zu belegen.

Offen bleibt die zukünftige Rolle des Datenschutzbeauftragten in Bezug auf den Informationszugang. Im ursprünglichen Entwurf war noch vorgesehen, dass ein Informations- und Datenschutzbeauftragter die Verwaltung und die Bürgerinnen und Bürger in Sachen Informationszugangsrecht und Datenschutz berät. Neuere Gesetzgebungen in der Schweiz (Bund, Kantone Solothurn und Aargau) wie auch im benachbarten Ausland sehen durchwegs diese Funktion vor. Sie widerspiegelt die gesamtheitliche Betrachtungsweise des Informationsprozesses. Der Regierungsrat hat die Funktion des Beauftragten für das Informationszugangsrecht indessen aus der Vorlage gestrichen.

Insgesamt bringt der Entwurf des Informations- und Datenschutzgesetzes (IDG) eine ausgewogene Regelung der Interessen am Zugang zu Informationen und am Schutz der Privatheit der Bürgerinnen und Bürger. Es ist zu hoffen, dass der Kantonsrat die Grundanliegen dieser Gesetzgebung breit unterstützen kann und – wo notwendig – allfällige Verbesserungen und Konkretisierungen anbringt.

Assoziierung an Schengen/Dublin

Im Juni des vergangenen Jahres hat die schweizerische Stimmbevölkerung der Assoziierung der Schweiz an Schengen und Dublin zugestimmt. Damit kommt es zu einer engen Zusammenarbeit der Schweiz mit der Europäischen Union im Bereich der Polizei und Justiz sowie im Asylwesen. Kernpunkt in der polizeilichen Zusammenarbeit ist das Schengener Informationssystem (SIS), eine europaweite Plattform zum Austausch von polizeilichen Fahndungsinformationen. Befürchtungen im Vorfeld der Abstimmung, es komme hier zu einem Polizeistaat, wurden zerstreut mit dem Hinweis, die EU habe auch klare Vorkehrungen zum Schutz der Privatheit der Bürgerinnen und Bürger getroffen.

Tatsächlich bestehen auf der Ebene der EU zahlreiche Vorgaben für den Umgang mit Personendaten. Im so genannten «Schengener Besitzstand», den die Schweiz nun übernommen hat und im nationalen Recht umsetzen muss, sind diese Vorgaben in Bezug auf den Datenschutz klar bezeichnet. Ihre Umsetzung ins nationale Recht ist aber nicht nur Aufgabe des Bundes, sondern insbesondere auch der Kantone.

Die Konferenz der Kantonsregierungen (KdK) und die Konferenz der kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) beschäftigt sich seither mit der Umsetzung dieser Vorgaben. Ein grosser Handlungsbedarf wurde dabei im Bereich des Datenschutzes festgestellt. Einerseits geht es darum, gewisse Aufgaben und Instrumente in den Datenschutzgesetzen zu konkretisieren, andererseits muss mit einer vollständigen Unabhängigkeit die Kontrolltätigkeit der Datenschutzbehörden verstärkt werden. Dazu sind institutionelle Garantien notwendig. Die KdK hat deshalb eine Wegleitung zur Umsetzung der Anforderungen an den Datenschutz in Auftrag gegeben, die in der Zwischenzeit fertig gestellt wurde. Ebenso hat die Vereinigung der schweizerischen Datenschutzbeauftragten anlässlich zweier Veranstaltungen und im Rahmen einer Arbeitsgruppe das Thema aufgenommen, um den Datenschutzbeauftragten die notwendigen Informationen weiterzugeben.

Kantonaler Handlungsbedarf

Im Kanton Zürich ergibt sich im Wesentlichen ein Handlungsbedarf auf der Ebene der Instrumente sowie der Funktion des Datenschutzbeauftragten. Bereits im vergangenen Jahr konnten wir auf diesen Handlungsbedarf hinweisen, so dass es möglich ist, im Rahmen der Diskussionen um den Entwurf des IDG diese Neuerungen einfliessen zu lassen.

Zur Hauptsache wird bei den Instrumenten die Vorabkontrolle verstärkt werden müssen. Die Vorabkontrolle bedeutet, dass Vorhaben, die ein hohes Risiko für die Persönlichkeitsrechte der Bürgerinnen und Bürger enthalten, vorgängig dem Datenschutzbeauftragten zur Beurteilung vorzulegen sind. Zwar ist diese Vorschrift bereits in der bestehenden Datenschutzverordnung enthalten, doch wurde sie in der Praxis nicht konsequent umgesetzt. Die Vorabkontrolle bedeutet neu, dass zwingend bei solchen Projekten eine Empfehlung des Datenschutzbeauftragten einzuholen ist.

Damit gelangen wir zur zweiten wichtigen Neuerung: Die Empfehlungen des Datenschutzbeauftragten müssen einer gerichtlichen Instanz zur Überprüfung vorgelegt werden können. Diese Anforderung ergibt sich aus dem Zusatzprotokoll der Europaratskonvention 108, dem das eidgenössische Parlament zugestimmt hat, das aber auch Bestandteil des Schengener Besitzstandes ist. In der Praxis bedeutet dies, dass der Datenschutzbeauftragte Empfehlungen, die nicht eingehalten oder abgelehnt werden, einer gerichtlichen Instanz vorlegen kann, die dann einen verbindlichen Entscheid fällt. Ebenso soll es einer Verwaltungsstelle möglich sein, Empfehlungen des Datenschutzbeauftragten bei einer gerichtlichen Instanz überprüfen zu lassen.

Unabhängigkeit des Datenschutzbeauftragten

Das EU-Recht setzt einen Schwerpunkt auf die vollständige Unabhängigkeit der Datenschutzbehörde. Dies soll insbesondere eine effiziente Kontrolltätigkeit ermöglichen. Die Frage der Unabhängigkeit des Datenschutzbeauftragten ist insbesondere eine Frage der institutionellen Garantien. Diesbezüglich muss die Funktion des Datenschutzbeauftragten auch im Kanton Zürich neu organisiert werden. Im Vordergrund stehen dabei die Regelung der Wahl und der Stellung und die Bestimmung von Budget und personellen Ressourcen. In einer ähnlichen Situation befindet sich in Bezug auf Unabhängigkeit und Selbständigkeit die Finanzkontrolle; da sich dieses Modell bewährt hat, scheint eine Anlehnung an diese Bestimmungen nahe liegend und sinnvoll.

Neue Herausforderungen

Mit diesen Anpassungen der Gesetzgebung in naher Zukunft ist der Kanton Zürich gut vorbereitet, um die Herausforderungen im Bereich des Informationszugangs und des Datenschutzes zu bewältigen. Es hat sich in den letzten Jahren gezeigt, dass die Information als Ressource immer mehr an Bedeutung gewinnt. Nicht nur der Staat ist auf mehr Informationen angewiesen, auch die Wirtschaft und die Bürgerinnen und Bürger wollen mehr Informationen. In diesem Umfeld über eine Gesetzgebung zu verfügen, die für die Verwaltungsstellen den Umgang mit Informationen klar regelt und für die Privaten den Zugang zu Infor-

mationen umschreibt, ist ein grosser Vorteil. Ebenso nimmt in diesem Zusammenhang das Bedürfnis nach mehr Schutz der Privatheit zu. Auch hier vermögen nur klare Regelungen einen angemessenen Schutz zu gewährleisten.

Technologische Entwicklungen

Ein Treiber im Hintergrund für diese gesellschaftlichen Entwicklungen ist zweifellos die Informationstechnologie. Sie ermöglicht erst die Bewältigung von riesigen Datenmengen und die Generierung von Informationen. Doch diese Technologie birgt nicht nur für die Informationen, die bearbeitet werden, zahlreiche Risiken, sondern auch in Bezug auf die Privatheit der betroffenen Personen. Deshalb ist wichtig, dass klare Rahmenbedingungen die Sicherheit in der Informationstechnologie vorschreiben. Damit wird nicht nur eine möglichst hohe Sicherheit der Daten und Informationen gewährleistet, sondern auch ein angemessener Schutz der Privatheit betroffener Personen. In Zukunft wird sich die Informationstechnologie noch vermehrt im Sinne einer «Privacy Enhancing Technology» (PET) entwickeln, um den gesetzlichen Anforderungen gerecht werden zu können. Im Interesse einer effizienten Informationsbearbeitung und eines adäquaten Schutzes der Privatheit ist der Gesetzgeber zu Recht aktiv geworden.

Vielfältige Beratungen

Der vorliegende 11. Tätigkeitsbericht zeigt, wie sich die Beratungs- und Kontrolltätigkeit des Datenschutzbeauftragten entwickelt hat. Immer mehr zeigen sich komplexe Fragestellungen im Bereich des Gesundheitswesen (S. 10 f.) oder bei der Einführung neuer Technologien wie der Biometrie (S. 12 f.). Ein wichtiger Themenbereich ist dabei auch immer die Sicherheit der Informatik, wobei es hier darum geht, die Risiken so weit wie möglich einzudämmen (S. 17 f.). Mit der Sicherheitsinitiative in diesem Bereich konnte der Datenschutzbeauftragte ein wichtiges Projekt erfolgreich zu Ende führen.

Auch auf rechtlicher Ebene stellen sich noch häufig grundlegende Fragen, die bisher nur wenig in ihrer gesamtheitlichen Bedeutung angegangen worden sind, wie beispielsweise die Geheimhaltungspflicht für Behördenmitglieder (S. 19 ff.).

Ein breites Spektrum nimmt die Beratungstätigkeit ein. Eine Auswahl der Empfehlungen ist in diesem Tätigkeitsbericht publiziert (S. 23 ff.). Im Übrigen werden die Ergebnisse aus der Beratungstätigkeit laufend auf der Website des Datenschutzbeauftragten veröffentlicht (www.datenschutz.ch).

Neben der Beratungs- und Prüfungstätigkeit (S. 28 ff. und 31 ff.) nimmt nach wie vor die Information einen wichtigen Stellenwert ein. Es geht darum, dass Daten bearbeitende Stellen wie auch Bürgerinnen und Bürger über die Anliegen des Datenschutzes und die neuen Herausforderungen informiert werden. Damit wird einerseits gewährleistet, dass die Verwaltungsstellen rechtzeitig die entsprechenden Massnahmen treffen können, und andererseits, dass die Bürgerinnen und Bürger ihre Rechte wahrnehmen und ihre Anliegen einbringen können.

Gesundheitswesen – komplexe Fragen

Im Gesundheitswesen stellt sich ein breites Spektrum an datenschutzrechtlichen Fragen.

Pflegefachpersonen, Ärztinnen und Ärzte sind Fachleute für Gesundheits- und nicht für Datenschutzprobleme. Im Alltag geht es jedoch häufig nicht nur um den Umgang mit Patienten, sondern auch um denjenigen mit Informationen. Dabei fehlt oft das Grundlagenwissen in Sachen Datenschutz; zudem geht es darum, die Vorgaben spital- oder praxistauglich umzusetzen. Vor allem bei der Bekanntgabe von Daten stellen sich immer wieder neue Fragen. So braucht es bestimmte gesetzliche Grundlagen, damit das ärztliche Berufsgeheimnis die Freigabe erlaubt. Dies wiederum bedeutet, dass ein Arzt oder eine Ärztin sich in den Bestimmungen auskennen muss, die ihrerseits zum Teil auf kantonaler und zum Teil auf Bundesebene in unterschiedlichen Erlassen festgehalten sind.

Gesundheitsfachleuten bleibt meist nur wenig Zeit, um Entscheide über die Geheimhaltung oder Bekanntgabe von Patientendaten zu treffen: Darf ich den Psychiatriepatienten in einem Wohnheim mitteilen, dass einer der Mitpatienten HIV-positiv ist? Darf eine Mutter die Patientendokumentation ihrer minderjährigen, aber urteilsfähigen Tochter einsehen? Für die Beantwortung dieser Fragen müssten die Gesundheitsfachleute einerseits den Überblick haben, in welchen Gesetzen sich die entsprechenden Bestimmungen finden, und diese andererseits anwenden können. Wichtig wäre zudem die Kenntnis der einschlägigen Rechtsprechung und herrschenden Lehrmeinung. Und selbst dann wäre zumindest bei der Beantwortung der ersten Frage eine Unsicherheit vorhanden: Kann sich der Arzt auf die Wahrung berechtigter Interessen berufen, wenn er anderen Personen, welche vom HIV-positiven Mitpatienten angesteckt werden könnten, dies mitteilt? Sind die Mitpatienten urteilsunfähig, ist diese Mitteilung für sie unter Umständen nicht verwertbar. Dann müssen andere Lösungen (Verlegung etc.) gesucht werden, um die anderen Mitpatienten wirksam zu schützen. Auch die Beantwortung der Frage, ob die Mutter in die Krankengeschichte ihrer urteilsfähigen, aber minderjährigen Tochter Einsicht nehmen kann, lässt sich nicht direkt aus dem Patientinnen- und Patientengesetz ablesen, sondern muss erst erarbeitet werden: Die Mutter kann nur Einsicht nehmen, wenn ihre Tochter damit einverstanden ist (§19 Abs. 1 Patientinnen- und Patientengesetz).

Praxistaugliche Lösungen

Die Gesundheitsfachleute können diese Fragen nicht selber beantworten. Sie sind daher auf die Hilfestellung des Datenschutzbeauftragten angewiesen, der mit ihnen gemeinsam die Fragestellungen aufnimmt, sie juristisch löst und ihnen anschliessend konkrete Vorgaben macht, wie die juristischen Lösungen im Spitalalltag praxistauglich umgesetzt werden können. Fehlentscheide können für die Patienten schwerwiegende Folgen haben und für medizinisches Personal zu einer Strafanzeige wegen Verletzung von Art. 321 des Strafgesetzbuches führen.

Auch Patientinnen und Patienten kennen ihre Rechte meist nur teilweise. Ihnen ist oft nicht bewusst, dass es beispielsweise unzulässig ist, Ärzten eine potenzielle Zugriffsmöglichkeit auf Krankengeschichten von Patienten einzurichten, an deren Behandlung sie nicht beteiligt sind. Viele Patienten wissen noch heute nicht, dass sie von ihrer Krankengeschichte inklusive Handnotizen des Arztes Kopien verlangen dürfen.

Die Probleme reichen über die Grenzen des Spitals oder der Praxis hinaus: Viele Spitäler sind heutzutage wegen der immer komplexeren Applikationen darauf angewiesen, dass externe Spezialisten die High-Tech-Software fernwarten. Dies widerspricht jedoch unter Umständen dem ärztlichen Berufsgeheimnis, da die externen Dienstleister potenziell Zugriff auf patientenbezogene Daten haben. Die Frage, ob sie als Hilfspersonen der Ärzte gelten und damit ebenfalls dem Berufsgeheimnis unterstehen, ist juristisch nicht geklärt. Besonders heikel wird die Frage dann, wenn IT-Dienstleistern

aus dem nahen und fernen Ausland (zum Beispiel Indien) eine Zugriffsmöglichkeit auf patientenbezogene Daten zwecks Fernwartung eingerichtet wird.

Der Bundesrat hat seine revidierte Strategie für eine Informationsgesellschaft in der Schweiz vorgestellt (abrufbar unter: www.news.admin.ch/NSBSubscriber/message/de/2252). Sie nimmt als einziges neues Thema den Bereich E-Health auf, dessen Strategie bis Ende 2006 konzipiert sein muss. Ziele sind eine Steigerung von Qualität, Effizienz und Sicherheit sowie die Reduktion der Kosten. Einen wichtigen Pfeiler bildet dabei eine Patientenkarte, auf welcher Patientendaten gespeichert werden sollen. Die Befürworter führen an, dass damit die Transparenz gegenüber dem Karteninhaber erhöht werde, weil er selber die Daten jederzeit einsehen könne. Andererseits kann eine derart umfängliche Sammlung von Informationen aber auch neue Begehrlichkeiten auslösen, zum Beispiel bei Arbeitgebern und Versicherern. Für Letztere ist die Versuchung zum Beispiel gross, die medizinischen Daten als Grundlage für Versicherungsanträge zu verlangen. Aspekte des Datenschutzes müssen jetzt diskutiert und in die E-Health-Strategie integriert werden. Da stellen sich Fragen verschiedenster Art: Wer genau soll auf die Informationen zugreifen können und welche Daten sollen gespeichert werden? Wie verhält es sich mit Gendaten? Bei der Beantwortung und Lösungssuche für diese Fragen müssen die Grundprinzipien des Datenschutzes wie Rechtmässigkeit, Verhältnismässigkeit, Transparenz etc. einfliessen und in einem entsprechenden Gesetz in konkreten Bestimmungen umgesetzt werden.

Die Patientenkarte ist nicht der einzige Punkt, der zu diskutieren gibt. E-Health könnte in Zukunft auch dazu führen, dass die Waage dem Kühlschrank automatisch weiterleitet, wenn jemand den Body Mass Index überschritten hat und jener infolgedessen per Internet nur noch Light-Produkte bestellt. Und E-Health könnte eines Tages zur Folge haben, dass die Krankenkasse die Prämie erhöht, weil jemand ein Bier zu viel getrunken hat.

Ein Pilotprojekt, das Fragen aufwirft, ist «My Heart». Es setzt auf Überwachung des Gesundheitszustandes (mehr Informationen unter www.hitech-projects.com/euprojects/myheart/). In funktionellen Kleidungsstücken sind Sensoren eingebaut, welche Gesundheitsdaten aufzeichnen und so den aktuellen Gesundheitszustand ermitteln. Hintergrund des Versuchs ist die Tatsache, dass Herz-Kreislauf-Erkrankungen in Westeuropa zu den häufigsten Todesursachen zählen und Kosten in Milliardenhöhe mit sich bringen. Von einer nahtlosen Überwachung und Analyse des Gesundheitszustandes erhofft man sich eine bessere Prävention. Konzepte für den Datenschutz sind in dem Projekt nicht enthalten. Und es sei unter dem Aspekt der Verhältnismässigkeit die Frage erlaubt, was eine solche Überwachung schliesslich bringt, wenn die überwachte Person sich nicht vernünftig ernährt und sich nicht ausreichend bewegt?

Biobanken und Humanforschung

Biobanken enthalten einerseits Körpersubstanzen und andererseits gesundheits- und lebensstilbezogene Daten von Patientinnen und Patienten. Es handelt sich dabei um hochsensible Informationen. Die zur Gewährleistung des Datenschutzes notwendigen Rahmenbedingungen sind jedoch kaum konkretisiert. Folgende Fragen stehen dabei im Vordergrund: Wie wird die freiwillige und transparente Einwilligung der betroffenen Personen bei der Erhebung und bei der Zweckänderung eingeholt? Mit welchen anderen Daten werden die erhobenen verknüpft? Hat die betroffene Person das Recht, die Analyseresultate der Proben zu erfahren, oder die Pflicht, sie zur Kenntnis zu nehmen? Es ist zu hoffen, dass das Bundesgesetz über die Forschung am Menschen konkrete und der Situation angemessene Lösungen beinhalten wird und nicht einfach auf die Grundprinzipien des Datenschutzes verweist.

Information und Ausbildung

Für Personen, die im Gesundheitswesen tätig sind, bietet der Datenschutzbeauftragte Schulungen und Vorträge an. Ziel ist es einerseits, die Grundlagen des Datenschutzes zu vermitteln, damit das Personal selber Antworten finden oder zumindest die Probleme erkennen kann. Andererseits stellt der Datenschutzbeauftragte aber auch konkrete Lösungen und Handlungsanleitungen für praktische Alltagsprobleme zur Verfügung. Geplant sind ferner mehrere kürzere Schulungen in Spitälern und eintägige Intensivschulungen im kantonseigenen Schulungszentrum.

Auf der anderen Seite müssen die Patientinnen und Patienten über ihre wichtigsten Rechte aufgeklärt werden. Zu diesem Zweck hat der Datenschutzbeauftragte eine Broschüre konzipiert und plant Veranstaltungen zu wichtigen Themen wie Patientenkarte, Biobanken oder Genetik. Darüber hinaus kontrolliert er im Rahmen der Datenschutz-Reviews die Einhaltung der entsprechenden Vorgaben in Spitälern, überprüft die Datenbearbeitungen und gibt Empfehlungen ab.

Fingerabdruck für den Schwimmbad-Eintritt

Für Schwimmbad-Benützerinnen und -Benützer ist es oft ein Leichtes, sich mit einer fremden Eintrittskarte Zutritt zu verschaffen, wodurch die Betreiber Verluste erleiden. Eine Gemeinde kam deshalb auf die Idee, Inhaberinnen und Inhabern von Jahres- oder Saisonkarten mit Hilfe ihres Fingerabdrucks Zugang zu gewähren.

Der Einsatz eines biometrischen Systems durch ein staatliches Organ muss wie jede andere Datenbearbeitung den verfassungs- und datenschutzrechtlichen Grundsätzen genügen. Im Falle des Schwimmbad-Eintritts, der via Fingerabdruck autorisiert werden soll, ist eine rechtskonforme Lösung möglich. Besonders zu beachten ist dabei das Gebot der Verhältnismässigkeit einerseits bei der Personenerkennung und andererseits bei der Speicherung und späteren Auswertung von Randdaten. Weiter gilt das Zweckbindungsgebot. Eine Umsetzung erfolgt hier vorab auf technischer Ebene.

Biometrie tangiert Grundrechte

Biometrische Daten sind körpereigene, einmalige Kennzeichen und untrennbar mit einer bestimmten Person verknüpft, wie zum Beispiel Gesichtsbild, Fingerabdruck, Irismuster, aber auch die Stimme oder der Gang. Wenn die Verwaltung entsprechende Informationen erfasst, speichert und abgleicht, so greift sie in die Grundrechte der Bürgerinnen und Bürger ein. Betroffen sein können die Menschenwürde, die persönliche Freiheit, die Privatsphäre und das Recht auf informationelle Selbstbestimmung. Grundrechte dürfen jedoch nur eingeschränkt werden, wenn eine gesetzliche Grundlage besteht, ein öffentliches Interesse vorliegt oder Grundrechte Dritter geschützt werden müssen und wenn der Eingriff verhältnismässig ist. Der Kerngehalt der Grundrechte bleibt auf jeden Fall unantastbar.

Biometrische Daten sind Personendaten

Biometrische Daten lassen für sich allein betrachtet Rückschlüsse auf einen bestimmten Menschen zu und gehören deshalb auch ohne weiteren Bezug wie zum Beispiel eine Namensnennung zu den Personendaten.

Unter bestimmten Voraussetzungen sind biometrische Daten besonders schützenswert. Dies ist jedoch nicht der Fall, wenn ein Fingerabdruck für die Autorisierung beim Eintritt in eine Badeanstalt verwendet wird. Wenn also die rechtliche Grundlage für den Betrieb eines Schwimmbads gegeben ist – in einem Gesetz oder einer Verordnung –, so besteht auch die Kompetenz, die notwendigen Personendaten zu bearbeiten.

Verhältnismässigkeit

Die Bearbeitung von Personendaten setzt eine ausreichende Begründung voraus; Kundenfreundlichkeit oder Bequemlichkeit genügen dafür nicht. Diese Massnahme darf nur dann vorgenommen werden, wenn sie im konkreten Fall sowohl geeignet als auch erforderlich ist. Verfahren zur Autorisierung des Schwimmbad-Eintritts, die auf Besitz oder Wissen beruhen, können leicht umgangen werden und so zu erheblichen Einnahmeausfällen führen. Es erscheint deshalb verhältnismässig, ein biometrisches Merkmal – Fingerabdruck oder Gesichtsbild – einzusetzen.

Für die Autorisierung genügt ein biometrisches Merkmal; der Name der Person oder weitere Angaben wie Geburtsdatum oder Adresse sind dafür nicht erforderlich.

Aus dem Verhältnismässigkeitsgrundsatz folgt auch, dass Rohdaten ohne besondere Begründung nur zur Erzeugung von Templates verwendet werden dürfen.

Bei jedem Schritt eines biometrischen Verfahrens muss separat geprüft werden, ob er zwingend durch das öffentliche Organ vorgenommen werden muss. Im Falle der Badanstalt ist es technisch durchaus möglich, dass die Bezügerinnen und Bezüger von Schwimmbad-Jahreskarten einzelne Bearbeitungsvorgänge an Orten ausführen, die ihrer eigenen Kontrolle unterstehen.

Für den Schwimmbad-Eintritt bedeutet dies, dass aus dem Fingerabdruck ein Template erstellt werden muss, das für das weitere Verfahren verwendet wird; die Rohdaten sind von diesem Moment an nicht mehr notwendig. Das Template muss auf einer bei der betroffenen Per-

son verbleibenden Smartcard abgelegt und beim Wiedereintritt mit dem erzeugten Prüfmuster verglichen werden. Aus datenschutzrechtlicher Sicht sind Systeme vorzuziehen, bei denen auch das Einlesen des Fingerabdrucks und der Verifizierungsvorgang in der Nutzersphäre stattfinden. Biometrische Daten dürfen nicht bei der Schwimmbad-Betreiberin abgelegt werden. Sie trägt damit auch keine entsprechende Verantwortung.

Besonders wichtig ist es bei der Bearbeitung personenbezogener Randdaten, den Verhältnismässigkeitsgrundsatz zu beachten. Die Prinzipien der Datenvermeidung, der Datensparsamkeit sowie der Pseudonymisierung und Anonymisierung gelten nicht nur für die maschinelle Erkennung von Personen, sondern auch für die Speicherung und spätere Auswertung der Resultate.

Nicht mehr benötigte Daten, die nicht archiviert werden müssen, sind zu vernichten.

Zweckbindung

Die technische Lösung muss auf das Ziel der Datenbearbeitung ausgerichtet sein und eine Änderung des ursprünglichen Bearbeitungszweckes möglichst ausschliessen. Datenschutzrechtliche Aspekte gehören deshalb bereits zur Evaluation und Planung eines Systems.

So muss zur Erfassung der Rohdaten sowie zur Erzeugung von Templates und Prüfmustern eine geschlossene Kompakteinheit verwendet und ein anwendungsspezifischer Algorithmus eingesetzt werden, der aus den Templates weder eine Wiederherstellung von Rohdaten noch Rückschlüsse auf Charaktereigenschaften oder eindeutige medizinische Diagnosen zulässt.

Um die Zweckbindung einzuhalten, sind Betreiberinnen und Betreiber bei personenbezogenen Randdaten zu einer engen Fassung und einer entsprechenden technischen Umsetzung des Verhältnismässigkeitsprinzips verpflichtet.

Richtigkeit

Biometrische Daten müssen richtig und, soweit es der Bearbeitungszweck verlangt, aktuell und vollständig sein. Es dürfen deshalb nur Verfahren eingesetzt werden, welche eine nahezu hundertprozentige Sicherheit der Identifikation oder Verifikation erlauben. Für Personen, die auf dem System nicht eingelernt werden können, ist ein Alternativszenario vorzusehen, welches nicht zu einer Diskriminierung führen darf.

Übrige datenschutzrechtliche Grundsätze

Für die Person, deren Merkmale erfasst wird, muss transparent sein, welche Daten erhoben werden; es ist nicht zulässig, zusätzliche biometrische Informationen ohne Wissen und Willen der Betroffenen festzuhalten.

Rechte, die das Datenschutzgesetz zusichert, sind auch bei der Bearbeitung von Personendaten mittels biometrischer Systeme uneingeschränkt zu gewährleisten.

Zuverlässigkeit ist ein wichtiges Merkmal für ein biometrisches System, da die Betreiberin das Risiko eines Ausfalls selber trägt. Der Vergleich von Template und Prüfmuster kann nicht manuell durchgeführt werden; es dürfen jedoch keine zusätzliche Daten erhoben werden, um sich vor einem Systemausfall zu schützen.

Für den Datenschutz ist dasjenige Organ verantwortlich, das die Personendaten bearbeitet oder bearbeiten lässt. Die Gemeinde als Schwimmbad-Betreiberin kann sich ihrer diesbezüglichen Verantwortung nicht entziehen.

Bis jetzt erfolgt die Autorisierung der Inhaberinnen und Inhaber von Jahres- oder Saisonkarten in der Regel durch das Vorweisen eines Ausweises mit aufgeklebtem Gesichtsbild. Auch dieses Vorgehen stellt eine Bearbeitung biometrischer Daten dar und hat denselben datenschutzrechtlichen Grundsätzen zu genügen wie der Einsatz eines Fingerabdruck-Erkennungssystems. Werden elektronische Systeme verwendet, so entstehen dadurch zusätzliche Risiken für den Persönlichkeitsschutz, denen mit organisatorischen und technischen Massnahmen begegnet werden muss.

Informationszugang und Datenschutz

Der Entwurf für ein Informations- und Datenschutzgesetz (IDG) wurde vom Regierungsrat verabschiedet.

Anfang 2005 konnte die Vernehmlassung für das Informations- und Datenschutzgesetz (IDG) abgeschlossen werden. Die zahlreichen Anregungen aus der Vernehmlassung wurden in den Entwurf des Regierungsrates eingearbeitet. Mit der Annahme der neuen Verfassung durch die Zürcher Bevölkerung konnte der Hauptstreitpunkt in der Vorlage – nämlich die Einführung des Öffentlichkeitsprinzips – erledigt werden: Die Verfassung legt das Öffentlichkeitsprinzip als neue Grundlage der Verwaltung fest. Somit handelt es sich beim IDG um die notwendige Konkretisierung dieses Grundsatzes auf Gesetzesstufe.

Bedeutung der Information

Das Öffentlichkeitsprinzip widerspiegelt die Bedeutung der Information in unserer Gesellschaft. Information wird immer wichtiger: Nicht nur als Grundlage für die demokratische Meinungsbildung der Bürgerinnen und Bürger, als Kontrollinstrument über eine immer mächtiger werdende Verwaltung, sondern auch als selbständige Ressource in der Informationsgesellschaft. Deshalb drängen sich Regelungen für den Zugang zu Informationen der Verwaltung auf.

Auf der anderen Seite sehen wir uns mit einer (informations)technischen Entwicklung konfrontiert, die immer mehr in die Privatheit der Bürgerinnen und Bürger eindringt. Das aktuelle Datenschutzgesetz kann diese technologischen Herausforderungen nur schwer erfassen. Mit dem Entwurf des IDG konnte deshalb auch die Gelegenheit wahrgenommen werden, die bewährten Prinzipien des Datenschutzes den neuen Herausforderungen anzupassen.

In den letzten Jahren haben verschiedene Kantone und der Bund auf Verfassungs- oder Gesetzesebene das Öffentlichkeitsprinzip eingeführt. Auch im europäischen Ausland, insbesondere in den EU-Staaten, ist der Informationszugang ein wichtiges Element des modernen demokratischen Staates geworden. Obwohl die Materien Datenschutz und Informationszugang in verschiedenen Bereichen miteinander verknüpft sind, sind nicht immer beide Bereiche konsequent aufeinander abgestimmt worden. Mit dem IDG legt der Kanton Zürich grossen Wert auf die Harmonisierung des Informationszugangs mit dem Datenschutz und folgt damit den beiden neuesten Gesetzgebungen in dieser Materie in den Kantonen Solothurn und Aargau.

