Nummer 14

Tätigkeitsbericht 1.–9.2008*

*letzte Berichterstattung nach Datenschutzgesetz (DSG)

dsb
datenschutzbeauftragter
kanton zürich

Nummer 14
Tätigkeitsbericht 2008

Der Datenschutzbeauftragte erstattet dem Regierungsrat jährlich oder nach Bedarf einen Bericht über seine Tätigkeit (§ 23 Datenschutzgesetz [DSG]). Der vorliegende Tätigkeitsbericht Nr. 14 [2008] ist die letzte Berichterstattung nach DSG und deckt den Zeitraum vom 1. Januar bis 30. September 2008 ab. Die nächste Berichterstattung wird sich nach dem Gesetz über die Information und den Datenschutz (IDG) richten, das per 1. Oktober 2008 in Kraft getreten ist.

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

Zürich, Januar 2009

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

Klare Rahmenbedingungen erforderlich

Das Recht auf Privatheit muss auf Gesetzesstufe konkretisiert werden.
Dies ist notwendig, um den Datenschutz effektiv und effizient umzusetzen.

Der vorliegende 14. Tätigkeitsbericht ist der letzte unter dem Datenschutzgesetz (DSG), das am 1. Oktober 2008 durch das Informations- und Datenschutzgesetz (IDG) abgelöst wurde. Dass ein Gesetz nach 14 Jahren bereits ersetzt wird, ist ungewöhnlich; im Bereich des Datenschutzes ist dies jedoch die Reaktion auf eine rasante gesellschaftliche und technologische Entwicklung.

Auf der gesellschaftlichen Ebene hat die Information als eigenständige Ressource markant an Bedeutung gewonnen. Die Informations- und Kommunikationsgesellschaft ist Wirklichkeit geworden. Sie erfordert einen umfassenden Blick auf den Umgang mit Informationen. Dazu zählt einerseits die Regelung des Zugangs zu den Informationen und andererseits – als Kehrseite derselben Medaille – die Festlegung der Schutzmechanismen für die Informationen.

Auf der technischen Ebene ist eine Entwicklung erfolgt, die bereits beim Inkrafttreten des DSG erkennbar war, deren Ausmass und Bedeutung auf die Informationsbearbeitung jedoch erst an Konturen gewinnt. Was mit dem Internet begann, zeichnet sich heute als allgegenwärtige und vernetzte Informationsbearbeitung ab. Das DSG, das noch auf einer Konzeption der Datenbearbeitung aus den 1960er Jahren beruhte, konnte auf diese Entwicklung keine Antwort geben.

Der Kanton Zürich hat mit dem IDG nicht nur das revisionsbedürftige DSG abgelöst, sondern auch eine moderne Gesetzgebung für die Informationsbedürfnisse von Gesellschaft und Verwaltung geschaffen, die in dieser Form in der Schweiz wegbereitend ist.

Blick zurück als Blick voraus

Im Rückblick zeigen sich die rund 14 Jahre des DSG als eine auch mit Blick auf die Zukunft des Datenschutzes sehr lehrreiche Phase. Drei Aspekte stehen im Vordergrund.

Bei den Diskussionen um den Datenschutz in der Schweiz stellte sich lange Zeit die Frage, ob eine spezifische Gesetzgebung geschaffen werden soll. Denn das Recht auf persönliche Freiheit und Privatsphäre hatte mit der Europäischen Menschenrechtskonvention (EMRK) und als ungeschriebenes Verfassungsrecht respektive im Zivilgesetzbuch seinen festen Platz in der Rechtsordnung. Wieweit der Datenschutz auf Gesetzesstufe konkretisiert werden sollte, war entsprechend umstritten. Die Grosscomputer, die in den 1960er Jahren aufkamen, führten zu ersten Überlegungen, dass konkretisierende Rahmenbedingungen für

Datenbearbeitungen zu schaffen seien. Erste Datenschutzgesetze entstanden in europäischen Ländern und in einzelnen Kantonen in den 1970er und 1980er Jahren. Als der Bund 1993 und der Kanton Zürich 1995 ihre entsprechenden Gesetze in Kraft setzten, bestand noch immer kein Konsens über deren Notwendigkeit: Die Gesetze wurden von den datenbearbeitenden Stellen mit Skepsis aufgenommen, im Gegensatz zur Bevölkerung, die im Kanton Zürich dem DSG mit einem Ja-Stimmen-Anteil von 76 Prozent zustimmte.

Rückblickend zeigt sich, dass die Konkretisierung des Rechts auf Privatheit auf Gesetzesstufe ein wichtiger Schritt war. Die datenbearbeitenden Stellen wurden sich über die Risiken der Datenbearbeitungen für die Privatheit der Bürgerinnen und Bürger bewusst und begannen, entsprechende rechtliche, organisatorische und technische Massnahmen für den Datenschutz zu treffen. Natürlich ist diese Phase nicht nur reibungslos verlaufen; vielfach brauchte es neben den Interventionen des Datenschutzbeauftragten auch die Hartnäckigkeit einzelner betroffener Personen, um den Datenschutz zu gewährleisten. Angesichts der zunehmend komplexen Informationsbearbeitungen ist indessen heute allen klar, dass Rahmenbedingungen notwendiger denn je sind. Besonders in sensitiven Bereichen – beispielsweise im Gesundheitswesen – macht sich deren Fehlen für die betroffenen Personen spürbar negativ bemerkbar.

Bei all den Diskussionen um die Konkretisierung des Datenschutzes wurde der Schutz der Privatheit der Bürgerinnen und Bürger nie grundsätzlich in Frage gestellt. Vielmehr konnte – und kann – von einer Grundakzeptanz des Schutzes der Privatheit als Fundament einer liberalen Gesellschafts-, Wirtschafts- und Rechtsordnung ausgegangen werden. Der Geheimnisschutz – beispielsweise das Bankkundengeheimnis, das Steuergeheimnis, das Patientengeheimnis – und die informationelle Selbstbestimmung – also das Recht, selbst zu bestimmen, welche privaten Informationen man preisgegeben möchte – sind fundamentale Bestandteile der autonomen Lebensgestaltung in der liberalen Gesellschaft. Der Staat hat hier nicht nur eine wichtige ordnungspolitische Rolle, sondern als Datenbearbeiter in zahlreichen sensitiven Bereichen auch eine Vorbildfunktion. Gerade die Auseinandersetzung mit dem Datenschutz bei der Umsetzung des DSG bot unzählige Gelegenheiten, diese grundsätzliche Ausgangslage anzusprechen. Damit konnte auch der Datenschutz als Fundament der liberalen Gesellschaft gestärkt werden. Gerade die Entwicklung zur Informations- und Kommunikationsgesellschaft rief immer wieder Apologeten auf den Plan, die das Ende der Privatsphäre predigten – doch ihre Aufrufe sind schnell verhallt. Denn ohne Privatheit ist eine liberale Gesellschaft kaum denkbar.

Die technologische Entwicklung der letzten Jahre beinhaltet zahlreiche Herausforderungen für den Schutz der Privatheit der Bürgerinnen und Bürger. Der Technologie wurde deshalb aus Datenschutzsicht vielfach skeptisch begegnet. Die Praxis zeigt jedoch, dass weniger die Technologien als deren Anwendung neue Datenbearbeitungen ermöglichten, die immer stärker in die Privatheit der einzelnen Personen eingriffen. Jede Nutzung der Informations- und Kommunikationstechnologie hinterlässt Datenspuren, und Anwendungsprogramme können eine Vielzahl von Daten auswerten, mit denen Persönlichkeitsprofile erstellt werden können. Die Allgegenwärtigkeit des Computers wird diese Tendenz noch verschärfen. Nicht die Technologie zeigt sich als Problem, sondern ihre Anwendung.

Das DSG – wie auch die übrigen schweizerischen Datenschutzgesetze – standen der technologischen Entwicklung unbeholfen gegenüber und zogen sich auf eine Technikneutralität zurück. Doch gerade bei Datenbearbeitungen braucht es konkretisierende Rahmenbedingungen für den Einsatz der Technologie: Neue gesetzgeberische Instrumente sind notwendig, die sowohl die Hersteller von neuen Technologien als auch die Datenbearbeiter dazu bringen, datenschutzfreundliche Technologien zu entwickeln und deren Einsatz zu fördern. Es ist nicht anders als beim Strassenverkehr, der sich an die Rechtsnormen und mit entsprechenden Technologien auch an die Umweltnormen zu halten hat.

Die Erfahrung, dass das Datenschutzrecht in Bezug auf die Technologie nicht genügend wirksam ist, hat im Kanton Zürich dazu geführt, dass das IDG neue, auf die Technologie bezogene Instrumente gefunden hat.

Effektivität und Effizienz

Die Ablösung des DSG durch das IDG ist eine Konsequenz aus diesen Entwicklungen: Das IDG bringt eine umfassende Betrachtung der Informationsordnung unter Einbezug der technischen Entwicklung. Es wird sich zeigen, wie sich die neuen Instrumente – neben den Bestimmungen, die aus dem DSG übernommen werden konnten – bewähren werden. Bereits unter dem DSG haben sich drei Bereiche herausgeschält, die auch unter dem IDG nicht ausser Acht zu lassen sind:

Die Effektivität der datenschutzrechtlichen Rahmenbedingungen für den Schutz der Privatheit der Bürgerinnen und Bürger wird auch künftig im Vordergrund stehen. Entwicklungen, die einen massiven Eingriff in die Privatheit befürchten lassen, müssen rechtzeitig gestoppt oder datenschutzfreundlich umgesetzt werden. In der Vergangenheit hat sich oft gezeigt, dass in einem Projekt gravierende Folgen für die Privatheit der Bürgerinnen und Bürger geschaffen wurden, weil es nur punktuell betrachtet wurde. Mit dem IDG wurde nun das Instrument der Vorabkontrolle eingeführt, das hier Abhilfe schaffen kann.

Auch weiterhin wird den datenschutzrechtlichen Anliegen entgegengehalten werden, dass sie die Effizienz eines Projektes in Frage stellten. Hier wird vermehrt auf die Bedeutung des Schutzes der Privatheit in der Informations- und Kommunikationsgesellschaft hinzuweisen sein. Die Betrachtung der Effizienz darf sich nicht nur auf ein einzelnes Projekt beziehen, sondern muss den Schutz der persönlichen Freiheit der Bürgerinnen und Bürger über die gesamte staatliche Tätigkeit miteinbeziehen. Eine aufeinander abgestimmte Betrachtung der Informationsordnung, wie sie das IDG beinhaltet, räumt dem Datenschutz den notwendigen Platz ein, selbst wenn dies für ein einzelnes Projekt eine Einschränkung bedeutet.

Damit ist auch ein dritter Bereich angesprochen: Anliegen der inneren und äusseren Sicherheit haben bei der Gesetzgebung in den letzten Jahren regelmässig zu Interessenabwägungen zulasten der Privatheit geführt. Fast ausnahmslos wurde akzeptiert, dass für mehr Sicherheit die Privatheit eingeschränkt wird. Die längerfristigen Auswirkungen dieser Entwicklung wurden indes nicht berücksichtigt. Dabei ist allen klar, dass Sicherheit nicht annähernd zu 100 Prozent garantiert werden kann, auch nicht mit Einschränkungen der Privatheit. Die Einschränkung der Privatheit bedeutet hingegen eine Abwertung der Grundwerte der liberalen Gesellschaft, weshalb sich die Frage stellt, welche Freiheits-

werte die Gesellschaft der Bedrohung entgegenzusetzen hat. Auch wenn hier ein gesellschaftlicher Konsens für die persönlich Freiheit besteht, war bei der Umsetzung des DSG im Speziellen und des Datenschutzes im Allgemeinen teilweise wenig zu spüren. Diese gesellschaftlichen Herausforderungen dürften sich in Zukunft aber vermehrt stellen.

Datenschutz in der Praxis

Mit Blick auf diese Entwicklungen lassen sich zahlreiche Themen des vorliegenden Tätigkeitsberichts einordnen. Das Gesundheitswesen bleibt ein sehr sensitiver Bereich, entsprechend heikel ist der Umgang mit den sensiblen Patientendaten. Zwischen Spitälern und Versicherern findet ein regelmässiger Datenaustausch statt, wobei mit der Einführung von Case-Managern die datenschutzrechtlichen Grenzen überschritten wurden (siehe Seite 10 f.). Umfassende Datenbearbeitungen finden auch im Rahmen des E-Government statt. Datenschutzrechtliche Rahmenbedingungen sind nun im Konzept des Regierungsrates berücksichtigt, und erste Ansätze für deren Umsetzung sind erfolgt (siehe Seite 12 f.). Personen werden oftmals aufgefordert, Vollmachten zu unterzeichnen, damit bestimmte Informationen beschafft werden können. Häufig sind solche Vollmachten aber wenig transparent (siehe Seite 14). Wenn Informationen öffentlich sind, kann nicht automatisch davon abgeleitet werden, dass sie auch dauernd öffentlich zugänglich sein müssen. Informationen, die im Internet publiziert werden, können jedoch kaum mehr gelöscht werden. Gerichtsurteile dürfen deshalb nur im Internet veröffentlicht werden, wenn sie korrekt anonymisiert sind (siehe Seite 15).

Zahlreiche weitere in diesem Tätigkeitsbericht dargestellte Sachverhalte zeigen, dass beinahe kein Lebensbereich mehr von Datenbearbeitungen ausgeschlossen ist. Umso mehr ist darauf zu achten, dass die datenschutzrechtlichen Rahmenbedingungen stets eingehalten werden.

Case-Management in Spitälern

Die Case-Management-Verträge zwischen öffentlich-rechtlichen Spitälern und Krankenversicherungen sind häufig rechtswidrig. Sie verletzen die Persönlichkeitsrechte der Patientinnen und Patienten.

Zwischen öffentlich-rechtlichen Spitälern und Krankenversicherungen bestehen Case-Management-Vereinbarungen. Zwar können diese Vereinbarungen begrifflich und inhaltlich voneinander abweichen, doch geht es stets darum, dass Krankenversicherungen Case-Manager einsetzen, die als alleinige Ansprechpartner für das Spital Behandlungsprozesse koordinieren. Dadurch sollen die Qualität der Behandlung verbessert und Kosten gesenkt werden. Die Koordination der Case-Manager setzt einen Informationsaustausch zwischen allen Beteiligten voraus.

Das Case-Management, wie es die Krankenversicherungen in unterschiedlicher Form betreiben, ist im Gesetz nicht vorgesehen. Auch sind weder Aufgabe noch Funktion der Case-Manager gesetzlich festgelegt. Geregelt ist hingegen der Umgang mit Gesundheitsdaten der Patientinnen und Patienten: Die Datenschutzgesetze unterstellen die Gesundheitsdaten einem erhöhten Schutz, weil aufgrund ihrer Bedeutung ein besonderes Risiko von Persönlichkeitsverletzungen besteht.

Regeln für das Case-Management, …

Der Datenschutzbeauftragte überprüfte diverse Case-Management-Vereinbarungen zwischen Spitälern und Krankenversicherungen. Eine ausdrückliche Einwilligung der Betroffenen in das Case-Management ist nicht vorgesehen. Weil keine gesetzliche Grundlage für eine Teilnahmepflicht an einem Case-Management besteht, ist es jedoch unerlässlich, dass Patientinnen und Patienten ausdrücklich und schriftlich ihre Einwilligung für ein Case-Management erteilen. Die Patientinnen und Patienten müssen ausserdem zuvor umfassend über den Zweck und den Inhalt des Case-Managements unterrichtet werden. So müssen sie darüber informiert sein, welche Daten im Rahmen des Case-Managements über sie bearbeitet werden, dass sie nicht zur Einwilligung verpflichtet sind und dass sie ihre Zustimmung jederzeit widerrufen können.