Informationen und Personendaten

Die Erarbeitung des Gesetzesentwurfes erfolgte in enger Zusammenarbeit mit dem Datenschutzbeauftragten. Damit war es auch möglich, die Erfahrungen aus den vergangenen Jahren mit dem Datenschutz im Kanton Zürich in die Gesetzgebung einfliessen zu lassen. Die Beratung im Bereich des Datenschutzes bedeutet ja implizit immer auch einen Entscheid in Bezug auf den Informationszugang: Datenschutzrechtliche Bestimmungen enthalten auch den Entscheid über die Bekanntgabe von Informationen, wenn bestimmte Voraussetzungen erfüllt sind – oder die Nichtbekanntgabe von Informationen, wenn dem Schutz der Privatheit der betroffenen Person Vorrang eingeräumt wird.

Das IDG geht deshalb konsequenterweise von einem umfassenden Begriff von Information aus. Personendaten sind dabei eine Teilmenge, nämlich Informationen, die sich auf eine bestimmte oder bestimmbare Person beziehen. Das Gesetz betrachtet daher die Information in einem Prozessablauf, von ihrer Entstehung bis zu ihrer Archivierung oder Löschung. Für die unterschiedlichen Stadien dieses Informationsprozesses werden sodann die Rahmenbedingungen formuliert, was mit diesen Informationen geschehen darf, je nachdem, ob es sich um «gewöhnliche» Informationen, als vertraulich klassifizierte Informationen, Personendaten oder besondere Personendaten handelt. Damit bestehen für die Verwaltungsstellen klare Vorgaben für den Umgang mit Informationen. Diese Vorgaben berücksichtigen sowohl das Informationszugangsrecht als auch den Schutz der Privatheit der Bürgerinnen und Bürger.

Interessenabwägung

Einen gewichtigen Teil nimmt die Regelung der Interessenabwägung im Gesetz ein. Bei einer Informationsbekanntgabe müssen allfällig überwiegende öffentliche oder private Interessen berücksichtigt werden. Das Verfahren auf Informationszugang hält im Einzelnen fest, wie

insbesondere die Interessen einer betroffenen Person zu berücksichtigen sind. Vor allem wird auch festgehalten, dass besondere Personendaten nur mit der Einwilligung der betroffenen Person zugänglich gemacht werden dürfen.

Technologische Entwicklung

Im Weiteren versucht das Gesetz die neuen technologischen Entwicklungen, welche insbesondere auch Risiken für die Privatheit der Bürgerinnen und Bürger enthalten, angemessen zu regeln. Die Massnahmen zur Gewährleistung der Informationssicherheit beruhen auf bewährten Standards. Vorgaben, dass Personendaten, wie sie beispielsweise für den Verbindungsaufbau in der Telekommunikation notwendig sind, nach deren Verwendung wieder zu löschen sind oder dass mittels Anonymisierung ein Personenbezug vermieden wird, helfen den Aufbau von Personendatensammlungen zu vermeiden, die für das Verwaltungshandeln nicht notwendig sind.

Einheitlicher Informationsprozess

Das IDG beinhaltet eine konsequente Verzahnung des Informationszugangs und des Datenschutzes. Leider hat es der Regierungsrat abgelehnt, auch die Funktion eines Informationszugangs- und Datenschutzbeauftragten zu schaffen, wie diese im ursprünglichen Gesetzesentwurf vorgesehen war. Alle neuen Gesetzgebungen im Bereich des Öffentlichkeitsprinzips in der Schweiz (Bund, Solothurn, Aargau) sehen diese Doppelfunktion vor. Sie ist die Konsequenz aus der Tatsache, dass der Informationszugang und der Datenschutz die Kehrseite der gleichen Medaille sind. Eine Beratungs- und Kontrolltätigkeit eines Beauftragten sollte sich auch im Sinne einer einheitlichen Umsetzung beider Materien um beides kümmern können. Möglicherweise kann hier der Kantonsrat noch korrigierend einwirken.

In Bezug auf die Rolle und Funktion des Datenschutzbeauftragten sind im Weiteren auch konkretere Regelungen betreffend die Gewährleistung einer unabhängigen Aufgabenerfüllung in Betracht zu ziehen. Diese drängen sich auch im Hinblick auf die Assoziierung der Schweiz an Schengen auf (siehe Seite 16).

Um die Arbeit des Datenschutzbeauftragten wirkungsvoll auszugestalten, wird im Weiteren zu überdenken sein, welche Rolle den Empfehlungen des Datenschutzbeauftragten zukommen soll. Es ist unbefriedigend, dass Empfehlungen, die nicht befolgt werden, nicht einer unabhängigen Instanz zum Entscheid vorgelegt werden können. Auch hier wird aufgrund des vom Bundesparlament genehmigten Zusatzprotokolls zur Europaratskonvention 108 eine Regelung einzuführen sein, die eine solche Möglichkeit beinhaltet.

Des Weiteren sollte der Datenschutzbeauftragte bei wichtigen Projekten, die die Privatheit der Bürgerinnen und Bürger in einem hohen Masse betreffen, bereits im Voraus seine Stellungnahme abgeben können. Nur damit wird gewährleistet, dass nicht nachträglich Projekte (aufwändig) geändert werden müssen, um die Bürgerinnen und Bürger angemessen zu schützen.

Insgesamt nimmt der Entwurf des IDG die neuen Herausforderungen des Informationszugangs und des Datenschutzes gut auf, und es ist zu hoffen, dass der Kantonsrat dieses Gesetz mit einigen notwendigen Anpassungen so verabschieden kann.

Auswirkungen von Schengen/Dublin

Die Assoziierung an Schengen und Dublin verlangt auch im Bereich des Datenschutzes Anpassungen.

Die Schweiz traf im Juni letzten Jahres die Entscheidung zur Teilnahme an den Abkommen von Schengen und Dublin. Die Inkraftsetzung der Abkommen ist für das Jahr 2008 vorgesehen. Durch die Assoziierung der Schweiz an Schengen und Dublin wird die internationale Zusammenarbeit in den Bereichen Polizei, Justiz, Visa und Asyl massiv ausgebaut. Im Kampf gegen die zunehmende grenzüberschreitende Kriminalität und gegen Missbräuche im Asylwesen werden die kantonalen Polizeikorps gestützt auf eine gesetzliche Grundlage direkten Zugriff auf die Schengener Informationssysteme (SIS II, VIS, Eurodac) haben. Dadurch erhalten die Polizeibehörden für ihre Aufgabenerfüllung ein mächtiges, wirkungsvolles Instrument. Ihre Ausschreibung im europäischen Fahndungsraum nach Personen oder Sachen verbreitet sich – nach der vollständigen Einbindung der neuen EU-Mitglieder ab voraussichtlich 2008 – in 27 Schengen-Staaten mit etwa 450 Millionen Einwohnern. Der Zugriff auf eine Datenbank mit mehreren Millionen Einträgen kann auf der anderen Seite schwerwiegende Eingriffe in die Persönlichkeitsrechte der betroffenen Personen bedeuten. Die erhöhten Risiken für die Verletzung von Grundrechten beziehungsweise widerrechtlichen oder zumindest sachlich fehlerhaften Bearbeitungen von Personendaten können sich für die Betroffenen in ganz Europa auswirken. Dem müssen die Kantone mit strengeren Datenschutzregeln und verstärkten aktiven Kontrollen bei den Datenbearbeitungen entgegenwirken.

In Absprache mit der Konferenz der kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) und gestützt auf einen Zirkulationsbeschluss des Leitenden Ausschusses der Konferenz der Kantone (KdK) wurde ein externer Experte damit beauftragt, zuhanden der Kantone eine Wegleitung zur Umsetzung der mit Schengen und Dublin übernommenen Datenschutzvorschriften auszuarbeiten.

Dieses Hilfsmittel dient den Kantonen dazu, die Vollständigkeit ihrer Datenschutzgesetzgebung zu überprüfen und den noch bestehenden Handlungsbedarf festzustellen.

Auch für den Datenschutz des Kantons Zürich stehen notwendige organisatorische und insbesondere legislatorische Änderungen an, welche noch im Rahmen des Entwurfs des Informations- und Datenschutzgesetzes (IDG) umgesetzt werden sollten. Der Datenschutzbeauftragte hat dem Regierungsrat die notwendigen Änderungs- und Ergänzungsvorschläge zukommen lassen. Deren weitere Bearbeitung wird alsdann der Regierungsrat respektive der Kantonsrat übernehmen.

Aufgrund der europarechtlichen Vorgaben, welche die völlige Unabhängigkeit der Datenschutzaufsicht verlangen, erfahren die Stellung und die Organisation des Datenschutzbeauftragten eine umfassende Änderung. Eine Anlehnung an die Regelung der Finanzkontrolle erscheint dabei sinnvoll. Die analoge Anwendung einiger Regelungen aus dem Finanzkontrollgesetz ist dabei möglich, weil die Aufgabenerfüllung der kantonalen Finanzkontrolle an ebenso strenge Voraussetzungen bezüglich Unabhängigkeit und Selbständigkeit geknüpft ist und sich diese Bestimmungen bereits bewährt haben. Dabei ist auch Gewicht auf die Ausstattung mit genügenden finanziellen und personellen Ressourcen zu legen, da nur so eine unabhängige, aktive und anlassfreie Kontrolle im Sinne der europarechtlichen Vorgaben möglich ist.

Falls die Bearbeitung von Personendaten aufgrund der Art der Bearbeitung besondere Risiken für die Rechte und die Freiheit der betroffenen Person mit sich bringt, muss diese Bearbeitung vorab durch den Datenschutzbeauftragten geprüft werden können. Kriterien für die Beurteilung der Risiken können zum Beispiel die Zahl der erfassten Personen, die Zahl der beteiligten öffentlichen Organe oder die Sensitivität der Daten sein. Objekt der Vorabkontrolle können vor allem Projekte für IT-Systeme, Datenbanken, Register usw. sein.

Die Übermittlung von Personendaten ins Ausland hat sich nach den entsprechenden internationalen Abkommen zu richten. Insbesondere muss bei einem Empfänger, welcher nicht Mitglied der Abkommen von Schengen und Dublin ist, ein adäquates Datenschutzniveau sichergestellt sein. Bedeutsam sind auch die Neuerungen, wonach der Datenschutzbeauftragte eine nicht befolgte Empfehlung über das Bearbeiten von Personendaten einer gerichtlichen Instanz zum Entscheid vorlegen kann.

Risiken im Informatikbereich eindämmen

Der Computer ist in der Arbeit von Verwaltungen allgegenwärtig und die damit verbundenen Risiken nehmen zu. Deshalb hat der Regierungsrat beschlossen, mit kurz- und mittelfristigen Massnahmen das Sicherheitsniveau in der Informatik der Amtsstellen anzuheben, um damit eine laufende Verschlechterung der Situation zu verhindern.

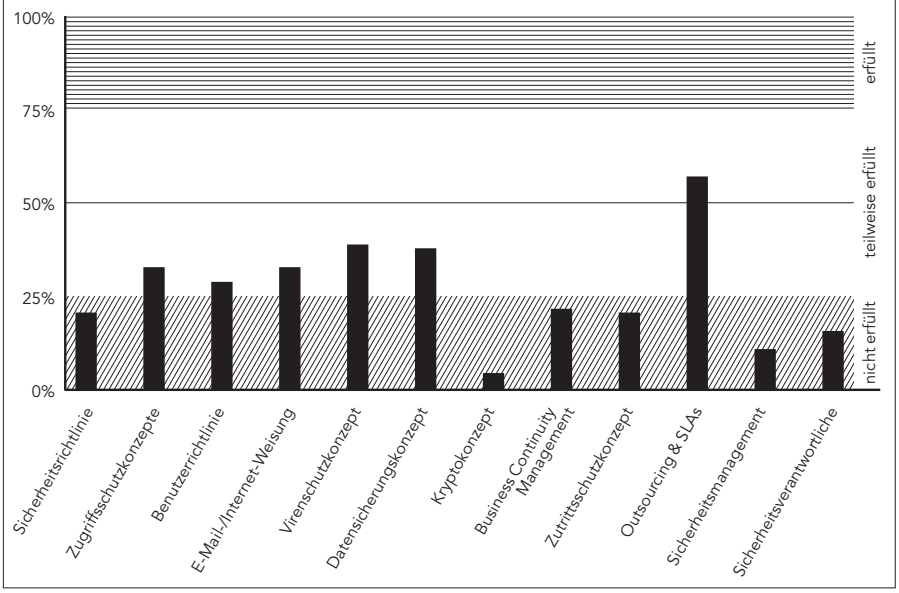
Um die Zielsetzung der Sicherheitsinitiative zu erreichen, wurden in einem ersten Schritt die Grundschutzmassnahmen für Informatiksicherheit überprüft und analysiert, damit anschliessend kostengünstige Sofortmassnahmen umgesetzt werden können. Gleichzeitig wurden die Amtsstellen angehalten, die mittel- bis langfristig notwendigen Massnahmenpläne zu erstellen. Ziel war es auch, alle Mitarbeitenden der kantonalen Verwaltung für das Thema Sicherheit zu sensibilisieren. Die Koordination dieses Projektes wurde dem Datenschutzbeauftragten übertragen, mit dem Auftrag, dem Regierungsrat einen Schlussbericht vorzulegen.

Sicherheitslandkarte

Die Zusammenarbeit mit den geprüften Stellen verlief sehr gut. Eine anfängliche Skepsis – es war die erste Prüfung in dieser Art und Breite in der kantonalen Verwaltung – legte sich bald und das Bedürfnis nach Unterstützung wurde laut. Die verantwortlichen Personen planten die notwendige Zeit für die Überprüfung ein und nutzten sie auch, um die eigene Kompetenz im Bereich der Informatiksicherheit auszubauen. Die Tests ergaben ein gutes Niveau der technisch umgesetzten Sicherheitsmassnahmen in den durch die Direktionen oder Amtsstellen selbst betriebenen Systemen. Im technischen Bereich besteht also kein unmittelbarer Handlungsbedarf. Trotzdem zeigen die Sicherheitsanalysen, dass bei der Informatiksicherheit in der kantonalen Verwaltung (vgl. Abb. 1) Sensibilisierungsbedarf besteht. Die organisatorischen Prüfungen der übergeordneten und operationellen Bereiche (vgl. Abb. 2) belegen, dass die meisten Direktionen oder Amtsstellen die gesetzlichen Anforderungen nicht erreichen und somit ein beträchtliches Risiko eingehen.

Potenzielle Risiken werden nicht laufend nach möglichem Schadenausmass und Eintretenswahrscheinlichkeit beurteilt, sondern fast immer aufgrund von subjektiven Annahmen der Systembetreuenden. Das Sicherheitsbewusstsein ist in den meisten Direktionen gering. So sind das Verhalten im Notfall (Notfallvorsorgeplanung, Geschäftsfortführung, Wiederanlauf) und das Krisenmanagement nur in wenigen Direktionen oder Amtsstellen konzeptionell festgelegt und dokumentiert. Damit erweisen sich die organisatorischen und betrieblichen Sicherheitsniveaus als vergleichsweise mangelhaft.

Abbildung 1



Erfüllungsgrad der konzeptionellen Detailanalyse, zusammengefasst nach Themen

Informationssicherheits-management

Mit den Anforderungen an die Informationstechnik ist auch deren Komplexität gewachsen. Ein angemessenes Sicherheitsniveau kann nur durch organisiertes Vorgehen aller Beteiligten erreicht und aufrechterhalten werden. Voraussetzung für die sinnvolle Umsetzung und Erfolgskontrolle von Massnahmen ist ein durchdachter und gesteuerter Informatiksicherheitsprozess. Dessen Planung und Lenkung – das Informationssicherheitsmanagement – können nur angemessen funktionieren, wenn sie in die bestehenden Strukturen der kantonalen Verwaltung eingebettet sind; der Erfolg hängt unmittelbar von der direktionsübergreifenden Zusammenarbeit ab. Dies setzt Rahmenbedingungen für die organisatorischen Bereiche und die Informatikbetriebe (zum Beispiel Prozesse, Service Management und Messungen) voraus und bedingt eine kantonsweite übergeordnete Koordination durch definierte Ansprechpersonen. Die Verantwortlichen legen die Sicherheitsstrategie fest und definieren die Ziele; sie koordinieren die Anliegen des gesamten Kantons und der einzelnen Direktionen und Amtsstellen, unterstützen diese in ihrem Sicherheitsmanagement und überwachen die Umsetzung der notwendigen Massnahmen. Dafür müssen ihnen entsprechende Ressourcen zur Verfügung stehen.

Verwaltungsweite Sicherheitskultur

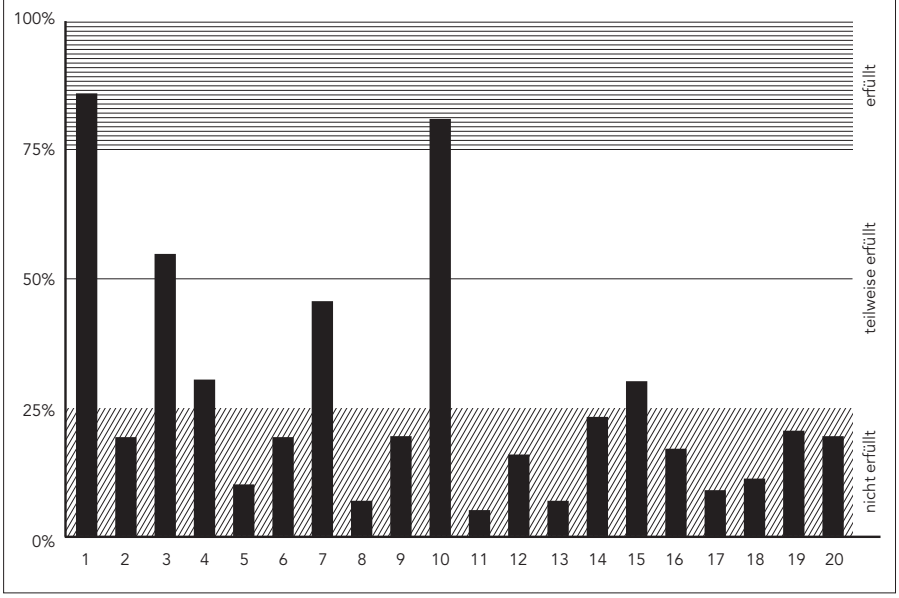
Für die Verwaltung stellt eine zuverlässige Informationstechnik die Basis für die täglichen Arbeitsabläufe dar. Damit diese auch in Zukunft funktioniert, sollte das Sicherheitsbewusstsein in allen Direktionen und auf allen Stufen weiter geschärft werden. Das bestehende technische Niveau innerhalb der kantonalen Verwaltung kann nur gehalten werden, wenn eine verwaltungsweite Sicherheitskultur entwickelt und weiter gepflegt wird. Diese setzt eine Sensibilisierung für die Bedeutung des Themas und die eigene Verantwortlichkeit voraus; erst dann kann von einer dezidierten Informatiksicherheitskompetenz in den Direktionen und Amtsstellen gesprochen werden.

Im Rahmen der Sicherheitsinitiative wurde deshalb in Zusammenarbeit mit einer spezialisierten Firma das webbasierte Lernprogramm (WBT) «Wie trage ich zur Sicherheit bei?» entwickelt, das allen Angestellten der kantonalen Verwaltung im Intranet und nun auch allen externen Interessierten im Internet (www.datenschutz.ch/wbt/sicherheit) zur Verfügung steht. Es macht die Teilnehmenden mit den wichtigsten Fragen in punkto Sicherheit vertraut, weist sie auf ihre Verantwortung im Bereich der Informatiksicherheit hin und gibt Anleitungen zu einem sicherheitsbewussten Verhalten.

Einheitliche Risikoanalysen

Eine Standardisierung (zum Beispiel nach ISO/IEC 27001:2005) ermöglicht eine Verminderung der Aufwände für Informationssicherheit und Datenschutz und verbessert so die Sicherheit und Wirtschaftlichkeit der Informatik innerhalb der kantonalen Verwaltung insgesamt. Deshalb sollte eine einheitliche Methode der Risikoanalyse eingeführt werden, die einen Vergleich zwischen den einzelnen Stellen erlaubt. Die bestehenden Fachstellen sollten dem Regierungsrat regelmässig Bericht über die Risikosituation erstatten, damit er die Tragbarkeit des daraus kumulierten Restrisikos abschätzen kann. Mit Hilfe von zusätzlichen regelmässigen Überprüfungen und zielgerichteten Schulungen kann kantonsweit eine sicherheitsbewusste Kultur geschaffen und der aktuelle technische Standard wirksam erhalten werden.

Abbildung 2



Erfüllungsgrad der konzeptionellen Detailanalyse, zusammengefasst nach Stellen

Geheimhaltungspflichten für Behörden

Behördenmitglieder unterliegen einerseits verschiedenen Geheimhaltungspflichten. Andererseits sind sie in gewissen Fällen jedoch auch verpflichtet, Informationen aus eigener Initiative, ohne eine entsprechende Anfrage und auch ohne Einwilligung der betroffenen Person, weiterzugeben.

Die Anzeige- und Mitteilungspflichten sowie die Melderechte bilden die gesetzliche Grundlage für eine Datenbekanntgabe.

Anzeigepflicht

Während Privatpersonen keiner Anzeigepflicht unterstehen, müssen Behörden und Beamte strafbare Handlungen, von denen sie in Ausübung ihrer Amtstätigkeit erfahren, grundsätzlich anzeigen (§ 21 Abs. 1 Strafprozessordnung, StPO). Tun sie dies nicht, so können sie sich dadurch der Begünstigung (Art. 305 Strafgesetzbuch, StGB) schuldig machen. Es bestehen jedoch verschiedene Einschränkungen. Darüber hinaus ist ein erheblicher und konkreter Verdacht auf eine strafbare Handlung Voraussetzung (vergl. Ziff. 31.8 der Weisungen der Staatsanwaltschaft für die Untersuchungsführung).

Mitteilungspflicht im Steuerbereich

Gemäss § 121 Abs. 1 Steuergesetz (StG) haben Verwaltungs- und Strafuntersuchungsbehörden sowie Gerichte von sich aus den Steuerbehörden Mitteilung zu machen, wenn sie im Zuge ihrer amtlichen Tätigkeit feststellen, dass die Wahrscheinlichkeit einer unvollständigen Versteuerung besteht. Eine weite Auslegung der Mitteilungspflicht läuft dem Prinzip der Selbstdeklaration im Steuerrecht entgegen.

Meldepflichten und -rechte im Gesundheitswesen

Für Personen, die in Gesundheitsberufen arbeiten, gelten Meldepflichten und -rechte in verschiedenen Bereichen. Der wichtigste Punkt ist die Verpflichtung, aussergewöhnliche Todesfälle, zum Beispiel Unglücksfälle und Selbstmorde, sofort der Polizeibehörde zu melden. Sie brauchen sich nicht an das Berufsgeheimnis zu halten, wenn es darum geht, der Polizei Wahrnehmungen zu melden, die auf ein Verbrechen oder Vergehen gegen Leib und Leben, gegen die öffentliche Gesundheit oder gegen die Sittlichkeit schliessen lassen (§ 15 Gesundheitsgesetz).

Gesetzliche Grundlage für die Bekanntgabe

Das Vorgehen und die Voraussetzungen für die Bekanntgabe von Personendaten durch öffentliche kantonale oder kommunale Organe im Kanton Zürich richten sich nach dem Datenschutzgesetz (DSG). Dies gilt auch, wenn kantonale Organe Bundesrecht vollziehen.

Personendaten dürfen bekannt gegeben werden, wenn es dafür gesetzliche Grundlagen gibt (§ 8 Abs. 1 DSG). Soweit es sich um besonders schützenswerte Personendaten handelt, etwa solche über strafrechtliche Verfolgungen und Sanktionen oder Massnahmen der sozialen Hilfe, muss sich die Zulässigkeit der Bekanntgabe aus einer gesetzlichen Grundlage klar ergeben (§ 5 lit. a DSG).

Die Anzeigepflicht (§ 21 StPO), die Mitteilungspflicht im Steuerbereich (§ 121 Abs. 1 StG) sowie die erwähnten Meldepflichten und -rechte (u.a. § 15 Gesundheitsgesetz) bilden gesetzliche Grundlagen für die entsprechende Bekanntgabe von Personendaten.

Einschränkungen der Datenbekanntgabe

Besteht eine gesetzliche Grundlage, vorliegend eine Anzeige-, Mitteilungs- oder Meldepflicht oder auch ein Melderecht, so muss im zweiten Schritt eine Interessenabwägung vorgenommen werden: Das öffentliche Organ lehnt gemäss § 10 DSG die Datenbekanntgabe ab, schränkt sie ein oder verbindet sie mit Auflagen, wenn es verlangt wird durch

- wesentliche öffentliche Interessen,
- schützenswerte Interessen einer betroffenen Person,
- gesetzliche Geheimhaltungspflichten (Bund oder Kanton) oder
- besondere Datenschutzvorschriften.

Wesentliche Interessen

Einer Anzeige, Mitteilung oder Meldung im Rahmen der skizzierten gesetzlichen Pflichten und Rechte stehen in der Regel keine überwiegenden öffentlichen oder schützenswerten Interessen einer betroffenen Person entgegen. Die Interessen-

abwägung im Einzelfall kann zu einem anderen Ergebnis führen.

Gesetzliche Geheimhaltungspflichten: Amtsgeheimnis

Gemäss Art. 320 Ziff. 1 Abs. 1 Strafgesetzbuch (StGB) wird bestraft, wer ein Geheimnis offenbart, das ihm in seiner Eigenschaft als Mitglied einer Behörde oder als Beamter anvertraut worden ist oder das er in seiner amtlichen beziehungsweise dienstlichen Stellung wahrgenommen hat. Die Schweigepflicht bleibt auch nach Beendigung des Dienstverhältnisses bestehen.

Dieses Amtsgeheimnis sowie dessen spezialgesetzliche Ausprägungen (unter anderem in § 51 Abs. 1 Personalgesetz, § 71 Gemeindegesetz, § 48 Sozialhilfegesetz, Art. 33 Bundesgesetz über den Allgemeinen Teil des Sozialversicherungsrechtes, ATSG) werden durchbrochen, wenn eine Anzeige-, Mitteilungs- oder Meldepflicht beziehungsweise ein Melderecht besteht.

Gesetzliche Geheimhaltungspflichten: Berufsgeheimnis

Das Berufsgeheimnis von Geistlichen, Rechtsanwälten, Verteidigern, Notaren, nach Obligationenrecht zur Verschwiegenheit verpflichteten Revisoren, Ärzten, Zahnärzten, Apothekern, Hebammen sowie ihrer Hilfspersonen (Art. 321 Ziff. 1 Abs. 1 StGB) und von Studierenden (§ 321 Ziff. 1 Abs. 2 StGB) wird durch allgemeine Anzeige- und Meldepflichten oder Melderechte (u.a. § 21 StPO, § 121 Abs. 1 StG, § 15 Gesundheitsgesetz) nicht durchbrochen. Diese sind zu wenig bestimmt, um den Anforderungen von § 321 Ziff. 3 StGB zur Aufhebung des Berufsgeheimnisses zu genügen. Anzumerken ist, dass den Geheimnisträgern in solchen Fällen die Möglichkeit bleibt, sich vom Berufsgeheimnis entbinden zu lassen (Art. 320 Ziff. 2 StGB).

Das Berufsgeheimnis wird nur durch die eidgenössischen und kantonalen Bestimmungen über die Zeugnispflicht und über die Auskunftspflicht gegenüber einer Behörde eingeschränkt (§ 321 Ziff. 3 StGB). Die angeführten Bestimmungen im Gesundheitswesen (§ 15 Gesundheitsgesetz, § 6 Abs. 3 der Verordnung über die Bestattungen, Art. 14 Abs. 4 Strassenverkehrsgesetz, Art. 27 Abs. 1 Epidemiengesetz) halten solche bereichsspezifischen, expliziten Auskunftspflichten fest.

Weitere gesetzliche Geheimhaltungspflichten

Für den Datenschutzbeauftragten und seine Mitarbeitenden gelten dieselben Verschwiegenheitspflichten (§ 25 DSG) im Hinblick auf Personendaten wie für das bearbeitende Organ.

Die Schweigepflicht für Personen, die bei einer Opferberatungsstelle arbeiten (Art. 4 OHG), kann nur mit Einwilligung des Opfers durchbrochen werden.

Besondere Datenschutzvorschriften

Zu prüfen ist gemäss § 10 DSG schliesslich, ob besondere Datenschutzvorschriften bestehen.

Wichtigstes Beispiel hierfür ist das Sozialversicherungsrecht: Organe, die mit dem Vollzug des Arbeitslosengesetzes (AVIG) oder mit deren Kontrolle beziehungsweise Beaufsichtigung betraut sind, dürfen Daten in Abweichung von der Schweigepflicht (Art. 33 ATSG) folgenden Stellen bekannt geben, sofern kein überwiegendes Privatinteresse entgegensteht:

- anderen Organen, die das AVIG durchführen oder mit der Kontrolle beziehungsweise Beaufsichtigung der Durchführung betraut sind, wenn sie für die Erfüllung ihrer gesetzlichen Aufgaben auf die Daten angewiesen sind;
- Organen einer anderen Sozialversicherung, wenn sich in Abweichung von Artikel 32 Absatz 2 ATSG eine Pflicht zur Bekanntgabe aus einem Bundesgesetz ergibt;
- den für die Quellensteuer zuständigen Behörden nach den Artikeln 88 und 100 des Bundesgesetzes vom 14. Dezember 1990 über die direkte Bundessteuer sowie den entsprechenden kantonalen Bestimmungen;
- den Organen der Bundesstatistik nach dem Bundesstatistikgesetz;
- den Strafuntersuchungsbehörden, wenn die Anzeige oder die Abwendung eines Verbrechens die Datenbekanntgabe erfordert (Art. 97a Abs. 1 lit. e AVIG).

Verschiedenen anderen Behörden werden Personendaten dagegen nur im Einzelfall auf schriftlich begründetes Gesuch hin (Amtshilfe) bekannt gegeben (Art. 97a Abs. 1 lit. f AVIG).

Im Hinblick auf § 21 StPO bedeutet dies, dass die Strafuntersuchungsbehörden unaufgefordert benachrichtigt werden dürfen, wenn die zuständige Person bei der Erfüllung ihrer Aufgaben erfährt, dass ein Verbrechen (im Sinne des Strafgesetzbuches) begangen wurde oder in Vorbereitung steht (BBL 2000 266).

Im Steuerstrafbereich gibt es Vergehen, jedoch keine Verbrechen (§ 238 ff. StG); eine Mitteilung an Steuerbehörden (auch als Strafuntersuchungsbehörden i.S. § 243 ff. StG) im Sinne von § 121 Abs. 1 StG ist ohne deren Anfrage deshalb ausgeschlossen.