Krankenversicherungen gelten nach dem Bundesgesetz über den Datenschutz im Bereich der sozialen Krankenversicherung (KVG) und der obligatorischen Unfallversicherung (UVG) als Bundesorgane (Art. 3 lit. h DSG). Wie öffentlich-rechtliche Spitäler sind sie an den verfassungsmässigen Grundsatz der Gesetzesmässigkeit gebunden. Ihr Handeln muss sich auf eine gesetzliche Grundlage stützen. Im Einzelfall kann zwar die Bearbeitung von Personendaten im Rahmen eines Case-Managements durch die Einwilligung der Betroffenen gerechtfertigt sein. Ohne hinreichend bestimmte gesetzliche Grundlage ist es jedoch nicht zulässig, über Einzelfälle hinaus ein standardisiertes Case-Management zu betreiben. Vereinbarungen zwischen Krankenversicherungen und öffentlich-rechtlichen Spitälern, ergänzt mit der Einwilligung der Betroffenen, können keine gesetzliche Grundlage ersetzen.

… für den Informationsfluss…

Case-Management-Vereinbarungen zwischen Spitälern und Krankenversicherungen sehen häufig vor, dass umfassende Informationen über Patientinnen und Patienten übermittelt werden. So teilen Spitäler beim Eintritt der Krankenversicherung Name, Eintrittsdatum, Notfall oder Reguläreintritt, Diagnose und so weiter mit. Weitere Angaben wie geplante Operationen, voraussichtliche Aufenthaltsdauer oder Arbeitgeber werden in den Case-Management-Vereinbarungen zwar nicht als obligatorisch, aber doch als wünschenswert bezeichnet. Den Patientinnen und Patienten ist in der Regel nicht bewusst, dass diese Gesundheitsdaten der Krankenversicherung weitergegeben werden. Zudem werden diese Daten bisweilen bereits weitergeleitet, bevor die Patientinnen und Patienten über ihre Diagnose und Behandlung informiert worden sind.

Gesundheitsdaten, die für die gesetzlichen Aufgaben der Krankenversicherungen nicht geeignet und erforderlich sind, dürfen vom Spital nur mit Einwilligung der betroffenen Patientinnen und Patienten übermittelt werden. Dies gilt sowohl für den Inhalt als auch für den

Zeitpunkt der Bekanntgabe von Patientendaten.

… und für Case-Manager

Case-Management-Vereinbarungen enthalten Klauseln, die Case-Manager in Planungs- und Entscheidungsprozesse der Spitäler integrieren. Konkret sollen Spitäler den Case-Managern die Koordination und somit den Austausch mit dem Personal und insbesondere mit Arztpersonen ermöglichen. Patientendaten dürfen indessen nur gestützt auf gesetzliche Meldepflichten und Melderechte oder eine Einwilligung des Betroffenen an Dritte bekannt gegeben werden. Eine Case-Management-Vereinbarung kann somit keine Grundlage dafür bilden, dass das Spital der Krankenkasse Gesundheitsdaten bekannt gibt. Auch der Hinweis, dass für Case-Manager, die an spitalinternen Besprechungen teilnehmen, das «Spitalgeheimnis» gelte, ist kein Rechtfertigungsgrund.

Case-Management-Vereinbarungen über den Kontakt von Case-Managern mit zugeordneten Vertrauensärzten werden teilweise mit der Klausel ergänzt, dass gegenüber Personen ausserhalb des Case-Managements und des vertrauensärztlichen Dienstes eine Schweigepflicht für medizinische Daten bestehe.

Vertrauensärzte müssen bestimmte Zulassungsvoraussetzungen erfüllen und bestimmen die Leistungspflicht von Krankenversicherungen im Einzelfall. Case-Manager hingegen können lediglich die Behandlungsprozesse von Patientinnen und Patienten koordinieren und unterstehen dabei weder dem ärztlichen Berufsgeheimnis im Sinne des Art. 321 StGB (so genanntes Patientengeheimnis) noch dem Amtsgeheimnis von Spitalangestellten nach Art. 320 StGB. Auch sind Case-Manager keine Hilfspersonen der Vertrauensärzte nach Art. 321 StGB. Schweigepflichtklauseln in Case-Management-Vereinbarungen rechtfertigen keine Verletzung von Persönlichkeitsrechten der Betroffenen. Case-Manager können somit weder Mittelspersonen zu Vertrauensarztpersonen sein noch deren Funktion übernehmen.

Case-Management-Vereinbarungen überprüfen

Wenn im Einzelfall keine Einwilligung der betroffenen Patientinnen und Patienten zur Bekanntgabe von Gesundheitsdaten an Case-Manager vorliegt und wenn sich diese Datenbekanntgabe nicht auf eine gesetzliche Grundlage abstützt, ist sie rechtswidrig. Der Datenschutzbeauftragte hat deshalb die Spitäler angehalten, ihre Case-Management-Vereinbarungen eingehend rechtlich zu prüfen und an die gesetzlichen Anforderungen anzupassen. Mit einem Kreisschreiben hat die Gesundheitsdirektion diese Bemühungen unterstützt.

E-Government-Strategie

In der E-Government-Strategie des Kantons Zürich für 2008–2011 wird festgehalten, dass die datenschutzrechtlichen Rahmenbedingungen bei der Umsetzung der einzelnen Projekte uneingeschränkt zu beachten sind.

Im Rahmen von E-Government werden öffentliche Leistungen mit Informations- und Kommunikationstechnologien bereitgestellt sowie Prozesse innerhalb der Verwaltung und mit Dritten unterstützt und gestaltet. Im Kanton Zürich wurde 2003 bei der Staatskanzlei eine Stabsstelle für E-Government errichtet. Seither wurden eine zentrale Web-Infrastruktur aufgebaut, die das Informationsangebot erfasst und präsentiert, und einzelne Projekte realisiert. Der Regierungsrat hat nun für die Legislatur 2008–2011 einen umfassenden elektronischen Amtsverkehr vorgegeben: Alle Bewilligungsverfahren und der gesamte Amtsverkehr im weiteren Sinn sollen bis 2011 über das Internet abgewickelt werden können.

Schweizweit vereinheitlichen

Die Verwaltungen von Bund, Kantonen und Gemeinden sind eng vernetzt. Seit einigen Jahren gibt es schweizweit zahlreiche Bestrebungen, gemeinsame Ziele, Grundsätze, Vorgehen und Instrumente zur Umsetzung von E-Government festzulegen. So hat das Informatikstrategieorgan des Bundes im April 2006 einen ausführlichen Leitfaden zu E-Government verfasst. Dieser stützt sich auf die E-Government-Standards des Vereins eCH, in dem auch der Kanton Zürich Mitglied ist. Mit der vom Bundesrat am 24. Januar 2007 verabschiedeten «E-Government-Strategie Schweiz» und der öffentlich-rechtlichen Rahmenvereinbarung über die E-Government-Zusammenarbeit in der Schweiz (2007–2011) sind die wichtigsten Weichen gestellt worden. Bund und Kantone haben sich verpflichtet, die «E-Government-Strategie Schweiz» koordiniert umzusetzen.

Gemäss Legislaturziel des Regierungsrates und unter Berücksichtigung der «E-Government-Strategie Schweiz» bereitete die Stabsstelle E-Government Ende April 2008 einen Regierungsratsbeschluss vor, der die E-Government-Strategie des Kantons Zürich für die derzeitige Legislaturperiode festlegen soll. Dazu führte sie ein Vernehmlassungsverfahren durch, an welchem sich auch der Datenschutzbeauftragte beteiligte.

Grundrechte respektieren

Der Datenschutzbeauftragte hält in seiner Stellungnahme fest, dass die vorgeschlagenen Leitlinien und Ziele der E-Government-Strategie des Kantons Zürich die Bürgerinnen und Bürger auf Konsumierende von Dienstleistungen reduziert. Die E-Government-Strategie verkennt, dass die Bürgerinnen und Bürger auch Rechte haben, die sie wahrnehmen können und die zu respektieren sind. Der Datenschutzbeauftragte fordert deshalb, dass der Schutz der Grundrechte, insbesondere der Schutz der Privatheit und der informationellen Selbstbestimmung der Bürgerinnen und Bürger, auch im Rahmen von E-Government gewährleistet werden muss. Gerade weil E-Government-Anwendungen hohe Risiken für die Grundrechte der betroffenen Personen beinhalten können, muss eine E-Government-Strategie die Grundrechte gewährleisten und somit die im Datenschutzrecht verankerten Grundsätze beachten.

Der Datenschutzbeauftragte verweist darauf, dass der Kanton Zürich – wie alle anderen Kantone und der Bund – die öffentlich-rechtliche Rahmenvereinbarung über die E-Government-Zusammenarbeit in der Schweiz unterzeichnet hat. Darin ist ausdrücklich festgehalten, dass die kantonalen Datenschutzbestimmungen gewährleistet werden müssen und ein Rechtsetzungsbedarf frühzeitig zu evaluieren ist. In der Vergangenheit sind diese Vorgaben bei E-Government-Projekten nur unzureichend umgesetzt worden, und die Rechtsetzung im Bereich E-Government steht erst am Anfang.

Oberste Priorität Datenschutz

Die Stabsstelle E-Government hat die Anliegen des Datenschutzbeauftragten aufgenommen: Die Orientierung an den Grundrechten wird in den Leitlinien verankert. Die Gewährleistung von Datenschutz und Datensicherheit ist kein strategisches Ziel, hat aber bei allen Projekten oberste Priorität. Der Datenschutzbeauftragte wird in der Organisation separat

erwähnt und muss rechtzeitig in die Projekte einbezogen werden.

Strategieschwerpunkte

Der Regierungsrat hat am 10. September 2008 die E-Government-Strategie des Kantons Zürich für 2008–2011 festgesetzt – mit folgenden Schwerpunkten:

- E-Government muss gemäss Leitlinien die Grundrechte berücksichtigen.
- Oberstes strategisches Ziel ist die Schaffung der notwendigen organisatorischen, rechtlichen und technischen Voraussetzungen für den Auf- und Ausbau des Leistungsangebots. Die Anforderungen bezüglich Datenschutz und Informationssicherheit werden gemäss Rahmenvereinbarung und Datenschutzgesetzgebung umgesetzt.
- Die Anforderungen für eine gesetzliche Grundlage gemäss Datenschutzgesetzgebung werden ausdrücklich genannt: Für die Bearbeitung von Personendaten muss eine gesetzliche Grundlage vorliegen. Sofern die Datenbearbeitung für eine geplante elektronische Dienstleistung nicht geregelt ist, müssen die entsprechenden rechtlichen Grundlagen vorgängig geschaffen werden. Die Bearbeitung oder Bekanntgabe besonderer Personendaten bedarf einer hinreichend bestimmten Regelung in einem formellen Gesetz.
- Das Recht auf Zugang zu amtlichen Dokumenten stellt Anforderungen an den Umgang auch mit elektronischen Dokumenten und findet seine Grenze beim verfassungsmässig garantierten Schutz der Privatsphäre. Die im neuen IDG formulierten Regeln für den Informationszugang werden beachtet.
- Die Strategie wird von den Direktionen und der Staatskanzlei umgesetzt. Diese sind verantwortlich, dass die Rahmenbedingungen und Vorgaben, insbesondere der gesetzlichen Vorschriften, eingehalten werden. Gemeinsam mit dem Datenschutzbeauftragten und der Koordinationsstelle IDG stellen sie die Einhaltung der Datenschutzgesetzgebung sicher.

In der E-Government-Strategie des Kantons Zürich für 2008–2011 wird somit festgehalten, dass die datenschutzrechtlichen Rahmenbedingungen bei der Umsetzung der einzelnen Projekte uneingeschränkt zu beachten sind.

Trend zur Generalvollmacht

Leistungserbringer verlangen von ihren Klientinnen und Klienten zunehmend bereits bei der Anmeldung eine Vollmacht für Abklärungsbefugnisse, die ihnen häufig erst im weiteren Verfahrensverlauf zustehen. Die informationelle Selbstbestimmung der Klientinnen und Klienten wird dadurch unnötig beeinträchtigt.

Der Datenschutzbeauftragte wurde von betroffenen Personen darauf aufmerksam gemacht, dass verschiedene Leistungserbringer im Sozial- und Gesundheitsbereich ihren Klientinnen und Klienten Vollmachten für zu weit reichende Abklärungsbefugnisse zur Unterschrift vorlegen würden. Er prüfte deshalb verschiedene Generalvollmachten und stellte fest, dass die meisten nicht verhältnismässig waren: So war in zahlreichen Vollmachten nicht ersichtlich, für welchen Zweck die Auskünfte eingeholt werden sollten. Oder es fehlte die genaue Bezeichnung der Stellen und Personen, die bestimmte Informationen bekannt geben sollten.

Leistungsanspruch klären …

Leistungserbringer müssen in der Lage sein, die gesetzlichen Voraussetzungen des Leistungsanspruchs im Einzelfall zu prüfen. Die Klientinnen und Klienten haben über ihre Verhältnisse wahrheitsgemäss Auskunft zu geben und Einsicht in ihre Unterlagen zu gewähren. Diese so genannten Mitwirkungspflichten finden sich in den meisten gesetzlichen Grundlagen der Leistungsverwaltung im Sozial- und Gesundheitsbereich.

Im Rahmen ihrer Abklärungsaufgaben müssen die Leistungserbringer auch den Anspruch bei Dritten wie Arbeitgebern, Ärztinnen oder Banken prüfen. Für solche Abklärungen brauchen sie eine Einwilligung der betroffenen Person. Diese erteilt die Einwilligung in der Regel in Form einer Vollmacht an den Leistungserbringer.

… mit geeigneten Vollmachten

Einige Leistungserbringer verlangen von den Klientinnen und Klienten bei der Anmeldung eine Vollmacht, die ihnen erlaubt, die benötigten Informationen direkt einzuholen. In diesen Einzelvollmachten wird sowohl die Stelle genannt, bei der eine Abklärung erfolgen soll, als auch die Thematik, die näher beleuchtet werden soll. Zunehmend holen Leistungserbringer jedoch Generalvollmachten unter dem Titel einer generellen Abklärungsbefugnis ein; diese Generalvollmachten sind weder thematisch noch stellenspezifisch eingegrenzt. Sie genügen den Voraussetzungen, die an eine Einwilligung gestellt werden, in den meisten Fällen nicht. Denn die Einwilligung in eine Datenbeschaffung oder eine Datenbekanntgabe ist nur gültig, wenn aus der Vollmacht hervorgeht, wer wem welche Daten zu welchem Zweck bekannt geben soll. Die einwilligende Person muss also wissen, für welche Daten sie ihre Einwilligung erteilt und was mit ihren Daten geschieht – inklusive möglicher Konsequenzen.

Bei besonderen Personendaten sind die Vorgaben für Vollmachten noch strenger: Will ein Leistungserbringer beispielsweise Angaben zur Gesundheit oder zu Sozialhilfemassnahmen eines Klienten einholen, müssen die verlangten Daten und das Organ, welches die Daten bekannt geben soll, in der Vollmacht genannt werden.

Eine einmal erteilte Einwilligung kann von der betroffenen Person jederzeit widerrufen werden. Dieses Widerrufsrecht unterliegt keinen Formvorschriften; es kann also auch mündlich widerrufen werden.

Unterstützung für Mustervollmachten

Damit beispielsweise Sozialhilfebehörden von ihren Klientinnen und Klienten künftig nur noch rechtmässige Generalvollmachten verlangen, wandte sich der Datenschutzbeauftragte an das Kantonale Sozialamt und schlug vor, den Gemeinden erweiterte Mustervollmachten im Sozialbehördenhandbuch zur Verfügung zu stellen, die den einzelnen Verfahrensstadien in der Sozialhilfe angepasst sind. Für die Ausarbeitung bot er seine Unterstützung an.

Urteilspublikationen im Internet

Gerichte publizieren ihre Urteile zunehmend auch auf ihren Websites. Rückschlüsse auf bestimmte oder bestimmbare Personen sind durch eine Anonymisierung zu vermeiden.

Immer mehr Gerichte unterschiedlicher Stufen und mit verschiedenen Zuständigkeitsbereichen publizieren ihre rechtskräftigen Urteile auf ihren Websites. Damit informieren sie interessierte Kreise über ihre Rechtsprechungstätigkeit und ermöglichen einfache Vergleiche zu ähnlichen Fällen.

Wenn ein Gericht nicht oder nicht hinreichend anonymisierte Urteile publiziert, entspricht dies einer Bekanntgabe von Personendaten. Gerichtsentscheide enthalten häufig sehr sensible Angaben über Personen, beispielsweise über deren Gesundheit, über Sozialhilfemassnahmen oder über strafrechtliche Verfolgungen und Sanktionen. Für die Bearbeitung solcher besonders schützenswerter Personendaten bedarf es einer gesetzlichen Grundlage (§ 2 lit. d DSG). Dies gilt auch dann, wenn ein Gerichtsentscheid zuvor mündlich eröffnet wurde, in der Gerichtskanzlei aufgelegen ist oder in einer amtlichen Sammlung publiziert wurde.

Keine gesetzliche Grundlage

Im Kanton Zürich gibt es keine gesetzliche Grundlage, die Gerichte ermächtigen würde, Entscheide mit Personendaten auf ihrer Website zu publizieren. Der verfassungsrechtlich verankerte Grundsatz der (Verfahrens-)Öffentlichkeit gibt zwar den Verfahrensbeteiligten und allenfalls auch jeder Bürgerin und jedem Bürger die Möglichkeit, eine Gerichtsverhandlung und gegebenenfalls auch die Eröffnung von Entscheiden persönlich im Gerichtssaal mitzuverfolgen (Art. 30 Abs. 3 BV und Art. 6 Ziff. 1 EMRK). Daraus lässt sich jedoch kein Recht ableiten, über das Internet Urteile mit personenbezogenen Angaben von Verfahrensbeteiligten ohne deren Einwilligung zu veröffentlichen. Der Eingriff in die Persönlichkeit der betroffenen Person wird auch nicht durch ein allfälliges Interesse der Allgemeinheit an Information aufgewogen.

Neue Dimension Internet

Eine Publikation eines Urteils im Internet hat eine andere Dimension als eine mündliche Urteilseröffnung im Gerichtssaal, eine Auflage des Entscheides in der Gerichtskanzlei oder eine Veröffentlichung in der amtlichen Sammlung. Denn mit der Publikation eines nicht oder nur teilweise anonymisierten Entscheides auf einer Website kann dieser Entscheid mit wenigen Kriterien wie Name und Geburtsdatum in der Suchfunktion der betreffenden Website gefunden und einer Person zugeordnet werden. Einträge auf einer Website sind weltweit und praktisch unbeschränkt abrufbar. Dabei verschwinden solche Einträge auch dann nicht zwingend aus dem Internet, wenn sie auf der Website, wo sie erstmals publiziert wurden, gelöscht werden. Einträge können unkontrolliert von anderen Personen oder Organisationen übernommen und auf weiteren Websites verbreitet werden, wo sie auch noch Jahre nach der ursprünglichen Publikation abrufbar bleiben.

Anonymisierte Entscheide

Auf einer (Gerichts-)Website publizierte oder künftig zu publizierende Entscheide sind so weit zu anonymisieren, dass keine Rückschlüsse auf betroffene Personen möglich sind. Ob sich ein Urteil für eine Publikation im Internet überhaupt eignet, beispielsweise wegen seiner präjudiziellen Bedeutung, und wenn ja, nach welchen Kriterien dieses zu anonymisieren ist, muss von Entscheid zu Entscheid beurteilt werden. Eine Anonymisierung dürfte erleichtert werden, wenn die publizierten Texte auf jene Sachumstände beschränkt werden, die für das Verständnis des konkreten Streitfalls unerlässlich sind. Auf personenbezogene Merkmale wie Name und Vorname, Initialen, Geburtsdatum und Adresse von Verfahrensbeteiligten ist generell zu verzichten.

Fälle aus der Beratungstätigkeit

Einen Schwerpunkt der Tätigkeit des Datenschutzbeauftragten bildet die Beratungstätigkeit.

01.–16. ***Die hier zusammengefassten Fälle sind ausführlich dargestellt im Anhang auf Seite 29 ff. und auf der Website des Datenschutzbeauftragten (www.datenschutz.ch).***

01. **IV-Stelle klärt Gesundheitszustand ab**
Sachbearbeitende der Invalidenversicherungsstelle sind berechtigt, Gesundheitsdaten von Versicherten zu bearbeiten, wenn sie die Voraussetzungen zur Leistungserbringung überprüfen müssen. Dazu gehören auch Unterlagen über den Gesundheitszustand.

02. **Backgroundcheck für Flughafenangestellte**
Bevor Personen, die im Sicherheitsbereich des Flughafens tätig sind, einen Flughafenausweis erhalten, erfolgt ein Backgroundcheck nach den Vorgaben des Nationalen Sicherheitsprogramms. Sie müssen dazu einen aktuellen Auszug des zentralen Strafregisters vorweisen, und die Polizei kann weitere Überprüfungen durchführen.

03. **Test über kognitive Fähigkeiten**
An den Mittelschulaufnahmeprüfungen wird ein vorerst noch freiwilliger Test zu den allgemeinen kognitiven Fähigkeiten der Kandidierenden (AKF-Test) durchgeführt. Dies erfolgt im Rahmen eines Forschungsprojektes.

04. **Informationen für schulische Heilpädagogen**
Die Umstellungen im Schulbereich aufgrund des revidierten Volksschulgesetzes ermächtigen den Schulpsychologischen Dienst nicht, Kopien seiner Abklärungsberichte an die schulischen Heilpädagogen abzugeben.

05. **Inhalt aufbewahrter Strafakten**
Bei der Aufbewahrung von Akten aus Strafverfahren ist der Grundsatz der Verhältnismässigkeit zu beachten. Personendaten dürfen so lange aufbewahrt werden, wie es für die Erfüllung der gesetzlichen Aufgaben der Strafverfolgungsbehörde geeignet und erforderlich ist.

06. **Rechtsweggarantie im Datenschutzrecht**
Die vorgesehenen Anpassungen im kantonalen Verfahrensrecht sollen gewährleisten, dass das Verwaltungsgericht als unabhängige richterliche Instanz grundsätzlich über alle datenschutzrechtlichen Streitigkeiten entscheidet.

07. **Schulungsfilm über Menschen mit Demenz**
In einem Filmprojekt über den emotionalen Ausdruck bei Menschen mit Demenz müssen gesetzliche Vertreter vor ihrer Einwilligung umfassend informiert und auf das Widerrufsrecht aufmerksam gemacht werden. Eine Drittfirma darf kein filmisches Rohmaterial weiterverwerten.

08. **Listen von HPV-Impfungen**
Um seine gesetzlichen Aufgaben zu erfüllen, kann der Kantonsärztliche Dienst Listen mit bestimmten Angaben über HPV-Impfungen verlangen. Dies teilte der Datenschutzbeauftragte einem Hausarzt mit, der im Rahmen des kantonalen Impfprogramms die Bewilligung für HPV-Impfungen mit entsprechenden Auflagen erhalten hat.

09. **Listen über Aufnahmeprüfung**
Bei der Amtshilfe ist die Bekanntgabe von Personendaten im Einzelfall möglich. Die regelmässige Anfrage von Listenauskünften sind keine Einzelfälle.

10. **Überwachung bei Sportveranstaltungen**
Ausschreitungen bei Sportveranstaltungen sind der Anlass, Zuschauerinnen und Zuschauer vermehrten Kontrollen zu unterziehen. Hierfür sind klare und verhältnismässige Rechtsgrundlagen notwendig.

11. **Computerverkauf durch ein Konkursamt**
Verwertet ein Konkursamt im Rahmen einer konkursamtlichen Liquidation Computer mit Personendaten, muss es sicherstellen, dass diese Daten gelöscht werden. Für die Löschung gibt es drei Möglichkeiten.

12. **Plagiaterkennung in Abschlussarbeiten**
Um Abschlussarbeiten im Mittelschul- und Berufsbildungsbereich auf Plagiate zu untersuchen, sind entsprechende gesetzliche Grundlagen nötig.

13. **Panaschierresultate im Internet**
Die Panaschierstatistik der Nationalratswahlen kann im Internet publiziert werden, und zwar sowohl nicht kandidatenbezogen als auch kandidatenbezogen.

14. **Kein aufsichtsrechtliches Einschreiten**
Stellt der Datenschutzbeauftragte fest, dass ein kommunaler Datenschutzbeauftragter die ihm gesetzlich zugewiesenen Aufgaben korrekt und in genügendem Mass wahrgenommen hat, besteht kein Grund für ein aufsichtsrechtliches Einschreiten.

15. **Schulärztliche Untersuchung durch Privatarzt**
Eltern haben die Möglichkeit, die schulärztliche Untersuchung statt durch den Schularzt durch den Haus- oder Kinderarzt vornehmen zu lassen. Der private Arzt darf dem Schularzt keine Gesundheitsdaten weiterleiten, sondern nur der Gemeinde die Untersuchung bestätigen.

16. **Anonyme Auswertung garantiert**
Wird bei Befragungen den Befragten Anonymität zugesichert, muss garantiert werden, dass ein Rückschluss auf bestimmte oder bestimmbare Personen ausgeschlossen ist. Die tiefste Teilnehmendenzahl, die Rückschlüsse ausschliesst, ist von der verantwortlichen Stelle in jedem Einzelfall zu prüfen und festzulegen.

Umfassende Akteneinsicht

Ein Vormund wandte sich wegen einer Akteneinsicht in ein Fürsorgedossier an den Datenschutzbeauftragten. Im Rahmen einer Vermittlung konnte dieser sowohl das Akteneinsichtsrecht klären als auch das Vertrauen zwischen dem Vormund und der Behörde wiederherstellen.

Ein Vormund verlangte bei der Fürsorgebehörde einer Gemeinde Einsicht in die Akten seiner Klientin, die Sozialhilfe bezieht. Obwohl er umfassende Einsicht in das Vormundschafts- und Fürsorgedossier erhielt, glaubte er, nicht über alle Akten zu verfügen. Er wandte sich deshalb an den Datenschutzbeauftragten.

Der Vormund monierte insbesondere, dass von einer externen Firma ein Bericht über das Fürsorgewesen der Gemeinde erstellt worden war, der auch den Fall seiner Klientin behandelte. Aufgrund des Berichtes korrigierte die Gemeinde Unregelmässigkeiten bei der Berechnung von Fürsorgeleistungen für seine Klientin. Sie integrierte die Informationen aus dem Bericht im Fürsorgedossier der Klientin und war deshalb der Auffassung, dem Vormund umfassende Akteneinsicht gewährt zu haben. Tatsächlich lag noch ein Entscheid des Verwaltungsgerichts vor, der den fraglichen Bericht als amtsinternes Dokument bezeichnete, das nicht Bestandteil des Klientendossiers sei.

Im Gespräch mit den Vertretenden der Gemeinde konnte der Datenschutzbeauftragte klären, dass die Informationen des Berichtes tatsächlich in das Klientendossier geflossen waren und sich auf die Auszahlungen auswirkten. Die Gemeinde hatte dem Vormund einen Beschluss eröffnet, der sich inhaltlich mit dem Ergebnis im fraglichen Bericht deckte. Obwohl der Abschnitt über die Klientin im Bericht nicht in Kopie im Fürsorgedossier der Klientin abgelegt war, sprach aus Sicht der Gemeinde nichts dagegen, dem Vormund eine solche Kopie herauszugeben. Damit konnte sein Akteneinsichtsgesuch vollständig befriedigt werden.

Der Datenschutzbeauftragte nahm in die Gesamtheit des Berichtes Einsicht und konnte dem Vormund bestätigen, dass keine weiteren Angaben zu seiner Klientin im Bericht standen. Gleichzeitig wies er den Vormund darauf hin, dass das Verwaltungsgericht im erwähnten Entscheid festgehalten habe, dass den Informationen im Bericht keine direkte Wirkung für die konkrete Bedarfsermittlung zukomme, weshalb eine Akteneinsicht aufgrund des Verfahrensrechts nicht zugestanden worden sei. Dies ist insofern relevant, als der Vormund davon ausgehen muss, dass die Informationen, die er nun zusätzlich aus dem Bericht erhalten hat, zu keiner anderen rechtlichen Würdigung des zugrunde liegenden Sachverhalts führen würden.

Mit seiner Vermittlung konnte der Datenschutzbeauftragte nicht nur in Bezug auf das Akteneinsichtsrecht Klarheit schaffen, sondern auch das Vertrauen zwischen der betroffenen Verwaltung und dem Vormund wiederherstellen.

Online-Zugriff auf Einwohnerregister

Damit Gerichte online auf die Daten der kommunalen Einwohnerregister zugreifen dürfen, muss das Gerichtsverfassungsgesetz angepasst werden. Zudem soll der Zugriff auf laufende Geschäfte beschränkt sein. Dies hält der Datenschutzbeauftragte in einer Stellungnahme zu einem Postulat aus dem Kantonsrat fest.

Mit einem Postulat aus dem Kantonsrat (KR-Nr. 270/2006) wurde der Regierungsrat eingeladen, eine gesetzliche Grundlage für den Online-Zugriff von Gerichten auf Daten der kommunalen Personenmeldeämter zu schaffen.

In einer Stellungnahme hält der Datenschutzbeauftragte einleitend fest, dass Datenschutz und Datensicherheit beim Online-Zugriff eine besondere Bedeutung haben. Je nach Anschluss erhält die abrufende Stelle – ohne Einzelentscheid der zuständigen Stelle – einen teilweisen oder auch einen vollständigen Zugriff auf den Informationsbestand der anderen Stelle. Die Beurteilung, ob die aus dem Informationsbestand bezogenen Personendaten zur Bearbeitung tatsächlich erforderlich sind, fällt weg. Zudem besteht ein Risiko, dass auf weitere, für die Bearbeitung nicht relevante Informationen zugegriffen wird oder dass bestimmte Personendaten zweckentfremdet werden.

Das neue IDG berücksichtigt, dass solche Verfahren mit erhöhten Risiken für die Rechte und Freiheiten von betroffenen Personen einhergehen: Im Rahmen der Vorabkontrolle müssen solche Vorhaben dem Datenschutzbeauftragten unterbreitet werden (§ 10 i.V.m. § 24 IDG).

Kantonale Zivil- und Strafgerichte sind verpflichtet, in Endentscheiden korrekte und vollständige Rubren zu erstellen (§§ 157 lit. a Ziff. 3 und 160 lit. a Ziff. 3 Gerichtsverfassungsgesetz [GVG]). Wegen der erforderlichen Aktualität sind diese Daten zwingend bei den Personenmeldeämtern zu beziehen. Seit dem 1. Januar 2007 ermächtigt die kantonale Strafprozessordnung die Untersuchungsbehörden, die für die Untersuchung notwendigen Personendaten online von den Personenmeldeämtern zu beziehen.

Der Datenschutzbeauftragte stellt fest, dass vorliegend keine besonderen Personendaten betroffen sind. Er betont indes, dass das zu redigierende Gerichtsverfassungsgesetz mindestens die Tatsache des Online-Zugriffs, den Zweck, die beteiligten Behörden und den Umfang der abrufbaren Daten festhalten müsse. Der Umfang der abzurufenden Personendaten durch die Zivil- und Strafgerichte ist im GVG limitiert (§ 157 lit. a Ziff. 3 resp. § 160 lit. a Ziff. 3 GVG).