Die Regelungen bei AHV und Ergänzungsleistungen entsprechen derjenigen der Arbeitslosenversicherung (Art. 50 lit. d AHVG; Art. 13 ELG).

Art. 97a Abs. 1 AVIG sowie Art. 50a Abs. 1 AHVG lassen zudem eine Datenbekanntgabe nur zu, wenn kein überwiegendes Privatinteresse entgegensteht.

Die schriftliche Einwilligung zur Offenbarung des Geheimnisses (Art. 320 Ziff. 2 StGB, Art. 321 Ziff. 2 StGB) ist gemäss § 143 der Vollzugsverordnung zum Perso-

nalgesetz in folgenden Fällen notwendig: «Angestellte dürfen sich als Partei, Zeugen oder gerichtliche Sachverständige über Wahrnehmungen in Ausübung ihrer Obliegenheiten nur äussern, wenn die Direktion oder das zuständige oberste kantonale Gericht sie dazu ermächtigt haben. Vorbehalten bleiben Auskunftspflichten im Sinne des Kantonsratsgesetzes.» Die blosse Anzeige, Mitteilung oder Meldung braucht keine Ermächtigung der vorgesetzten Behörde.

Übrige Datenbearbeitungsvorschriften

Besteht eine gesetzliche Grundlage und führt die Interessenabwägung zum Ergebnis, dass die Daten bekannt zu geben sind, hat dies unter Beachtung der allgemeinen Gebote für Datenbearbeitungen (§ 4 DSG: Zweckbindung, Richtigkeit, Verhältnismässigkeit, Sicherheit) zu erfolgen:

- Die Verwendung der Daten muss mit dem ursprünglichen Zweck vereinbar sein (§ 4 Abs. 4 DSG).
- Werden Daten bekannt gegeben, müssen sie richtig und, soweit es der Zweck des Bearbeitens verlangt, vollständig sein (§ 4 Abs. 2 DSG).
- Es dürfen nur diejenigen Daten weitergegeben werden, die für die Erfüllung der Aufgaben des Empfängers geeignet und erforderlich beziehungsweise unentbehrlich sind (§ 4 Abs. 3 DSG; § 5 lit. b DSG).
- Die Daten sind bei der Übermittlung durch angemessene organisatorische und technische Massnahmen gegen unbefugtes Bearbeiten zu schützen (§ 4 Abs. 5 DSG).

Anzeigepflicht beim Vollzug des Arbeitslosenversicherungsrechtes

Das kantonale Amt für Wirtschaft und Arbeit vollzieht das Arbeitslosenversicherungsrecht. Dabei erfahren Mitarbeitende immer wieder von tatsächlicher oder angeblicher Schwarzarbeit. Klienten und Dritte werden verdächtigt, gegenüber den Steuer- und Sozialversicherungsbehörden falsche Angaben zu machen, was zu unvollständiger Besteuerung, zu tieferen Sozialversicherungsbeiträgen oder zum Doppelbezug von Sozialversicherungsleistungen führen kann. Einzelne Personen werden verdächtigt, sich illegal in der Schweiz aufzuhalten.

Beim Verdacht auf strafbares Verhalten besteht im Rahmen von § 21 StPO nicht nur ein Melderecht, sondern eine Anzeigepflicht. Eine Meldepflicht gilt auch im Rahmen von § 121 StG.

Die Interessenabwägung nach § 10 DSG führt zu folgenden Ergebnissen:

- Es sind keine wesentlichen öffentlichen Interessen ersichtlich, welche der Datenbekanntgabe entgegenstehen.
- Es liegen keine offensichtlich schützenswerten Interessen der betroffenen Person vor, die das öffentliche Interesse an der Rechtsstaatlichkeit und einer korrekten Besteuerung überwiegen. Diese Interessenabwägung kann im Einzelfall zu einem anderen Ergebnis führen.
- Gesetzliche Geheimhaltungspflicht: Das Amtsgeheimnis wird durch die Anzeige- und Meldepflicht durchbrochen.
- Besondere Datenschutzvorschriften: In Abweichung von Art. 33 ATSG dürfen gemäss Art. 97a Abs. 1lit. e AVIG Daten den Strafuntersuchungsbehörden gemeldet werden, wenn die Anzeige eines Verbrechens die Datenbekanntgabe erfordert; eine solche Ausnahme ist für den Steuerbereich nicht vorgesehen.
- Art. 97a AVIG beinhaltet eine weitere besondere Datenschutzvorschrift: Die Datenbekanntgabe ist nur zulässig, wenn kein überwiegendes Privatinteresse entgegensteht. Ein solches liegt in der Regel jedoch nicht vor.

Unter diesen Umständen muss das kantonale Amt für Wirtschaft und Arbeit in der Regel Strafuntersuchungsbehörden im Rahmen von § 21 StPO Anzeige erstatten, und zwar von sich aus und ohne Einwilligung der betroffenen Person. Die Grundsätze von § 4 DSG (Zweckbindung, Richtigkeit, Verhältnismässigkeit, Sicherheit) müssen dabei beachtet werden.

Meldungen an die Steuerbehörden gemäss § 121 StG sind dagegen zu unterlassen; ihnen muss nur im Einzelfall auf schriftliches Gesuch hin Auskunft erteilt werden (Art. 97a Abs. 1 lit. f Ziff. 5 AVIG).

Unproblematisch ist die Bekanntgabe von Informationen an Organe, die mit der Durchführung, Kontrolle oder Beaufsichtigung des AVIG betraut sind; eine Anfrage ist dafür nicht notwendig (Art. 97a Abs. 1 lit. a AVIG).

Gegenüber Organen einer anderen Sozialversicherung erfolgt die Bekanntgabe von Personendaten dagegen grundsätzlich nur auf Anfrage, im Rahmen der Amtshilfe (Art. 32 Abs. 2 ATSG), ausser wenn in einem Ausführungserlass eine Mitteilungspflicht festgehalten ist (Art. 97a Abs. 1 lit. b AVIG).

Keine Datenbekanntgabe bei Sperre

Eine zentrale Stelle für die Sperrung von Daten gibt es nicht. Die Einwohnerkontrolle, das Gemeindesteueramt sowie das Strassenverkehrsamt dürfen Adressdaten voraussetzungslos jedermann bekannt geben; es ist aber möglich, bei diesen drei Amtsstellen eine Datensperre zu erwirken.

Kantonale und kommunale Organe dürfen auf Anfrage von privater Seite Adressen und weitere Personendaten nur bekannt geben, wenn dafür gesetzliche Grundlagen bestehen, die betroffene Person ihre Daten allgemein zugänglich gemacht oder im Einzelfall eingewilligt hat beziehungsweise wenn die Einwilligung den Umständen nach vorausgesetzt werden darf (§ 8 Abs. 1 DSG). Derzeit gibt es folgende gesetzliche Grundlagen:

Einwohnerkontrolle (§ 9 DSG)

«Die Einwohnerkontrolle gibt einer privaten Person oder Organisation im Einzelfall auf Gesuch ohne Einschränkung Name, Vorname, Adresse, Datum von Zu- und Wegzug sowie Beruf einer Person bekannt.

Zuzugsort und Wegzugsort, Geburtsdatum, Geschlecht, Zivilstand und Heimatort einer Person werden bekannt gegeben, wenn ein berechtigtes Interesse glaubhaft gemacht wird.

Werden diese Daten mit Ausschluss von Zu- und Wegzugsort ausschliesslich für schützenswerte ideelle Zwecke verwendet und nicht an Dritte weitergegeben, so können sie nach bestimmten Gesichtspunkten geordnet bekannt gegeben werden.

Weitere Personendaten können bekannt gegeben werden, wenn ein besonders schützenswertes Interesse nachgewiesen wird.»

Steuerausweis/Gemeindesteueramt (§ 122 StG)

«Gemeindesteuerämter stellen gegen Gebühr Ausweise über das steuerbare Einkommen und Vermögen, den steuerbaren Reingewinn und das steuerbare Kapital gemäss der letzten rechtskräftigen Einschätzung oder aufgrund der letzten Steuererklärung aus. Ausnahmsweise können auch Ausweise über frühere Einschätzungen ausgestellt werden.

Die Bestimmungen des kantonalen Datenschutzgesetzes bleiben vorbehalten.»

Fahrzeughalter und -halterinnen/Strassenverkehrsamt (Art. 126 Abs. 1 VZV)

«Namen und Adresse von Inhabern eines Kontrollschildes können jedermann bekannt gegeben werden.»

Datensperre

Wir empfehlen Personen, die eine Datenbekanntgabe in diesen Fällen ausschliessen wollen, bei den entsprechenden Amtsstellen mittels schriftlicher Mitteilung eine Datensperre zu errichten. § 11 Datenschutzgesetz enthält dazu folgende Regelung:

«Die betroffene Person kann die Bekanntgabe ihrer Daten an private Personen und Organisationen sperren lassen.

Die Bekanntgabe ist trotz Sperrung zulässig, wenn

a) das öffentliche Organ hiezu gesetzlich verpflichtet ist oder

b) die gesuchstellende Person oder Organisation glaubhaft macht, dass die Sperrung sie in der Verfolgung eigener Rechte gegenüber der betroffenen Person behindert.»

Die Datensperre wirkt somit gegenüber Privaten nicht absolut und entfaltet keine Wirkung bei Anfragen von anderen Amtsstellen. Der unkontrollierten Datenbekanntgabe an Private wird jedoch ein Riegel vorgeschoben.

Fälle aus der Beratungstätigkeit

Ein Schwerpunkt der Tätigkeit des Datenschutzbeauftragten bildet die Beratungstätigkeit.

01. – 27. ***Die hier zusammengefassten Fälle sind ausführlich dargestellt im Anhang auf Seite 39 ff. und auf der Website des Datenschutzbeauftragten (www.datenschutz.ch).***

01. **Telefonaufzeichnungen**
Es ist nicht zulässig, dass eine Amtsstelle vor der Entgegennahme sämtlicher Telefonanrufe ein Tonband mit einem Hinweis auf eine Aufnahmemöglichkeit zu Schulungszwecken vorspielt, mit dem Zweck, Anrufende von verbalen Entgleisungen abzuhalten.

02. **DNA-Analysen in Strafverfahren**
In der kantonalen DNA-Verordnung sind nur noch Ausführungsbestimmungen zum neuen eidgenössischen DNA-Profil-Gesetz enthalten.

03. **Sockelbeiträge und Arztgeheimnis**
Neu haben die Wohngemeinden die Sockelbeiträge beim Spitalaufenthalt ihrer Einwohner in der privaten Abteilung zu übernehmen, so halten es die §§ 39 Abs. 3 und 40 Abs. 2 des Gesundheitsgesetzes fest. Dies ist jedoch keine genügende Rechtsgrundlage für die Spitäler, um das Berufsgeheimnis nach Art. 321 Strafgesetzbuch zu durchbrechen.

04. **Wochenaufenthalt: Nicht verhältnismässige Angaben**
Die Angaben über Wochenaufenthalter bei der Einwohnerkontrolle dürfen den Umfang des Notwendigen nicht übersteigen. Nicht gefragt werden darf nach den Zahlen der letzten Steuerveranlagung, nach der Anzahl der Zimmer der Mietwohnung, nach Name, Vorname und Geburtsdatum des Konkubinatspartners, nach Name, Vorname, Adresse und Geburtsdatum der nächsten Familienangehörigen sowie nach Mitgliedschaften in Vereinen sowie nach deren Name und Ort des Vereins. Diese Angaben sind allesamt nicht erforderlich und daher unverhältnismässig.

05. **E-Learning-Plattform und Schweigepflicht**
Eine E-Learning-Plattform für Studierende, welche besonders schützenswerte Personendaten enthält, darf unter Einhaltung gewisser Bedingungen eingerichtet werden. Besonders zu beachten sind Sicherheitsvorschriften wie der Passwortschutz sowie Geheimhaltungsbestimmungen.

06. **Bekanntgabe der aus dem Lotteriefonds Begünstigten**
Eine interkantonale Vereinbarung sieht die Veröffentlichung sowohl der zugesprochenen Beiträge aus dem Lotteriefonds als auch der Begünstigten vor. Bis die Vereinbarung jedoch in Kraft gesetzt ist, kann der Regierungsrat selber entscheiden, ob er diese Beschlüsse veröffentlicht. Diejenigen des Kantonrates hingegen sind grundsätzlich öffentlich.

07. **Psychologische Tests und Videoaufnahmen von Mitarbeitenden**
Psychologische Tests und Videoaufnahmen sind nur mit ausdrücklicher Einwilligung der betroffenen Personen erlaubt. Willigt eine Person nicht ein, dürfen ihr daraus keine Nachteile erwachsen.

08. **Datenschutz im Gesundheitsförderungsprojekt**
Ohne ausdrückliche Einwilligung ist ein Arzt nicht zur Bekanntgabe von Adressen seiner Patientinnen und Patienten befugt – auch dann nicht, wenn es der Gesundheitsförderung der betroffenen Person dient und ihr in Form von kostenloser Beratung zugute kommt.

09. **Verwendung von internen Geschäftsinformationen im Anstellungsverfahren**
Informationen aus einem internen Geschäftsverzeichnis – konkret zu gelöschten Einträgen im Strafregister – dürfen nur zum Zweck der Geschäftsverwaltung genützt werden. Eine anderweitige Verwendung, im vorliegenden Fall zur Beurteilung der Eignung für die Anstellung bei einer Strafuntersuchungsbehörde, widerspricht der ursprünglichen Zweckbestimmung und ist daher rechtswidrig.

10. **Separates Konkursverzeichnis im Internet**
Der Kanton Zürich kann im Internet ein eigenes Konkursverzeichnis führen. Es muss sich allerdings auf die Bekanntgabe derjenigen Personendaten beschränken, welche – gestützt auf entsprechende Grundlagen im Schuldbetreibungs- und Konkursrecht – bereits im Schweizerischen Handelsamtsblatt publiziert werden.

11. **Personalien von Opfern in Strafverfahrensakten**
Werden die Opfereigenschaft und die besondere Schutzbedürftigkeit einer geschädigten Person bejaht, hat sie ein Recht darauf, dass ihre Identität dem mutmasslichen Täter nicht preisgegeben wird. Aus praktischer Sicht empfiehlt es sich, die Vorkehrungen bereits im Stadium der ersten Kontaktaufnahme des Opfers mit der Polizei zu treffen.

12. **Beurteilung der Fahrtauglichkeit**
Die Erhebung der Arbeitssituation und des sozialen Umfeldes ist für die Überprüfung der Fahrtauglichkeit einer querschnittgelähmten Person weder geeignet noch erforderlich und somit unzulässig.

13. **Automatische Mutationsmeldungen**
Es gibt ausreichende gesetzliche Grundlagen für automatische Mutationsmeldungen aus den Einwohnerregistern an das Amt für Militär und Zivilschutz über das Datentransportsystem von e-Voting an die Datendrehscheibe MILVA, doch sind die Meldungen nicht in allen Fällen verhältnismässig.

14. **Videoaufnahmen von Psychiatriepatientinnen und -patienten**
Für die Videoaufzeichnung von Patientinnen und Patienten in der Psychiatrie müssen Prozesse definiert werden, um die Persönlichkeitsrechte der Aufgezeichneten zu schützen.

15. **Datenbearbeitung durch das Sozialamt**
Sozialhilfeempfangende sind gesetzlich zur Mitwirkung verpflichtet. Die Datenbearbeitungen durch das Sozialamt dürfen den Umfang des Notwendigen jedoch nicht übersteigen. So müssen die Kontoauszüge im Falle der wirtschaftlichen Hilfe nicht im Detail eingereicht werden; zu belegen sind nur Datum und Höhe der Ausgaben oder Einnahmen. Die Betroffenen brauchen keine Rechenschaft darüber abzulegen, was sie genau mit dem jeweiligen Betrag erworben haben.

16. **Ärztliches Zeugnis für Anmeldung**
Für die Abklärung der gesundheitlichen Eignung zum Lehrberuf darf ein Arztzeugnis bei der Anmeldung verlangt werden, da hierfür gesetzliche Grundlagen bestehen. Dabei dürfen jedoch nur die Angaben erfragt werden, die für die Beurteilung der Eignung zur Ausbildung und zum späteren Beruf geeignet und erforderlich sind.

17. **Einwilligung der Eltern in die Befragung von Jugendlichen für eine Langzeitstudie**
Jugendliche müssen sich mit der Befragung im Rahmen einer Langzeitstudie einverstanden erklären. Für Fragen, die ausschliesslich sie selber betreffen, sind sie ab ungefähr 14 Jahren urteilsfähig. Die Einwilligung der Eltern ist deshalb nicht nötig. Das Forschungsprojekt ist ihnen altersentsprechend zu erklären. Eine Information der Eltern ist jedoch sinnvoll.

18. **Auskunfts- und Berichtigungsrechte**
Der Verein «Verdingkinder suchen ihre Spur» bemüht sich um Klärung der persönlichen und rechtlichen Verhältnisse von Menschen, die verdingt oder in Heime abgeschoben worden sind. Die betroffenen Personen haben grundsätzlich ein uneingeschränktes und kostenloses Auskunftsrecht in ihre bei den entsprechenden öffentlichen Organen vorhandenen Daten. Zudem können sie deren Berichtigung und Vernichtung verlangen.

19. **Namensnennung bei parlamentarischen Vorstössen und Initiativen**
Die Bekanntgabe von Kantonsratsakten ist abzulehnen oder einzuschränken, wenn offensichtlich schützenswerte Interessen einer betroffenen Person es verlangen. Ob ein solches Interesse vorliegt, kann erst nach einer Interessenabwägung im Einzelfall entschieden werden. Blosse Namensnennungen ohne verletzende oder diskriminierende Ausführungen sind in Kantonsratsakten unter Vorbehalt von § 10 Datenschutzgesetz möglich.

20. **Einsicht in Prüfungen an der Medizinischen Fakultät**
Die Einsicht in Prüfungen an der Medizinischen Fakultät ist grundsätzlich vollumfänglich zu gewähren. Sie darf jedoch aus Gründen des öffentlichen Interesses eingeschränkt werden. Dies ist der Fall bei Fragen, die für die Beurteilung der Prüfung grundlegend sind (so genannte «Ankerfragen»). Hier ist eine Einschränkung auf die reine Einsichtnahme ohne Abgabe von Kopien möglich, da die Fragen sonst künftigen Prüflingen zukommen könnten. Zur Verdeutlichung ist eine gesetzliche Grundlage zu schaffen, welche das geschilderte öffentliche Interesse präzisiert.

21. **Bekanntgabe des Aufenthaltsortes eines Inhaftierten zwecks Betreibung**
Gegenüber dem Gläubiger kann der Aufenthaltsort des inhaftierten Schuldners nur mit dessen Einwilligung bekannt gegeben werden. Das Betreibungsamt kann sich hingegen auf Amtshilfe berufen, um diese Informationen zu erhalten.

22. **Videoüberwachung**
Eine Videoüberwachung ist auch bei Vorliegen einer gesetzlichen Grundlage nur dann zulässig, wenn sie verhältnismässig ist. Neben der Bewilligung sind somit rechtliche Rahmenbedingungen sowie konkrete Anweisungen für den Betrieb der Videoüberwachung des Eingangsbereichs der Garderoben auf dem Sportplatz einer Gemeinde zu schaffen.

23. **Kostenlosigkeit der Auskunft**
Die Auskunft gemäss Datenschutzgesetz ist ohne Kostenauflage zu erteilen. Eine Kostenauflage für das Auskunftsrecht rechtfertigt sich nur, wenn für die Auskunftserteilung ein besonders grosser Arbeitsaufwand nötig ist.

24. **Online-Zugriffe auf Daten der Gebäudeversicherung**
Die Gebäudeversicherung darf einer Bank nur für diejenigen Daten einen Online-Zugriff einrichten, für welche die Einwilligung der betroffenen Person vorliegt. Ein Zugriff für die Kantonspolizei ist mangels gesetzlicher Grundlagen unzulässig.

25. **Fahrzeughalterdaten im Internet**
Unter der Internetadresse www.autoindex.zh.ch und über die Website des Strassenverkehrsamtes können die Daten der rund 800 000 Fahrzeughalterinnen und -halter im Kanton Zürich abgefragt werden. Diese Möglichkeit entspricht nicht den datenschutzrechtlichen Vorschriften.

26. **Sozialhilfestatistik**
Die Angaben für die Sozialhilfestatistik dürfen für die Übermittlung von der Gemeinde an das Bundesamt für Statistik nur die zur Identifikation absolut notwendigen Daten enthalten. Dazu gehören die Dossiernummer, das Erhebungsjahr, das Aufnahmedatum sowie die AHV-Nummer.

27. **Personendaten-Pool**
Die Schaffung von zentralen Personendatensammlungen, auf die verschiedene Amtsstellen Zugriff haben, so genannte Personendaten-Pools, sind nur zulässig, wenn entsprechende gesetzliche Grundlagen vorhanden sind.

Vernehmlassung zum Polizeigesetz

Der Entwurf des neuen Polizeigesetzes ist aus datenschutzrechtlicher Sicht in einigen Punkten zu überarbeiten. Im Vernehmlassungsverfahren wurden entsprechende Vorbehalte angebracht.

Das Datenschutzgesetz knüpft seinen Geltungsbereich daran, ob ein Verfahren eröffnet ist (§ 3 Abs. 2 lit. b DSG). Damit zieht es nicht die gleiche Grenze der Anwendbarkeit im Rahmen der Strafverfolgung wie das vorgeschlagene Polizeigesetz.

Erhebliche Schwierigkeiten bei der Feststellung der Identität allein vermögen die Vornahme einer solchen nicht zu rechtfertigen. Erkennungsdienstliche Massnahmen dürfen deshalb ausserhalb von Strafverfahren nur angeordnet werden, wenn sie dem entsprechenden Zweck dienen.

Die polizeilichen Fahndungsmittel müssen auf formellgesetzlicher Ebene konkret bezeichnet und inhaltlich kurz umschrieben werden.

Gemäss Vernehmlassungsentwurf können die Rückführung von ausreisepflichtigen Personen und der Transport von Gefangenen spezialisierten privaten Organisationen übertragen werden. Vorgesehen ist die Übertragung einer hoheitlichen Aufgabe an Private. Untrennbar damit verbunden ist die Bekanntgabe von besonders schützenswerten Personendaten an die private Organisation im Sinne von §§ 8 und 10 Datenschutzgesetz und ihre weitere Bearbeitung durch diese Organisation. Unter diesen Umständen sind die Grundzüge der Datenbearbeitung auf Gesetzesstufe zu umschreiben; Aufsicht und Kontrolle müssen sichergestellt werden. Das Amtsgeheimnis sowie allfällige Berufs- und Spezialgeheimnisse sind durch funktionale Unterstellung den einzelnen Mitarbeitenden der privaten Organisation zu überbinden. § 13 Abs. 2 Datenschutzgesetz genügt dafür nicht.

Polizeiliche Berichte zur Person widersprechen dem Grundsatz, wonach Personendaten in der Regel bei der betroffenen Person zu beschaffen sind (§ 7 Abs. 1 DSG). Damit diese ihre Rechte gemäss §§ 17 ff. Datenschutzgesetz geltend machen kann, muss für sie transparent werden, dass Daten bearbeitet werden oder wurden. In diesem Sinne hat die Polizei die Informationen bei der betroffenen Person oder für diese erkennbar zu beschaffen, es sei denn, dass dadurch die Erfüllung der polizeilichen Aufgabe ernsthaft gefährdet ist oder die Datenbeschaffung auf diesem Weg in keinem Verhältnis zum Aufwand steht. Ist die Datenbeschaffung für die betroffene Person nicht erkennbar, so hat die Polizei sie nachträglich zu informieren, sobald der Zweck der Datenbeschaffung es zulässt.

Die Grundzüge von Registern der privaten Sicherheitsdienste sowie der im privaten Sicherheitsgewerbe und im Bereich der Verkehrsregelung tätigen oder potenziell tätigen Personen sind auf Gesetzesstufe zu umschreiben.

Die eingesetzten Datenbearbeitungssysteme müssen auf formellgesetzlicher Ebene konkret bezeichnet und inhaltlich kurz umschrieben sein. Als Anhaltspunkt dienen die entsprechenden Regelungen des Bundes.

Die vorgeschlagenen Anforderungen der Bearbeitung von Personendaten für nicht personenbezogene Zwecke genügen dem Datenschutzgesetz nicht.

Der Begriff der Gewaltbereitschaft sowie die Grundzüge von Registern über gewaltbereite Personen sind auf formellgesetzlicher Ebene zu umschreiben. Auf Gesetzesstufe zu klären sind auch die Abgrenzungen zwischen Anzeigerecht, Amtsgeheimnis, besonderen Geheimhaltungspflichten sowie dem vorgeschlagenen allgemeinen Melde- und Auskunftsrecht.

Die Bekanntgabe von Daten ist nur im Rahmen von § 8 Datenschutzgesetz zulässig. Die vorgeschlagene Generalermächtigung zum Austausch von Daten zwischen Polizeistellen im In- und Ausland, inner- und interkantonal stellt keine ausreichende gesetzliche Grundlage dar; die einzelnen Umstände des Austausches müssen auf Gesetzesstufe geregelt werden. Als Anhaltspunkt dienen auch hier die entsprechenden Regelungen des Bundes.

Identifikation und Behandlung von Spam-Mails

Die Verordnung über die Nutzung von Internet und E-Mail erlaubt den Mitarbeitenden ausdrücklich die Nutzung von E-Mail für private Zwecke (§ 4 Abs. 1). Die Direktionen können die private Nutzung einschränken (§ 5), im Hinblick auf § 4 aber nicht untersagen.

Private E-Mails sind – analog der als persönlich/vertraulich bezeichneten Briefpost – dem Adressaten oder der Adressatin persönlich zuzustellen. Sofern es ohne Kenntnisnahme des Inhaltes oder des Betreffs nicht möglich ist, eine E-Mail eindeutig als geschäftlich zu klassieren, ist sie wie private Korrespondenz zu behandeln. In der Praxis sind deshalb in der Regel alle an eine persönliche Adresse gerichteten E-Mails wie private zu behandeln.

Die Verordnung über Nutzung von Internet und E-Mail enthält lediglich Regeln und Einschränkungsmöglichkeiten für das Versenden von privaten E-Mails. Eine Rechtsgrundlage für die Filterung von geschäftlichen oder privaten E-Mails und die entsprechende Behandlung (Nichtzustellung oder veränderte Zustellung) fehlt dagegen.

Aus diesem Grund empfahl der Datenschutzbeauftragte dem kantonalen IT-Team KITT, auf eine Anpassung der Verordnung über Nutzung von Internet und E-Mail hinzuwirken und darin folgende Grundzüge zu regeln:

- Schaffung einer Rechtsgrundlage für die Installation eines Spam-Filters für die Zustellung von E-Mails an alle E-Mail-Adressen der kantonalen Verwaltung sowie seiner unselbständigen Anstalten;
- Definition der unter den Begriff «Spam-Mail» fallenden unerwünschten E-Mails;
- Definition von Kriterien und Regeln der Einteilung der E-Mails in Klassen und Festlegung der Folgen der Filterung für die einzelnen Klassen.

Jede Entscheidung über Zustellung oder Nichtzustellung eines Mails hat sich nach dem Verhältnismässigkeitsprinzip zu richten: Es gilt abzuwägen zwischen dem grundsätzlichen Anspruch auf Zustellung und der durch das Zustellen und unnötige Bearbeiten von Spam-Mails durch die einzelnen Mitarbeitenden verursachten technischen und zeitlichen Belastung kantonaler Ressourcen sowie der Sicherheitsrisiken.

Eine Filterung als abstrakte technische Regel setzt diese Abwägung im Einzelfall um; für die Nichtzustellung muss eine E-Mail mit hoher Wahrscheinlichkeit als Spam qualifiziert werden können. Aus datenschutzrechtlicher Sicht nicht zulässig ist die Einrichtung eines Sammel-«Quarantäne»-Postfaches für mehrere persönliche E-Mail-Adressen. Nichts einzuwenden ist gegen individuelle «Quarantäne»-Postfächer, je separat für jede E-Mail-Adresse.

Umfassende Sicherheitsberatung

Die Sicherheit der Informatik ist ein wesentlicher Bestandteil eines umfassenden Datenschutzes. Im Bereich der Informationssicherheit ist deshalb eine nachhaltige Beratung erforderlich.

Informatiksicherheit geht alle Verwaltungsbereiche etwas an, denn sie betrifft auch die Geschäftsprozesse und die Organisation. Das Informationssicherheitsmanagement muss deshalb einerseits Vorgaben für den Informatikbetrieb definieren und andererseits deren Einhaltung überwachen sowie Abweichungen erkennen und beheben. Die Sicherheit beschränkt sich nicht auf die Technologie allein. Es muss strategisch, taktisch und operationell sichergestellt werden, dass Organisation, Prozesse und Technologien aufeinander und auf die Informationssicherheitsstrategie abgestimmt sind.

Beratung des Datenschutzbeauftragten

Die Beratungsstelle für Informatiksicherheit (BIS) des Datenschutzbeauftragten erhielt von einer Amtsstelle den Auftrag, die Bereiche zu identifizieren, die es abzusichern oder zu überprüfen galt. In einem ersten Schritt definierte sie gemeinsam mit der Amtsleitung die Sicherheitsziele und hielt sie in einer Informationssicherheitspolitik fest. Auf dieser Grundlage erstellte sie dann ein Konzept, das sämtliche Themenbereiche umfasst und detailliert die Vorgaben und konkreten Schritte beschreibt. Besonders ins Gewicht fällt der Einsatz der Informatikmittel und der damit verbundenen Aktivitäten:

- Organisation der Informatik-Funktionsträger;
- physische und logische Sicherheitsvorkehrungen;
- Sicherheitsverfahren und -massnahmen für die Erfassung, Verarbeitung, Übermittlung, Speicherung, Aufbewahrung, Archivierung, Löschung und Vernichtung von Informationen (Daten und Programme);
- Programmentwicklung und -unterhalt beziehungsweise Anwendung von Standardprodukten (auch wenn diese vollständig oder teilweise ausgelagert sind);
- Ausdruck auf Papier oder Ausgabe auf einem anderen Medium.

Weiter definiert das Sicherheitskonzept die Verantwortlichkeiten aller Mitarbeitenden im Informatikbereich. Die Vorgaben entsprechen dem Stand der aktuellen Technik und der Gesetzgebung.

Anschliessend wurden in Zusammenarbeit mit dem Informatikverantwortlichen die übergeordneten Dokumente wie Benutzerweisungen, Betriebsrichtlinien sowie Konzepte für den operationellen Betrieb – rollenbasierte Zugriffe, Notfallvorsorge, Virenschutz und Datensicherung – überarbeitet und teilweise ergänzt.

Informationssicherheitsbeauftragter

Da die Verantwortung für Informationssicherheit genauso in der Linie delegiert wird wie die die Aufgaben selbst, besteht bei unklarer Zuweisung die Gefahr, dass sich zuletzt niemand dafür verantwortlich fühlt. Um dies zu vermeiden, sollte die Verantwortung einer Funktion – dem Informationssicherheitsbeauftragten – übertragen werden. Dieser ist dann innerhalb eines Organs für alle Bereiche der Informationssicherheit zuständig.