Im Weiteren verlangt der Datenschutzbeauftragte, dass der Zugriff auf Personendaten, die im Zusammenhang mit einem laufenden Geschäft stehen, zu beschränken ist. Der Kreis der Zugriffsberechtigten ist genau zu bestimmen und auf ein Minimum zu begrenzen. Der Zugriff ist mittels Passwort zu schützen und die Abrufe sind zu protokollieren. Protokolldaten können stichprobenweise oder bei Verdachtsfällen ausgewertet werden.

Gesundheit von Einbürgerungswilligen

Für ein Einbürgerungsverfahren müssen nur Personen, die ihre nicht genügende Integration mit gesundheitlichen Gründen rechtfertigen, Angaben über ihre Gesundheit machen. Welche Angaben dies konkret umfasst, muss in den entsprechenden Gesetzen und Verordnungen genauer umschrieben werden.

Im Rahmen der Erarbeitung des Gesetzes und der Verordnung über das Kantons- und Gemeindebürgerrecht bat das Gemeindeamt den Datenschutzbeauftragten, die Bestimmungen über die Bearbeitung und die Bekanntgabe von Personendaten mitzugestalten. Die Bestimmungen beinhalten einen Katalog mit jenen Personendaten, die von den Einbürgerungsorganen bearbeitet werden dürfen – so auch jene zur Gesundheit. Das Gemeindeamt wies zudem auf Fälle hin, in denen die Gesuchstellenden geltend machen, dass sie sich aus gesundheitlichen Gründen nicht genügend integrieren könnten und ihnen die Einbürgerung deshalb verwehrt sei.

Der Datenschutzbeauftragte wies darauf hin, dass es sich bei der Gesundheit um besondere Personendaten handelt, deren Bearbeitung strengen Voraussetzungen unterliegt. Er hielt fest, dass im Einbürgerungsverfahren Gesundheitsdaten nur in denjenigen Fällen bearbeitet werden dürfen, in denen eine nicht genügend integrierte Person ihr Einbürgerungsgesuch damit begründet, dass gesundheitliche Gründe die Integration verhinderten oder erschwerten.

Weil die gesetzlichen Bestimmungen keine Angaben enthielten, welche Unterlagen die Gesuchstellenden in den genannten Fällen beizubringen haben, riet der Datenschutzbeauftragte gemäss dem Grundsatz der Transparenz, diese Angaben genauer zu umschreiben.

Zugriffe auf das Mailkonto

Auf das persönliche E-Mail-Konto können auch Systemadministratoren zugreifen. Organisatorische und technische Massnahmen können ein unbefugtes Bearbeiten verhindern.

Ein Benutzer einer öffentlichen Stelle realisierte, dass in seinem Mailkonto eine E-Mail plötzlich fehlte, obwohl er wusste, dass er sie sicher nicht gelöscht hatte. Er stellte sich deshalb die Frage, wer überhaupt Zugriff auf sein Mailkonto habe.

Die Abklärungen des Datenschutzbeauftragten zeigten, dass ein Zugriff von berechtigten Drittpersonen nicht auszuschliessen war. Der geschilderte Vorfall liess sich im Einzelnen nicht mehr rekonstruieren. Soweit eine E-Mail fehlte, hätte sie anhand einer Tages- oder Wochensicherung wiederhergestellt werden können.

In der fraglichen Organisationseinheit hat eine Administratorengruppe von fünf Personen einen uneingeschränkten Zugriff auf die Mailkonten. Da der Mailservice an eine Drittfirma ausgelagert ist, sind diese Administratoren Angestellte dieser Drittfirma. Der Inhaber eines Mailkontos kann weitere Personen auf sein Konto mit unterschiedlichen Möglichkeiten berechtigen. Die Zugriffe auf ein Konto werden aufgezeichnet. Festgehalten werden Datum, Lesezugriffe, Schreibzugriffe und die Benutzenden. Hingegen werden die E-Mails nicht verschlüsselt abgelegt. Damit können sie von den berechtigten Benutzenden gelesen werden. Eine Verschlüsselung hat der Inhaber eines Mailkontos individuell einzurichten. In der betroffenen Organisationseinheit hatten die Verantwortlichen der Informatik keine tieferen Kenntnisse über das Mailsystem und wussten auch nicht, wie die Sicherheit einer E-Mail konkret gewährleistet wird oder werden könnte.

Der Datenschutzbeauftragte stellte fest, dass die Vertraulichkeit der E-Mails in dieser Organisationseinheit lückenhaft war: Die Benutzenden waren über die Möglichkeit der verschlüsselten Ablage der E-Mails nicht informiert, und die zuständigen Informatikverantwortlichen verfügten nicht über die notwendigen Grundlagen für Aufklärung und Schulung. Der Datenschutzbeauftragte bot für die Umsetzung entsprechender Sicherheitsmassnahmen seine Unterstützung an.

Sicherheit weiterhin im Blickfeld

Nachkontrollen des Datenschutzbeauftragten zeigen klare Defizite bei den Massnahmen für ICT-Sicherheit im strategischen Bereich auf.

Die Nachkontrollen des Datenschutzbeauftragten von Stellen in der kantonalen Verwaltung und in Kliniken haben in der Berichtsperiode von Januar bis September 2008 kein positives Bild ergeben. Änderungen und Neuerungen im operativen Umfeld schränkten die Kapazität der kontrollierten Stellen für die notwendigen organisatorischen Verbesserungen im Sicherheitsbereich stark ein.

Trotz Hinweisen in früheren Datenschutzreviews wurden der strategische Bereich vernachlässigt und die geforderten organisatorischen Grundlagen nicht erstellt. Dies führte zu unklaren oder unvollständigen Aufträgen an die Informatikabteilungen, die dieses Defizit mit organisatorischen und technischen Massnahmen nicht ausgleichen. Klare Anzeichen für diesen Mangel sind beispielsweise zu einfache Berechtigungsvergaben sowie fehlende Rollenkonzepte, ungenügende Betriebsdokumentationen oder der unkontrollierte Einsatz von mobilen Geräten wie Personal Digital Assistants und Speichermedien wie USB-Datenträger.

In den Gemeinden bestätigten die Nachkontrollen die bereits in früheren Jahren festgestellten Mängel. Im Gegensatz zu den früheren Prüfungen sind die Verantwortlichen bei den geprüften Gemeinden nun jedoch eher bereit, die Hinweise und Bemerkungen des Datenschutzbeauftragten in der vorgelegten Massnahmenplanung nach der Prüfung umzusetzen.

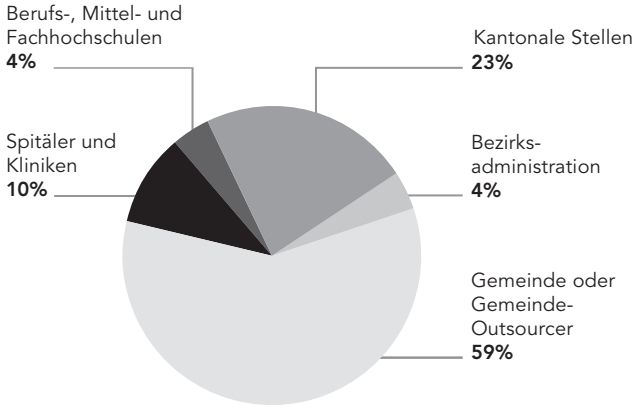
Die Gemeinden bildeten auch in dieser Berichtsperiode das Hauptgewicht der Kontrollen. Umfang und Zielsetzungen der Prüfungen wurden nicht angepasst, da sich die Risiken im Umfeld der geprüften Stellen gegenüber dem Vorjahr nicht stark geändert haben. Die Zusammenarbeit mit der Finanzkontrolle ermöglichte erneut vertiefte Prüfungen im organisatorischen und technischen Bereich.

Datenschutzreviews

Nach DSG geprüfte Stellen von 12.2000 bis 9.2008

Der Datenschutzbeauftragte prüfte insgesamt 71 Stellen

Durchgeführte Prüfungen	Anzahl
Kantonale Stellen	16
Bezirksadministration	3
Gemeinde oder Gemeinde-Outsourcer	42
Spitäler und Kliniken	7
Berufs-, Mittel- und Fachhochschulen	3



Unterstützung für ICT-Sicherheit

Der Datenschutzbeauftragte bietet kleinen und mittleren Stellen Vorgehensweisen und Hilfsmittel für die Umsetzung von Informatiksicherheitsmassnahmen (siehe Tätigkeitsbericht Nr. 13 [2007], S. 19 ff.). Eine Pilotgemeinde hat diese Hilfestellungen angewendet. Das Verfahren ist im Grundsatz gut einsetzbar. Detailfragen konnten in Zusammenarbeit mit der Interessengemeinschaft EDV Zürcher Gemeinden (IG EDV) besprochen werden. Die eingebrachten Erfahrungen wurden in den Hilfestellungen bereits angepasst und werden nach Einsatz bei zwei weiteren Pilotgemeinden für alle Amtsstellen und Gemeinden zur Verfügung stehen.

Anpassungen an das IDG

In der Berichtsperiode wurden alle Leistungsprozesse des Bereichs Kontrolle an das IDG angepasst. Die bisherige Datenschutzreview wurde neu in die Typen «Standard» und «Vertieft» unterteilt. Beim Typ «Standard» werden wie bisher die Prüfungszielsetzungen jeweils zu Beginn des Jahres festgelegt. Mit diesen Vorgaben wird weiterhin eine Auswahl aus den Bereichen Kantonale Stellen, Bezirksadministration, Gemeinde oder Gemeinde-Outsourcer, Spitäler und Kliniken sowie Berufs-, Mittel- und Fachhochschulen geprüft. Beim Typ «Vertieft» werden ausgewählte Stellen geprüft, wobei die Prüfungszielsetzungen individuell pro Stelle ausgearbeitet werden. Der Know-how-Aufbau über die Stelle wird sich dadurch längerfristig einfacher gestalten, und das Prüfungswissen und die Erfahrungen aus den Prüfungen können sowohl von den geprüften Stellen als auch vom Datenschutzbeauftragten besser genutzt werden.

Neu wird im Bericht der Datenschutzreview zwischen Hinweis und Bemerkung unterschieden. Ein Hinweis verlangt die Implementierung von neuen Massnahmen oder die Änderung von Verfahren und Prozessen bei wichtigen oder dringenden Mängeln. Eine Bemerkung verlangt dies bei geringfügigen bis mittleren Mängeln. Das Ziel der Prozesse ist es, ein Verfahren oder eine getroffene Massnahme zuerst zu bewerten und wo nötig eine Bemerkung mit Termin zu formulieren. In einem nächsten Schritt ist bei einem Hinweis oder einer Bemerkung der Erreichungsgrad der Massnahmen oder Verfahren nach Ablauf einer bestimmten Frist festzustellen.

Ausblick

Die Nachprüfungen haben gezeigt, dass der Fokus des Datenschutzbeauftragten auf die wichtigsten organisatorischen Grundlagen wie Sicherheitsstrategie und -konzepte, Verantwortlichkeiten, Weisungen, Betriebsdokumentationen und nicht zuletzt Rollen- und Zugriffskonzepte immer noch notwendig ist. Solange der Auftrag an die Informatikorganisationen nicht klar formuliert ist, kann nicht damit gerechnet werden, dass die Stellen bei einer sicheren Leistungserbringung durch die Umsetzungsverantwortlichen im Informatikbereich angemessen unterstützt werden. Die Lücken müssen von den Leitungsverantwortlichen der Stellen möglichst rasch und nachhaltig geschlossen werden.

Informationsbedarf nimmt zu

Die Nachfrage nach datenschutzrechtlichen Informationen nimmt weiter zu. Der Datenschutzbeauftragte greift zusätzlich vordringliche Aspekte zum Schutz der Privatheit auf – und nutzt Synergien durch Vernetzung.

Der Datenschutzbeauftragte hat seine Informationstätigkeit in der Berichtsperiode weiter intensivieren müssen. Weil den Bürgerinnen und Bürgern bewusst wird, dass ihre Privatheit zunehmend gefährdet ist, wird Datenschutz zu einem gesellschaftlichen Thema. Der Informationsbedarf nimmt entsprechend zu: So ist die Zahl der Anfragen von Bürgerinnen und Bürgern beim Datenschutzbeauftragten weiter gestiegen, und mehrere politische Vorstösse befassen sich mit dem Datenschutz. Gleichzeitig hat die Nachfrage nach datenschutzrechtlichen Informationen durch die Medien stark zugenommen. Ungebremst ist ausserdem die Nachfrage nach Gastreferaten des Datenschutzbeauftragten. Im Rahmen seines Sensibilisierungs- und Informationsauftrags kommt der Datenschutzbeauftragte dieser steigenden Nachfrage nach datenschutzrechtlichen Informationen, priorisiert nach Wirkung, so weit wie möglich nach.

Vordringliche Themen kommunizieren

Der Datenschutzbeauftragte greift zusätzlich vordringliche datenschutzrechtliche Aspekte auf. Insbesondere das Gesundheitswesen erforderte eine aktive Informationspolitik. Ein weiterer Schwerpunkt seiner Kommunikation waren die Auswirkungen des neuen IDG, das am Tag nach der Berichtsperiode in Kraft getreten ist. Für die verschiedenen Ansprechgruppen traf der Datenschutzbeauftragte unter anderem folgende Begleitmassnahmen:

- Verschiedene Informationsveranstaltungen wurden in Zusammenarbeit mit anderen öffentlichen Organen durchgeführt.
- Eine praxisnahe Einführung über die wichtigsten Änderungen durch das IDG bietet online das überarbeitete Lernprogramm Datenschutz sowohl den Angestellten der Verwaltung als auch der interessierten Öffentlichkeit (www.datenschutz.ch/wbt/datenschutz). Mit einem Flyer wurden alle Angestellten der öffentlichen Organe über das aktualisierte Lernangebot informiert.
- Der gesamte Inhalt der Website – von juristischen Praxisbeispielen für Fachleute bis zu Musterbriefen für Bürgerinnen und Bürger – wurde an das IDG angepasst; eine Übersicht zeigt die wichtigsten Neuerungen (www.datenschutz.ch).

Im Rahmen seines gezielten Aus- und Weiterbildungsangebots für Personen, die speziell Personendaten bearbeiten, führte der Datenschutzbeauftragte weitere Seminare durch. Die Teilnehmenden werden so befähigt, den Datenschutz selbständig in ihrem Wirkungskreis sicherzustellen.

Gezielte Kooperationen

Für eine grössere Wirkung bei ausgewählten datenschutzrechtlichen Themen setzt der Datenschutzbeauftragte weiterhin auf Kooperationen: So führte er in Zusammenarbeit mit Privatim, der Vereinigung der schweizerischen Datenschutzbeauftragten, anlässlich des 2. Europäischen Datenschutztages das Seminar «Datenschutz: Was er schützt und wem er nützt» für Medienschaffende durch. Und in Zusammenarbeit mit der Stiftung für Datenschutz und Informationssicherheit veranstaltete der Datenschutzbeauftragte das Seminar «Wirkung von Datenschutzregulierung und Evaluation» sowie das «13. Symposium on Privacy and Security 2008» zum Thema «Informatik und Datenschutz im Widerstreit?» für Entscheidungsträger aus Wirtschaft, Verwaltung und Politik. Die Veranstaltungen fanden grossen Anklang und bestätigten den Bedarf an datenschutzrechtlicher Information auch in dieser Form.

Videoüberwachung bleibt aktuell

Immer mehr öffentliche Organe wenden sich wegen einer geplanten Videoüberwachung an den Datenschutzbeauftragten. Stets gilt: Eine Videoüberwachung braucht eine gesetzliche Grundlage und muss verhältnismässig sein. Und für jede Überwachungsanlage müssen konkrete Betriebsanweisungen geschaffen werden.

Ob Videoüberwachung auf öffentlichen Plätzen, im öffentlichen Verkehr oder in öffentlichen Gebäuden: Der Datenschutzbeauftragte bietet öffentlichen Organen, die Videoüberwachungen planen, seit Jahren Empfehlungen und eine Checkliste (www.datenschutz.ch). Trotzdem wird er zunehmend um Stellungnahmen zu geplanten Videoüberwachungen gebeten. Denn immer mehr öffentliche Organe prüfen den Einsatz von Videokameras, und die Technologie ermöglicht neue Arten von Überwachungskameras wie Drohnen und Unterwasserkameras.

Aus Datenschutzsicht sind bei der Videoüberwachung stets folgende Punkte zentral: Die Aufzeichnung von Personen auf Video stellt eine Bearbeitung von Personendaten dar und bedeutet einen Eingriff in das Grundrecht auf Privatheit der betroffenen Personen. Auch bei Vorliegen einer gesetzlichen Grundlage ist eine Videoüberwachung nur zulässig, wenn sie verhältnismässig ist (§ 4 Abs. 3 DSG). Eine Videoüberwachung, die Diebstähle oder Vandalismus verhindern soll, darf erst in Betracht gezogen werden, wenn andere Massnahmen, welche weniger in die Privatheit von betroffenen Personen eingreifen, nachweislich versagt haben. Der Einsatz der Kameras ist auf jene Zeiten zu beschränken, zu welchen die früheren Diebstähle und Sachbeschädigungen stattgefunden haben.

Wird der Datenschutzbeauftragte von öffentlichen Organen um eine Stellungnahme oder um eine Konzeptüberprüfung gebeten, prüft er jeweils die Verhältnismässigkeit und schlägt Lösungen zur Umsetzung vor, wie die folgenden zwei Beispiele aufzeigen:

Beispiel Kantonsschule

In einer Kantonsschule nahmen Diebstähle in der Tiefgarage, in Schulzimmern und aus Garderobenkästen zu. Gleichzeitig häuften sich Fälle von Vandalismus im Velokeller und auf dem Sportplatz, und die Schulhausfassade wurde wiederholt besprayt. Weil weder bauliche noch personelle Massnahmen die Situation verbesserten, erarbeitete die Schule ein Konzept mit Videoüberwachungsmassnahmen. Sie bat den Datenschutzbeauftragten, dieses zu überprüfen.

Der Datenschutzbeauftragte empfahl der Kantonsschule, das ausführliche Konzept in ein Reglement zu überführen, das die wesentlichen Punkte kurz erfasst und für alle betroffenen Personen einsehbar ist. Zu nennen sind der Zweck der Videoüberwachung, die verantwortliche Stelle, Ort, Zeit und Art der Überwachung, die Auswertung des Bildmaterials und das Vorgehen im Schadensfall, die Aufbewahrungsdauer sowie die organisatorischen und technischen Massnahmen zur Datensicherung. Ausserdem muss die Überwachung mit entsprechenden Hinweisschildern transparent gemacht und aufgezeigt werden, wo und bei wem das Auskunftsrecht geltend gemacht werden kann.

Beispiel Kirche

Wegen mehrerer Sachbeschädigungen in einer Kirche fragte die Kirchgemeinde den Datenschutzbeauftragten an, wie die gesetzliche Grundlage für eine Videoüberwachung geschaffen werden könne. Der Anfrage legte sie die Bestimmungen der Kirchgemeindeordnung bei.

In seiner Stellungnahme wies der Datenschutzbeauftragte darauf hin, dass die Kirchenpflege die gesetzliche Grundlage beschliessen könne. Denn gemäss Kirchgemeindeordnung obliegt der Kirchgemeinde die Verwaltung – und somit auch das Kirchengut sowie das Reglement, wie die kirchlichen Liegenschaften benutzt werden sollen.

Institutionalisierte Zusammenarbeit

Eine parlamentarische Initiative gab dem Datenschutzbeauftragten die Gelegenheit aufzuzeigen, wie die Datenflüsse innerhalb der Verwaltung geregelt sind und wie allenfalls eine institutionalisierte Zusammenarbeit zu gestalten wäre.

Sowohl die Bundesverfassung (Art. 36 BV) als auch die Kantonsverfassung (Art. 38 lit. b KV) garantieren die persönliche Freiheit der Bürgerinnen und Bürger und halten fest, dass eine Einschränkung dieses Grundrechts nur aufgrund einer gesetzlichen Grundlage erfolgen darf. Jede Bearbeitung von Informationen über Bürgerinnen und Bürger durch den Staat bedeutet einen Eingriff in das Grundrecht auf persönliche Freiheit: Ein Aspekt dieses Grundrechts ist das Recht auf Privatheit und die informationelle Selbstbestimmung. Das DSG respektive neu das IDG halten diese Rahmenbedingungen fest. So wird als Rechtfertigungsgrund für den Eingriff in die Privatheit eine gesetzliche Grundlage verlangt, die verhältnismässig sein muss. Die Datenbearbeitung ist zudem auf einen im Voraus festgelegten Zweck beschränkt.

Rechtsgrundlage und Amtshilfe

Die Verwaltungsstellen haben verschiedene Rechtsgrundlagen, die ihnen einen Informationsaustausch ermöglichen. In erster Linie sind dies Mitteilungsrechte und Mitteilungspflichten in bereichsspezifischen Gesetzen. Im Einzelfall kann aber auch die Einwilligung der betroffenen Person eingeholt werden. Sofern diese Voraussetzungen nicht gegeben sind, besteht die Möglichkeit der Amtshilfe: Eine Verwaltungsstelle kann bei einer anderen Stelle die gewünschte Information nachfragen, sofern sie diese für ihre Verwaltungsaufgaben unabdingbar braucht. Eine Pflicht zur Amtshilfe ist im Verfahrensrecht statuiert, wobei sich die Amtshilfe nur auf einen Einzelfall beziehen kann.

Der Austausch von besonderen Personendaten ist grundsätzlich nur aufgrund einer formellgesetzlichen Rechtsgrundlage möglich, da die Bearbeitung von sensiblen Daten immer einen schweren Eingriff in die persönliche Freiheit bedeutet.

Verschiedene Varianten

Soll nun die Zusammenarbeit von Verwaltungsstellen in einem bestimmten Bereich institutionalisiert werden, stellt sich die Frage nach einer entsprechenden Rechtsgrundlage. Eine solche Rechtsgrundlage könnte sich im bereichsspezifischen Recht der Verwaltungsstelle befinden, indem beispielsweise ein Mitteilungsrecht oder eine Mitteilungspflicht statuiert ist. Dieser amtsspezifischen Betrachtungsweise steht eine aufgabenspezifische Betrachtungsweise gegenüber. Es wäre auch denkbar, dass in einer aufgabenspezifischen Zusammenarbeit, die in einem spezifischen Fachgesetz geregelt ist, die Möglichkeit der Bekanntgabe von personenbezogenen Informationen vorgesehen wäre. In beiden Fällen braucht es aber eine transparente Regelung, aus der klar hervorgeht, welche Informationen zu welchem Zweck an welche Amtsstelle weitergegeben werden. Damit einher muss auch die Regelung der Verantwortlichkeiten der involvierten Verwaltungsstellen gehen.

Die institutionalisierte Zusammenarbeit zeigt sich in erster Linie als fachspezifischer Datenaustausch. Der Datenschutzbeauftragte ist deshalb der Auffassung, dass entsprechende Rahmenbedingungen in der materiellen Fachgesetzgebung zu schaffen sind und eher nicht in der Datenschutzgesetzgebung.

Vorzeitige Löschung von Daten im Polis

Das Bundesgericht kommt in einem neuen Entscheid zum Schluss, dass sich eine vorzeitige Löschung im Polizei-Informationssystem Polis im Einzelfall rechtfertigen lässt – und bestätigt damit die Haltung des Datenschutzbeauftragten.

Wegen Registrierungen im Polizei-Informationssystem Polis wenden sich Bürgerinnen und Bürger immer wieder an den Datenschutzbeauftragten – hauptsächlich weil sie Daten löschen oder berichtigen wollen. Die Verordnung über das Polizei-Informationssystem Polis (Polis-Verordnung) ist seit dem 1. Januar 2006 in Kraft. Polis dient nicht nur der Ermittlung und Fahndung, sondern dokumentiert auch das polizeiliche Handeln. Die im Polis erfassten Daten entsprechen dem Erkenntnisstand zum Zeitpunkt der Eingabe und werden – vorbehältlich der Löschung – nicht von Amtes wegen nachgeführt. Bei einem Freispruch, einer Verfahrenseinstellung oder wenn ein Strafverfahren sistiert oder nicht weiterverfolgt wird, können betroffene Personen unter Vorlage eines rechtskräftigen Entscheides eine ergänzende Eintragung erwirken.

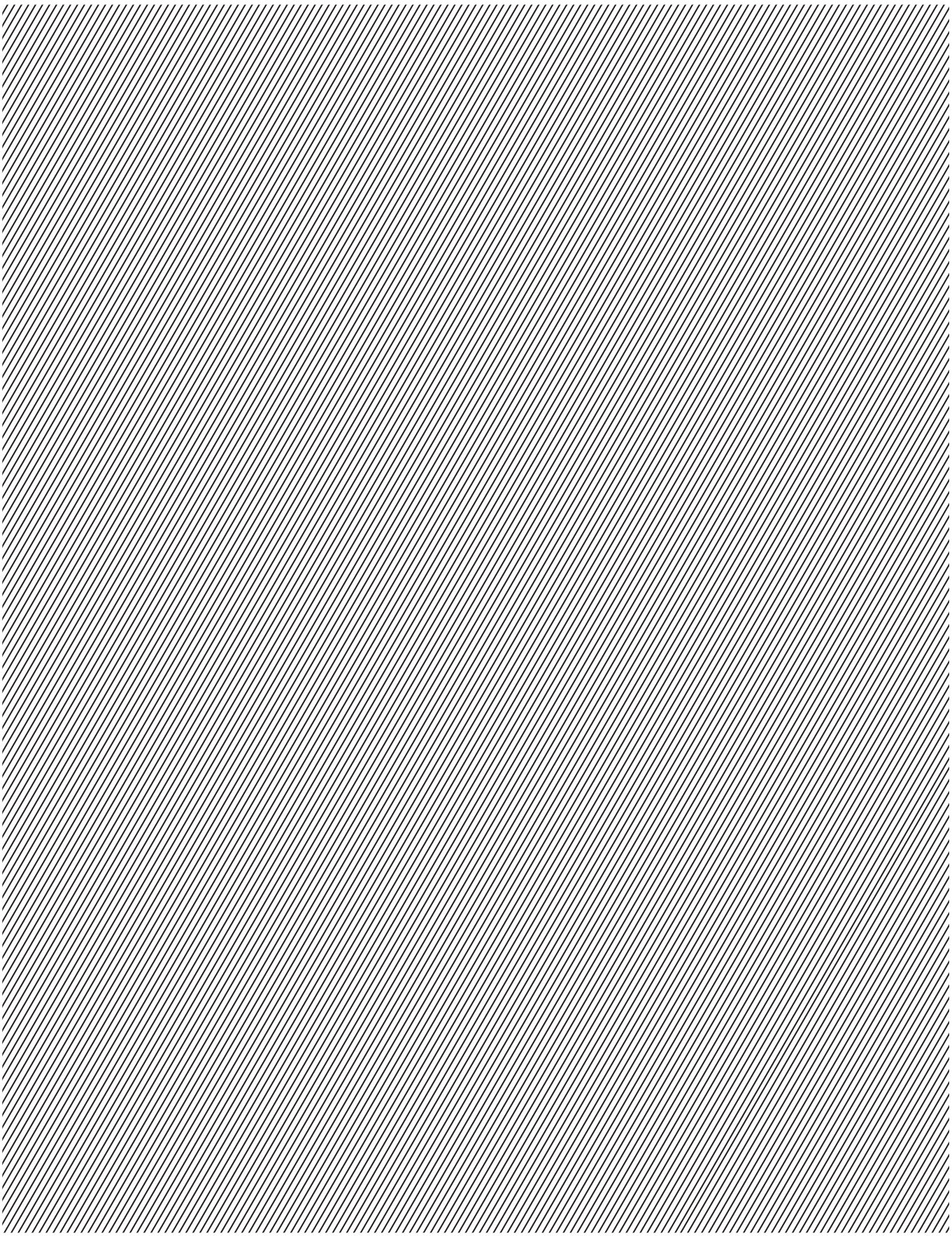
Der Datenschutzbeauftragte hat wiederholt darauf hingewiesen, dass die starre Anwendung der im Polis festgelegten Löschfristen im Einzelfall unverhältnismässig ist. Ausserdem sollten Berichtigungen von Amtes wegen erfolgen (siehe Tätigkeitsbericht Nr. 11 [2005], S. 35, und Tätigkeitsbericht Nr. 2 [1996], S. 11).

Der Kantonsrat hat Ende April 2007 zwei Motionen der Geschäftsprüfungskommission an den Regierungsrat überwiesen, die fordern, dass Polis in ein operatives System und in ein Archivsystem aufgeteilt werden soll. Zudem soll die Nachführung oder Aktualisierung der Polis-Daten regelmässig vom Datenschutzbeauftragten kontrolliert werden (siehe Tätigkeitsbericht Nr. 13 [2007], S. 33).

Das Bundesgericht hat sich in seinem Urteil vom 30. September 2008 (1C_51/2008) mit dem Löschungsbegehren eines Verdächtigen auseinandergesetzt, dessen Personendaten im Zusammenhang mit seiner Verhaftung im Polis erfasst wurden. Die Strafuntersuchung wurde kurze Zeit später eingestellt. Das kantonale Verwaltungsgericht lehnte das Begehren des Beschwerdeführers auf Löschung seiner Personendaten im Polis ab. Zur Begründung führte es an, dass das Interesse an einer lückenlosen Dokumentation polizeilicher Ereignisse im Polis bis zum Ablauf der Frist gemäss Polis-Verordnung (§ 18) gegenüber dem privaten Anliegen einer vorzeitigen Datenlöschung überwiege.

Gemäss Rechtsprechung kann die Aufbewahrung erkennungsdienstlichen Materials (DNA-Profile) gegen die Unschuldsvermutung verstossen, wenn die Behörden damit ausdrücken, die betroffene Person sei doch schuldig, obwohl sie freigesprochen oder das Strafverfahren eingestellt worden ist (BGE 124 I 80 E. 2e S. 84; 128 II 259 E. 3.6 S. 275 f.).

Das Bundesgericht hat nun ausgeführt, dass die Kantone bei polizeilichen Datensammlungen einen gewissen Spielraum bei der Festlegung der Zeiträume für die Datenaufbewahrung nach Abschluss der erfassten Geschäfte besässen. Wesentlich sei, ob die fraglichen Personendaten für die polizeiliche Arbeit bei der Verfolgung und Aufklärung oder bei der Verhütung von Delikten nicht mehr nötig seien. Wenn der Betroffene nicht nur erwiesenermassen unschuldig sei, sondern auch versehentlich in eine Strafuntersuchung geraten sei, beispielsweise aufgrund einer Verwechslung, sei hingegen der Einzelfall zu prüfen. Das Verwaltungsgericht habe das rechtliche Gehör des Beschwerdeführers verletzt, indem es beim umstrittenen Löschungsbegehren die Gründe, die zur Einstellung der Strafuntersuchung geführt hätten, nicht ausreichend geprüft habe. Das Verwaltungsgericht habe sich mit dem blossen Nachtrag über die Einstellung des Strafverfahrens im Polis begnügt. Dies genüge einer verfassungskonformen Handhabung der Berichtigungspflicht gemäss Polis-Verordnung nicht (§ 13 Abs. 3) und erfülle auch die Erfordernisse des Gehörsanspruchs nicht. Polis müsse technisch so eingerichtet sein, dass der frühere Status als Angeschuldigter sofort erkennbar relativiert werde, wenn der strafrechtliche Verfahrensabschluss nachgetragen und eine vorzeitige Löschung zu Recht abgelehnt werde. Andernfalls könne trotz allem der Eindruck entstehen, die weiterhin erfasste Person werde immer noch als tatverdächtig betrachtet.