Diese Funktion würde in etwa folgende Aufgaben beinhalten:

- definierter Ansprechpartner für die Organisation in Informationssicherheitsfragen,
- Mitwirkung im gesamten Informationssicherheitsprozess,
- Erstellen der Informationssicherheitsleitlinie (Security Policy),
- Erarbeiten und Begutachten von Informationssicherheitsstrategien und -konzepten,
- Erstellung des Notfallvorsorgekonzepts und dessen Koordination mit anderen übergeordneten Konzepten der Direktionen und der kantonalen Verwaltung,
- Definition von Sicherheitsstandards und Erstellen von Richtlinien, Weisungen sowie Empfehlungen zur Umset-

zung der Informatiksicherheitsverordnung (ISV),
- Erstellung des Realisierungsplans für übergeordnete Informationssicherheitsmassnahmen sowie Initiierung und Überprüfung der Realisierung gemäss ISV,
- Planung und Durchführung von Sensibilisierungsprogrammen und Schulungen im Bereich der Informationssicherheit,
- Begleitung von Projektleitungsaufgaben und Ansprechpartner für alle Belange der Informationssicherheit,
- Bericht gegenüber dem Team des Informationssicherheitsmanagements und der Leitungsebene,
- Informationsfluss zwischen anderen kantonalen Informationssicherheitsbeauftragten sicherstellen sowie
- möglicherweise auftretende sicherheitsrelevante Zwischenfälle feststellen und untersuchen.

Diese Funktion gehört in das Organigramm, kann jedoch als Mandat durch eine externe Stelle wahrgenommen werden.

Zur Erfüllung der Aufgaben braucht der Informationssicherheitsbeauftragte fundiertes Wissen, Erfahrung in den Gebieten Informationssicherheit und -technologien sowie die nötigen vielseitigen Qualifikationen. Die Beratungsstelle für Informatiksicherheit (BIS) deckt diese vollständig ab. Deshalb haben vier unterschiedliche Organisationen der kantonalen Verwaltung die BIS für diese Funktion auf Mandatsbasis beauftragt.

Projekt Sicherheitskonzept

Eine grosse Amtsstelle beauftragte die Beratungsstelle für Informatiksicherheit damit, den Entwurf eines Datenschutz- und Datensicherheitskonzepts für ein bestimmtes Projekt zu beurteilen. Nach einer eingehenden Studie der Dokumentation gelangte die Beratungsstelle zu folgenden Erkenntnissen:

Die professionellen Ausführungen wurden generell sehr präzise und zielgruppenorientiert formuliert. Form und Inhalt des Konzepts entsprechen den gängigen Sicherheitsmodellen und können gut nachvollzogen werden. Einige wenige Abschnitte sind jedoch etwas unklar formuliert oder sollten allenfalls präzisiert werden.

So wurde unter anderem begründet, dass das interne Netzwerk sicherer sei als ein externes. Die Ergebnisse mehrerer unabhängiger Studien über Computerkriminalität belegen jedoch, dass über 75 Prozent aller Angriffe auf Informationsnetzwerke von innen erfolgen. Hinzu kommt, dass ein Angriff von innen (also unter Mitwirkung der Mitarbeitenden) potenziell erfolgreicher ist als einer von aussen und dass es schwierig ist, einen Betrieb davor zu schützen. Zudem besteht die Gefahr, dass Daten in Klartext übermittelt werden und somit während der Übertragung ohne Aufwand oder grösseres technisches Wissen mit gängigen Sniffer-Programmen (Netzwerk-Schnüfflern) von jedem Ort innerhalb des Netzwerkes aufgezeichnet beziehungsweise mitgelesen werden können. Zudem wurde der Umstand nicht berücksichtigt, dass durch ein einfaches Zurückladen (Restore) der Datensicherung das Risiko eines nicht berechtigten Datenzugriffs besteht, wenn die Daten unverschlüsselt auf den Backup-Bändern ausgelagert werden. Vorsichtshalber sollten sensible Informationen deshalb bei Ablage und Transport durch Verschlüsselungstechnologien nur autorisierten Mitarbeitenden zugänglich gemacht werden.

Aus Sicht des Datenschutzes wurde am Konzept weiter bemängelt, dass sämtliche Manipulationen zwar durch Protokollierung der Änderungen und Zugriffe zugeordnet werden können, diese Protokolle jedoch ihrerseits durch die Administratoren manipuliert werden können. Die Beratungsstelle empfahl deshalb, die Protokolle beziehungsweise Log-Dateien auf einmalbeschreibbare Datenträger (wie zum Beispiel DVD-ROM) aufzuzeichnen oder durch geeignete Verschlüsselungstechnologien (signierter Hashwert) das Manipulationsrisiko der Log-Dateien zu minimieren.

Das Sicherheitskonzept definierte eine starke Authentisierung als Voraussetzung für eine rollenbasierte Zugriffsberechtigung. Der Zugriff auf alle Informatiksysteme oder Daten der ISV-Sicherheitsstufe 3 muss durch Identifikation und Authentifikation der zugreifenden Benutzer oder Informatiksysteme abgesichert werden. Beim Zugriff aus externen Netzen sind die im vorgelegten Sicherheitskonzept definierten starken Authentisierungsverfahren einzusetzen, also solche, die zum Beispiel auf dem Einsatz von Einmalpasswörtern oder dem Besitz von Chipkarten basieren. Für den generellen Abruf von gespeicherten Informationen muss die Zugriffs- beziehungsweise Zugangskontrolle formell geregelt sein. Neben den Kontrollen, die an den einzelnen Informatikkomponenten eingerichtet werden sollten, braucht es auch eine übergreifende Richtlinie, welche die Grundsatzfragen regelt. Diese Regelungen müssen den Schutzbedarf der Daten widerspiegeln. Es empfiehlt sich, für nutzungsberechtigte Personen aufgrund ihrer Funktionen und Aufgaben Standard-Rechteprofile festzulegen. Die Benutzerrechte für Zugriffe auf Dateien und Programme müssen abhängig von der jeweiligen Rolle, den Bedürfnissen für die Bearbeitung und der Sensitivität der Daten definiert sein. Falls über den Standard hinausgehende Rechte vergeben werden, sollte dies durch das verantwortliche Organ schriftlich in einem Auftrag mit Begründung festgehalten werden. Die Richtlinien für die Zugriffskontrolle müssen allen Verantwortlichen für Informatikanwendungen vorliegen. Darauf aufbauend können dann Zugriffsregelungen abgeleitet und eingerichtet

werden. Für jedes einzelne Informatiksystem und jede -anwendung sollten schriftliche Regelungen sowie die Dokumentation der Einrichtung von Benutzern und der Rechtevergabe vorhanden sein. Hierbei müssen die system- beziehungsweise anwendungsspezifischen Besonderheiten und Sicherheitsanforderungen berücksichtigt werden. Verantwortlich für die Erstellung und Aktualisierung der Vorgaben sind meistens die jeweiligen Informatikverantwortlichen. Werden an Mitarbeitende besonders weitgehende Rechte vergeben (zum Beispiel an Administratoren), so sollte dies möglichst restriktiv erfolgen, indem zum einen der Kreis der privilegierten Benutzer eingeschränkt wird und zum anderen nur die für die Arbeit benötigten Rechte vergeben werden.

Evaluation einer komplexen Sicherheitslösung

Die Beratungsstelle für Informatiksicherheit (BIS) wurde im Rahmen einer Grobevaluation angefragt, vier mögliche Varianten einer sicheren Anbindung von Benutzersystemen an die Applikationsserver zu beurteilen, welche bei einer externen Firma (Outsourcing) betrieben werden. Die Beurteilung ergab:

- Nur eine der aufgezeigten Lösungen entspricht den Sicherheitsanforderungen der ISV Stufe S3, sofern sich die digitalen Zertifikate auf einer Smartcard oder einem USB Token befinden. Die vom Projektteam aus Kostengründen angestrebte Verwendung von Soft Tokens genügt jedoch dem geforderten Sicherheitsanspruch gemäss ISV nicht.
- Die Umsetzung einer Variante ohne zusätzliche Sicherheitsmassnahmen (mindestens Passwort, besser aber eine starke Authentisierung und ein besonderer Schutz für die temporären Zertifikate) ist nicht zu empfehlen.
- Bei einer Verwirklichung der anderen Varianten müssen sich die Projektverantwortlichen vorgängig vergewissern, dass alle angebundenen Netzwerke (auch das LEUnet) die Sicherheitsanforderungen gemäss der ISV Stufe 3 erfüllen. Dafür muss die externe Firma ihrerseits die restliche Wegstrecke zwischen den VPN Gateways und den Applikationsservern verschlüsseln.

Gemäss der Informatiksicherheitsverordnung müssen Verschlüsselungstechnologien eingesetzt werden, wenn bearbeitete Informationen der Schutzstufe 3 zugeordnet sind. Der Einsatz kryptographischer Verfahren wird von einer grossen Zahl von Einflussfaktoren bestimmt, zum Beispiel von den Informatiksystemen, den Datenvolumen, den angestrebten Sicherheitsniveaus und den Verfügbarkeitsanforderungen. Daher ist zunächst die Entwicklung eines Konzepts angesagt, in dem alle Einflussgrössen und Entscheidungskriterien für die Wahl eines konkreten kryptographischen Verfahrens und der entsprechenden Produkte berücksichtigt werden und das trotzdem wirtschaftlich vertretbar ist.

Sicherheitsüberprüfung in Kliniken

Die Beratungsstelle für Informatiksicherheit hatte den Auftrag, die implementierten Sicherheitsvorkehrungen von drei Kliniken zu verifizieren. Für die Überprüfung bewertete sie die übergeordneten Komponenten (Konzepte, Weisungen und Stellenbeschreibungen) sowie die Betriebshandbücher der jeweiligen Systeme. In einer technischen Detailanalyse testete sie die Sicherheit aller Systeme innerhalb des Netzwerkes der Kliniken und erprobte Schwachstellen beim Zugriff auf die Systeme der Kliniken mit denselben Werkzeugen und Techniken, die ein Hacker verwenden würde.

Es wurden einige teils kritische Schwachstellen gefunden, die rasch abgedeckt werden müssen. Sie lassen sich allerdings mit der konsequenten Anwendung der in einzelnen Produkten bereits verfügbaren Sicherheitsfunktionen sowie der Aktualisierung spezifischer Sicherheitskonfigurationen weitgehend eliminieren.

Die Prüfungen zeigten, dass ein eigentliches Sicherheitsmanagement bei allen untersuchten Kliniken fehlt. Dieser Umstand stellt ein enormes Risiko bezüglich Kontinuität und Sicherheit dar. So war es möglich, innert kürzester Zeit vollumfänglich auf alle (Patienten-)Daten und Geschäftsapplikationen der Kliniken zuzugreifen. Eine unberechtigte Person wäre somit in der Lage, als schwerwiegendste Tat beispielsweise sämtliche Daten der Kliniken zu bearbeiten oder zu löschen.

Aufgrund der zur Verfügung stehenden Informationen beurteilte die Beratungsstelle zusammenfassend die Informationssicherheit der geprüften Kliniken nur in wenigen Bereichen als gut, in den meisten jedoch als mangelhaft.

Die technische Sicherheit der Informatikinfrastrukturen der Kliniken könnte mit einem geringen Aufwand erhöht und dann mit einem vertretbaren Restrisiko betrieben werden.

Eine Sicherheitsüberprüfung ist ein bekanntes Instrument, um die Sicherheit der bereitgestellten Informationsdienste zu verifizieren. Die Durchführung von regelmässigen Tests durch qualifizierte Spezialisten wird ausdrücklich empfohlen, um die laufenden Anpassungen der Infrastrukturen zu kontrollieren. Allerdings gibt sie nur Aufschluss über den aktuellen Stand der bestehenden Konfiguration. Genauso wichtig ist ein sorgfältiger Umgang auch im laufenden Betrieb. Für eine ganzheitliche Sicherheit ist es deshalb besonders beim Umgang mit besonders schützenswerten Personendaten notwendig, die Sicherheits- und Prozessrisiken in einem Informationssicherheitsmanagement (ISM) nachhaltig zu erfassen und zu bewirtschaften.

Regelmässige Kontrollen sind notwendig

Die Datenschutzreview als Kontrollinstrument des Datenschutzbeauftragten weist immer wieder auf Lücken bei der Umsetzung der Massnahmen für Sicherheit im rechtlichen, organisatorischen und technischen Bereich hin.

Im Jahr 2005 wurde das Schwergewicht bei der Auswahl der zu prüfenden Stellen in der Datenschutzreview auf Gemeinden und Kliniken gelegt.

Das Vorgehen blieb gleich wie im Vorjahr. Grundlage bildeten die von der Verwaltungsstelle eingesandten Unterlagen, die Antworten aus dem Review Tool (www.review.datenschutz.ch), Interviews und eine kurze technische Überprüfung vor Ort sowie die Diskussion des Berichtentwurfs bei der Schlussbesprechung mit den zuständigen Vertretern der Gemeinde respektive Klinik. Nach Ablauf der Frist für Ergänzungen oder Berichtigungen wird der Bericht versandt.

Die Zielsetzungen der Prüfung wurden an die veränderte Gefahrenlage angepasst. Die bisherigen Erfahrungen in den als mittel klassifizierten Gemeinden (4500 bis knapp 10 000 Einwohner) flossen mit ein. Genauer oder neu untersucht wurden Zugriffskonzept (mit der Netzwerkanbindung und Anwendung von drahtlosen Netzwerken), mobile Arbeitsplätze (zusammen mit mobilen Datenträgern) und der Internet-Auftritt (Serverbetrieb und Dienstleistungen). Die permanente Ausrichtung auf aktuell hinzukommende Gefahren hat sich bewährt. Statistik 2 zeigt für das Jahr 2005 auch die neu aufgenommenen Empfehlungen aufgrund dieser Anpassungen.

Besonders folgende drei Bereiche entwickeln sich positiv:

a) Netzwerk

Die Zusammenarbeit mit der IG-EDV spart Kosten und Supportaufwand, wenn es um die Anbindung der Gemeindenetzwerke (Sicherheitsgateway; Firewall) in Form einer Zusammenfassung verschiedener Gemeinden in eine vertragliche Lösung geht (nicht zuletzt auch bei den Gemeindestellen, die im Bereich Sicherheit vom Kenntnisstand her einen grossen Nachholbedarf haben). Zurzeit ergibt sich in vielen Gemeinden ein Problem aus dem Zugriff von Dienstleistenden mit Support-Funktion. Eine Lösung ist hier in Arbeit (siehe auch die Empfehlung «Netzwerk» in der Statistik 2).

b) Mobile Arbeitsplätze und mobile Geräte

Der Einsatz an Arbeitsplätzen ausserhalb von Amtsräumen ist im Moment noch beschränkt; entsprechende Weisungen fehlen weitgehend. Der Zeitpunkt, um eine Kultur für Sicherheit zu fördern und zu erhalten, ist optimal. Technische Mittel werden in nächster Zeit «gemeindetauglich» verfügbar sein, so kryptographische Massnahmen zur Vertraulichkeit und Integrität der mobilen Daten sowie zur Authentizität und Nichtabstreitbarkeit bei Zugriffen auf das Gemeindenetzwerk. Grosser Handlungsbedarf besteht bei mobilen Geräten (PDA, Handy, alle USB-Geräte). Mit dem Erlass von Weisungen kann die Tragfähigkeit der Kultur für Sicherheit verbessert werden.

c) Einsatz WLAN

Die Zurückhaltung der Gemeinden beim Einsatz von WLAN (drahtlose lokale Netzwerke) ist gerechtfertigt. Gemäss neuer Network Security Policy NSP des Kantons Zürich und der Subdomäne Gelb-Gemeinden ist WLAN zurzeit nicht erlaubt. Eine richtige und angemessene Anwendung kann jetzt noch bestimmt werden, indem man die Randbedingungen in den Gemeinden und in Zusammenarbeit mit dem Kanton Zürich durch die IG-EDV in den entsprechenden Gremien diskutiert und festlegt.

Empfehlungen

Die häufigsten Empfehlungen betreffen den Aufbau und die Pflege einer internen Kultur für Sicherheit (Konzept, Verantwortlichkeiten, Weisungen, Sensibilisierung). Die Umsetzung des Konzepts mit Hilfe von Massnahmenplänen wird mit Vorarbeiten der Datenschutzreview unterstützt: Die wichtigsten Schritte sind die obligatorischen Eingaben im Review Tool in der Systemanalyse, die Beschäftigung

Statistik 1

Vergleich der Empfehlungen des Jahres 2005 für Gemeinden und Kliniken mit dem Niveau der Resultate der Gruppe aus Ämtern, Kliniken und Spitälern sowie Gemeinden (als repräsentativer Querschnitt durch die kantonalen Stellen und Gemeinden) gemäss Tätigkeitsbericht Nr. 9 [2003]

Vergleich zum Querschnitt[1]	Niveau deutlich tiefer 30–50%	Niveau tiefer 10–29%	gleich 0–9%
Bewertung durch den Datenschutzbeauftragten		X	
Umsetzung Informatiksicherheitsverordnung ISV		X	
Nachholbedarf Vertragswesen		X	
Verantwortung, Sensibilisierung der Mitarbeitenden			X
Verantwortung, ITC-Sicherheit – Umsetzung ISV		X	
Verantwortung, Revision und Kontrolle	X		
Verantwortung, Umsetzung Datenschutz	X		
Passwörter, Anforderungen durch Weisung festgelegt		X	
Passwörter, Anforderungen technisch umgesetzt		X	
Zugriffe, Einzelmassnahmen in Konzept überführen	X		
Zugriffe, Ersatz von nicht sicheren Verbindungen			X
Zusammenfassung	**3**	**6**	**2**

[1] Da die Prüfungsschwergewichte angepasst oder erweitert wurden (auch im Sinne der Anpassung an die Gefahrenlage), sind nicht alle Punkte aus der Auswertung des Tätigkeitsberichts Nr. 9 [2003] vergleichbar.

Statistik 2

Wichtigste Empfehlungen an die geprüften Stellen im Jahr 2005

		in Prozent
ICT-Konzept	Erstellen und Massnahmepläne umsetzen	100
Passwörter	Anforderungen in (PC-)Weisung festlegen	100
Verantwortung	ICT-Sicherheit zuweisen	100
Verantwortung	Kontrolle zuweisen	100
Verantwortung	Sensibilisierung zuweisen	100
Weisungen	Für Benützende (PC-)Weisung gesamthaft (Internet, E-Mail, mobile Geräte etc.) festlegen	100
Vertragswesen	AGB Sicherheit einfügen	92
Zugriffe	Einzelmassnahmen in Konzept überführen	92
Passwörter	Anforderungen technisch umsetzen	75
Weisungen	Betriebskonzept und -handbücher erstellen	67
Aufbewahrungsfristen	Festlegen und kommunizieren	58
Mobile Geräte	Anforderungen in (PC-)Weisung festlegen	50
Netzwerk	Nicht sichere Verbindungen ersetzen	50
Verantwortung	Datenschutz zuweisen	50
Mobile Geräte	Anforderungen technisch umsetzen	42

mit den zentralen Massnahmen aufgrund der Fragenkataloge und die gemeinsam mit den Gemeinden oder Kliniken erstellte Risikoanalyse bei der Prüfung vor Ort. Eine detaillierte Hilfestellung für ein Zugriffskonzept unterstützt die Stellen bei konzeptionellen Arbeiten. Die Liste der wesentlichsten Empfehlungen ist aus Statistik 2 ersichtlich.

Die geprüften Stellen bewerten Vorgehen und Umfang der Datenschutzreview positiv. Der Einsatz des Review Tools sowie die Abgabe detaillierter Checklisten und Hilfestellungen geben ihnen die Möglichkeit, einerseits schnell und einfach zu Resultaten zu kommen sowie andererseits ihren Dienstleistenden entsprechend fundierte Vorgaben zu machen. Mehrfach wurde die externe Kontrolle als gute Standortbestimmung, zum Beispiel gegenüber dem Gemeinderat, begrüsst.

Die Datenschutzreview ist ein sinnvolles Instrument zum Aufbau einer Sicherheitskultur innerhalb der Gemeinden (Sicherheitskonzept, Weisungen, Sensibilisierung). Zusätzliche Ressourcen beim Datenschutzbeauftragten könnten auch mehr Stellen positiv beeinflussen und zum Um- und Weiterdenken im Bereich Sicherheit animieren.

Vergleich der Empfehlungen

Die Empfehlungen des Jahres 2005 für Gemeinden und Kliniken wurden mit dem Niveau der Resultate der Gruppe aus Ämtern, Kliniken und Spitälern sowie Gemeinden (als repräsentativer Querschnitt durch die kantonalen Stellen und Gemeinden) gemäss Tätigkeitsbericht Nr. 9 [2003], S.31, verglichen. Die Statistik 1 zeigt, dass das Massnahmenniveau der geprüften Gemeinden und Kliniken deutlich tiefer ist als der Querschnitt. Besonders der Nachholbedarf bei grundlegenden Themen – nicht zugewiesene Verantwortlichkeiten, Einzelmassnahmen ohne übergreifendes Zugriffskonzept – bestätigt ein mangelndes Verständnis

des Auftrags für Sicherheit und entsprechend die fehlende Bereitschaft, die notwendigen Ressourcen zuzuordnen. Die knappen Ressourcen der Gemeinden in finanzieller und zeitlicher Hinsicht dürfen nicht dazu führen, dass die notwendigen Aufgaben vernachlässigt oder von Jahr zu Jahr übertragen werden. Der Datenschutzbeauftragte gab genügend Hilfestellungen zu den meist organisatorischen Verbesserungen ab und diskutierte die Möglichkeiten während der Vor-Ort-Prüfung, was die prüfenden Stellen auch sehr begrüssten.

Die Statistik 2 zeigt den Nachholbedarf bei den geprüften Stellen im Detail auf. Das Fehlen des Konzepts, des genauen Auftrags und der Massnahmen zur Sensibilisierung und Schulung zeigt auf, dass eine meist vorhandene, gewachsene Struktur in eine umfassende Kultur für Sicherheit in den Gemeinden und Kliniken überführt werden muss. Diese Arbeiten dürfen nicht im so genannten Tagesgeschäft untergehen, sie sind zu planen, die entsprechende Zeit ist bereitzustellen und die Massnahmen sind adressatengerecht durchzuführen.

Der Vergleich der Resultate mit den Messungen aus den Vorjahren ergibt bei den geprüften Gemeinden einen erheblichen Nachholbedarf. Besonders die Bereiche Konzept, Weisungen an die Benützenden und Massnahmen zur Sensibilisierung sind zu priorisieren, da sie einerseits die knappen Ressourcen der Gemeinden wenig belasten, andererseits jedoch die Realisierung der gemeindeweiten Sicherheitskultur optimal unterstützen.

Wichtige Informationstätigkeit

Die kontinuierliche Information über die Anliegen des Datenschutzes und die Aus- und Weiterbildung bleiben zentrale Punkte bei den Aufgaben des Datenschutzbeauftragten.

Wichtige Themen werden in die vierteljährlich erscheinende Zeitschrift digma (www.digma.info) aufgenommen. Aufgrund einer engen Zusammenarbeit sind die Themen abgestimmt auf aktuelle Fragestellungen und Diskussionen im Bereich des Datenschutzes und der Informationssicherheit. So wurden unter anderen ausführliche Beiträge zu Fragen der Einführung des Öffentlichkeitsprinzips und dessen Verhältnis zum Datenschutz publiziert (digma 2005.1). Eine weitere Schwerpunktnummer befasste sich mit der Problemstellung rund um die Verwendung biometrischer Systeme zur Identifikation von Personen (digma 2005.2).

Aus- und Weiterbildung

Neben spezifischen Ausbildungsveranstaltungen haben wir auch das 10-jährige Bestehen des Datenschutzgesetzes zum Anlass genommen, in einer Veranstaltung auf Entwicklungen im Datenschutz in den letzten zehn Jahren zurückzuschauen, um auch wichtige Themen für die Zukunft diskutieren zu können. Die Referate sind in einem Tagungsband publiziert worden (Datenschutzbeauftragter des Kantons Zürich [Hrsg.] «Herausforderung Datenschutz», Verlag Schulthess, Zürich 2005).

Im vergangen Jahr konnte auch das Symposium for Privacy and Security zum zehnten Mal durchgeführt werden. Dieses Symposium ist ein fester Bestandteil im Aus- und Weiterbildungsangebot des Datenschutzbeauftragten.

Medienberichterstattung

Häufig wurde der Datenschutzbeauftragte auch von Medien angefragt. Einerseits ging es hier um konkrete Fragestellungen oder Stellungnahmen zu Einzelfällen, andererseits um generellere Einschätzungen zu aktuellen Entwicklungen im Bereich des Datenschutzes und der Informationssicherheit. Die Berichterstattung in den Medien ist ein wichtiges Element bei der Sensibilisierung der Bürgerinnen und Bürger, aber auch der verantwortlichen Datenbearbeiter in Bezug auf die Herausforderungen im Bereich des Datenschutzes. Es lässt sich feststellen, dass sich in immer mehr Bereichen Fragen des Datenschutzes stellen – beispielsweise im Gesundheitswesen –, wobei diese häufig nicht mit der notwendigen Konsequenz einer Lösung zugeführt werden. Damit stellen sich im Einzelfall zahlreiche Fragen, die wiederum die Aufmerksamkeit der Öffentlichkeit auf sich ziehen. Nicht zuletzt deshalb sollte die Berichterstattung in den Medien auch zu einer besseren Sensibilisierung der Entscheidungsträger und des Gesetzgebers für die Anliegen des Datenschutzes führen.

Sensibilisierung im Internet

Für alle Angestellten der kantonalen Verwaltung wurde in Zusammenarbeit mit einer externen Firma ein Lernprogramm Sicherheit entwickelt, das zuerst im Intranet und später auch im Internet zur Verfügung gestellt wurde.

Die Benutzenden werden mit den wichtigsten Fragen in punkto Sicherheit vertraut gemacht, auf ihre Verantwortung im Bereich der Informatiksicherheit hingewiesen und zu einem sicherheitsbewussten Verhalten angeleitet. Themen sind unter anderem der Umgang mit sensiblen Daten und die sichere Benutzung von Internet und E-Mail. Besonderes Gewicht wurde auf die Verwendung von starken Passwörtern und die richtige Reaktion bei einem Virenbefall gelegt.

Vereinigung der Datenschutzbeauftragten

Seit fünf Jahren besteht die Vereinigung der schweizerischen Datenschutzbeauftragten (DSB+CPD.CH), in der alle kantonalen Datenschutzbeauftragte sowie einige kommunale Datenschutzbeauftragte vertreten sind. Diese Vereinigung erfüllt eine wichtige Funktion beim gegenseitigen Informationsaustausch. Des Weiteren nimmt sie sich schwerpunktmässig gewisser Themen an – zurzeit sind dies das Gesundheitswesen, das Öffentlichkeitsprinzip sowie die europarechtlichen Fragen. Die Ergebnisse fliessen dabei als Arbeitspapiere oder im Rahmen von Veranstaltungen wieder zurück zu den Mitgliedern. Die Vereinigung hat sich auch zum Ziel gesetzt, die aktuellen Fragen des Datenschutzes proaktiv zu bearbeiten, um möglichst frühzeitig den betroffenen Stellen datenschutzkonforme Lösungen zu präsentieren. Sie spielt dabei eine wichtige Rolle in der Datenschutzdiskussion in der Schweiz. Der Datenschutzbeauftragte ist in den verschiedenen Arbeitsgruppen vertreten und nimmt zurzeit das Präsidium der Vereinigung war.

Verordnungen im Polizeibereich

Die revidierte Verordnung über die erkennungsdienstliche Behandlung von Personen sowie die POLIS-Verordnung – das Polizei-Informationssystem betreffend – sind in Kraft.

Im Tätigkeitsbericht Nr. 2 [1996], S. 11, hat der Datenschutzbeauftragte auf den Handlungsbedarf in Bezug auf die Verordnung über die erkennungsdienstliche Behandlung von Personen vom 22. Dezember 1960 aufmerksam gemacht.

Die knapp zehn Jahre später in Kraft getretene revidierte Verordnung über die erkennungsdienstliche Behandlung von Personen (ED-VO) trägt den datenschutzrechtlichen Anforderungen in weiten Teilen Rechnung. Im Besonderen sind die erkennungsdienstlichen Massnahmen, der erfasste Personenkreis, die Aufbewahrung sowie die Vernichtungsgründe detailliert geregelt. Zudem ist in § 12 ED-VO die Pflicht der Strafverfolgungs- und Strafvollzugsbehörden festgelegt, der Kantonspolizei die für die Vernichtung bedeutsamen Vorgänge von Amtes wegen mitzuteilen.

Zwei Punkte sind aus datenschutzrechtlicher Sicht nicht befriedigend umgesetzt:

Erkennungsdienstliches Material wird nach Erlass einer definitiven und rechtskräftigen Einstellung einer Strafuntersuchung gemäss § 10 Abs. 2 lit. b ED-VO nach einer Frist von fünf Jahren vernichtet. Im Gegensatz dazu ist ein gerichtlicher Freispruch mit einer sofortigen Vernichtung des Materials verbunden (§ 10 Abs. 2 lit. a ED-VO).

Bei einer Verurteilung wegen eines Verbrechens oder Vergehens ist in § 10 Abs. 2 lit. c ED-VO eine generelle Aufbewahrungsfrist von 20 Jahren festgelegt. Diese beginnt nach dem Vollzug einer unbedingten Strafe, bei einer bedingten Strafe nach dem Ablauf der Probezeit oder nach der einstweiligen Einstellung eines Strafverfahrens. Eine Abstufung nach Straftat und/oder Strafmass wäre jedoch angezeigt.

Die Verordnung über die erkennungsdienstliche Behandlung von Personen ist, soweit sie datenschutzrechtliche Regelungen enthält, als lex specialis zum Datenschutzgesetz (DSG) anzusehen. Die Rechte der betroffenen Personen lassen sich deshalb wie folgt umschreiben:

Die Erhebung von erkennungsdienstlichem Material ist in der Verordnung über die erkennungsdienstliche Behandlung von Personen geregelt. Das Recht auf Auskunft richtet sich nach § 17 Datenschutzgesetz und § 1 Abs. 1 ED-VO: Jede Person kann Auskunft darüber verlangen, welche erkennungsdienstlichen Daten dort über sie bearbeitet werden.

Die Aufbewahrungsdauer von erkennungsdienstlichem Material sowie dessen Vernichtung sind in der Verordnung geregelt; wie erwähnt ist in § 12 ED-VO die Pflicht der Strafverfolgungs- und Strafvollzugsbehörden statuiert, der Kantonspolizei die für die Vernichtung bedeutsamen Vorgänge von Amtes wegen mitzuteilen.