Fälle aus der Beratungstätigkeit
Anhang

Titel: IV-Stelle klärt Gesundheitszustand ab
URL: http://www.datenschutz.ch/themen/1383.php
Datum: 03.03.2009

01.

IV-Stelle klärt Gesundheitszustand ab

Sachbearbeitende der Invalidenversicherungsstelle sind berechtigt, Gesundheitsdaten von Versicherten zu bearbeiten, wenn sie die Voraussetzungen zur Leistungserbringung überprüfen müssen. Dazu gehören auch Unterlagen über den Gesundheitszustand.

Der Datenschutzbeauftragte wurde von betroffenen Personen angefragt, ob Sachbearbeitende der Invalidenversicherungsstelle (IV-Stelle) Gesundheitsdaten bearbeiten dürften. Nach Abklärung bei der Sozialversicherungsanstalt (SVA) gelangte er zu folgender Einschätzung:

Eine versicherte Person stellt der Invalidenversicherung (IV) ein Gesuch um eine Leistung, beispielsweise für medizinische Eingliederungsmassnahmen oder Rentenleistungen. Weil für sie eine Auskunftspflicht gegenüber der IV-Stelle besteht, unterschreibt sie mit der Anmeldung zum Leistungsbezug eine Ermächtigung, mit der sie die erwähnten Personen und Stellen gegenüber der IV von der Schweigepflicht entbindet (Art. 6a Abs. 1 Invalidenversicherungsgesetz [IVG]). Für weitere Personen und Stellen, die in der Anmeldung nicht erwähnt sind, erteilt die versicherte Person im Voraus eine Generalvollmacht (Art. 6a Abs. 2 IVG); diese Personen und Stellen können jedoch nicht zu einer Auskunft verpflichtet werden.

Bei einem Leistungsbegehren an die IV ist die IV-Stelle einzige Anlaufstelle. Zu ihren Aufgaben gehört die Abklärung der versicherungsmässigen Leistungsvoraussetzungen. Dazu kann sie die erforderlichen Unterlagen über den Gesundheitszustand beschaffen (Art. 69 Abs. 2 Verordnung über die Invalidenversicherung [IVV]).

Der Regionale Ärztliche Dienst (RAD) steht der IV-Stelle als Fachstelle zur Beurteilung der medizinischen Voraussetzungen des Leistungsanspruchs zur Verfügung. Die IV-Stelle erteilt dem RAD entsprechende Abklärungsaufträge. Der RAD setzt die für die Invalidenversicherung massgebende funktionelle Leistungsfähigkeit der Versicherten für eine zumutbare Erwerbstätigkeit oder eine Tätigkeit in deren Aufgabenbereich fest. Der RAD ist in seinem medizinischen Sachentscheid im Einzelfall unabhängig (Art. 59 Abs. 2 und 2bis IVG und Art. 69 Abs. 4 IVV).

Die administrativen Abläufe erfolgen während der gesamten Abklärung über die IV-Stelle, welche die notwendigen medizinischen und beruflichen Informationen beim Versicherten, bei den Arztpersonen, Arbeitgebern und weiteren Abklärungsstellen einholt.

Der RAD erstattet der IV-Stelle Bericht. Die IV-Stelle entscheidet sodann über die medizinischen oder beruflichen Massnahmen oder über eine Berentung. Der RAD untersteht keiner beruflichen Schweigepflicht gegenüber der IV-Stelle: Die angestellten Arztpersonen müssen der IV-Stelle gegenüber Auskunft erteilen.

Weil die IV-Stelle die versicherungsmässigen Voraussetzungen zur Leistungserbringung überprüfen muss, sind deren Sachbearbeitende somit berechtigt, Gesundheitsdaten von Versicherten zu bearbeiten und dazu die erforderlichen Unterlagen über den Gesundheitszustand einzuholen.

Titel: Backgroundcheck für Flughafenangestellte
URL: http://www.datenschutz.ch/themen/1384.php
Datum: 03.03.2009

02.

Backgroundcheck für Flughafenangestellte

Bevor Personen, die im Sicherheitsbereich des Flughafens tätig sind, einen Flughafenausweis erhalten, erfolgt ein Backgroundcheck nach den Vorgaben des Nationalen Sicherheitsprogramms. Sie müssen dazu einen aktuellen Auszug des zentralen Strafregisters vorweisen, und die Polizei kann weitere Überprüfungen durchführen.

Eine Stellenbewerberin für Reinigungsarbeiten in Flugzeugen beim Flughafen Zürich hat eine ihr bereits zugesagte Stelle nicht erhalten, nachdem die Airport Security der Reinigungsfirma als zukünftige Arbeitgeberin mitgeteilt hatte, dass die Stellenbewerberin die Bedingungen für einen Flughafenausweis nicht erfülle.

Daraufhin wandte sich der Rechtsvertreter der Stellenbewerberin an den Datenschutzbeauftragten mit der Frage, ob die Kantonspolizei einen Fehler gemacht habe, als sie aufgrund von Informationen aus der Datenbank Polis gegenüber der Airport Security empfohlen hatte, seiner Mandantin keinen Flughafenausweis abzugeben. Weiter wollte der Rechtsvertreter wissen, ob allenfalls Schadenersatz verlangt werden könne.

Die Abklärungen des Datenschutzbeauftragten ergaben Folgendes: Der Flughafen Zürich ist in verschiedene Zutrittszonen unterteilt. Das als Sicherheitsbereich definierte Gebiet darf nur betreten oder befahren, wer als Fluggast abfliegt oder einreist oder ein dienstliches Bedürfnis nachweist und durch den Besitz eines gültigen Ausweises als zutrittsberechtigt gekennzeichnet ist. Vor Abgabe eines Flughafenausweises erfolgt ein Backgroundcheck nach den Vorgaben des Nationalen Sicherheitsprogramms Luftfahrt. Für dessen Durchführung muss die Kantonspolizei von der betroffenen Person die vorgängige schriftliche Einwilligung einholen.

Art. 4 der Verordnung UVEK über Sicherheitsmassnahmen im Luftverkehr (SR 748.122) bildet im konkreten Fall die gesetzliche Grundlage für die Bekanntgabe dieser besonders schützenswerten Personendaten. Die betroffene Stellenbewerberin hat vorgängig explizit dazu eingewilligt, dass die Kantonspolizei Einsicht in die polizeilichen Register nimmt, um der Airport Security eine Empfehlung abzugeben, ob ihr ein Flughafenausweis ausgestellt werden solle. Die Kantonspolizei hat nur eine Empfehlung und keine detaillierten Registerauszüge aus Polis bekannt gegeben, was als verhältnismässig erscheint.

Titel: Test über kognitive Fähigkeiten
URL: http://www.datenschutz.ch/themen/1385.php
Datum: 03.03.2009

03.

Test über kognitive Fähigkeiten

An den Mittelschulaufnahmeprüfungen wird ein vorerst noch freiwilliger Test zu den allgemeinen kognitiven Fähigkeiten der Kandidierenden (AKF-Test) durchgeführt. Dies erfolgt im Rahmen eines Forschungsprojektes.

Eltern informierten den Datenschutzbeauftragten, dass an den Mittelschulen zusätzlich zu den Aufnahmeprüfungen ein Test zu den allgemeinen kognitiven Fähigkeiten der Kandidatinnen und Kandidaten durchgeführt werde. Sie verlangten Einsicht in die Tests.

Der Datenschutzbeauftragte unterbreitete dem Mittelschul- und Berufsbildungsamt verschiedene Fragen zum Test für Allgemeine Kognitive Fähigkeiten (AKF-Test). Er verlangte Aufschluss über den Zweck und Ablauf des Tests sowie über die Aufbewahrung und die Auswertung der Antworten. Das Mittelschul- und Berufsbildungsamt beantwortete die Fragen und wies darauf hin, dass sich der AKF-Test noch in der Erprobungsphase befinde.

Werden Personendaten für Forschungszwecke bearbeitet, ist eine erleichterte Bearbeitung zugelassen, da diese nach der Auswertung schnellstmöglich zu anonymisieren sind und die Ergebnisse nur so veröffentlicht werden dürfen, dass die betroffenen Personen nicht bestimmbar sind.

Der Datenschutzbeauftragte kam zum Schluss, dass während der Erprobungsphase des AKF-Tests noch kein personenbezogener Zweck verfolgt wird. Vielmehr soll erforscht werden, ob die Erfolgschancen von Kandidierenden, welche die entsprechenden intellektuellen Fähigkeiten zwar besitzen, in den geprüften Fächern aber aus anderen Gründen benachteiligt sind, erhöht werden können. Die Auswertung der Tests erfolgt zentral, so dass weder die Kandidatinnen und Kandidaten noch die Schulen die Einzelergebnisse erfahren. Während der Erprobungsphase hat nur das auswertende Institut Zugriff auf die Tests. Der zusammenfassende Bericht zuhanden der Bildungsdirektion erfolgt als Forschungsbericht und ohne Bezug zu einzelnen Personen. Während der Erprobung hat das Testergebnis zudem keinen Einfluss auf den Promotionsentscheid. Somit kann davon ausgegangen werden, dass die Ergebnisse so veröffentlicht werden, dass die betroffenen Personen nicht bestimmbar sind.

Der Datenschutzbeauftragte wies das Mittelschul- und Berufsbildungsamt darauf hin, dass die Erprobungsphase des AKF-Tests gesetzlich nicht geregelt ist und deshalb niemand zur Teilnahme gezwungen werden kann. Aus Transparenzgründen müssen die Kandidatinnen und Kandidaten sowie deren gesetzliche Vertretungen vorgängig über Sinn und Zweck des Tests aufgeklärt werden. Sie müssen auch informiert werden, dass der Test freiwillig ist und eine Nichtteilnahme keinerlei Konsequenzen hat. Gleichzeitig müssen sie Angaben darüber erhalten, wie lange die Fragebogen aufbewahrt werden, was danach mit ihnen geschieht und welche organisatorischen und technischen Massnahmen gegen deren unbefugte Bearbeitung getroffen wurden.

Weil die Ergebnisse in der Erprobungsphase anonymisiert veröffentlicht werden, entfällt das Auskunftsrecht der betroffenen Personen.

Für den Fall, dass aufgrund der Erprobungsergebnisse der AKF-Test promotionsentscheidend eingeführt werden sollte, hielt der Datenschutzbeauftragte fest, dass die entsprechenden gesetzlichen Grundlagen geschaffen werden müssten. Weil es sich um besondere Personendaten handelt, braucht es eine hinreichend bestimmte Regelung in einem formellen Gesetz.

Titel: Informationen für schulische Heilpädagogen
URL: http://www.datenschutz.ch/themen/1386.php
Datum: 03.03.2009

04.

Informationen für schulische Heilpädagogen

Die Umstellungen im Schulbereich aufgrund des revidierten Volksschulgesetzes ermächtigen den Schulpsychologischen Dienst nicht, Kopien seiner Abklärungsberichte an die schulischen Heilpädagogen abzugeben.

Die Delegiertenkommission des Zweckverbandes für den Schulpsychologischen Dienst (SPD) eines Bezirkes befasste sich mit der Frage, ob schulische Heilpädagoginnen, die als Verantwortliche für die therapeutische Förderung der Kinder eine zentrale Funktion innehaben, neu eine Kopie des SPD-Abklärungsberichtes erhalten sollen. Bisher hatten die schulischen Heilpädagogen nur Einsichtsrecht im Schulsekretariat oder bei der Schulleitung. Der Datenschutzbeauftragte wurde um eine Stellungnahme gebeten.

Ein öffentliches Organ kann besondere Personendaten unter anderem bekannt geben, wenn eine hinreichend bestimmte Regelung dieses in einem formellen Gesetz ausdrücklich dazu ermächtigt. Einem anderen öffentlichen Organ gibt es im Einzelfall besondere Personendaten ausserdem bekannt, wenn das Organ, das besondere Personendaten verlangt, diese zur Erfüllung seiner gesetzlichen Aufgaben benötigt.

Seit den organisatorischen Umstellungen im Rahmen des revidierten Volksschulgesetzes haben sich keine Änderungen bei den Anfragen schulischer Heilpädagoginnen an den Schulpsychologischen Dienst ergeben. Die schulischen Stellen benötigen somit nur jene Informationen, die für die Beschulung geeignet und erforderlich sind. Die Berichte des SPD enthalten in aller Regel jedoch weit mehr als diese Informationen.

Der Datenschutzbeauftragte schlug vor, dass der SPD zuhanden der schulischen Stellen einen Kurzbericht erstellt, mit den für die Beschulung notwendigen Informationen über die Schülerinnen und Schüler sowie mit den empfohlenen Massnahmen. Der Kurzbericht geht statt wie bisher an die Schulpflege neu an die Schulleitung. Weitere beteiligte Lehrpersonen wie Heilpädagoginnen erhalten dort Einsicht. Die Berichte sind sicher aufzubewahren.

Titel: Inhalt aufbewahrter Strafakten
URL: http://www.datenschutz.ch/themen/1387.php
Datum: 03.03.2009

05.

Inhalt aufbewahrter Strafakten

Bei der Aufbewahrung von Akten aus Strafverfahren ist der Grundsatz der Verhältnismässigkeit zu beachten. Personendaten dürfen so lange aufbewahrt werden, wie es für die Erfüllung der gesetzlichen Aufgaben der Strafverfolgungsbehörde geeignet und erforderlich ist.

Ein Mann wurde verdächtigt, eine strafbare Handlung begangen zu haben. Er wurde von der Polizei verhaftet und erkennungsdienstlich behandelt. Das Foto des Verhafteten wurde dem Polizeirapport beigeheftet. Weil sich der Tatverdacht nicht erhärten liess, stellte die Staatsanwaltschaft das Verfahren ein.

Der Mann stellte bei der Polizei das Gesuch, das elektronisch gespeicherte Foto aus dem Polizei-Informationssystem Polis zu löschen. Die Polizei kam diesem Ersuchen nach.
Die Staatsanwaltschaft hingegen weigerte sich, das Foto aus den aufbewahrten Originalakten zu entfernen. Der Rekurs an die Oberstaatsanwaltschaft wurde abgewiesen. Der Rekursentscheid wurde nicht an die nächste Instanz weitergezogen und wurde damit rechtskräftig.

Der Mann wollte vom Datenschutzbeauftragten wissen, ob mit der bevorstehenden Einführung des IDG ein neuer Anspruch auf Löschung des Fotos bestehen werde.

Das DSG ist nur auf abgeschlossene Strafverfahren anwendbar (§ 3 Abs. 2 lit. a DSG). Das IDG dagegen gilt sowohl für abgeschlossene als auch für hängige Strafverfahren. Nicht vom IDG erfasst wird die Rechtsprechungstätigkeit von Gerichten (§ 2 Abs. 1 IDG). Bei abgeschlossenen Strafverfahren bestehen damit keine grundlegenden Unterschiede zwischen DSG und IDG. Die Bearbeitung von Personendaten bei abgeschlossenen Strafverfahren muss den datenschutzrechtlichen Grundsätzen der Verhältnismässigkeit entsprechen: Die Archivierung der Personendaten muss für die gesetzlichen Aufgaben geeignet und erforderlich sein. Die Strafverfolgungsbehörde ist grundsätzlich zur vollständigen Aktenführung verpflichtet. Sind jedoch im Einzelfall bestimmte Personendaten nicht geeignet und erforderlich, um das abgeschlossene Verfahren zu dokumentieren, können sie gelöscht werden.

Der Datenschutzbeauftragte nahm Einsicht in die aufbewahrten Akten der Staatsanwaltschaft und gelangte zum Ergebnis, dass es nicht erforderlich sei, das Foto aufzubewahren. Weil die Staatsanwaltschaft diese Auffassung nicht teilte, beliess sie es in den Akten.

Titel: Rechtsweggarantie im Datenschutzrecht
URL: http://www.datenschutz.ch/themen/1388.php
Datum: 03.03.2009

06.

Rechtsweggarantie im Datenschutzrecht

Die vorgesehenen Anpassungen im kantonalen Verfahrensrecht sollen gewährleisten, dass das Verwaltungsgericht als unabhängige richterliche Instanz grundsätzlich über alle datenschutzrechtlichen Streitigkeiten entscheidet.

Das kantonale Verwaltungsgericht ist in der Vergangenheit auf mehrere Beschwerden im Zusammenhang mit Datenschutzstreitigkeiten auf dem Gebiet des Strafrechts nicht eingetreten. Zur Begründung führte es jeweils aus, dass sich vor Verwaltungsgericht keine Streitigkeiten über Daten austragen liessen, welche in einem förmlichen, zu einer erstinstanzlichen Anordnung führenden Verfahren erhoben worden seien, dessen Grundmaterie ein Anrufen des Verwaltungsgerichtes ausschliesse. Gemäss § 43 Abs. 1 lit. g Verwaltungsrechtspflegegesetz handelt es sich bei der zur Frage stehenden Grundmaterie um Anordnungen in Straf- und Polizeistrafsachen, einschliesslich Vollzug von Strafen.

Ein Beschwerdeführer wandte sich an den Datenschutzbeauftragten mit der Frage, bei welcher unabhängigen gerichtlichen Instanz er einen ablehnenden Rekursentscheid der Oberstaatsanwaltschaft anfechten könne (Rechtsweggarantie). Im fraglichen Entscheid seien seine geltend gemachten datenschutzrechtlichen Ansprüche im Zusammenhang mit einer gegen ihn geführten und inzwischen eingestellten Strafuntersuchung abgelehnt worden.

Die Anfrage fiel zeitlich in die Vernehmlassungsfrist zu den Änderungen im kantonalen Verfahrensrecht, das im Zusammenhang mit der Rechtsweggarantie an übergeordnetes Recht angepasst werden muss (Art. 29a Bundesverfassung, Art. 130 Bundesgesetz über das Bundesgericht und Art. 76 f. i.V.m. Art. 138 Kantonsverfassung).

Der Datenschutzbeauftragte nahm den konkreten Fall zum Anlass, die zuständigen Behörden darauf aufmerksam zu machen, dass datenschutzrechtliche Streitigkeiten durch ein unabhängiges Gericht beurteilt werden sollten, und zwar unabhängig davon, auf welche Grundmaterie ein erstinstanzlicher Rekursentscheid sich abstützt.

Titel: Schulungsfilm über Menschen mit Demenz
URL: http://www.datenschutz.ch/themen/1389.php
Datum: 03.03.2009

07.

Schulungsfilm über Menschen mit Demenz

In einem Filmprojekt über den emotionalen Ausdruck bei Menschen mit Demenz müssen gesetzliche Vertreter vor ihrer Einwilligung umfassend informiert und auf das Widerrufsrecht aufmerksam gemacht werden. Eine Drittfirma darf kein filmisches Rohmaterial weiterverwerten.

Die Universität Zürich wollte einen Film zum emotionalen Ausdruck von Menschen mit Demenz produzieren. Emotionen im Alltag von Demenzpatientinnen und -patienten sollten in Körperhaltung, Mimik und Verhalten exemplarisch dargestellt werden. Der Film sollte für die Schulung von Pflegepersonal sowie in der universitären Forschung und Lehre eingesetzt werden. Beabsichtigt war, den Film durch eine private Produktionsfirma realisieren zu lassen, die das filmische Rohmaterial auch für ein Nachfolgeprojekt hätte verwenden dürfen. Vor der Unterzeichnung der Produktionsverträge hat die Universität Zürich den Datenschutzbeauftragten um eine rechtliche Beurteilung der Projektunterlagen gebeten.

Demenzpatientinnen und -patienten können mangels Urteilsfähigkeit keine Einwilligung für ihre Darstellung im Filmprojekt geben. Die Universität Zürich hat deshalb ein Formular für die Einwilligung der gesetzlichen Vertreter und Angehörigen erstellt. Dieses beschreibt in groben Umrissen Ziel und Inhalt des Films sowie den Ablauf der Dreharbeiten. Im Formular wird auch darauf hingewiesen, dass der Rohschnitt des Films den Unterzeichneten zur Ansicht gezeigt werde.

Der Datenschutzbeauftragte wies in seiner Stellungnahme darauf hin, dass bei Urteilsunfähigkeit der Betroffenen nur ein Vormund oder Beistand in die Bearbeitung der besonderen Personendaten im Rahmen dieses Filmprojekts einwilligen könne. Urteilsunfähige Personen ohne Vormund oder Beistand könnten in dieser Sache nicht durch deren Angehörige vertreten werden. Verwandtschaft und persönliche Verbundenheit begründeten keine rechtliche Vertretungsmacht.

Der Datenschutzbeauftragte verlangte eine umfassende Aufklärung der Personen, welche die Einwilligung erteilen sollen: Sowohl der Adressatenkreis des Schulungsfilms als auch dessen Inhalt müssen konkreter umschrieben sein. Zudem soll Klarheit darüber bestehen, ob die Demenzpatientinnen und -patienten namentlich erwähnt und im Kontext des Pflegeheims gezeigt werden. Auf dem Einwilligungsformular soll ferner ausdrücklich auf das Widerrufsrecht hingewiesen werden. Dabei soll das Recht, die Einwilligung bei der Sichtung des Rohschnitts des Films zu widerrufen, explizit erwähnt werden. Entsprechend ist eine Frist festzusetzen, bis zu deren Ablauf ein allfälliger Widerruf spätestens zu erfolgen hat.

In seiner Stellungnahme wies der Datenschutzbeauftragte auch auf die datenschutzrechtliche Verantwortlichkeit der Universität Zürich hin: Zieht die Universität Zürich eine Drittfirma für die Produktion des Films bei, muss sie den Datenschutz durch Auflagen und Vereinbarungen sicherstellen. Eine pauschale Überlassung von Urheberrechten und Rohmaterial ist nicht zulässig.

Die Universität Zürich berücksichtigte die Hinweise des Datenschutzbeauftragten und passte das Formular der Einwilligungserklärung entsprechend an. An die produzierende Drittfirma wurden zudem keine Rechte am Rohmaterial des Filmes übertragen.

Titel: Listen von HPV-Impfungen
URL: http://www.datenschutz.ch/themen/1390.php
Datum: 03.03.2009

08.

Listen von HPV-Impfungen

Um seine gesetzlichen Aufgaben zu erfüllen, kann der Kantonsärztliche Dienst Listen mit bestimmten Angaben über HPV-Impfungen verlangen. Dies teilte der Datenschutzbeauftragte einem Hausarzt mit, der im Rahmen des kantonalen Impfprogramms die Bewilligung für HPV-Impfungen mit entsprechenden Auflagen erhalten hat.

Im Kanton Zürich wurde im Sommer 2008 das Impfprogramm für Mädchen und junge Frauen gegen Humane Papillomaviren (HPV) gestartet. Die Kosten werden von den Krankenkassen getragen. Der Kanton tritt gegenüber den Krankenversicherungen respektive Santésuisse als Rechnungssteller auf und vergütet Hausärzten pro Injektion inklusive Information eine Pauschale von 15 Franken.

Hausärzte, die HPV-Impfungen durchführen wollen, können bei der Gesundheitsdirektion ein Gesuch stellen. Sie erhalten eine Bewilligung für HPV-Impfungen mit der Auflage, dass sie eine Liste der geimpften Frauen mit Name, Vorname, Wohnort und Geburtsdatum führen. Die Liste muss dem Kantonsärztlichen Dienst jeweils Ende Jahr zugestellt werden.

Ein Hausarzt, der HPV-Impfungen vornimmt, fragte den Datenschutzbeauftragten, ob die Datenerhebung durch den Kantonsärztlichen Dienst rechtmässig sei. Der Datenschutzbeauftragte hielt dazu Folgendes fest:

Der Kantonsärztliche Dienst darf Personendaten erheben, soweit dies zur Erfüllung der gesetzlich umschriebenen Aufgaben geeignet und erforderlich ist.

Der Kantonsarzt ist – neben der Gesundheitsdirektion und den Bezirksärzten – für den Vollzug der eidgenössischen Epidemiegesetzgebung zuständig (§ 1 Vollzugsverordnung zur eidgenössischen Epidemiegesetzgebung).

Bei Impfungen, die in der Verordnung des Eidgenössischen Departements des Inneren über Leistungen in der obligatorischen Krankenpflegeversicherung (KLV) aufgeführt sind, stellen die ärztlichen Leistungserbringer direkt unter Angabe der Personalien der versicherten Personen und der erbrachten Leistungen über den TARMED Rechnung. Im Gegensatz dazu wird die Kostenübernahme für die HPV-Impfung an ein kantonales Impfprogramm nach Epidemiegesetz gebunden. Die Listenführung über HPV-Impfungen dient einerseits der Kontrolle des Kantons gegenüber den Leistungserbringern, andererseits um im Bedarfsfall Rechenschaft gegenüber den Krankenversicherungen ablegen zu können.

Die Impflisten werden vom Kantonsärztlichen Dienst fünf Jahre aufbewahrt und anschliessend vernichtet. Die verzeichneten Personendaten werden ausschliesslich für Kontroll- und Dokumentationszwecke verwendet und keinen Drittpersonen bekannt gegeben. Insbesondere werden die Daten auch nicht für die Durchimpfungsrate ausgewertet.

Der Datenschutzbeauftragte gelangte zum Schluss, dass die Impflisten zur Erfüllung der gesetzlich umschriebenen Aufgaben des Kantonsärztlichen Dienstes geeignet und erforderlich sind. Dem anfragenden Arzt wurde bestätigt, dass die Datenbearbeitung durch den Kantonsärztlichen Dienst rechtmässig ist.

Titel: Listen über Aufnahmeprüfung
URL: http://www.datenschutz.ch/themen/1391.php
Datum: 03.03.2009

09.

Listen über Aufnahmeprüfung

Bei der Amtshilfe ist die Bekanntgabe von Personendaten im Einzelfall möglich. Die regelmässige Anfrage von Listenauskünften sind keine Einzelfälle.

Eine Kantonsschule wurde vermehrt von Schulpflegen angefragt, ob Schülerinnen und Schüler aus ihrer Schulgemeinde die Aufnahmeprüfung bestanden hätten. Die Kantonsschule gelangte an den Datenschutzbeauftragten mit der Frage, ob sie Schulpflegen diese Auskünfte erteilen dürfe.

Weil keine gesetzliche Grundlage für die gewünschte Datenbekanntgabe an Schulpflegen besteht, prüfte der Datenschutzbeauftragte, ob die Daten amtshilfeweise übermittelt werden dürfen.

Im Einzelfall dürfen Personendaten bekannt gegeben werden, wenn sie für die öffentlichen Aufgaben des Empfängers notwendig sind (§ 8 Abs. 1 lit. a DSG). Werden ganze Listen von Schülerinnen und Schülern über das Bestehen von Aufnahmeprüfungen eingefordert und erfolgt dies regelmässig, so liegt jedoch kein Einzelfall vor.

Der Datenschutzbeauftragte beurteilte die regelmässige Bekanntgabe unter diesen Umständen als nicht rechtmässig, bis eine gesetzliche Grundlage hierfür geschaffen wird.

Titel: Überwachung bei Sportveranstaltungen
URL: http://www.datenschutz.ch/themen/1392.php
Datum: 03.03.2009

10.

Überwachung bei Sportveranstaltungen

Ausschreitungen bei Sportveranstaltungen sind der Anlass, Zuschauerinnen und Zuschauer vermehrten Kontrollen zu unterziehen. Hierfür sind klare und verhältnismässige Rechtsgrundlagen notwendig.

Die Geschäftsprüfungskommission des Kantonsrates (GPK) hat sich in einem Schwerpunktthema über die datenschutzrechtlichen Rahmenbedingungen bei Vorkehrungen gegen Gewalt bei Sportveranstaltungen vom Datenschutzbeauftragten informieren lassen.

Im Rahmen einer Revision des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) wurden verschiedene Instrumente geschaffen, um Gewaltausschreitungen bei Sportveranstaltungen zu verhindern. Als zentrales Mittel der Informationsbearbeitung wurde eine Hooligandatenbank (Hoogan) eingerichtet. Da die Bundeszuständigkeit für diese Massnahmen nicht gegeben ist, sollen die Bestimmungen per 1. Januar 2010 in ein Konkordat der Kantone überführt werden. Aus datenschutzrechtlicher Sicht sind sowohl die Angaben, die in Hoogan geführt werden, als auch die weiteren Massnahmen zu wenig bestimmt. So bleibt unklar, welches Verhalten zu einem Eintrag in die Datenbank führt und wie die Richtigkeit der Einträge gewährleistet wird. Zudem stehen den betroffenen Personen in Bezug auf ihr verfassungsmässiges Recht auf persönliche Freiheit nur ungenügende Verfahrensrechte zur Verfügung – beispielsweise für die Berichtigung oder Löschung von falschen Einträgen. Auch die aufsichtsrechtlichen Zuständigkeiten sind unklar geregelt.

Weil Zuschauerinnen und Zuschauer bei Sportveranstaltungen vermehrt kontrolliert und überwacht werden sollen, fordert der Datenschutzbeauftragte, dass in diesem Bereich die Zuständigkeit der involvierten öffentlichen Organe und deren Zusammenarbeit mit privaten Veranstaltern oder Stadionbetreibern klar geregelt wird. Zudem müssen die eingeführten und die geplanten Massnahmen auf ihre Verhältnismässigkeit hin überprüft werden.

Angesichts der geplanten Einführung eines biometrischen Gesichtserkennungssystems und der offenen Frage nach einer ausreichenden gesetzlichen Grundlage erachtet die GPK weitere Abklärungen als notwendig. Auch der Datenschutzbeauftragte verfolgt diese Entwicklungen intensiv, um rechtzeitig einerseits die Frage nach einer verhältnismässigen Rechtsgrundlage für die involvierten öffentlichen Organe klären und andererseits die Massnahmen auf ihre Verhältnismässigkeit prüfen zu können. Die Zusammenarbeit mit der GPK in diesem Themenbereich erweist sich dabei als sehr konstruktiv.

Titel: Computerverkauf durch ein Konkursamt
URL: http://www.datenschutz.ch/themen/1393.php
Datum: 03.03.2009

11. Computerverkauf durch ein Konkursamt

Verwertet ein Konkursamt im Rahmen einer konkursamtlichen Liquidation Computer mit Personendaten, muss es sicherstellen, dass diese Daten gelöscht werden. Für die Löschung gibt es drei Möglichkeiten.

In einem Konkursverfahren muss das Konkursamt möglichst sämtliche verbleibenden Vermögenswerte bestmöglich verwerten. Dabei sind allfällige Personendaten vor Missbrauch zu schützen.