Liegt ein Vernichtungsgrund vor, ohne dass eine Mitteilung von Amtes wegen erfolgt wäre, beispielsweise, weil es sich um einen ausserkantonalen Entscheid handelt, steht der betroffenen Person das Recht zu, die Vernichtung gestützt auf § 19 Abs. 2 lit. a DSG zu verlangen.

Polizei-Informationssystem POLIS

Im Tätigkeitsbericht Nr. 8 [2002], S. 15, machte der Datenschutzbeauftragte auf den gesetzgeberischen Handlungsbedarf in Bezug auf das Informationssystem POLIS der Kantonspolizei aufmerksam. Anstoss gaben zahlreiche Beschwerden von Bürgerinnen und Bürgern betreffend ihre Registrierung, insbesondere in Bezug auf die Löschung oder Berichtigung von Daten.

Per 1. Januar 2006 trat die Verordnung über das Polizei-Informationssystem POLIS (POLIS-VO) in Kraft. Die neue Verordnung nimmt die offenen datenschutzrechtlichen Fragen im Wesentlichen auf: Wenn auch nur auf Verordnungs- und nicht auf Gesetzesstufe werden Ziel und Zweck der Datenbank, die Datenkategorien, die -bekanntgabemöglichkeiten, der -zugriff, die -sicherheit sowie auch die Aufbewahrungsdauer der Daten geregelt.

Soweit sie datenschutzrechtliche Regelungen enthält, ist auch die POLIS-Verordnung als lex specialis zum Datenschutzgesetz (DSG) anzusehen. Akteneinsichts- und Auskunftsrecht sind darin festgelegt. Bei einem Freispruch, der Einstellung eines Verfahrens, der Sistierung oder der Nichtanhandnahme eines Strafverfahrens können betroffene Personen unter Vorlage eines rechtskräftigen Entscheides eine ergänzende Eintragung erwirken. Diese Regelung widerspricht jedoch dem Datenschutzgesetz, welches festlegt, dass die entsprechenden Personendaten zu löschen oder mindestens die Zugriffsrechte einzuschränken sind. Zudem müsste eine Berichtigung von Amtes wegen erfolgen.

Patientinnen- und Patientengesetz

Das Patientinnen- und Patientengesetz ersetzt die Patientenrechtsverordnung. Neben diversen Bestimmungen, welche vor allem das Behandlungsverhältnis betreffen, enthält das Gesetz auch datenschutzrechtliche Regelungen.

Der Patient hat das Recht auf Aufklärung (§13). Diese kann nur unterbleiben, wenn der Patient schriftlich bestätigt, dass er darauf verzichtet. Schadet die Aufklärung mehr, als sie nützt, kann darauf verzichtet werden, es sei denn, der Patient wünsche sie ausdrücklich.

Der Patient hat weiter das Recht, seine Dokumentation einzusehen (§ 19). Für die Abgabe von Kopien soll eine kostendeckende Gebühr verlangt werden können. Damit wird das Recht des Patienten auf Einsicht in seine eigenen Daten jedoch geschwächt. Die Eidgenössische Datenschutzkommission befasste sich 1998 und 1999 mit dieser Frage und legte Kriterien für die Kostenbeteiligung beim Auskunftsrecht fest. Der Datenschutzbeauftragte empfiehlt den Spitälern, nur bei besonders hohem Arbeitsaufwand Gebühren zu verlangen, jedoch nicht, wenn zum Beispiel nur ein Dossier oder einzelne Unterlagen kopiert werden müssen.

Im Spital stellen sich häufig Fragen zur Rechtmässigkeit von Datenbekanntgaben. Um dem Spitalalltag gerecht zu werden, stellt § 15 Abs. 2 eine Vermutung auf: Sofern sich Patienten nicht dagegen aussprechen, wird vermutet, sie seien damit einverstanden, dass gegenüber der gesetzlichen Vertretung, ihren Bezugspersonen, vor- und nachbehandelnden Ärztinnen und Ärzten sowie anderen weiterbehandelnden Personen Informationen über den Gesundheitszustand weitergegeben werden. Diese Bestimmung versucht dem Berufsalltag entgegenzukommen, was besonders wichtig ist, wo Patientinnen und Patienten nicht in der Lage sind, die Einwilligung für solche Datenbekanntgaben zu geben. Ein Problem besteht allerdings darin, dass nicht genau definiert ist, was unter den Begriff «Informationen über den Gesundheitszustand» fällt.

§ 18 bestimmt, dass die Patientendokumentation Eigentum der Institution bleibt und nach Abschluss der letzten Behandlung zehn Jahre lang aufbewahrt werden muss. Nach Ablauf dieser Frist können Patientinnen und Patienten die Vernichtung oder die Herausgabe der Dokumentation verlangen, sofern für eine weitere Aufbewahrung kein öffentliches Interesse mehr besteht. Im privatrechtlichen Verhältnis zwischen Patient und Arzt besteht gemäss Bundesgericht ein Herausgabeanspruch aufgrund des Auftragsrechts (BGE 119 II 222). Warum für das öffentlich-rechtliche Verhältnis ein Unterschied gemacht werden soll, ist nicht nachvollziehbar. Um Forderungen, die sich aus dem Behandlungsverhältnis ergeben, geltend zu machen, reicht das Aufbewahren von Kopien aus. Verzichtet der Patient auf Geltendmachung sämtlicher Ansprüche, erübrigt sich sogar die Aufbewahrung von Kopien.

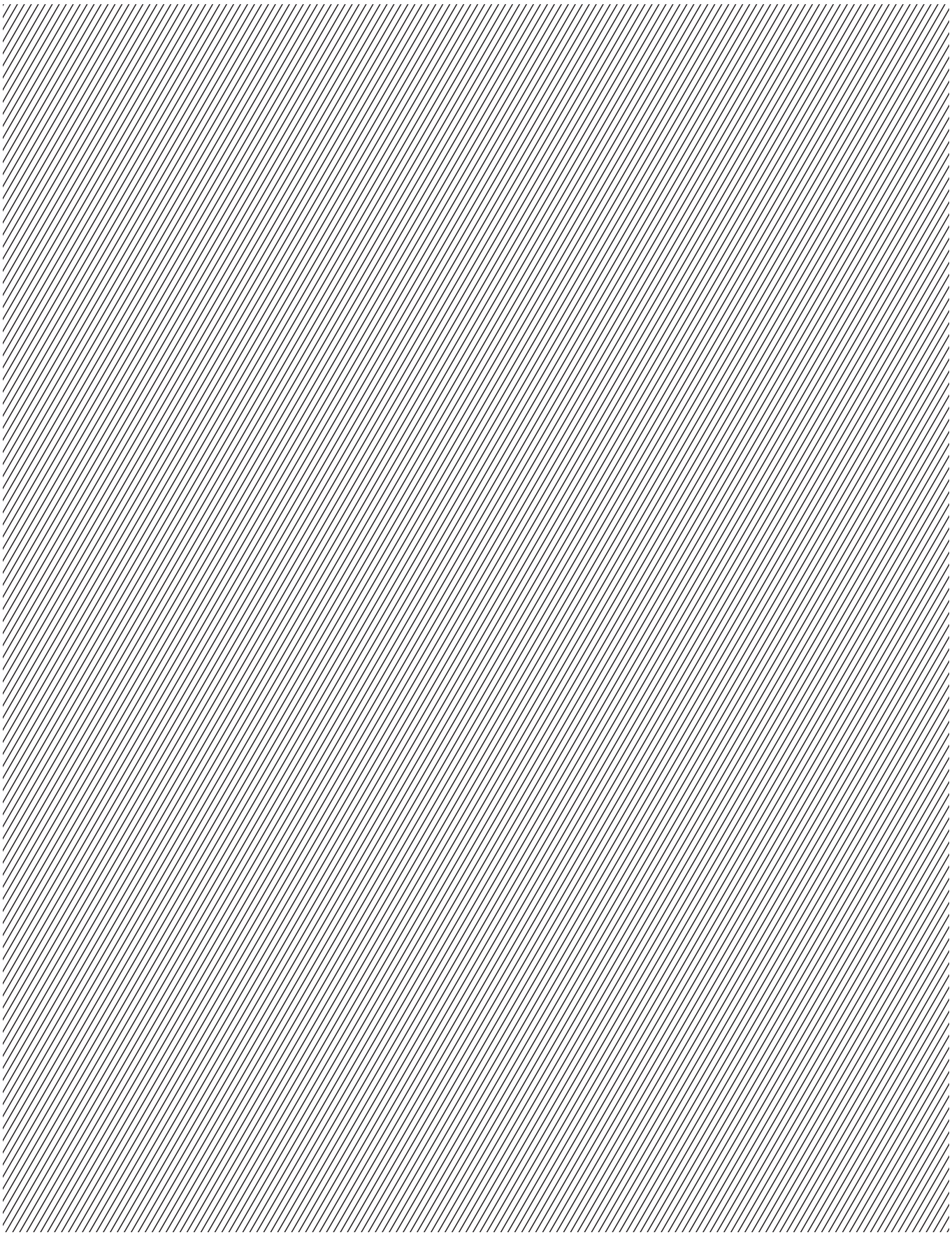
E-Voting-Projekt abgeschlossen

Das Projekt E-Voting im Kanton Zürich wurde Ende 2005 abgeschlossen und die Projektorganisation hat sich aufgelöst. Der Datenschutzbeauftragte war im Projektausschuss vertreten und hat die datenschutzrechtlichen und sicherheitstechnischen Aspekte dieses Projektes beurteilt.

Das E-Voting-Projekt im Kanton Zürich war Teil eines vom Bund mit den Kantonen zusammen durchgeführten Pilotprojektes. Die Schwerpunkte im Kanton Zürich lagen einerseits bei der elektronischen Führung eines zentralen Wahlregisters und andererseits auf der Nutzung von Mobiltelefonie (SMS) zur Abstimmung neben der Internet-Plattform.

Die Versuche, die im Kanton Zürich zuerst mit den Studentenratswahlen an der Universität und anschliessend mit ausgewählten Gemeinden durchgeführt worden waren, verliefen grundsätzlich erfolgreich. Die datenschutzrechtlichen Aspekte wie auch die sicherheitstechnischen Anforderungen wurden so weit wie möglich in diesem Pilotprojekt berücksichtigt.

Die generellen Vorbehalte, die sich aus Sicht des Wahl- und Abstimmungsgeheimnisses und der Sicherheit der Technologie ergeben, waren nicht Teil dieses Pilotprojektes. Vielmehr liegt es hier am Bund zu entscheiden, wie weit die eingesetzte Technologie diesen Anforderungen zu genügen vermag. Die Zürcher Projektleitung hat ihren Schlussbericht zuhanden der Bundeskanzlei verabschiedet.



Fälle aus der Beratungstätigkeit
Anhang

Titel: Telefonaufzeichnungen
URL: http://www.datenschutz.ch/themen/1252.php
Datum: 17.07.2006

01.

Telefonaufzeichnungen

Es ist nicht zulässig, dass eine Amtsstelle vor der Entgegennahme sämtlicher Telefonanrufe ein Tonband mit einem Hinweis auf eine Aufnahmemöglichkeit zu Schulungszwecken vorspielt, mit dem Zweck, Anrufende von verbalen Entgleisungen abzuhalten.

Während den Auskunftszeiten werden seit Februar 2005 alle Anrufe auf die zentrale Telefonnummer des Migrationsamtes nicht direkt durch eine Mitarbeiterin oder einen Mitarbeiter angenommen, sondern es wird zuerst ein Tonband abgespielt. Dasselbe gilt für direkte Anrufe ohne Vorwahl innerhalb der Verwaltung.

Der im April 2005 verwendete Text lautete wie folgt: «Migrationsamt des Kantons Zürich. Grüezi. Haben Sie Verständnis, dass das Gespräch aus Gründen der internen Weiterbildung und Qualitätskontrolle aufgezeichnet werden kann. Der Hinweis erfolgt ausschliesslich auf Deutsch. Sind Sie damit nicht einverstanden, richten Sie Ihre Anfrage schriftlich an das Migrationsamt des Kantons Zürich. Vielen Dank.»

Die Möglichkeit der Telefonaufzeichnung ist gemäss Ausführungen des Migrationsamtes auf die Auskunftsstelle beschränkt; von dieser intern weitergeleitete Anrufe oder Anrufe von oder zu anderen Nummern des Migrationsamtes können nicht aufgezeichnet werden. Die Mitarbeitenden der Auskunftsstelle haben ihr Einverständnis zur Gesprächsaufzeichnung schriftlich erteilt; konkrete Aufzeichnungen erfolgen nach schriftlicher Ankündigung der Teamleitung durch diese. Andere Mitarbeitende des Migrationsamtes sind von allfälligen Aufzeichnungen nicht betroffen.

Im Zeitraum zwischen 1. April 2005 und 31. März 2006 sind auf der zentralen Telefonnummer des Migrationsamtes rund 165 000 Anrufe eingegangen. Davon wurden im Juli/August 2005 rund fünfzig Gespräche aufgezeichnet, für jede-/n der fünf Mitarbeitenden der Auskunftsstelle durchschnittlich zehn Gespräche. Die maximale Gesamtaufzeichnungsdauer lag bei einer Stunde pro Person. Die aufgezeichneten Gespräche wurden unmittelbar nach der anschliessenden Schulung wieder gelöscht.

Einer anrufenden Person, welche mit der Aufzeichnung nicht einverstanden ist, wird zugesichert, dass das Gespräch nicht aufgezeichnet wird.

Der Hinweis auf die bestehende Aufzeichnungsmöglichkeit wird nicht nur bei einer geringen Zahl von Anrufen im Zeitraum der Schulungen abgespielt, sondern bei sämtlichen Gesprächen während des ganzen Jahres. Damit wird der Zweck verfolgt, die Anzahl der Gespräche, bei welchen sich Anrufende in Ton und/oder Wortwahl vergreifen, zu vermindern.

Strafrechtlicher Rahmen der Aufnahme von Telefongesprächen

Artikel 179ter StGB bedroht mit Strafe, wer als Gesprächsteilnehmer ein nichtöffentliches Gespräch, ohne die Einwilligung der andern daran Beteiligten, auf einen Tonträger aufnimmt. Davon ausgenommen sind Gespräche im Geschäftsverkehr, welche Bestellungen, Aufträge,

Reservationen und ähnliche Geschäftsvorfälle zum Inhalt haben (Art. 179quinquies Abs. 1 lit. b StGB).

Der Inhalt der Anrufe zum Migrationsamt kann nicht unter Art. 179quinquies Abs. 1 lit. b StGB subsumiert werden; die Einwilligung aller am Gespräch Beteiligten ist deshalb für eine straflose Aufzeichnung notwendig.

Es ist davon auszugehen, dass die Einwilligung der Mitarbeitenden zu einer Aufzeichnung vorliegt. Ob das Vorspielen des Tonbandes aus strafrechtlicher Sicht den Anforderungen einer Einwilligung zur Aufnahme im Sinne von Art. 179bis StGB auch bezüglich der die Auskunftsstelle Anrufenden genügt, muss durch die zuständigen Behörden im konkreten Einzelfall beurteilt werden.

Anwendbarkeit des Datenschutzgesetzes

Jede tatsächliche oder vorgetäuschte Überwachung stellt einen Eingriff in die Persönlichkeitsrechte der betroffenen Person dar. Das Datenschutzgesetz ist anwendbar für das Bearbeiten von Daten, jeden Umgang mit Daten, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben oder Vernichten von Daten, die sich auf eine bestimmte oder bestimmbare Person beziehen (§ 2 lit. a und f DSG).

Die Entgegennahme eines Gespräches durch die Auskunftsstelle stellt eine Datenbearbeitung dar. Diese beginnt mit der Wahrnehmung der Nummer der anrufenden Person, spätestens mit der Herstellung der Verbindung. Eine technische Aufzeichnung oder Aufzeichnungsmöglichkeit wird nicht vorausgesetzt. Das Datenschutzgesetz ist deshalb auf den gesamten Umgang des Migrationsamtes mit Anrufen zur Auskunftsstelle anwendbar.

Aufnahme des Gespräches zu Schulungszwecken

Gemäss § 4 Abs. 3 DSG dürfen personenbezogene Datenbearbeitungen vorgenommen werden, soweit sie für die Erfüllung der jeweiligen Aufgabe geeignet und erforderlich sind; sie dürfen den Umfang des Notwendigen nicht übersteigen. Telefonaufzeichnungen verbunden mit Auswertungen zum Zwecke der Schulung als Teil der Qualitätssicherung dürfen deshalb nur während eines dazu angemessenen Zeitraums erfolgen. Dieser dürfte sich pro Mitarbeitende/-n auf wenige Gespräche/Stunden pro Jahr beschränken.

Bei der Aufnahme eines Telefongespräches werden Daten aller teilnehmenden Personen bearbeitet. Eine Beschränkung der Aufzeichnung auf die zur Schulung überwachte Person ist aufwändig und würde dem angestrebten Zweck widersprechen. Es ist deshalb vertretbar, Gespräche in voller Länge aufzuzeichnen.

Die Mitarbeitenden sind über die Aufzeichnungsmöglichkeit orientiert und um ihre Einwilligung gebeten worden; eine konkrete Aufzeichnung wird vorher angekündigt. Die Aufzeichnungen erfolgen zu Schulungszwecken. Sie sind bei einer zentralen Telefonannahme- und -vermittlungsstelle ein dafür geeignetes Mittel. Der beschriebene Umfang der konkreten Aufzeichnung erscheint angemessen. Die aufgezeichneten Gespräche werden zum

angestrebten Zweck verwendet und anschliessend wieder gelöscht. Die datenschutzrechtlichen Anforderungen werden mit diesem Vorgehen gegenüber den Mitarbeitenden eingehalten.

Die Anrufenden können in eine Aufzeichnung zum Zweck der internen Schulung der Mitarbeitenden der Auskunftsstelle einwilligen. Offene Begriffe wie «Qualitätskontrolle» oder «Qualitätssicherung» sind deshalb zu vermeiden; es ist eine klare einfach verständliche Sprache zu wählen.

Soweit der Zweck der Aufzeichnung ausschliesslich die Überwachung von gewissen Mitarbeitenden und nicht des/der Anrufenden ist, erschient es im Rahmen des skizzierten Aufzeichnungsumfanges vertretbar, die Einwilligungserklärung nur in Deutscher Sprache einzuholen. Der Hinweis, dieser erfolge nur in Deutsch, kann weggelassen werden.

Grundsätzlich stehen allen Bürgern alle Kommunikationswege mit der Verwaltung gleichermassen offen; die Aufzeichnung von Telefongesprächen ist strafbar, mit Ausnahme bestimmter gesetzlich geregelter Fälle. Der Hinweis, sich bei Nicht-Einverständnis mit der Gesprächsaufnahme schriftlich an das Migrationsamt wenden zu müssen, ist unter diesen Umständen nicht statthaft. Anstelle desselben ist darauf hinzuweisen, dass auf Wunsch des/der Anrufenden keine Gesprächsaufzeichnung erfolge. Dieses Vorgehen entspricht auch Ihrer Praxis.

Zu Schulungszwecken ist die Aufnahme von rund fünfzig Gesprächen pro Jahr erforderlich. Es ist zu prüfen, ob die automatisierte Tonbanderklärung unter diesen Umständen durch eine persönliche Frage an die anrufenden Personen um eine Einwilligung zur Aufzeichnung ersetzt werden kann.

Datenbearbeitung zur Verminderung von verbalen Entgleisungen

Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist (§ 4 Abs. 4 des Datenschutzgesetzes, DSG).

Bei allen Anrufen verfolgt das Migrationsamt den Zweck der Verminderung von verbalen Entgleisungen. Ziel ist es, die Anrufenden einem Gefühl des Überwachtwerdens auszusetzen und diese so zu einem bestimmten Verhalten zu bewegen. Der angegebene Schulungszweck betrifft dagegen die Mitarbeitenden und greift nur bei jedem dreitausendsten Anruf. Entgegen § 4 Abs. 4 DSG wird somit nicht der tatsächliche Zweck der Aufzeichnungsmöglichkeit transparent gemacht. Dies ist nicht zulässig.

Erfolgt die Gesprächsaufzeichnung zur Überwachung der Anrufenden, genügt eine vorgeschaltete Tonbanderklärung in Deutsch den Anforderungen an eine Einwilligung keineswegs. Eine solche setzt voraus, dass die betroffene Person die vorgesehene Datenbearbeitung und deren Zweck kennt und dann frei entscheiden kann.

Eine Datenbearbeitung zur Verminderung von verbalen Entgleisungen ist unter diesen Umständen nicht zulässig. Die Aufzeichnungsinfrastruktur ist in jedem Fall nur zu Schulungszeiten betriebsbereit zu halten; durch organisatorische und technische Massnahmen ist eine zweckwidrige Verwendung derselben zu verhindern (§ 2 Datenschutzverordnung).

Empfehlung des Datenschutzbeauftragten

Zusammenfassend haben wir folgendes Vorgehen empfohlen

1. Die Aufzeichnung von Gesprächen hat ausschliesslich zu Schulungszwecken der Mitarbeitenden Auskunftsstelle unter Einhaltung der skizzierten Rahmenbedingungen (u.a. pro Mitarbeitende/-n wenige Gespräche pro Jahr; Orientierung/Einwilligung der Mitarbeitenden; konkrete Aufzeichnung angekündigt; Löschung) zu erfolgen.
2. Es ist zu pürfen, ob die automatisierte Tonbanderklärung durch eine persönliche Frage um eine Einwilligung zur Aufzeichnung ersetzt werden kann.
3. Wird auf eine Tonbanderklärung nicht verzichtet, hat diese nur zu erfolgen, wenn eine Aufzeichnung konkret geplant ist und (nur) noch von der Einwilligung der anrufenden Person abhängt. Die Erklärung hat den Hinweis auf eine Aufzeichnungsmöglichkeit zum Zweck der internen Schulung der Mitarbeitenden der Auskunftsstelle, sowie den Hinweis, dass auf Wunsch des/der Anrufenden keine Gesprächsaufzeichnung erfolgt, zu beinhalten.
4. Die Aufzeichnungsinfrastruktur ist nur zu Schulungszeiten betriebsbereit zu halten. Zur Verhinderung einer zweckwidrigen Verwendung sind geeignete organisatorische und technische Massnahmen zu treffen.

Das Migrationsamt teilte dem Datenschutzbeauftragten mit, dass es diese Empfehlungen umsetzen werde.

Titel: DNA-Analysen in Strafverfahren
URL: http://www.datenschutz.ch/themen/1253.php
Datum: 17.07.2006

02.

DNA-Analysen in Strafverfahren

In der kantonalen DNA-Verordnung sind nur noch Ausführungsbestimmungen zum neuen eidgenössischen DNA-Profil-Gesetz enthalten.

DNA-Analysen werden bei der Identifizierung von Personen immer wichtiger. Im Tätigkeitsbericht Nr. 4 [1998] S. 22 ff. befasste sich der Datenschutzbeauftragte ausführlich mit entsprechenden Fragestellungen. Mit Datum vom 18. April 2001 erliess der Regierungsrat die Verordnung über die Erhebung und Bearbeitung von DNA-Analysen im Strafverfahren. Der Datenschutzbeauftragte hatte in einer Arbeitsgruppe zur Erstellung eines Entwurfes mitgewirkt.

Mit der neuen Bundesverfassung wurde die Kompetenz zur Gesetzgebung im Bereich des Strafprozessrechtes dem Bund übertragen (Art. 123 Abs. 1 BV). In der Zwischenzeit sind verschiedene Teilbereiche des Strafprozessrechtes gesamtschweizerisch vereinheitlicht, so auch die Verwendung von DNA-Profilen in Strafverfahren und zur Identifizierung von unbekannten oder vermissten Personen. Die Bundesgesetzgebung regelt abschliessend, unter welchen Voraussetzungen DNA-Profile in Strafverfahren verwendet werden können (Art. 1 Abs. 1 lit. a DNA-Profil-Gesetz). Festgelegt sind auch die Anordnung und Vernichtung von DNA-Proben, der Vergleich von Profilen und die Löschung aus dem durch den Bund betriebenen DNA-Profilsystem. Die kantonale Verordnung vom 18. April 2001 wurde damit weit gehend obsolet.

Vor dem Inkrafttreten des entsprechenden Bundesgesetzes und der zugehörigen Verordnung per 1. Januar 2005 setzte die Direktion der Justiz und des Innern erneut eine Arbeitsgruppe ein, die die kantonalen Ausführungsbestimmungen erarbeitete. Eines der wesentlichen Probleme, die sich dabei zeigten, betraf die Vernichtung von DNA-Proben und die Löschung von DNA-Profilen, die sich in der Praxis vor allem bei komplexen Strafverfahren, bei welchen verschiedene Behörden und Kantone beteiligt sind, als schwierig erweisen dürfte.

Titel: Sockelbeiträge und Arztgeheimnis
URL: http://www.datenschutz.ch/themen/1254.php
Datum: 17.07.2006

03.

Sockelbeiträge und Arztgeheimnis

Neu haben die Wohngemeinden die Sockelbeiträge beim Spitalaufenthalt ihrer Einwohner in der privaten Abteilung zu übernehmen, so halten es die §§ 39 Abs. 3 und 40 Abs. 2 des Gesundheitsgesetzes fest. Dies ist jedoch keine genügende Rechtsgrundlage für die Spitäler, um das Berufsgeheimnis nach Art. 321 Strafgesetzbuch zu durchbrechen.

Per 1. Januar 2005 sind die neuen Bestimmungen der §§ 39 Abs. 3 und 40 Abs. 2 des Gesundheitsgesetzes des Kantons Zürich in Kraft getreten. Sie legen fest, dass nun die Wohngemeinden die Sockelbeiträge ihrer Einwohnerinnen und Einwohner übernehmen müssen und nicht mehr wie bis anhin die Gemeinden, in deren Region das Spital liegt.

Um diese Bestimmungen umzusetzen, verschickte die Gesundheitsdirektion ein Kreisschreiben an die Gemeinden sowie an die kantonalen und staatsbeitragsberechtigten Spitäler mit Angeboten für zusatzversicherte Patientinnen und Patienten. Darin wurden die Betriebe angewiesen, den Wohnsitzgemeinden zwei Dokumente zuzustellen; einerseits eine Sammelrechnung und andererseits eine Kontrollliste mit detaillierteren personenbezogenen Angaben, unter anderem mit den Personalien des Patienten sowie dem Ein- und Austrittsdatum. Da jeweils ersichtlich ist, von welcher Institution die Rechnung stammt, wies die Gesundheitsdirektion die psychiatrischen Kliniken an, diese Dokumente mit dem Vermerk *«persönlich-vertraulich»* an den Gemeindeschreiber zu senden.

Art. 321 des Strafgesetzbuches (StGB) bestraft Ärzte und ihre Hilfspersonen, die ein Geheimnis offenbaren, das ihnen infolge ihres Berufes anvertraut worden ist oder das sie in dessen Ausübung wahrgenommen haben, auf Antrag mit Gefängnis oder Busse. Ein Arztbesuch fällt unter den Geheimnisbegriff. Gemäss Art. 321 Ziff. 2 StGB ist die Offenbarung jedoch nicht strafbar, wenn die Bekanntgabe mit Einwilligung des Berechtigten oder aufgrund einer Entbindung der Aufsichtsbehörde geschieht. Dieser Fall liegt bei einer eidgenössischen oder kantonalen Bestimmung über die Zeugnis- oder Auskunftspflicht einer Behörde vor (Art. 321 Ziff. 3 StGB).

Die §§ 39 Abs. 3 und 40 Abs. 2 des Gesundheitsgesetzes sind nicht bestimmt genug, um als ausreichende gesetzliche Grundlage für eine Bekanntgabe von Patientendaten an die Gemeinde zu gelten. § 39 Abs. 3 Gesundheitsgesetz spricht lediglich davon, dass die Wohngemeinde den Sockelbeitrag übernehmen muss. Der Gesetztestext äussert sich nicht dahingehend, dass die Leistungserbringer dafür Patientendaten an die Wohngemeinde liefern sollen. Für die Patienten ist nicht transparent, dass das Spital aufgrund der neuen Bestimmungen im Gesundheitsgesetz Daten an ihre Wohngemeinde weiterleitet und damit das Patientengeheimnis aufgehoben wird. Daran ändert auch die Massnahme nichts, dass die psychiatrischen Kliniken ihre Rechnungen an den Gemeindeschreiber mit dem Vermerk «persönlich-vertraulich» schicken sollen. Hinzu kommt, dass die Mitarbeitenden einer Gemeinde zwar dem Amtsgeheimnis unterworfen sind, dies aber für die betroffene Person nicht gleichbedeutend mit Patientengeheimnis ist. Zudem sind Gemeindeangestellte in einem anderen Umfeld tätig als Medizinalpersonen, die täglich mit Gesundheitsdaten arbeiten und

sich der Konsequenzen einer Offenbarung stärker bewusst sind. Gerade in kleinen Gemeinden, wo teilweise verschiedene Verwaltungsfunktionen von derselben Person wahrgenommen werden, kann sich die Information, dass jemand beispielsweise in einer psychiatrischen Anstalt war, stigmatisierend auswirken.

Eine mögliche Lösung wäre die Zwischenschaltung einer Clearingstelle, welche die Rechnungen der Spitäler – ohne Angabe des Rechnungsstellers – an die Gemeinde weiterleiten und auch die Einzahlungen entgegennehmen könnte. Auf diese Weise würden Datenschutz-Aspekte ausreichend berücksichtigt.

Eine Clearingstelle könnte zusätzlich die Funktion eines «Trust Centers» übernehmen, wie sie der Eidgenössische Datenschutzbeauftragte in seinem Bericht aus dem Jahr 2004 «Tarmed und Datenschutz», S. 17, fordert (vgl. Tätigkeitsbericht Nr. 10 [2004], S. 32). Für die Ausgestaltung sind verschiedene Möglichkeiten denkbar: Das Trust Center kann von der Gesundheitsdirektion, einem einzelnen Spital oder einer externen Stelle übernommen werden.

Solange keine derartige Stelle eingerichtet ist, muss als Minimallösung die ausdrückliche Einwilligung der betroffenen Patientinnen und Patienten eingeholt werden.

Titel: Wochenaufenthalt: Nicht verhältnismässige Angaben
URL: http://www.datenschutz.ch/themen/1255.php
Datum: 17.07.2006

04.

Wochenaufenthalt: Nicht verhältnismässige Angaben

Die Angaben über Wochenaufenthalter bei der Einwohnerkontrolle dürfen den Umfang des Notwendigen nicht übersteigen. Nicht gefragt werden darf nach den Zahlen der letzten Steuerveranlagung, nach der Anzahl der Zimmer der Mietwohnung, nach Name, Vorname und Geburtsdatum des Konkubinatspartners, nach Name, Vorname, Adresse und Geburtsdatum der nächsten Familienangehörigen sowie nach Mitgliedschaften in Vereinen sowie nach deren Name und Ort des Vereins. Diese Angaben sind allesamt nicht erforderlich und daher unverhältnismässig.

Die Frage, welche Angaben über Wochenaufenthalter in einer Gemeinde erfasst werden dürfen, stellt sich in regelmässiger Weise. Bereits früher hat der Datenschutzbeauftragte ausführlich zu diesen Fragen Stellung bezogen und definiert, welche Daten über Wochenaufenthalter bearbeitet werden dürfen. Dabei wurde auch ein Musterfragebogen für den Wochenaufenthalt erstellt.

Titel: E-Learning-Plattform und Schweigepflicht
URL: http://www.datenschutz.ch/themen/1256.php
Datum: 17.07.2006

05.

E-Learning-Plattform und Schweigepflicht

Eine E-Learning-Plattform für Studierende, welche besonders schützenswerte Personendaten enthält, darf unter Einhaltung gewisser Bedingungen eingerichtet werden. Besonders zu beachten sind Sicherheitsvorschriften wie der Passwortschutz sowie Geheimhaltungsbestimmungen.

In ein E-Learning-Tool für Studierende der Psychopathologie sollen anonyme Videoaufnahmen von Patienten integriert werden. Für den Schulungszweck ist es unabdingbar, dass die Gesichter der Patienten und deren Mimik zu sehen sind. Da Videoaufnahmen, auf welchen bestimmte Personen und deren Krankheitszustand zu erkennen sind, besonders schützenswerte Personendaten darstellen, wirft die Entwicklung eines solchen Tools verschiedene datenschutzrechtliche Fragen auf.

Gemäss § 5 Datenschutzgesetz dürfen besonders schützenswerte Personendaten nur bearbeitet werden, wenn sich die Zulässigkeit aus einer gesetzlichen Grundlage klar ergibt, es zur Erfüllung einer in einem Gesetz klar umschriebenen Aufgabe unentbehrlich ist oder die betroffene Person im Einzelfall eingewilligt hat.

Da in Bezug auf das E-Learning-Tool weder eine gesetzliche Grundlage besteht noch von Amtshilfe auszugehen ist, muss bei der gefilmten Person oder ihrer gesetzlichen Vertreitung eine Einwilligung eingeholt werden. Zudem müssen die Patientinnen und Patienen in vollem Umfang über die Verwendung ihrer Daten informiert werden.

Weiter stellt sich die Frage, wie man die Studierenden, welche die Aufnahmen zu Gesicht bekommen, in die Pflicht nehmen kann und ob ihnen bei der Verletzung einer allfälligen Schweigepflicht juristische Folgen angedroht werden können.

In Bezug auf die Verletzung beruflicher Schweigepflichten finden sich Strafbestimmungen in Art. 321 des Strafgesetzbuch (StGB) und in Art. 35 des Bundesgesetzes über den Datenschutz. Art. 321 StGB (Verletzung des Berufsgeheimnisses) ist jedoch nur anwendbar, wenn Psychopathologen im Auftrag eines Arztes in dessen Räumen tätig sind. Studierende fallen von Gesetzes wegen in ihrer Funktion als Auszubildende unter die jeweilige Strafandrohung. Eine explizite Einwilligung in die Schweigepflicht oder der Hinweis darauf ist deshalb in beiden Fällen nicht notwendig.

Im vorliegenden Fall gelangt Art. 35 des Bundesgesetzes über den Datenschutz (Verletzung der beruflichen Schweigepflicht) zur Anwendung. Sein Geltungsbereich ist breiter als derjenige von Art. 321 StGB, welcher die einzelnen Berufsgattungen abschliessend aufzählt. Die strafrechtlichen Konsequenzen von Art. 35 (Haft oder Busse) können den Studierenden somit angedroht werden.

Zudem kann von den Studierenden verlangt werden, beweisbar zu bestätigen, dass sie ihre Schweigepflicht zur Kenntnis nehmen, sich daran halten und sich der Folgen einer Verletzung bewusst sind. Insofern ist eine Erklärung zur Schweigepflicht, ob schriftlich oder elektronisch erfasst, nur noch deklaratorischer Natur.

Die Strafbestimmung gilt jedoch nicht nur für die User, sondern auch für die Verantwortlichen der Lernplattform. Die technische Ausgestaltung der Lernplattform muss den Sicherheitsanforderungen entsprechen, welche an die Bearbeitung von besonders schützenswerten Personendaten gestellt werden. Es handelt sich gemäss Vorgaben der Informatiksicherheitsverordnung (ISV) um die höchste Sicherheitsstufe. Wir der erforderliche hohe Schutzstandard nicht eingehalten, können die Verantwortlichen zur Rechenschaft gezogen werden. Unter anderem ist sicherzustellen, dass der Zugriff von Seiten der Lernenden auf die Lernplattform passwortgeschützt ist.

Titel: Bekanntgabe der aus dem Lotteriefonds Begünstigten
URL: http://www.datenschutz.ch/themen/1257.php
Datum: 17.07.2006

06.

Bekanntgabe der aus dem Lotteriefonds Begünstigten

Eine interkantonale Vereinbarung sieht die Veröffentlichung sowohl der zugesprochenen Beiträge aus dem Lotteriefonds als auch der Begünstigten vor. Bis die Vereinbarung jedoch in Kraft gesetzt ist, kann der Regierungsrat selber entscheiden, ob er diese Beschlüsse veröffentlicht. Diejenigen des Kantonrates hingegen sind grundsätzlich öffentlich.

Um die Verwendung der Gelder aus dem Lotteriefonds transparenter zu machen, wollte die Finanzdirektion im Internet bekannt geben, welcher Organisation welcher Betrag zu welchem Zweck zugesprochen worden war.

Gemäss § 8 Abs. 1 DSG erfordert eine Datenbekanntgabe eine gesetzliche Grundlage.

Zu diesem Zeitpunkt (Januar 2005) war gerade die *«Interkantonale Vereinbarung über die Aufsicht sowie die Bewilligung und Ertragsverwendung von interkantonal oder gesamtschweizerisch durchgeführten Lotterien und Wetten»* von der Fachdirektorenkonferenz Lotteriemarkt und Lotteriegesetz zur Ratifizierung in den Kantonen verabschiedet aber noch nicht in Kraft gesetzt worden. Art 28 dieser Vereinbarung enthält eine Regelung, welche vorsieht, dass die Namen der aus dem Fonds Begünstigten, die Art der unterstützten Projekte sowie die Rechnung des Fonds veröffentlicht werden. Die Ratifizierung wird auch für den Kanton Zürich eine entsprechende Rechtsgrundlage schaffen.

Gemäss Beschluss des Kantonsrates über die Neuregelung der Finanzkompetenzen zwischen Kantons- und Regierungsrat bezüglich des Fonds für gemeinnützige Zwecke (LS 172.122) kann der Regierungsrat Einzelbeiträge bis maximal Fr. 400 000.– bewilligen; grössere Zuwendungen liegen in der Kompetenz des Kantonsrates. Dessen Beschlüsse sind aufgrund von § 9 Abs. 1 des Kantonsratsgesetzes grundsätzlich öffentlich. Die Publikation einer Liste im Internet ist insofern unproblematisch, da keine besonders schützenswerten Personendaten betroffen sind.

Die Beschlüsse des Regierungsrates hingegen sind grundsätzlich nicht öffentlich. In diesem Fall kann er sie jedoch, gestützt auf § 51 Abs. 1 des Organisationsgesetzes des Regierungsrates, bekannt geben. Wenn davon Gebrauch gemacht wird, ist eine Publikation der Liste im Internet möglich.

Bis also die interkantonale Vereinbarung in Kraft tritt, entscheidet der Regierungsrat über eine Veröffentlichung seiner Beschlüsse.

Titel: Psychologische Tests und Videoaufnahmen von Mitarbeitenden
URL: http://www.datenschutz.ch/themen/1258.php
Datum: 17.07.2006

07.

Psychologische Tests und Videoaufnahmen von Mitarbeitenden

Psychologische Tests und Videoaufnahmen sind nur mit ausdrücklicher Einwilligung der betroffenen Personen erlaubt. Willigt eine Person nicht ein, dürfen ihr daraus keine Nachteile erwachsen.

Im Rahmen eines Optimierungsprojektes in einem Betrieb des Kantons Zürich erhielt eine externe Firma den Auftrag, die Aufbauorganisation und die Prozesse des Auftraggebers effizienzsteigernd zu definieren und anzupassen. In diesem Zusammenhang wurden mit den Mitarbeitenden psychologische Selbsteinschätzungstests durchgeführt, welche die Wahrnehmung für die eigenen Präferenzen schärfen sollten. Einerseits informierte ein Coach die am Test beteiligten Angestellten in einem Einzelgespräch über die Resultate, andererseits wurden die Ergebnisse auch in Gruppen diskutiert, was die Mitarbeitenden faktisch zwang, sie den Arbeitskollegen gegenüber offenzulegen. Die Testresultate bewahrte die externe Firma auf, die elektronischen Daten lagen bei einem Unternehmen in den USA, welches sie wissenschaftlich auswertete. Im Weiteren führte die externe Firma Workshops zu diversen Themen durch und zeichnete diese teilweise auf Video auf. Nicht allen Mitarbeitenden war bewusst, dass sie aufgenommen wurden.

Psychologische Tests

Psychologische Tests dienen dazu, Persönlichkeitsprofile zu erstellen. Dabei handelt es sich um besonders schützenswerte Personendaten (§ 2 lit. e Datenschutzgesetz). Für die Durchführung von psychologischen Tests ist entweder eine klare gesetzliche Grundlage oder die Einwilligung der betroffenen Person nötig (§ 5 lit. a und c Datenschutzgesetz). Eine gesetzliche Grundlage war im konkreten Fall nicht ersichtlich.

Weigert sich jemand, einen solchen Test durchzuführen oder die Ergebnisse in der Gruppe zu besprechen, dürfen ihr oder ihm daraus keine Nachteile entstehen.

Gemäss § 4 Abs. 4 Datenschutzgesetz dürfen Personendaten nur zu einem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgeschrieben ist. Damit eine beteiligte Person ihre Präferenzen besser einschätzen kann, genügt es, wenn die Testergebnisse ihr selber zur Verfügung stehen, allenfalls verbunden mit der Erläuterung durch eine fachkundige Person. Externe Firmen benötigen die ausdrückliche Genehmigung der betroffenen Angestellten, um diese Tests für andere Zwecke weiterzuverwenden. Dieses Erfordernis entfällt, wenn die Daten vollständig anonymisiert werden, was mit der Trennung von Test- und Personaldaten in einer Datenbank, auf welche ein und dieselbe Stelle zugreifen kann, nicht gewährleistet ist. Die USA verfügt nicht über eine der Schweiz gleichwertige Datenschutzgesetzgebung, sodass ein Datentransfer in die USA für die am Test Beteiligten mit einem Verlust ihrer Rechte verbunden ist. Der Weitergabe der Informationen in die USA ist daher nur rechtmässig, wenn die ausdrückliche Einwilligung der betroffenen Person vorliegt.

Videoaufnahmen

Für Videoaufnahmen gilt ebenfalls, dass entweder eine entsprechende gesetzliche Grundlage oder die Einwilligung der gefilmten Person vorliegen muss. Willigen Anwesende nicht in die Videoaufnahmen ein, bedeutet dies in den meisten Fällen, dass die Kamera überhaupt nicht eingeschaltet werden darf; andernfalls lassen sich Ton- und Bildaufnahmen der nicht einverstandenen Personen kaum vermeiden.

Gerade bei einem kleineren Kreis von Beteiligten sind Rückschlüsse auf die Einzelnen leicht möglich.

Wird die Einwilligung aller betroffenen Personen jeweils vor Beginn der Videoaufnahmen und unter Angabe des Zwecks eingeholt, können die Aufzeichnungen bis Projektschluss aufbewahrt werden. Sollte dies am Anfang versäumt worden sein, müssen die Zustimmungen nachträglich eingeholt oder die Videobänder sofort vernichtet werden.

Titel: Datenschutz im Gesundheitsförderungsprojekt
URL: http://www.datenschutz.ch/themen/1259.php
Datum: 17.07.2006

08.

Datenschutz im Gesundheitsförderungsprojekt

Ohne ausdrückliche Einwilligung ist ein Arzt nicht zur Bekanntgabe von Adressen seiner Patientinnen und Patienten befugt – auch dann nicht, wenn es der Gesundheitsförderung der betroffenen Person dient und ihr in Form von kostenloser Beratung zugute kommt.

Eine Gemeinde hatte aufgrund der grosszügigen Spende einer Privatperson die Möglichkeit, ein Gesundheitsförderungsprojekt durchzuführen, mit dem Ziel, die Pflegebedürftigkeit bei älteren Menschen möglichst lange zu vermeiden. Die diesbezügliche Projektberatung erfolgte durch eine externe Stelle, die Leitung übernahm die Gemeinde.

Die Teilnahme am Projekt war freiwillig. Die Teilnehmenden mussten einen sehr detaillierten Fragebogen ausfüllen, unter anderem zu den Bereichen medizinische Vorgeschichte, Gesundheitszustand, Psyche und Wohlbefinden, Medikamente, soziales Umfeld sowie Zigaretten- und Alkoholkonsum. Die elektronische Erfassung und Auswertung erledigte ein externes Rechenzentrum. Im Anschluss daran erhielten die Teilnehmenden ihren Gesundheitsbericht mit massgeschneiderten Vorschlägen für Gesundheitsförderung und Prävention. In der Folge sollten der Hausarzt und eine Gesundheitsberaterin den Partizipanten oder die Partizipantin bei der Umsetzung der Vorschläge begleiten. Um an die Zielgruppe zu gelangen, schrieb die Projektleitung die Ärztinnen und Ärzte der Gemeinde an und bat sie um Bekanntgabe der Adressen aller von ihnen behandelten Patientinnen und Patienten ab 65 Jahren.

Gemäss Art. 321 Strafgesetzbuch (StGB) werden Ärzte, die ein Geheimnis offenbaren, das ihnen in Ausübung ihres Berufes anvertraut worden ist oder das sie in dessen Ausübung wahrgenommen haben, auf Antrag mit Gefängnis oder Busse bestraft. Auch die Tatsache, dass jemand in ärztlicher Behandlung ist, fällt unter den Begriff des Geheimnisses. Diese Information an Dritte weiterzugeben ist nur erlaubt, wenn eine ausreichende gesetzliche Grundlage, die Einwilligung des betroffenen Patienten oder die Entbindung vom Arztgeheimnis durch die vorgesetzte Behörde vorliegt (Art. 321 Ziff. 2 und 3 StGB).

Für die Ärzte war es unmöglich, die Zustimmung aller Patientinnen und Patienten einzuholen. Ebenso wenig lag eine gesetzliche Grundlage oder eine Entbindung der Gesundheitsdirektion vor. Die Adressbekanntgabe war also nicht zulässig.

Es gäbe jedoch andere Wege, die erforderlichen Daten zu beschaffen:

Listen von Einwohnerinnen und Einwohnern können für schützenswerte ideelle Zwecke nach gewissen Gesichtspunkten durch die Einwohnerkontrolle geordnet bekannt gegeben werden (§ 9 Abs. 3 Datenschutzgesetz), vorausgesetzt, die Daten werden nicht an Dritte weitergegeben. Eine andere Möglichkeit besteht darin, eine Information bei den Ärztinnen und Ärzten zu platzieren, damit sich die interessierten Personen selber bei der Projektleitung melden können.

Bei der Durchführung eines solchen Projektes sind zudem folgende Punkte zu beachten:

- Nur die für die Gesundheitsförderung geeigneten und erforderlichen Daten dürfen erhoben werden.
- Den Teilnehmenden müssen die Möglichkeit haben, nur einen Teil des Fragebogens auszufüllen.
- Gegenüber den Teilnehmenden ist absolute Transparenz hinsichtlich der Datenbearbeitungen zu gewährleisten. Aus der Information muss hervorgehen, welchen Zwecken die Daten dienen, wer namentlich auf sie zugreifen und oder sie einsehen kann und wie lange sie aufbewahrt werden. Ohne Zustimmung der betroffenen Personen darf der Zweck nicht geändert oder erweitert werden. Eine Verwendung für andere Projekte ist allenfalls dann erlaubt, wenn die Daten so anonymisiert werden, dass keine Rückschlüsse auf die Befragten möglich sind.
- Verzichtet ein Patient beziehungsweise eine Patientin auf eine weitere Teilnahme am Projekt, sind seine oder ihre Daten umgehend zu vernichten – es sei denn er oder sie sei ausdrücklich mit der weiteren Aufbewahrung und Verwendung der Daten im Rahmen des Projektes einverstanden.
- Jegliche Weitergabe der Daten erfordert die ausdrückliche Zustimmung des Teilnehmers.
- Die Verträge mit den externen Dienstleistern sind schriftlich aufzusetzen und der Zweck der Datenbearbeitung im Auftrag genau zu regeln. Die Allgemeinen Geschäftsbedingungen Sicherheit des Kantons Zürich sind in die Verträge zu integrieren. Ferner sollte ein Hinweis auf die §§ 13 Abs. 2 und 26 Datenschutzgesetz nicht fehlen. Diese Bestimmungen halten fest, dass die von einem öffentlichen Organ mit einer Datenbearbeitung betraute Stelle die Personendaten nur für den Auftraggeber verwenden und nur diesem bekannt geben dürfen. § 26 enthält die zugehörige Strafbestimmung bei Zuwiderhandlung.

Titel: Verwendung von internen Geschäftsinformationen im Anstellungsverfahren
URL: http://www.datenschutz.ch/themen/1260.php
Datum: 17.07.2006

09. Verwendung von internen Geschäftsinformationen im Anstellungsverfahren

Informationen aus einem internen Geschäftsverzeichnis – konkret zu gelöschten Einträgen im Strafregister – dürfen nur zum Zweck der Geschäftsverwaltung genützt werden. Eine anderweitige Verwendung, im vorliegenden Fall zur Beurteilung der Eignung für die Anstellung bei einer Strafuntersuchungsbehörde, widerspricht der ursprünglichen Zweckbestimmung und ist daher rechtswidrig.

Die Direktion der Justiz und des Innern führt ein Geschäftsinformationssystem (Rechtsinformationssystem; RIS). Darin werden sämtliche Geschäftsfälle der Strafuntersuchungsbehörden eingetragen. Eine Person, in deren Strafregisterauszug sich keine Einträge befanden, bewarb sich bei der Staatsanwaltschaft. Die Stelle wurde mündlich zugesichert, später erhielt die Person jedoch die Mitteilung, eine Anstellung sei nicht mehr möglich, gestützt auf einen Eintrag im Geschäftsinformationssystem RIS, welches eine im Jahr 1993 gelöschte Vorstrafe enthalte.

Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, der aus den Umständen ersichtlich oder der gesetzlich vorgesehen ist (§ 4 Abs. 4 Datenschutzgesetz). Daten müssen durch angemessene organisatorische und technische Massnahmen gegen unbefugtes Bearbeiten geschützt werden (§ 4 Abs. 5 Datenschutzgesetz). Nicht mehr benötigte Personendaten sind zu vernichten; das verantwortliche Organ legt für jede Datensammlung fest, wann dies zu geschehen hat. Vorbehalten bleiben die Bestimmungen über die Archivierung (§ 14 Datenschutzgesetz).

Ein Geschäftsinformationssystem dient vorwiegend der Verwaltung der laufenden Geschäfte eines öffentlichen Organs. Die darin enthaltenen Informationen dürfen ausschliesslich für diese Zwecke verwendet werden. Eine andere Nutzung, zum Beispiel um die Eignung für eine Anstellung zu beurteilen, stellt eine unerlaubte Zweckänderung dar. Diese ist rechtswidrig.

Ein Geschäftsinformationssystem ist zudem durch angemessene organisatorische und technische Massnahmen so auszugestalten, dass nur diejenigen Personen auf die Informationen zugreifen können, welche mit der Geschäftsverwaltung unmittelbar befasst sind und die entsprechenden Angaben tatsächlich benötigen. Ein Zugriff für Unbefugte muss mit technischen Massnahmen verhindert werden.

Zudem müssen auch für Geschäftsinformationssysteme Regelungen für die Archivierung und Löschung nicht mehr benötigter Einträge festgelegt sein; sie dürfen nicht unbeschränkt im System belassen werden.

Titel: Separates Konkursverzeichnis im Internet
URL: http://www.datenschutz.ch/themen/1261.php
Datum: 17.07.2006

10.

Separates Konkursverzeichnis im Internet

Der Kanton Zürich kann im Internet ein eigenes Konkursverzeichnis führen. Es muss sich allerdings auf die Bekanntgabe derjenigen Personendaten beschränken, welche – gestützt auf entsprechende Grundlagen im Schuldbetreibungs- und Konkursrecht – bereits im Schweizerischen Handelsamtsblatt publiziert werden.

Das Notariatsinspektorat des Kantons Zürich plant als Dienstleistung für Gläubiger und weitere Personen, welche an einem Konkursverfahren beteiligt sind, die Publikation eines Konkursverzeichnisses auf www.notariate.zh.ch. Es soll sämtliche hängigen Verfahren im Kanton Zürich – jährlich zwischen 600 und 700 – auflisten. Die Daten werden beim Schweizerischen Handelsamtsblatt beschafft.

Öffentliche Organe dürfen gemäss § 8 Abs. 1 Datenschutzgesetz Personendaten bekannt geben, wenn dafür gesetzliche Grundlagen bestehen. Die Informationen im Konkursverzeichnis des Kantons Zürich entsprechen denjenigen, welche durch die Konkursämter gemäss den Vorgaben des Schuldbetreibungs- und Konkursrechts im Schweizerischen Handelsamtsblatt publiziert werden. Eine gesetzliche Grundlage für die Publikation ist demnach gegeben. Wird das Verfahren mit der Schlusspublikation abgeschlossen, sind die Angaben noch während zwei Monaten abrufbar. Danach werden sie aus dem Verzeichnis entfernt.

Titel: Personalien von Opfern in Strafverfahrensakten
URL: http://www.datenschutz.ch/themen/1262.php
Datum: 17.07.2006

11.

Personalien von Opfern in Strafverfahrensakten

Werden die Opfereigenschaft und die besondere Schutzbedürftigkeit einer geschädigten Person bejaht, hat sie ein Recht darauf, dass ihre Identität dem mutmasslichen Täter nicht preisgegeben wird. Aus praktischer Sicht empfiehlt es sich, die Vorkehrungen bereits im Stadium der ersten Kontaktaufnahme des Opfers mit der Polizei zu treffen.

Die Persönlichkeitsrechte der Parteien werden in einem Strafverfahren durch das geltende Prozessrecht geregelt; das Opferhilfegesetz dient dem Schutz des Opfers. Das Datenschutzgesetz ist in hängigen Verfahren der Strafrechtspflege nicht anwendbar.

Die Behörden haben die Persönlichkeitsrechte der Geschädigten in allen Abschnitten des Strafverfahrens zu wahren und informieren sie über ihre Rechte. Liegen besondere Gründe vor, werden die Personalien des Opfers dem Angeschuldigten nicht bekannt gegeben, sofern dies den überwiegenden Interessen der Strafverfolgung nicht widerspricht (Art. 19 Abs. 2 und 3 StPO). Die kantonale Opferhilfestelle geht von einer entsprechenden Schutzbedürftigkeit zum Beispiel dann aus, wenn die Tatumstände oder Drohungen des Täters zur Befürchtung Anlass geben, der Täter werde sich an dem Opfer für die Anzeigeerstattung oder die Bereitschaft zur Aussage rächen.

Die praktische Umsetzung des Identitätsschutzes des Opfers stellt für die Behörden eine besondere Herausforderung dar, sind doch auch die Rechte des Angeschuldigten und seines Verteidigers zu wahren. Damit die Personalien der oder des Geschädigten nicht bekannt werden, ist ihm beziehungsweise ihr gemäss Oberstaatsanwaltschaft des Kantons Zürich unmittelbar bei Einleitung des Verfahrens ein Beistand zu bestellen, welcher sie oder ihn neben der Betreuungsfunktion auch mit einer separaten Zustellungsadresse abschirmt. Auf diese Weise kann verhindert werden, dass der Angeschuldigte die Personalien des Opfers den Polizei- oder Untersuchungsakten entnehmen kann.

Titel: Beurteilung der Fahrtauglichkeit
URL: http://www.datenschutz.ch/themen/1263.php
Datum: 17.07.2006

12. Beurteilung der Fahrtauglichkeit

Die Erhebung der Arbeitssituation und des sozialen Umfeldes ist für die Überprüfung der Fahrtauglichkeit einer querschnittgelähmten Person weder geeignet noch erforderlich und somit unzulässig.

Eine querschnittgelähmte Person, welche im Besitz eines Führerscheines für Personenwagen ist, musste nach fünf Jahre ihre Fahrtauglichkeit überprüfen lassen. Im Rahmen der Überprüfung wurde ein ärztliches Zeugnis verlangt, welches über den Gesundheitszustand Auskunft gab. Auf dem Fragebogen der Abteilung für Administrativmassnahmen im Strassenverkehr des Strassenverkehrsamtes Zürich wurden zusätzlich Fragen zur Arbeitssituation und zum sozialen Umfeld gestellt.

Gemäss § 4 Abs. 3 des kantonalen Datenschutzgesetzes dürfen kantonale Organe nur Personendaten bearbeiten, welche für die Erfüllung der öffentlichen Aufgabe geeignet und erforderlich sind (Grundsatz der Verhältnismässigkeit). Zur Prüfung der Fahrtauglichkeit dürfen demzufolge diejenigen Daten erhoben werden, welche entsprechend der gesundheitlichen Beeinträchtigung des Lenkers oder der Lenkerin für das Verhalten im Strassenverkehr relevant sein können.

Das Strassenverkehrsamt und das von ihm mit den medizinischen Abklärungen beauftragte Institut für Rechtsmedizin gaben an, die Fragen nach der Arbeits- sowie der sozialen Situation seien für die Fahrtauglichkeitsprüfung einer querschnittsgelähmten Person irrelevant; sie seien jedoch sinnvoll bei Sucht- und psychischen Erkrankungen und irrtümlicherweise ins Formular «Verlaufbericht zur Fahreignung», welches an die querschnittgelähmte Person versandt wurde, übernommen worden. Dieser Beurteilung kann sich der Datenschutzbeauftragte anschliessen.

Titel: Automatische Mutationsmeldungen
URL: http://www.datenschutz.ch/themen/1264.php
Datum: 17.07.2006

13. Automatische Mutationsmeldungen

Es gibt ausreichende gesetzliche Grundlagen für automatische Mutationsmeldungen aus den Einwohnerregistern an das Amt für Militär und Zivilschutz über das Datentransportsystem von e-Voting an die Datendrehscheibe MILVA, doch sind die Meldungen nicht in allen Fällen verhältnismässig.

Im Hinblick auf die Abschaffung der Sektionschefs in den Gemeinden plante das Amt für Militär und Zivilschutz automatische Mutationsmeldungen von den Einwohnerkontrollen der Gemeinden an das Amt für Militär und Zivilschutz über das Datentransportsystem von e-Voting an die Datendrehscheibe MILVA. Diese erfasst sämtliche Mutationen in den Gemeinden, indem die Zu- und Wegzüge sowie die Änderungen der Personalien aller Einwohnerinnen und Einwohner zwischen 18 und 50 Jahren von den Einwohnerkontrollen an MILVA gemeldet werden.

Öffentliche Organe dürfen gemäss § 8 Abs. 1 Datenschutzgesetz Personendaten bekannt geben, wenn dafür gesetzliche Grundlagen bestehen. Das Bearbeiten von Personendaten muss zudem gemäss dem Prinzip der Verhältnismässigkeit für die Erfüllung der Aufgaben geeignet und erforderlich sein (§ 4 Abs. 3 Datenschutzgesetz).

Die gesetzlichen Grundlagen für die Erhebung der benötigten Personendaten im Einzelfall bei den Gemeinden liegen vor. Es handelt sich um die Zu- und Wegzugsmeldungen sowie um die Änderungen der Personalien derjenigen Personen, welche mit der Militärverwaltung in Verbindung stehen. Diese machen allerdings nur einen Bruchteil der Bevölkerung aus. Alle anderen sind von den bestehenden rechtlichen Grundlagen der bundesrechtlichen Militär- und Zivilschutzgesetzgebung nicht betroffen. Eine Meldung sämtlicher Mutationen ist für deren Aufgabenerfüllung weder geeignet noch erforderlich. Die Gemeinden haben deshalb lediglich die Mutationen von Personen zu melden, welche tatsächlich mit der Militärverwaltung in Verbindung zu stehen haben.

Da eine solche Lösung den beteiligten Stellen technisch als zu aufwändig erschien, werden künftig sämtliche Zu- und Wegzüge sowie die Änderungen der Personalien aller Einwohnerinnen und Einwohner zwischen 18 und 50 Jahren von den Einwohnerkontrollen an MILVA gemeldet. Die Meldungen werden im Übermittlungskanal automatisch plausibilisiert, indem nicht benötigte Informationen ausgeschieden werden. Die Gemeinden lösen zwar sämtliche Mutationsmeldungen selbstständig aus, das Amt für Militär und Zivilschutz erhält jedoch nur die Änderungen, die es für die Erfüllung seiner Aufgaben tatsächlich braucht, also diejenigen der mit der Militärverwaltung in Verbindung stehenden Personen. Zudem gibt es keine Zugriffsmöglichkeiten auf den Übermittlungskanal; die Mutationsmeldungen erfolgen eingleisig, ohne Rückführ- und Abgleichmöglichkeiten.

Titel: Videoaufnahmen von Psychiatriepatientinnen und -patienten
URL: http://www.datenschutz.ch/themen/1265.php
Datum: 17.07.2006

14. Videoaufnahmen von Psychiatriepatientinnen und -patienten

Für die Videoaufzeichnung von Patientinnen und Patienten in der Psychiatrie müssen Prozesse definiert werden, um die Persönlichkeitsrechte der Aufgezeichneten zu schützen.

Ein Psychiatriepatient willigte in die Videoaufnahme seiner Therapiegespräche ein. Diese Aufzeichnungen sollten in erster Linie Forschungszwecken dienen und nur so lange verwendet werden, wie sich der Patient damit einverstanden erklärte. Mehrere Jahre nach Abschluss seiner Behandlung, nach der Besserung seines Gesundheitszustandes, verlangte der Patient die Vernichtung der Aufnahmen. Die Klinik konnte sie allerdings nicht mehr finden und entsprechend weder ihre Vernichtung bestätigen, noch sicherstellen, dass sie nicht für andere Zwecke verwendet wurden.

Für solche Videoaufnahmen sind Prozesse zu definieren, welche folgende Punkte gewährleisten:

- Videoaufnahmen von Psychiatriepatientinnen und -patienten sind nur möglich, wenn die betroffene Person oder ihre gesetzliche Vertretung eingewilligt hat. Dabei muss ihr im jeweiligen Fall klar sein, wofür sie ihr Einverständnis gibt; eine Blankovollmacht genügt nicht. Bei urteilsunfähigen Personen ist die Einwilligung der gesetzlichen Vertretung einzuholen. Ohne diese muss auf die Videoaufnahme verzichtet werden.
- Das Zweckbindungsgebot im Datenschutz verlangt vom verantwortlichen Organ, dass die erhobenen Personendaten nur für die Zwecke bearbeitet werden, die bei der Beschaffung der Informationen angegeben wurden. Im Zusammenhang mit Videoaufnahmen müssen deshalb die gefilmten Personen vor der Einwilligung über den genauen Zweck der Aufnahmen informiert sein; eine nachträgliche Zweckänderung ist nur mit Einwilligung der Aufgenommenen möglich. Zweck und Zustimmung sollten schriftlich festgehalten werden.
- Für den Datenschutz und die Datensicherheit ist dasjenige Organ verantwortlich, welches die Personendaten zur Erfüllung seiner Aufgaben bearbeitet (§ 6 DSG). Die Klinik muss die gespeicherten Videoaufnahmen durch technische und organisatorische Massnahmen vor unbefugter Datenbearbeitung schützen. Dabei empfiehlt es sich, schriftlich festzuhalten, wo und wie lange die Videoaufnahmen gelagert werden, wer zu deren Auswertung beziehungsweise Weiterverarbeitung berechtigt ist und wem Zutritt zum Aufbewahrungsort gewährt wird. Das Personal muss entsprechend instruiert sein.
- Um sicherzustellen, dass die gefilmten Personen ihre Rechte auf Auskunft, Berichtigung oder Vernichtung (§ 17 ff. Datenschutzgesetz) ausüben können, sind Videoaufzeichnungen zu registrieren; auch ihre Vernichtung muss in den Akten vermerkt sein.

Titel: Datenbearbeitung durch das Sozialamt
URL: http://www.datenschutz.ch/themen/1266.php
Datum: 17.07.2006

15.

Datenbearbeitung durch das Sozialamt

Sozialhilfeempfangende sind gesetzlich zur Mitwirkung verpflichtet. Die Datenbearbeitungen durch das Sozialamt dürfen den Umfang des Notwendigen jedoch nicht übersteigen. So müssen die Kontoauszüge im Falle der wirtschaftlichen Hilfe nicht im Detail eingereicht werden; zu belegen sind nur Datum und Höhe der Ausgaben oder Einnahmen. Die Betroffenen brauchen keine Rechenschaft darüber abzulegen, was sie genau mit dem jeweiligen Betrag erworben haben.

Personendaten können gemäss § 8 Abs. 1 Datenschutzgesetz bearbeitet werden, wenn eine gesetzliche Grundlage besteht. Die Datenbearbeitungen dürfen den Umfang des Notwendigen nicht übersteigen. Dieser Grundsatz der Verhältnismässigkeit gemäss § 4 Abs. 3 Datenschutzgesetz verlangt, dass nur Informationen erhoben werden, die für die Erfüllung der Aufgaben geeignet und erforderlich sind.

Leistet die Sozialhilfebehörde wirtschaftliche Hilfe, überprüft sie gemäss § 33 der Verordnung zum Sozialhilfegesetz jährlich alle Fälle, wobei der Sozialhilfebezüger gestützt auf § 18 Sozialhilfegesetz und § 28 Verordnung zum Sozialhilfegesetz zur Mithilfe verpflichtet ist. Die jährliche Überprüfung umfasst unter anderem die finanziellen Verhältnisse.

Kontoauszüge sind dafür grundsätzlich ein sinnvolles Mittel, doch braucht es nur die für die Sozialhilfe geeigneten und erforderlichen Angaben. Der Zweck der Sozialhilfe besteht darin, eine Person finanziell zu unterstützen, wenn ihre eigenen Mittel nicht ausreichen. Um die finanziellen Verhältnisse zu überprüfen ist es deshalb kein detaillierter Bankauszug mit sämtlichen Einnahmen und Ausgaben (zum Beispiel 22.6.05; Globus Fr. 110.–) erforderlich, wie dies auch beim Barkauf nicht nötig und zudem nicht praktikabel ist, weil dabei die entsprechenden Belege oft fehlen.

Es genügt somit ein teilweise abgedeckter oder auf die nötigen Informationen reduzierter Bankauszug (Einschränkung auf Datum und Höhe der Ausgabe oder Einnahme).

Verlangt das Sozialamt detaillierte Bankauszüge, empfehlen wir zur Vermeidung einer Leistungskürzung im Sinne von § 24 Sozialhilfegesetz, die eingeforderten Bank- und Kontoauszüge abgedeckt einzureichen.

Titel: Ärztliches Zeugnis für Anmeldung
URL: http://www.datenschutz.ch/themen/1267.php
Datum: 17.07.2006

16.

Ärztliches Zeugnis für Anmeldung

Für die Abklärung der gesundheitlichen Eignung zum Lehrberuf darf ein Arztzeugnis bei der Anmeldung verlangt werden, da hierfür gesetzliche Grundlagen bestehen. Dabei dürfen jedoch nur die Angaben erfragt werden, die für die Beurteilung der Eignung zur Ausbildung und zum späteren Beruf geeignet und erforderlich sind.

Die Pädagogische Hochschule Zürich verlangt bei der Anmeldung von den Studierenden ein ärztliches Zeugnis. Die Rechtsgrundlagen dafür finden sich in § 8 des Gesetzes über die Pädagogische Hochschule (LS 414.41): «Die Zulassung zum Studium setzt einen guten Leumund und Vertrauenswürdigkeit sowie persönliche und gesundheitliche Eignung zum Lehrberuf voraus», in § 8 Abs. 2 des Fachhochschulgesetzes (LS 414.11): «Die Schule kann für Studiengänge, welche eine spezifische Eignung, Berufs-, Arbeitserfahrung oder Begabung erfordern, zusätzliche Zulassungsvoraussetzungen oder spezielle Zulassungsbedingungen vorsehen», sowie in § 4 des Reglements über die Zulassung an die Pädagogische Hochschule Zürich (LS 414.412) «Zur Abklärung der gesundheitlichen Eignung ist ein ärztliches Zeugnis zuhanden der Schulärztin oder des Schularztes der Pädagogischen Hochschule einzureichen.»

Die Ausbildung an der Pädagogischen Hochschule ist vergleichbar mit einer Lehre oder einer sonstigen Berufsausbildung. Die Studierenden haben sich bereits zu Anfang der Ausbildung in der Praxis zu bewähren und stehen vor Schülerinnen und Schülern. Zu prüfen ist deshalb neben der Eignung zum Beruf bereits diejenige zur Ausbildung. Da sich sehr viele Studierende anmelden, kann nicht mit jeder oder jedem Kandidierenden ein Gespräch geführt werden, weshalb ein Fragebogen verwendet wird. Dieser wird verschlossen an den Schularzt weitergeleitet.

Das vierseitige ärztliche Zeugnis ist in Form eines Fragebogens gehalten. Insgesamt sieben Fragen betreffen die Anamnese. Zudem werden unter der Rubrik «Untersuchung» Angaben zum Allgemeinzustand, zu Sprechstörungen, zu Beeinträchtigungen von acht Funktionen sowie zu Verhalten und Kontaktfähigkeit verlangt.

Unter dem Gesichtspunkt der Verhältnismässigkeit gemäss § 4 Abs. 3 Datenschutzgesetz, wonach das Bearbeiten von Personendaten für die Erfüllung der Aufgaben geeignet und erforderlich sein muss, dürfen nur Fragen gestellt werden, welche für die Beurteilung der Eignung zum Lehrberuf notwendig sind. Dies ist beim derzeitigen Fragebogen nicht in allen Punkten gegeben. So sind zum Beispiel bei der Rubrik «Untersuchung» Fragen nach Grösse, Gewicht, Puls und Fernvisus irrelevant. Es genügen der korrigierte Visus, das Gehör sowie der Farbsinn. Es werden insgesamt zu viele und zu weit reichende Gesundheitsdaten erfragt. Die Pädagogische Hochschule hat in Aussicht gestellt, den Fragebogen künftig entsprechend anzupassen.

Titel: Einwilligung der Eltern in die Befragung von Jugendlichen für eine Langzeitstudie
URL: http://www.datenschutz.ch/themen/1268.php
Datum: 17.07.2006

17. Einwilligung der Eltern in die Befragung von Jugendlichen für eine Langzeitstudie

Jugendliche müssen sich mit der Befragung im Rahmen einer Langzeitstudie einverstanden erklären. Für Fragen, die ausschliesslich sie selber betreffen, sind sie ab ungefähr 14 Jahren urteilsfähig. Die Einwilligung der Eltern ist deshalb nicht nötig. Das Forschungsprojekt ist ihnen altersentsprechend zu erklären. Eine Information der Eltern ist jedoch sinnvoll.

Das Jakobs Center for Productive Youth Development führt im Auftrag des Schweizerischen Nationalfonds hierzulande erstmals eine Befragung von Kindern und Jugendlichen durch. Dabei sollen unter anderem 15-jährige Jugendliche persönlich zu ihren Lebensbedingungen, zu ihrer Entwicklung sowie zu ihrem Bildungsverlauf Auskunft geben.

Dies wirft das Problem auf, ob mit minderjährigen Personen mündliche Befragungen zu Forschungszwecken ohne vorgängige Einwilligung der Eltern durchgeführt werden dürfen.

Das Informationelle Selbstbestimmungsrecht ist in der Verfassung festgehalten. Es gilt auch für Jugendliche unter 18 Jahren. Soweit sie urteilsfähig sind, können sie Rechte ausüben, die ihnen um ihrer Persönlichkeit willen zustehen (Art. 19 Abs. 2 Zivilgesetzbuch). Die im Forschungsprojekt gestellten Fragen betreffen ausschliesslich die Jugendlichen selber und werden ihnen zudem in einer Art und Weise gestellt, die ihnen eine selbstständige Beantwortung erlaubt. Die Jugendlichen werden in einem ersten Schritt angefragt, ob sie zu einem freiwilligen Interview bereit sind. Dabei werden ihnen Zweck und Ablauf der Befragung erklärt. Willigen sie ein, erfolgt das Interview bei ihnen zu hause. Im nächsten Schritt kommt bei entsprechender Einwilligung die Befragung der Eltern sowie der Lehrpersonen hinzu. Lehnen die Jugendlichen ab, werden auch die Eltern und Lehrpersonen nicht befragt.

Jugendliche sind im Rahmen einer derartigen Langzeitstudie ab ungefähr 14 Jahren urteilsfähig, wenn es um Fragen geht, die ausschliesslich ihre Belange betreffen. Sie müssen sich als betroffene Personen mit der Befragung einverstanden erklären. Das Forschungsprojekt ist ihnen altersentsprechend zu erklären und sie sind ausdrücklich darauf aufmerksam zu machen, dass eine Teilnahme freiwillig ist. Eine vorgängige Einwilligung der Eltern ist nicht nötig, da die Jugendlichen in Bezug auf die gestellten Fragen urteilsfähig sind. Eine entsprechende Information der Eltern im Rahmen der notwendigen Erklärungen an die Jugendlichen in Form eines Beiblattes oder im Rahmen der anschliessenden schriftlichen Befragung der Eltern ist jedoch sinnvoll.

Titel: Auskunfts- und Berichtigungsrechte
URL: http://www.datenschutz.ch/themen/1269.php
Datum: 17.07.2006

18. Auskunfts- und Berichtigungsrechte

Der Verein «Verdingkinder suchen ihre Spur» bemüht sich um Klärung der persönlichen und rechtlichen Verhältnisse von Menschen, die verdingt oder in Heime abgeschoben worden sind. Die betroffenen Personen haben grundsätzlich ein uneingeschränktes und kostenloses Auskunftsrecht in ihre bei den entsprechenden öffentlichen Organen vorhandenen Daten. Zudem können sie deren Berichtigung und Vernichtung verlangen.

Der Verein «Verdingkinder suchen ihre Spur» hat die Klärung der persönlichen und rechtlichen Verhältnisse von Menschen zum Ziel, welche verdingt oder in Heime abgeschoben worden sind. Für die betroffenen Personen stellen sich Fragen der Akteneinsicht, der Möglichkeiten der Berichtigung und Vernichtung ihrer Daten sowie der möglichen Rechtsmittel.

Gemäss § 17 Datenschutzgesetz kann jede Person, nachdem sie sich ausgewiesen hat, von einem Organ Auskunft darüber verlangen, welche sie betreffenden Daten dort bearbeitet werden. Dies gilt für alle Verwaltungsstellen; eine Begründung ist nicht nötig. Das Gesuch ist schriftlich an die jeweilige Stelle zu richten.

Die Auskunft wird normalerweise schriftlich erteilt, kann aber auf Wunsch auch mündlich erfolgen, beispielsweise am Schalter. Gewährt die Verwaltungsstelle Einsicht, so muss sie kostenlos Auskunft über sämtliche von ihr bearbeiteten Daten, einschliesslich Handnotizen, geben. Einzig Gedächtnisstützen – beispielsweise die Notiz, man solle jemanden zurückrufen, oder Termineinträge in einer Agenda – fallen nicht darunter. Zudem besteht ein Anspruch auf Kopien. Der Datenschutzbeauftragte empfiehlt, diese umsonst abzugeben.

Eine vollständige Auskunft enthält:

- alle Daten, welche über die Gesuch stellende Person bearbeitet werden,
- die gesetzliche Grundlage der Datensammlung,
- Angaben über den Zweck dieser Datenbearbeitung,
- die Bezeichnung weiterer an der Datensammlung beteiligter Stellen sowie
- die Angabe der regelmässigen Datenempfänger.

Gemäss § 18 Datenschutzgesetz darf die Auskunft unter bestimmten Umständen aufgeschoben, eingeschränkt oder verweigert werden, wenn besondere Gesetzesbestimmungen sowie überwiegende öffentliche oder schützenswerte private Interessen dem Begehren entgegenstehen. In diesem Fall ist die Verwaltung zu einer schriftlichen Begründung der Einschränkung verpflichtet, die auf dem Rechtsweg überprüft werden kann. Wenn die Auskunft einen unverhältnismässigen Verwaltungsaufwand mit sich bringt, kann sie vom Nachweis eines schützenswerten Interesses der gesuchstellenden Person abhängig gemacht werden.

Wer ein schützenswertes Interesse hat, kann gemäss § 19 Datenschutzgesetz vom verantwortlichen Organ verlangen, dass es a) Daten berichtigt oder vernichtet und b) den Entscheid oder die Berichtigung Dritten mitteilt oder veröffentlicht. Kann weder die Richtigkeit

noch die Unrichtigkeit von Daten bewiesen werden, bringt das verantwortliche Organ einen entsprechenden Vermerk an. Bestreitet es die Unrichtigkeit von Daten, liegt es an ihm, die Richtigkeit zu beweisen, wenn dies der gesuchstellenden Person nicht ohne weiteres zugemutet werden kann.

Entspricht ein Organ einem Begehren aufgrund des Datenschutzgesetzes nicht, erlässt es gemäss § 20 Datenschutzgesetz einen begründeten Entscheid. Bearbeiten mehrere Organe Personendaten aus einer gemeinsamen Datensammlung, kann die betroffene Person ihre Rechte bei jedem beteiligten Organ geltend machen. Wer dies tun möchte, muss sich an die Stelle wenden, welche für die entsprechende Datensammlung verantwortlich ist, also meistens diejenige, welche die in Frage stehende Bearbeitung vorgenommen hat. Dabei ist ein schriftliches Begehren zu stellen. Das Schreiben sollte Auskunft darüber geben, welche Datenbearbeitung beanstandet und was genau verlangt wird.

Fazit: Stellt eine betroffene Person im Rahmen der Wahrnehmung des Auskunftsrechts fest, dass Akteneinträge nicht korrekt sind, kann sie gemäss § 19 Datenschutzgesetz deren Berichtigung oder Löschung verlangen. Das öffentliche Organ hat, kommt es diesem Begehren nicht nach, in dieser Angelegenheit eine beschwerdefähige Verfügung zu erlassen. Ist die betroffene Person mit diesem Entscheid nicht einverstanden, kann sie in der Folge den Rechtsweg beschreiten.

Titel: Namensnennung bei parlamentarischen Vorstössen und Initiativen
URL: http://www.datenschutz.ch/themen/1270.php
Datum: 17.07.2006

19. Namensnennung bei parlamentarischen Vorstössen und Initiativen

Die Bekanntgabe von Kantonsratsakten ist abzulehnen oder einzuschränken, wenn offensichtlich schützenswerte Interessen einer betroffenen Person es verlangen. Ob ein solches Interesse vorliegt, kann erst nach einer Interessenabwägung im Einzelfall entschieden werden. Blosse Namensnennungen ohne verletzende oder diskriminierende Ausführungen sind in Kantonsratsakten unter Vorbehalt von § 10 Datenschutzgesetz möglich.

Die Bekanntgabe von Kantonsratsakten ist abzulehnen oder einzuschränken, wenn darin Namen genannt werden und offensichtlich schützenswerte Interessen einer betroffenen Person es verlangen. Ob ein solches Interesse vorliegt, kann erst nach einer vorgängigen Güterabwägung im Einzelfall entschieden werden. Blosse Namensnennungen ohne verletzende oder diskriminierende Ausführungen sind in Kantonsratsakten unter Vorbehalt von § 10 Datenschutzgesetz möglich.

Stellt das Präsidium fest, dass mit einem parlamentarischen Vorstoss das Grundrecht auf Schutz der Privatheit verletzt wird, hat es die entsprechenden verletzenden oder diskriminierenden Ausführungen und Titel von sich aus zu ändern.

Wenn die Geschäftsleitung feststellt, dass mit einer Einzelinitiative das Grundrecht auf Schutz der Privatheit verletzt wird, ist sie verpflichtet, die Bekanntgabe der entsprechenden Personendaten aufgrund von § 10 Datenschutzgesetz abzulehnen oder einzuschränken. Der Text muss dem Initianten oder der Initiantin daher mit der Aufforderung zurückzugeben werden, ihn umzuformulieren und ohne Verletzung der Grundrechte der betroffenen Person erneut einzureichen.

Bei Namensnennungen in parlamentarischen Vorstössen und Initiativen stehen sich einerseits das Grundrecht auf Schutz der Privatheit und andererseits dasjenige auf Gewährleistung der politischen Rechte gegenüber (Art. 10 und 13 sowie 34 Bundesverfassung). Das Datenschutzgesetz konkretisiert das Grundrecht auf Privatheit.

Gemäss § 8 Datenschutzgesetz dürfen öffentliche Organe Personendaten bekannt geben, wenn dafür gesetzliche Grundlagen bestehen oder wenn a) die Daten für den Empfänger im Einzelfall zur Erfüllung seiner öffentlichen Aufgaben notwendig sind, b) die betroffene Person im Einzelfall eingewilligt hat oder die Einwilligung nach den Umständen vorausgesetzt werden darf oder wenn c) die betroffene Person ihre Daten allgemein zugänglich gemacht hat.

Das Ratsprotokoll enthält eingereichte parlamentarische Vorstösse und Einzelinitiativen (§ 51 Abs. 1 und 3 des Geschäftsreglements des Kantonsrats). Die Sitzungen und die Protokolle des Kantonsrats sind öffentlich und werden publiziert (§ 9 Abs. 1 Kantonsratsgesetz, § 54 des Geschäftsreglements des Kantonsrats). Eine gesetzliche Grundlage ist somit gegeben und eine Datenbekanntgabe grundsätzlich zulässig.

Die Bekanntgabe unterliegt jedoch Einschränkungen. Gemäss § 10 Datenschutzgesetz lehnt das öffentliche Organ die Bekanntgabe ab, schränkt sie ein oder verbindet sie mit Auflagen, wenn wesentliche öffentliche Interessen oder offensichtlich schützenswerte Interessen einer betroffenen Person beziehungsweise gesetzliche Geheimhaltungspflichten oder besondere Datenschutzvorschriften es verlangen.

Ob offensichtlich schützenswerte Interessen vorliegen, kann jeweils erst nach einer Güterabwägung im Einzelfall entschieden werden. Blosse Namensnennungen ohne verletzende oder diskriminierende Ausführungen sind unter Vorbehalt von § 10 Datenschutzgesetz möglich.

Parlamentarische Vorstösse

§ 44 Abs. 1 Geschäftsreglement des Kantonsrats lautet: «Parlamentarische Vorstösse sind dem Ratssekretariat während den Ratssitzungen schriftlich und unterzeichnet im Doppel einzureichen. Das Präsidium kann weitschweifige Begründungen kürzen sowie verletzende und diskriminierende Ausführungen und Titel ändern.»

Stellt das Präsidium fest, dass mit einem parlamentarischen Vorstoss das Grundrecht auf Schutz der Privatheit verletzt wird, muss es die verletzenden oder diskriminierenden Ausführungen und Titel von sich aus ändern. § 44 Abs. 1 Geschäftsreglement beinhaltet damit eine Konkretisierung von § 10 Datenschutzgesetz.

Einzel- und Behördeninitiativen

«Einzel- und Behördeninitiativen werden der Geschäftsleitung des Kantonsrats eingereicht» (§ 139 Abs. 1 Gesetz über die politischen Rechte).

Hier fehlt eine § 44 Abs. 1 des Geschäftsreglements des Kantonsrats analoge Bestimmung, wonach die Geschäftsleitung verletzende und diskriminierende Ausführungen und Titel ändern kann. Es ist deshalb davon auszugehen, dass sie grundsätzlich keine Änderungen am Text vornehmen darf.

Stellt die Geschäftsleitung fest, dass mit einer Einzelinitiative das Grundrecht auf Schutz der Privatheit verletzt wird, ist sie jedoch verpflichtet, die Bekanntgabe der entsprechenden Personendaten aufgrund von § 10 Datenschutzgesetz abzulehnen oder einzuschränken. Der Text ist dem Initianten daher mit der Aufforderung zurückzugeben, ihn umzuformulieren und ohne Verletzung der Grundrechte der betroffenen Person erneut einzureichen.

Titel: Einsicht in Prüfungen an der Medizinischen Fakultät
URL: http://www.datenschutz.ch/themen/1271.php
Datum: 17.07.2006

20.

Einsicht in Prüfungen an der Medizinischen Fakultät

Die Einsicht in Prüfungen an der Medizinischen Fakultät ist grundsätzlich vollumfänglich zu gewähren. Sie darf jedoch aus Gründen des öffentlichen Interesses eingeschränkt werden. Dies ist der Fall bei Fragen, die für die Beurteilung der Prüfung grundlegend sind (so genannte «Ankerfragen»). Hier ist eine Einschränkung auf die reine Einsichtnahme ohne Abgabe von Kopien möglich, da die Fragen sonst künftigen Prüflingen zukommen könnten. Zur Verdeutlichung ist eine gesetzliche Grundlage zu schaffen, welche das geschilderte öffentliche Interesse präzisiert.

Das Einsichtsrecht in Prüfungen ist grundsätzlich vollumfänglich zu gewähren, gestützt auf § 17 Datenschutzgesetz, wonach jede Person, die sich ausgewiesen hat, vom verantwortlichen Organ Auskunft verlangen kann, welche Daten über sie in dessen Datensammlungen bearbeitet werden.

Die Auskunft darf gemäss § 18 Abs. 1 Datenschutzgesetz aufgeschoben, eingeschränkt oder verweigert werden, wenn eine gesetzliche Bestimmung, überwiegende öffentliche Interessen oder überwiegende schützenswerte Interessen Dritter dies verlangen.

Zum Einsichtsrecht gehört normalerweise die kostenlose Abgabe von Kopien.

Die Medizinische Fakultät plant, die Einsicht in bestimmte Fragen einzuschränken. Die sogenannten Ankerfragen betreffen einen Fünftel der Prüfung. Im Multiple-Choice-Verfahren garantieren sie deren Qualität; ihre Beantwortung entscheidet über die Eignung zum späteren Beruf als Medizinerin oder Mediziner. Sie werden vorwiegend bei den Vorprüfungen zum Staatsexamen eingesetzt. Die Erstellung von Ankerfragen ist sehr aufwändig und entsprechend kostenintensiv. Zudem ist es faktisch nicht möglich, für jede Prüfung neue Ankerfragen zu erstellen, weil es davon zu wenige gibt. Es besteht ein überwiegendes öffentliches Interesse an einer jährlichen, rechtsgleichen Durchführung der Prüfungen mit einem ausreichenden Anteil an Ankerfragen.

Somit darf die Einsicht aus Gründen des öffentlichen Interesses an einer qualitativ hoch stehenden medizinischen Ausbildung insofern eingeschränkt werden, als sämtliche Fragen und Antworten wohl vor Ort eingesehen, Ankerfragen jedoch nicht kopiert oder abgeschrieben werden dürfen. Ansonsten könnten sie auf einfache Art künftigen Prüflingen zur Kenntnis gelangen.

Zu diesem Zweck sowie im Sinne der Transparenz ist eine entsprechende gesetzliche Grundlage zu schaffen, welche die Einschränkung der Einsicht in diesem Sinne regelt und so das überwiegende öffentliche Interesse präzisiert.

Titel: Bekanntgabe des Aufenthaltsortes eines Inhaftierten zwecks Betreibung
URL: http://www.datenschutz.ch/themen/1272.php
Datum: 17.07.2006

21. Bekanntgabe des Aufenthaltsortes eines Inhaftierten zwecks Betreibung

Gegenüber dem Gläubiger kann der Aufenthaltsort des inhaftierten Schuldners nur mit dessen Einwilligung bekannt gegeben werden. Das Betreibungsamt kann sich hingegen auf Amtshilfe berufen, um diese Informationen zu erhalten.

Das Amt für Justizvollzug (JuV) wird immer wieder von Gläubigern und Betreibungsämtern angefragt, ob eine gewisse Person inhaftiert sei und falls ja, wo sie sich aufhalte. Dabei geht es meist um die Anhebung einer Betreibung beziehungsweise um die Zustellung eines Zahlungsbefehls.

Gemäss § 8 Datenschutzgesetz dürfen öffentliche Organe Personendaten bekannt geben, wenn dafür gesetzliche Grundlagen bestehen, die betroffene Person im Einzelfall eingewilligt hat oder die Einwilligung nach den Umständen vorausgesetzt werden darf. Fragen öffentliche Organe an, kommt zusätzlich die Möglichkeit der Amtshilfe in Betracht. Im vorliegenden Fall bezieht sich die bekannt zu gebende Information auf eine strafrechtliche Sanktion. Diese Information gehört zu den besonders schützenswerten Personendaten (§ 2 lit. d Datenschutzgesetz). Daher sind die erhöhten Anforderungen an die gesetzliche Grundlage und an die Amtshilfe zu beachten (§ 5 Datenschutzgesetz): Die Zulässigkeit der Bekanntgabe muss sich aus einer gesetzlichen Grundlage klar ergeben oder die Information muss für die Erfüllung einer gesetzlich klar umschriebenen Aufgabe unentbehrlich sein. In einem zweiten Schritt muss das öffentliche Organ prüfen, ob wesentliche öffentliche oder offensichtlich schützenswerte Interessen einer betroffenen Person oder spezielle Geheimhaltungspflichten die Bekanntgabe verhindern oder einschränken (§ 10 DSG).

Weder bei der Anfrage durch eine Privatperson noch bei der Anfrage durch das Betreibungsamt ist eine gesetzliche Grundlage für die Bekanntgabe ersichtlich. Der Aufenthaltsort eines Inhaftierten kann also nur mit seiner Einwilligung bekannt gegeben werden. In den meisten Fällen dürfte diese nicht vorliegen.

Fragt das Betreibungsamt an, ist zusätzlich die Möglichkeit der Amtshilfe zu prüfen. Diese ist unter folgenden Voraussetzungen zulässig:

1. Die Bekanntgabe des Datums ist zur Erfüllung einer gesetzlich klar umschriebenen Aufgabe unentbehrlich.
2. Die gesetzliche Aufgabe kann vom Datenempfänger nicht auf andere Weise erfüllt werden (Prinzip der Subsidiarität).
3. Die Daten müssen für die Erfüllung der Aufgabe des Empfängers geeignet und erforderlich sein (Prinzip der Verhältnismässigkeit).

Die anfragende Stelle muss darlegen, für welche Aufgaben sie die Daten benötigt. Der bekannt gebenden Stelle obliegt es dann, diese Darlegung summarisch auf ihre Plausibilität zu prüfen.

Im vorliegenden Fall lassen sich die Aufgaben des Betreibungsamtes wie folgt zusammenfassen:

- Der Gläubiger muss dem Betreibungsamt gemäss Art. 67 des Bundesgesetzes über Schuldbetreibung und Konkurs (SchKG) diverse Angaben liefern. Unter anderem muss er Namen und Wohnort beziehungsweise Zustelladresse des Schuldners nennen. Das Betreibungsamt prüft anhand dieser Angaben seine Zuständigkeit. Ist der Betreibungsort der Wohnort, kann aber an dieser Adresse der Zahlungsbefehl nicht zugestellt werden, muss das Betreibungsamt von Amtes wegen seine Zuständigkeit überprüfen. Allenfalls ändert die Zuständigkeit, weil der Schuldner an seinem Aufenthaltsort betrieben werden muss (Art. 48 SchKG).
- Gemäss Art. 60 SchKG muss einem inhaftierten Schuldner, der keinen Vertreter hat, Rechtsstillstand gewährt werden. Dafür braucht das Betreibungsamt die Information, dass sich der Schuldner in Haft befindet.
- Art. 64–66 SchKG regeln die Zustellung der Betreibungsurkunden. Gemäss BGE116 III 8 muss dem Schuldner die Betreibungsurkunde von Angesicht zu Angesicht übergeben werden. Wird dieser am Zustellungsort nicht angetroffen und ist auch keine Ersatzzustellung möglich, kann die Betreibungsurkunde auch nicht korrekt überbracht werden.
- Die Zustellung wird durch öffentliche Bekanntmachung ersetzt, wenn der Wohnort des Schuldners unbekannt ist oder er sich beharrlich der Zustellung entzieht (SchKG 66 Abs. 4). Das Bundesgericht hat strenge Anforderungen an diese so genannte Ediktalzustellung aufgestellt: Sie ist das letzte Mittel, um die Betreibungsurkunde zuzustellen. Sowohl Gläubiger als auch Betreibungsamt haben alle Nachforschungen zu unternehmen, um eine mögliche Zustelladresse des Schuldners ausfindig zu machen.

Unter dem Aspekt der Subsidiarität ist zu prüfen, ob die Aufgaben des Betreibungsamtes nicht auch auf andere, für den inhaftierten Schuldner weniger einschneidende Weise erfüllt werden können:

Je nach Fall könnten die erforderlichen Daten über die Einwohnerkontrolle beschafft werden. Dort ist allenfalls eine bereits bestehende Vormundschaft registriert, so dass die Betreibungsurkunden direkt dem gesetzlichen Vertreter oder der Vormundschaftsbehörde zugestellt werden können (Art. 68c SchKG). Generell müsste das JuV – bevor es den Aufenthaltsort des Inhaftierten bekannt gibt – diesem die Möglichkeit geben, einen Vertreter zu bezeichnen, welchem die Betreibungsurkunden zugestellt werden können. Diese Option ist vor allem dann von Interesse, wenn die Information über den Aufenthaltsort des Schuldners nicht nur seine Inhaftierung betrifft, sondern weitere Informationen wie gesundheitliche Probleme, beispielsweise bei Aufenthalt in einer psychiatrischen Anstalt, beinhaltet. Für die Gewährung des Rechtsstillstandes nach Art. 60 SchKG, wozu das Betreibungsamt verpflichtet ist, dürfte vorderhand die Angabe genügen, dass sich der Schuldner in Haft befindet.

Im Weiteren darf dem Betreibungsamt nur der *Aufenthaltsort* bekannt gegeben werden. Angaben über Grund oder Dauer der Inhaftierung benötigt das Betreibungsamt nicht.

Spezielle Geheimhaltungsbestimmungen, welche eine Datenbekanntgabe im Sinne von § 10 Datenschutzgesetz verhindern, sind nicht ersichtlich. Hingegen können Interessen wie dasjenige des Staates, den Aufenthaltsort des Inhaftierten aus bestimmten Gründen nicht bekannt zu geben, einer Datenbekanntgabe entgegenstehen oder sie einschränken. Die Evaluation der Interessen im Sinne von § 10 Datenschutzgesetz und deren Abwägung obliegen der bekannt gebenden Stelle.

Zu beachten ist, dass die Bekanntgabe des Aufenthaltsortes durch das Betreibungsamt an den Gläubiger ebenfalls eine gesetzliche Grundlage oder die Einwilligung des Schuldners voraussetzt, sonst darf der Aufenthaltsort des Schuldners dem Gläubiger nicht bekannt gegeben werden. Dies muss durch entsprechende Massnahmen sichergestellt werden.

Fazit: Gegenüber einer Privatperson darf der Aufenthaltsort eines Inhaftierten zwecks Anhebung einer Betreibung nur mit dessen Einwilligung bekannt gegeben werden. Im Falle des Betreibungsamtes liegt die Sache anders: Dieses ist zur Erfüllung seiner Aufgaben auf bestimmte Informationen angewiesen. Unter Beachtung der Prinzipien der Subsidiarität und der Verhältnismässigkeit und nach einer Interessenabwägung gemäss §10 Datenschutzgesetz kann das JuV dem Betreibungsamt den Aufenthaltsort des inhaftierten Schuldners bekannt geben. Es empfiehlt sich, die Abläufe bei einer Datenbekanntgabe in Prozessen zu konkretisieren, um den gesetzlichen Anforderungen und den Prinzipien der Subsidiarität und Verhältnismässigkeit Rechnung zu tragen.

Titel: Videoüberwachung
URL: http://www.datenschutz.ch/themen/1273.php
Datum: 17.07.2006

22. Videoüberwachung

Eine Videoüberwachung ist auch bei Vorliegen einer gesetzlichen Grundlage nur dann zulässig, wenn sie verhältnismässig ist. Neben der Bewilligung sind somit rechtliche Rahmenbedingungen sowie konkrete Anweisungen für den Betrieb der Videoüberwachung des Eingangsbereichs der Garderoben auf dem Sportplatz einer Gemeinde zu schaffen.

Eine Gemeinde beabsichtigt, nachdem mehrmals in Garderobenkästen des Sportplatzes eingebrochen wurde, den Eingangsbereich der Garderoben mittels Videokamera zu überwachen.

Der Liegenschaftenausschuss der Gemeinde bewilligte die Installierung der Videokamera mit Beschluss. Zugleich wurden die rechtlichen Rahmenbedingungen sowie die konkreten Anweisungen für den Betrieb der Videoüberwachungsanlage gemäss den Empfehlungen und Checklisten des Datenschutzbeauftragten (www.datenschutz.ch) erstellt und vom Liegenschaftenausschuss genehmigt.

Gemäss § 4 Abs. 3 Datenschutzgesetz müssen Datenbearbeitungen laut dem Grundsatz der Verhältnismässigkeit zur Erfüllung einer öffentlichen Aufgabe geeignet und erforderlich sein. Eine Videoüberwachung zwecks Diebstahlsverhinderung entspricht dieser Bedingung nur, wenn sie einerseits tatsächlich geeignet ist, die Diebstähle zu verhindern (Zwecktauglichkeit) und andererseits diejenige Massnahme darstellt, welche die Interessen der betroffenen Personen am meisten schont.

Eine Videoüberwachung von Garderoben ist in der Regel weder notwendig noch geeignet, um Diebstähle zu verhindern. Sie kann erst in Betracht gezogen werden, wenn andere Massnahmen, welche weniger in die Privatheit von betroffenen Personen eingreifen, nachweislich versagt haben. Der angestrebte Zweck, Diebstähle zu verhindern, kann auf einfache Weise mit anderen, weniger weit gehenden Mitteln erreicht werden, beispielsweise mit abschliessbaren Garderobenkästen und -räumen. Erst nachdem solche Massnahmen versagt haben, ist eine Videoüberwachung verhältnismässig. Ihr Einsatz ist auf diejenigen Zeiten zu beschränken, zu welchen die früheren Diebstähle stattfanden.

Titel: Kostenlosigkeit der Auskunft
URL: http://www.datenschutz.ch/themen/1274.php
Datum: 17.07.2006

23. Kostenlosigkeit der Auskunft

Die Auskunft gemäss Datenschutzgesetz ist ohne Kostenauflage zu erteilen. Eine Kostenauflage für das Auskunftsrecht rechtfertigt sich nur, wenn für die Auskunftserteilung ein besonders grosser Arbeitsaufwand nötig ist.

Immer wieder erhalten wir Anfragen, ob Verwaltungsstellen aufgrund von § 13 des Verwaltungsrechtspflegegesetzes Gebühren verlangen dürfen, wenn Bürgerinnen und Bürger ihr Auskunftsrecht in Bezug auf sie betreffende Daten geltend machen. Dazu haben wir bereits früher verschiedentlich Stellung genommen (vgl. Fakten 3 [2000], S. 11 f. und Tätigkeitsberichte Nr. 6 [2000], S. 37 und Nr. 7 [2001], S. 19.) Wir sind der Meinung, dass in Anlehnung an die Bundesgesetzgebung für Auskunftsbegehren grundsätzlich keine Kosten auferlegt werden sollten. Eine Kostenauflage rechtfertigt sich nur, wenn für die Auskunftserteilung ein besonders grosser Arbeitsaufwand nötig ist. Eine gerichtliche Klärung dieser Grundsatzfrage für den Kanton Zürich ist unseres Wissens aber noch nicht erfolgt. Der Entwurf für ein Informations- und Datenschutzgesetz (IDG) sieht die Kostenlosigkeit der Auskunft über die eigenen Daten explizit vor.

Titel: Online-Zugriffe auf Daten der Gebäudeversicherung
URL: http://www.datenschutz.ch/themen/1275.php
Datum: 17.07.2006

24. Online-Zugriffe auf Daten der Gebäudeversicherung

Die Gebäudeversicherung darf einer Bank nur für diejenigen Daten einen Online-Zugriff einrichten, für welche die Einwilligung der betroffenen Person vorliegt. Ein Zugriff für die Kantonspolizei ist mangels gesetzlicher Grundlagen unzulässig.

Die Gebäudeversicherung des Kantons Zürich bat den Datenschutzbeauftragten, die Rechtmässigkeit zweier Abrufverfahren abzuklären: Einerseits ging es um den Online-Zugriff auf Gebäudedaten durch eine Bank, andererseits um den Ausbau einer bereits bestehenden Zugriffsmöglichkeit der Kantonspolizei Zürich.

Im Zusammenhang mit Hypothekargeschäften beziehen diverse Banken regelmässig Gebäudedaten bei der GVZ. Diese wollte aus Ressourcengründen den Vorgang modernisieren und den im Hypothekargeschäft tätigen Banken die Daten per gesichertem Internetzugang zur Verfügung stellen. Die Bank sollte dabei potentiellen Zugriff auf Gebäudedaten aller Personen im Kanton Zürich erhalten, sich aber verpflichten müssen, nur auf diejenigen zuzugreifen, die in einem direkten Zusammenhang mit einem Kundengeschäft stehen und bei denen ein ausdrückliches Einverständnis der betroffenen Person für den Datenzugriff vorliegt. Die Einhaltung dieser Verpflichtungen sollte von der Abteilung Datenlogistik / Gebäudedaten mittels Überprüfung der Protokollierungen gewährleistet werden.

Die Kantonspolizei Zürich verfügte bereits über einen Online-Zugriff auf bestimmte GVZ-Daten. Neu wünschte sie zusätzlich eine personenbezogene Suchmöglichkeit. Das hätte ihr erlaubt, alle Gebäude abzufragen, welche im Eigentum einer bestimmten Person stehen. Die Daten hätten für die polizeiliche Ermittlungstätigkeit verwendet werden sollen.

Gemäss § 8 DSG dürfen öffentliche Organe Personendaten bekannt geben, wenn dafür gesetzliche Grundlagen bestehen, die Daten für den Empfänger im Einzelfall zur Erfüllung seiner öffentlichen Aufgaben notwendig sind, die betroffene Person im Einzelfall eingewilligt hat oder ihre Einwilligung nach den Umständen vorausgesetzt werden darf oder wenn die betroffene Person ihre Daten allgemein zugänglich gemacht hat. Gemäss § 10 lehnt das öffentliche Organ die Bekanntgabe ab, schränkt sie ein oder verbindet sie mit Auflagen, wenn wesentliche öffentliche oder offensichtlich schützenswerte Interessen einer betroffenen Person, gesetzliche Geheimhaltungsbestimmungen oder besondere Datenschutzvorschriften es verlangen.

Bereits 1997 liess der Datenschutzbeauftragte mit einem Rechtsgutachten abklären, welchen Anforderungen die Bestimmtheit einer Rechtsgrundlage genügen muss, die ein Abrufverfahren (Online-Zugriff) legitimieren soll: Für ein Abrufverfahren von besonders schützenswerte Personendaten ist ein Gesetz im formellen Sinne nötig. Für den Online-Zugriff auf andere Personendaten genügt ein Gesetz im materiellen Sinne, sofern es sich dabei um eine Delegationsverordnung handelt. Die gesetzlichen Grundlagen müssen mindestens die Tatsache des Abrufverfahrens, die berechtigten Behörden und den Umfang der abrufbaren Daten festhalten.

Für das Abrufverfahren der Bank sind keine Rechtsgrundlagen ersichtlich (Art. 111m der Verordnung betreffend das Grundbuch kann in diesem Fall nicht beigezogen werden). Daher kommt nur die Bekanntgabe auf der Grundlage einer Einwilligung der betroffenen Person im Einzelfall in Frage. Dabei dürfen ausschliesslich diejenigen Daten bekannt gegeben werden, für welche eine Einwilligung vorliegt. Dabei ist zu beachten, dass bereits bei der Einrichtung des Abrufverfahrens, das heisst bei der Erteilung der Zugriffsberechtigungen eine Datenbekanntgabe vorliegt. Die Protokollierung der Zugriffe und entsprechende Kontrollen stellen angemessene Sicherheitsmassnahmen im Sinne von § 4 Abs. 5 DSG dar, vermögen aber für sich allein nicht zu genügen. Die Zugriffsmöglichkeiten müssen auf diejenigen Personen beschränkt werden, welche ihre Einwilligung erteilt haben, und auch in diesen Fällen braucht es eine zeitliche und/oder qualitative Beschränkung.

Die Daten, welche die Kantonspolizei abrufen kann, werden für die polizeiliche Ermittlungstätigkeit verwendet und müssen somit als besonders schützenswert eingestuft werden (§ 2 lit. d Datenschutzgesetz). Demzufolge ist für dieses Abrufverfahren eine formellgesetzliche Grundlage notwendig.

Die §§ 22 StPO und 72 a GVG, die Kantonspolizeiverordnung sowie das Dienstreglement für das Polizeikorps des Kantons Zürich genügen den oben genannten Anforderungen nicht. Weder die Tatsache des Abrufverfahrens noch die berechtigten Behörden oder der Umfang der abrufbaren Daten sind in einem Gesetz im formellen Sinn festgehalten. Aus denselben Gründen vermag auch die GIS-Verordnung den Anforderungen nicht zu genügen und § 9 a Abs. 2 des Gesetzes über die Gebäudeversicherung hält nur in sehr allgemeiner Form fest, dass die Anstalt den Gemeinden, den Grundbuch- und Vermessungsämtern sowie den kantonalen Amtsstellen diejenigen Daten mitteilt, welche diese für die Erfüllung ihrer Aufgaben benötigen. Unseres Erachtens bildet diese Bestimmung nur die Grundlage für Amtshilfe im Einzelfall und stellt ebenfalls keine Legitimation für regelmässige Datenbekanntgaben beziehungsweise Abrufverfahren dar.

Dabei ist es irrelevant, dass der Kantonspolizei keine Personensuche, sondern nur eine Suche nach Gebäuden zur Verfügung steht, denn bereits durch die bestehende Zugriffsmöglichkeit wurden personenbezogene Daten zugänglich gemacht.

Weitere Ausführungen dazu finden sich in den Tätigkeitsberichten Nr. 4 [1998], S. 41 f. und Nr. 6 [2000], S. 35.

Die GVZ verzichtete in der Folge auf das Einrichten des Abrufverfahrens für Banken. Der Online-Zugriff der Polizei blieb bestehen, jedoch wurde die personenbezogene Suchmöglichkeit nicht eingerichtet.

Titel: Fahrzeughalterdaten im Internet
URL: http://www.datenschutz.ch/themen/1276.php
Datum: 17.07.2006

25. Fahrzeughalterdaten im Internet

Unter der Internetadresse www.autoindex.zh.ch und über die Website des Strassenverkehrsamtes können die Daten der rund 800 000 Fahrzeughalterinnen und -halter im Kanton Zürich abgefragt werden. Diese Möglichkeit entspricht nicht den datenschutzrechtlichen Vorschriften.

Gesetzliche Grundlage

Das kantonale Datenschutzgesetz (DSG ZH) verlangt in § 8 für die Bekanntgabe von Personendaten entweder eine gesetzliche Grundlage oder die Einwilligung der betroffenen Person, von der im vorliegenden Fall nicht ausgegangen werden kann.

Gemäss eidgenössischer Verkehrzulassungsverordnung (VZV) sind die von den Kantonen und Bundesstellen zu führenden Register und Kontrollen im Strassenverkehr nicht öffentlich (Art. 125 Abs. 1 VZV); Auskünfte werden nur Behörden erteilt. Eine Ausnahme bilden diejenigen über Fahrzeugzulassungen: Art. 126 Abs. 1 VZV erlaubt, dass Name und Adresse von Inhabern eines Kontrollschildes jedermann bekannt gegeben werden. Gemäss Art. 104 Abs. 5 Satz 2 des Strassenverkehrsgesetzes (SVG) kann das Verzeichnis der Namen der Fahrzeughalter veröffentlicht werden.

Der Begriff der Öffentlichkeit ist im konkreten Fall jedoch auslegungsbedürftig. Die öffentliche Auflage auf der Amtsstelle oder die Veröffentlichung in einem Verzeichnis in Buchform entsprechen nicht der Öffentlichkeit des Internets, das sich in der Art des Zungangs und in der Anzahl der Adressaten gravierend von gedruckten Publikationen unterscheidet. Zudem lassen sich im Internet publizierte Daten automatisiert durchsuchen, abspeichern und weiterverarbeiten; eine Kontrolle über die Verwendung des Datenbestandes ist praktisch ausgeschlossen und die Bekanntgabe von Personendaten in Länder ohne gleichwertiges Datenschutzniveau nicht zu verhindern.

Zu beachten ist auch, dass die Bereitstellung von Daten via Internet ein Abrufverfahren im Sinne von Art. 19 Abs. 3 des eidgenössischen Datenschutzgesetzes (DSG Bund) darstellt.

Die in Art. 126 Abs. 1 VZV geregelte Bekanntgabe von Namen und Adresse an jedermann sowie die in Art. 104 Abs. 5 SVG legitimierte Veröffentlichung in einem Verzeichnis stellen in Verbindung mit Art. 19 Abs. 3 Datenschutzgesetz Bund daher keine genügende rechtliche Grundlage für eine Bereitstellung der Daten auf dem Internet dar.

In diesem Zusammenhang ist darauf hinzuweisen, dass es sich beim Namen und der Adresse sowie der Kontrollschildnummer grundsätzlich nicht um besonders schützenswerte Personendaten handelt. Vorliegend geht es jedoch nicht nur um die Bekanntgabe dieser Daten. In der Regel wird ein Fahrzeug vom Halter oder der Halterin benutzt und bei der Adresse handelt es sich um die feste Wohnadresse. Die Verknüpfung dieser Angaben mit dem sich ändernden Standort des Fahrzeuges lässt verschiedene Rückschlüsse zu.

Zweckbindung

Die Bekanntgabe von Daten hat, wie jede andere Datenbearbeitung, dem Grundsatz der Zweckbindung zu entsprechen (§ 4 Abs. 4 Datenschutzgesetz ZH). Dies bedeutet vorliegend, dass Halterauskünfte nur für rechtlich zulässige Verwendungen im Zusammenhang mit dem Strassenverkehr bekannt gegeben und von der Empfängerin oder dem Empfänger nur zu diesem Zweck genützt werden dürfen. Jede anderweitige Verwendung, seien es kommerzielle Absichten oder auch bloss die Befriedigung von Neugier, ist nicht statthaft. Eine Kontrolle des Verwendungszweckes ist bei der Vielzahl (anonymer) Anfragen, wie dies bei einem Internetabrufverfahren der Fall ist, völlig ausgeschlossen.

Datensicherheit

Gemäss § 4 Abs. 5 Datenschutzgesetz ZH sind Daten durch angemessene organisatorische und technische Massnahmen gegen unbefugtes Bearbeiten zu schützen. Die im Internet eingebauten technischen Hürden zur Eindämmung der erwarteten Missbräuche können jedoch ohne Weiteres umgangen werden: Mit geeigneter Software ist es möglich, die zu Beginn einer Abfragesession als Grafik präsentierte Zahl einzulesen. Versierte Benutzer können dieses Hindernis umgehen und einen automatisierten Zugang aufbauen. Durch Löschen des Cookies kann die zahlenmässige Beschränkung der Abfrage auch von Laien problemlos ausgehebelt werden. Die Datensicherheit ist somit nicht gewährleistet.

Datensperre

Ende 2004 waren im Kanton Zürich knapp 800 000 Motorfahrzeuge immatrikuliert. Die Fahrzeughalterinnen und -halter wurden mit einem Schreiben Mitte November 2005 zwar informiert, dass als neue Dienstleistung Halterauskünfte über das Internet abrufbar sind. Es wurde jedoch nicht auf den Umstand hingewiesen, dass § 11 Datenschutzgesetz ZH jeder betroffenen Person ein Sperrrecht einräumt.

Erhöhte Missbrauchsgefahr

Mit der Einrichtung eines für jedermann via Internet zugänglichen Abrufverfahrens steigt die Gefahr, dass die Daten zweckentfremdet verwendet werden, erheblich:

- Die Daten von rund 800 000 Fahrzeughalter sind rund um die Uhr weltweit auf einfachste Weise erhältlich.
- Sie können auf allen – auch mobilen – Geräten, mit welchen Zugang zum Internet möglich ist, bezogen werden.
- Die elektronischer Form der Datenbekanntgabe erlaubt eine unbeschränkte Weiterverarbeitung.
- Die technischen Hindernisse zur Umgehung von Beschränkungen des Abrufs sind leicht zu umgehen.

Folgende Beispiele mögen die erhöhte Missbrauchsgefahr verdeutlichen:

- Die Wohnadresse von Fahrzeughaltern, die mit dem Fahrzeug unterwegs sind, kann überall und jederzeit in Erfahrung gebracht werden. Dieser Umstand kann für Einbrüche am Wohnort ausgenutzt werden.

- Zu nächtlicher Stunde wird eine Automobilistin ohne es zu merken auf ihrer Fahrt verfolgt. Ihre Wohnadresse – das vermutete Ziel ihrer Fahrt – kann sofort abgefragt werden. Für Belästigungen aller Art werden neue Türen geöffnet.
- Es lässt sich herausfinden, ob es sich beim Personenwagen um ein Geschäftsauto oder einen Mietwagen handelt.
- Eine kommerzielle Verwertung der aus dem Internet bezogenen Daten kann kaum verhindert werden.
- Daten der Fahrzeughalter lassen sich mit anderen Datenbeständen (Telefonverzeichnis, GIS-Daten) automatisiert auswerten. Für kommerzielle Zwecke wie auch bei der logistischen Unterstützung von Straftaten ergeben sich neue Möglichkeiten.

Errichtung einer Datensperre

Den betroffenen Fahrzeughalterinnen und -haltern empfiehlt der Datenschutzbeauftragte, beim Strassenverkehrsamt eine Datensperre zu errichten. § 11 Datenschutzgesetz ZH enthält dazu folgende Regelung:

Die betroffene Person kann die Bekanntgabe ihrer Daten an private Personen und Organisationen sperren lassen.
Die Bekanntgabe ist trotz Sperrung zulässig, wenn
a) das öffentliche Organ hiezu gesetzlich verpflichtet ist oder
b) die gesuchstellende Person oder Organisation glaubhaft macht, dass die Sperrung sie in der Verfolgung eigener Rechte gegenüber der betroffenen Person behindert.

Die Datensperre wirkt somit gegenüber Privaten nicht absolut und entfaltet keine Wirkung bei Anfragen von anderen Amtsstellen (vorliegend vorab Polizei und Strafuntersuchungsbehörden). Der unkontrollierten Datenabfrage über das Internet wird jedoch ein Riegel vorgeschoben: Das Strassenverkehrsamt sperrt die Daten für die Internetabfrage.

Will eine betroffene Person die Bekanntgabe ihrer Daten an private Personen und Organisationen sperren lassen, muss sie dies den verantwortlichen Organen schriftlich mitteilen (§ 7 Datenschutzverordnung). Das Strassenverkehrsamt stellt ein entsprechendes Formular zur Verfügung.

Titel: Sozialhilfestatistik
URL: http://www.datenschutz.ch/themen/1277.php
Datum: 17.07.2006

26. Sozialhilfestatistik

Die Angaben für die Sozialhilfestatistik dürfen für die Übermittlung von der Gemeinde an das Bundesamt für Statistik nur die zur Identifikation absolut notwendigen Daten enthalten. Dazu gehören die Dossiernummer, das Erhebungsjahr, das Aufnahmedatum sowie die AHV-Nummer.

Der Datenschutzbeauftragte hat bei der Sozialhilfestatistik für seinen Zuständigkeitsbereich folgende Empfehlung erlassen:

«Empfehlungen für die Bekanntgabe von Personendaten im Zusammenhang mit der Schweizerischen Sozialhilfestatistik vom 30. Januar 2001:

Für Datenbearbeitungen zu statistischen Zwecken gelten gegenüber den allgemeinen Datenschutzgrundsätzen erleichterte Voraussetzungen gemäss § 12 Datenschutzgesetz (DSG). Danach dürfen Personendaten für nicht personenbezogene Zwecke bekannt gegeben werden, wenn keine Geheimhaltungspflicht oder andere Bestimmung dies ausschliesst und Rückschlüsse auf die betroffenen Personen möglichst erschwert sind (§ 12 Abs. 2 DSG).

Die Gemeinden und Kantone sind gemäss den Bestimmungen des Bundesstatistikgesetzes sowie der dazugehörigen Verordnung verpflichtet, den Bund beim Aufbau der Sozialhilfestatistik zu unterstützen.

Die Personendaten, welche vom Bundesamt für Statistik (BFS) für die Sozialhilfestatistik benötigt werden, beruhen auf den Angaben, welche der bzw. die Hilfesuchende gegenüber der Sozialbehörde gestützt auf seine bzw. ihre Auskunfts- und Mitwirkungspflicht bereits im Rahmen seines Gesuches gemacht und schriftlich bestätigt hat (§18 Sozialhilfegesetz, §§ 27 und 28 Sozialhilfeverordnung). Es werden somit Personendaten bekannt gegeben, welche bereits in einem früheren Zeitpunkt erhoben wurden. Die Bekanntgabe wird zudem nicht durch entgegenstehende Geheimhaltungsvorschriften ausgeschlossen. Die dem BFS für die Sozialhilfestatistik zur Verfügung gestellten Personendaten werden anonymisiert, womit ein späterer Rückschluss auf betroffene Personen ausgeschlossen wird.

Da es sich bei den vom BFS benötigten Personendaten um äusserst sensible bzw. besonders schützenswerte Daten handelt, sind bei der Datenbekanntgabe durch die Gemeinde die folgenden Punkte zu beachten:

- Die für die Datensammlung der Sozialbehörde verantwortliche Person oder deren Stellvertretung gibt dem BFS die für die Sozialhilfestatistik benötigten Personendaten bekannt.
- Es dürfen nur die vom BFS verlangten Daten bekannt gegeben werden.
- Die Daten müssen richtig und vollständig sein.
- Verfügt die Gemeinde nicht über eine EDV-Unterstützung, muss der schriftliche Erhebungsbogen des BFS ausgefüllt werden.

- Verfügt die Gemeinde über eine Fallführungssoftware oder arbeitet sie mit Sostat, ist im entsprechenden EDV-Programm bereits ein Exportmodul integriert. Die verantwortliche Person speichert die vom BFS benötigten Daten auf einer Diskette. Die Daten werden dabei automatisch verschlüsselt.
- Die schriftlichen Erhebungsbogen müssen dem BFS in verschlossenen Couverts geschickt werden. Es dürfen keine Fenstercouverts verwendet werden.
- Die Disketten sind dem BFS in verschlossenen Couverts zuzustellen.
- Weder die schriftlichen Erhebungsbogen noch die Disketten dürfen kopiert werden.
- Nur die für die Datensammlung der Sozialbehörde verantwortliche Person oder deren Stellvertretung darf in die schriftlichen Erhebungsbogen oder die Disketten Einsicht nehmen.
- Es darf weder anderen Behörden noch Dritten Einsicht in die bekannt gegebenen Daten gewährt werden.»

Einzelne Personen machen geltend, beim Versand der Erhebungsbogen per Briefpost werde der Datenschutz nicht eingehalten. Sie sind der Meinung, die Trennung des Identifikationsblattes vom Rest des Erhebungsbogens und der separate Versand von Erhebungsbogen und Identifikationsblatt an das Bundesamt für Statistik (BFS) stellten keine genügende Datenschutzmassnahme dar.

Entsprechend § 4 Abs. 3 Datenschutzgesetz müssen Datenbearbeitungen gemäss dem Grundsatz der Verhältnismässigkeit zur Erfüllung einer öffentlichen Aufgabe geeignet und erforderlich sein. Dies gilt auch für das Bearbeiten zu nicht personenbezogenen Zwecken im Rahmen der Statistik gemäss § 12 Datenschutzgesetz.

Vom Erhebungsbogen in das Identifikationsblatt werden die Dossiernummer, die AHV-Nummer, das Erhebungsjahr und das Aufnahmedatum übertragen.

Gemäss den Angaben der Durchführungsstelle für die Sozialhilfestatistik BFS im Kanton Zürich verschicken nahezu alle Gemeinden die Erhebungsbogen elektronisch in verschlüsselter Form. Ein Versand in Papierform findet nur noch vereinzelt statt. Die vier zu übertragenden Angaben sind zur zuverlässigen Identifizierung und korrekten Erfassung für die Statistik unabdingbar. Ein Verzicht auf eine der Angaben verunmöglicht den Zweck der Sozialhilfestatistik. Die meisten Gemeinden, welche noch von einer Papiererhebung mit entsprechendem Versand Gebrauch machen, verschicken beide Bogen zudem eingeschrieben. Unbefugte Dritte dürfen zur Wahrung des Brief-, des Amts- sowie des Statistikgeheimnisses weder bei der Post noch in der Gemeindeverwaltung oder im Bundesamt für Statistik Zugang zu den Erhebungsbogen haben.

Somit sind die vier zu übertragenden Angaben für die Aufgabenerfüllung der Sozialhilfestatistik geeignet und erforderlich. Zudem ist davon auszugehen, dass die Empfehlungen für die Bekanntgabe von Personendaten im Zusammenhang mit der Schweizerischen Sozialhilfestatistik vom 30. Januar 2001 befolgt werden.

Titel: Personendaten-Pool
URL: http://www.datenschutz.ch/themen/1278.php
Datum: 17.07.2006

27. Personendaten-Pool

Die Schaffung von zentralen Personendatensammlungen, auf die verschiedene Amtsstellen Zugriff haben, so genannte Personendaten-Pools, sind nur zulässig, wenn entsprechende gesetzliche Grundlagen vorhanden sind.

Wenn eine Einwohnerin oder ein Einwohner aus einer Gemeinde wegzieht, erfasst diese den neuen Wohnort als so genannten «Wegzugsort». Das Steueramt der Gemeinde benötigt unter Umständen auch spätere Wegzugsadressen.

Weil der IT-Dienstleister einer Gemeinde alle Personenstammdaten (Name, Adresse etc.) in einem Pool führte, wurden die späteren Wegzugsorte beziehungsweise -adressen, welche das Steueramt erfasste, auch in der Applikation der Einwohnerkontrolle mutiert. Grund für diesen Pool war die Überlegung, dass Daten auf diesem Weg nicht mehrfach gespeichert werden müssen und alle Amtsstellen über die gleichen aktuellen Personendaten verfügen. Die Folge war einerseits, dass die Einwohnerkontrolle nun nicht mehr über den ersten Wegzugsort nach dem Auszug verfügte, sondern über den jeweils aktuellen Wohnort. Dadurch konnten Wegzugsbescheinigungen nicht mehr korrekt ausgestellt werden. Andererseits stellen solche Mutationen auch Datenbekanntgaben durch das Steueramt an die Einwohnerkontrolle dar. Dafür jedoch braucht es gesetzliche Grundlagen.

Datenschutzbeauftragter des Kantons Zürich
Postfach, 8090 Zürich
Tel.: 043 259 39 99
Fax: 043 259 51 38
datenschutz@dsb.zh.ch
www.datenschutz.ch

Datenschutzbeauftragter
Dr. iur. Bruno Baeriswyl

Stellvertreter
lic. iur. Beda Harb

Juristisches Sekretariat
lic. iur. Barbara Mathis
lic. iur. Karin Schoch
lic. iur. Karin Brunner Steib

IT-Revision und -Kontrolle
Andrea C. Mazzocco, CISA

Beratungsstelle für Informatiksicherheit (BIS)
Oliver Wyler, NDS FH Informatiksicherheit

Sekretariat
Martina Richard

Tätigkeitsbericht Nr. 11 (2005)
ISSN 1422-5816

Konzeption und Produktion
Fabian Elsener Mediengestaltung, Zürich

Druck
KDMZ
Gedruckt auf Recyclingpapier

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

www.datenschutz.ch