Ein Konkursamt fragte den Datenschutzbeauftragten, wie die Computer eines konkursiten Unternehmens, die Personendaten der Mitarbeitenden enthalten, korrekt verkauft werden könnten.

Der Datenschutzbeauftragte kam zum Schluss, dass nur geschäftsrelevante Daten veräussert und weiterverwendet werden dürfen. Die übrigen Angaben, insbesondere die Personendaten der Mitarbeitenden, sind unwiderruflich und unwiederbringlich zu löschen. Das Konkursamt muss die Löschung sicherstellen. Der Datenschutzbeauftragte zeigte dazu drei Vorgehensmöglichkeiten auf:

- Das Konkursamt, eine Drittperson oder die Konkursitin löscht die Personendaten, bevor die Computer der Käuferschaft ausgeliefert werden.
- Das Konkursamt kopiert die geschäftsrelevanten Daten auf DVD und löscht die Festplatten, bevor die Computer der Käuferschaft ausgeliefert werden.
- Das Konkursamt verkauft die Computer mit sämtlichen Daten, die zum Zeitpunkt des Konkurses gespeichert waren. Im Rahmen einer schriftlichen Vereinbarung verpflichtet es vorab die Käuferschaft, nur die geschäftsrelevanten Daten weiterzuverwenden. Die Käuferschaft muss alle anderen Daten, insbesondere die Personendaten der Mitarbeitenden der Konkursitin, unwiderruflich und unwiederbringlich löschen; sonst drohen strafrechtliche und zivilrechtliche Sanktionen.

Titel: Plagiaterkennung in Abschlussarbeiten
URL: http://www.datenschutz.ch/themen/1394.php
Datum: 03.03.2009

12.

Plagiaterkennung in Abschlussarbeiten

Um Abschlussarbeiten im Mittelschul- und Berufsbildungsbereich auf Plagiate zu untersuchen, sind entsprechende gesetzliche Grundlagen nötig.

Das Mittelschul- und Berufsbildungsamt bat den Datenschutzbeauftragten, die gesetzlichen Grundlagen zur Plagiaterkennung bei Abschlussarbeiten im Mittelschul- und Berufsbildungsbereich zu beurteilen. Die drei gleich lautenden Bestimmungen sollen unter dem Randtitel «Plagiat und ungenügende Quellenangaben» im «Prüfungsreglement Allgemeinbildung», in der «Verordnung zum Einführungsgesetz zum Berufsbildungsgesetz» sowie im «Reglement für die Maturitätsprüfungen» verankert werden.

Um Plagiate in den Abschlussarbeiten zu erkennen, werden die Abschlussarbeiten in einer Datenbank beim Mittelschul- und Berufsbildungsamt erfasst. Dann werden sie an das Institut für angewandte Lerntechnologien der Universität Braunschweig geschickt und dort auf eine Plagiierung im Internet überprüft. Die Datenbank beim Mittelschul- und Berufsbildungsamt dient zudem dazu, erkennen zu können, wenn die Abschlussarbeiten selber später plagiiert werden. Deshalb sollen die geprüften Abschlussarbeiten für mehrere Jahre in der Datenbank gespeichert bleiben.

Der Datenschutzbeauftragte ging in seiner Stellungnahme davon aus, dass es geeignet und erforderlich und somit rechtmässig sei, Abschlussarbeiten in einer Datenbank zu erfassen, um Plagiate zu erkennen. Da einerseits die Abschlussarbeiten auf Plagiate überprüft werden sollen und andererseits geprüft werden soll, ob die erfassten Abschlussarbeiten zu einem späteren Zeitpunkt plagiiert werden, würden zwei Zwecke bestimmt, die beide in der gesetzlichen Grundlage zu nennen seien. Die zweite Zweckbestimmung rechtfertige die lange Aufbewahrungsdauer der Abschlussarbeiten.

Die drei Bestimmungen enthielten die Formulierung, dass der Datenschutz zu gewährleisten sei. Diese Formulierung ist zu wenig transparent. Die gesetzliche Grundlage muss Auskunft geben über folgende Punkte:

- Zweckbestimmungen
- Personenkreis, der Zugriff auf die Arbeiten hat
- Protokoll der Zugriffe
- Bearbeitungen der Personendaten, die in und aus der Datenbank erfolgen
- Modalitäten über die Datenbekanntgabe an Dritte
- Aufbewahrungsfristen, Zeitpunkt der Löschung und/oder der Archivierung der Arbeiten
- organisatorische und technische Massnahmen gegen unbefugte Datenbearbeitung

Der Datenschutzbeauftragte hat das Mittelschul- und Berufsbildungsamt aufgefordert, die drei Bestimmungen gemäss diesen Vorgaben zu konkretisieren.

Titel: Panaschierresultate im Internet
URL: http://www.datenschutz.ch/themen/1395.php
Datum: 03.03.2009

13. Panaschierresultate im Internet

Die Panaschierstatistik der Nationalratswahlen kann im Internet publiziert werden, und zwar sowohl nicht kandidatenbezogen als auch kandidatenbezogen.

Das Statistische Amt gelangte an den Datenschutzbeauftragten mit der Frage, ob die Panaschierresultate der Nationalratswahlen auf Kandidaten- und Wahlkreisebene im Internet aufgeschaltet werden könnten.

Der Datenschutzbeauftragte hielt in seiner Stellungnahme fest, dass bei einer Publikation auf Wahlkreisebene keine Personendaten bekannt gegeben würden; deshalb stehe einer Veröffentlichung nichts im Weg. Eine Publikation der Panaschierresultate auf Kandidatenebene enthält jedoch Personendaten der Kandidatinnen und Kandidaten, weshalb eine Publikation nur möglich ist, wenn weitere Voraussetzungen erfüllt sind.

Öffentliche Organe dürfen Personendaten bekannt geben, wenn dafür gesetzliche Grundlagen bestehen (§ 8 Abs. 1 DSG). Das Gesetz über die politischen Rechte hält in § 8 Abs. 2 fest, unter Wahrung des Stimmgeheimnisses sei es zulässig, das Stimmverhalten der Bevölkerung auszuwerten und zu publizieren. Die Weisung des Regierungsrates zu seinem Antrag vom 28. August 2002 an den Kantonsrat betreffend das Gesetz über die politischen Rechte hält dazu erläuternd fest, dass die kandidierenden Personen bei Verhältniswahlen keinen Schutz hinsichtlich des Panaschierverhaltens der Stimmbevölkerung verdienen. Diese Bestimmung stellt die gesetzliche Grundlage gemäss § 8 Abs. 1 DSG dar, welche es erlaubt, das Panaschierverhalten der Stimmbürgerschaft kandidatenbezogen auszuwerten und zu publizieren.

Das Statistische Amt hat die Panaschierstatistik der Nationalratswahlen 2007 auf seiner Website aufgeschaltet.

Titel: Kein aufsichtsrechtliches Einschreiten
URL: http://www.datenschutz.ch/themen/1396.php
Datum: 03.03.2009

14.

Kein aufsichtsrechtliches Einschreiten

Stellt der Datenschutzbeauftragte fest, dass ein kommunaler Datenschutzbeauftragter die ihm gesetzlich zugewiesenen Aufgaben korrekt und in genügendem Mass wahrgenommen hat, besteht kein Grund für ein aufsichtsrechtliches Einschreiten.

Ein Einwohner beschwerte sich bei einem kommunalen Datenschutzbeauftragten darüber, wie die Polizei der Gemeinde ihm einen Zahlungsbefehl zustellte. Sie habe versucht, ihn in der Nacht zuzustellen und ihn auf seine nicht öffentlich zugängliche Mobiltelefonnummer anzurufen. Er verlangte, dass den involvierten Beamten ein Verweis erteilt werde. Der kommunale Datenschutzbeauftragte prüfte die Angelegenheit und kam zum Schluss, dass die Polizeiorgane korrekt gehandelt hätten. Darauf beschwerte sich der Einwohner beim Datenschutzbeauftragten über die Amtsführung des kommunalen Datenschutzbeauftragten.

Die Gemeinde, in der der Einwohner lebt, hat einen eigenen kommunalen Datenschutzbeauftragten. Dieser überwacht die Anwendung der Vorschriften über den Datenschutz und berät betroffene Personen. Er wird vom kantonalen Datenschutzbeauftragten beaufsichtigt.

Mit der Aufsichtsbeschwerde kann jede Person eine Aufsichtsinstanz über Missstände bei einer Behörde informieren. Die Aufsichtsbeschwerde ist kein formelles Rechtsmittel, sondern ein formloser Rechtsbehelf und im Gesetz deshalb auch nicht ausdrücklich vorgesehen. Die Aufsichtsbehörde entscheidet nach Ermessen, wie sie eine Aufsichtsbeschwerde behandelt.

Zu den Aufgaben des Betreibungsamtes gehört die Zustellung des Zahlungsbefehls an den Schuldner. Der Zahlungsbefehl muss persönlich ausgehändigt werden. Er ist einem Gemeinde- oder Polizeibeamten zu übergeben, wenn eine persönliche Zustellung am Wohn- oder Arbeitsort des Schuldners fehlgeschlagen ist. Die Polizei handelt dann als Hilfsperson des Betreibungsamtes. Sie ist verpflichtet, den Zahlungsbefehl persönlich zu übergeben. Wie sie dies tut, liegt in ihrer Verantwortung; sie hat jedoch die Bestimmungen über die polizeiliche Tätigkeit zu beachten. Dies bedeutet, dass der Eingriff verhältnismässig sein muss.

Der kommunale Datenschutzbeauftragte hatte die Stadtpolizei befragt sowie Einsicht in den Polizeibericht genommen. Dieser hielt fest, dass es der Stadtpolizei nicht möglich gewesen sei, den Zahlungsbefehl persönlich auszuhändigen, weil der Einwohner die Tür nicht geöffnet habe. Da sie verpflichtet ist, den Zahlungsbefehl zu übergeben, versuchte sie es zu verschiedenen Tages- und Nachtzeiten. Betreibungshandlungen dürfen nur zwischen 7 Uhr und 20 Uhr vorgenommen werden. In Ausnahmefällen darf die Polizei aber auch während der Nachtzeit Betreibungshandlungen vornehmen, so, wenn der Zustellungsversuch bereits mehrfach gescheitert ist. Die Polizei darf dann als unaufschiebbare Massnahme auch während Sperrzeiten Zahlungsbefehle zustellen. Da die Polizei den Zahlungsbefehl mit möglichst milden Mitteln aushändigen muss, versuchte sie, den Einwohner telefonisch zu erreichen. Die Beschaffung einer Telefonnummer eignet sich zur Information. Sie ist erforderlich, da keine mildere Massnahme vorstellbar ist, die das verfolgte Ziel gleich effektiv erreicht. Die Massnahme ist somit zumutbar.

Der Datenschutzbeauftragte kam zum Schluss, dass der kommunale Datenschutzbeauftragte seine Aufgaben korrekt wahrgenommen habe, dass Abklärungen und Stellungnahme nicht zu beanstanden seien. Er sah deshalb keinen Grund für ein aufsichtsrechtliches Einschreiten.

Titel: Schulärztliche Untersuchung durch Privatarzt
URL: http://www.datenschutz.ch/themen/1397.php
Datum: 03.03.2009

15.

Schulärztliche Untersuchung durch Privatarzt

Eltern haben die Möglichkeit, die schulärztliche Untersuchung statt durch den Schularzt durch den Haus- oder Kinderarzt vornehmen zu lassen. Der private Arzt darf dem Schularzt keine Gesundheitsdaten weiterleiten, sondern nur der Gemeinde die Untersuchung bestätigen.

Kanton und Gemeinden sorgen dafür, dass die Schülerinnen und Schüler der Volks-, Mittel- und Berufsschulen angeleitet werden, ihre Gesundheit zu fördern und Erkrankungen zu verhüten (§ 49 Abs. 1 Gesundheitsgesetz [GesG]). Die Gemeinden sorgen für die Prävention und ärztliche Überwachung der Gesundheit der Schülerinnen und Schüler an der Volksschule (§ 50 Abs. 1 GesG). Die Gemeinden lassen auf ihre Kosten die Schülerinnen und Schüler auf der Kindergartenstufe und auf der Sekundarstufe schulärztlich untersuchen (§ 17 Abs. 1 Volksschulverordnung [VSV]). Die Untersuchungen umfassen Grösse, Gewicht, Seh- und Hörvermögen sowie die Kontrolle des Impfzustandes. An der Sekundarstufe kann die Untersuchung durch ein Gespräch mit den Jugendlichen ergänzt werden (§ 18 Abs. 1 VSV). Die Eltern werden über den Umfang und die Ergebnisse der Untersuchungen informiert (§ 18 Abs. 2 VSV). Untersuchungen, die über den Umfang gemäss § 18 Abs. 1 VSV hinausgehen, sind nur mit Zustimmung der Eltern zulässig.

Eltern haben die Möglichkeit, die Untersuchung durch eine Ärztin oder einen Arzt ihrer Wahl durchführen zu lassen. In diesem Fall tragen sie die Kosten selbst (§ 17 Abs. 2 VSV).

Die Gemeinden können auch auf die Organisation der schulärztlichen Untersuchungen verzichten. In diesem Fall leisten sie den Eltern eine Kostengutsprache. Die Eltern sind dann verpflichtet, die Untersuchung bei einer Privatärztin oder einem Privatarzt durchführen zu lassen (§ 17 Abs. 2 und 3 VSV). Bei diesen Reihenuntersuchungen tritt der Privatarzt an die Stelle des Schularztes. Für die Schulgemeinde muss sichergestellt sein, dass die Untersuchung im vorgesehenen Masse stattgefunden hat. Denn die Gemeinden müssen mit dem schulärztlichen Dienst für die ärztliche Überwachung der Schülerinnen und Schüler sorgen (§ 50 Abs. 1 GesG).

Eine Bekanntgabe der vom Haus- oder Kinderarzt gemäss § 18 Abs. 1 VSV erhobenen Gesundheitsdaten der Kinder und Jugendlichen müsste sich, da es sich um besondere Personendaten handelt, auf eine klare gesetzliche Grundlage stützen. Da keine solche gesetzliche Grundlage besteht, dürfen dem Schularzt keine Gesundheitsdaten bekannt gegeben werden. Es erfolgt lediglich eine Bestätigung der Privatärztin an die Gemeinde über die Durchführung der Untersuchung und über die Einleitung der erforderlichen Massnahmen (§ 17 Abs. 4 VSV).

Titel: Anonyme Auswertung garantiert
URL: http://www.datenschutz.ch/themen/1398.php
Datum: 03.03.2009

16.

Anonyme Auswertung garantiert

Wird bei Befragungen den Befragten Anonymität zugesichert, muss garantiert werden, dass ein Rückschluss auf bestimmte oder bestimmbare Personen ausgeschlossen ist. Die tiefste Teilnehmendenzahl, die Rückschlüsse ausschliesst, ist von der verantwortlichen Stelle in jedem Einzelfall zu prüfen und festzulegen.

Eine Institution, die beauftragt wurde, Absolvierende der Sekundarstufe II zu befragen, gelangte an den Datenschutzbeauftragten mit der Frage, wo bei einer Befragung zahlenmässig die unterste Schwelle gesetzt werden müsse, damit keine Rückschlüsse auf bestimmte oder bestimmbare Personen möglich seien. Die Institution hatte an knapp 50 Schulen eine Vollerhebung durchgeführt und von den rund 8000 Absolvierenden rund 3000 Antworten erhalten. Die Auswertung erfolgte pro Schule im Vergleich mit anderen Schulen des gleichen Typs und zusätzlich nach Fach. Dies führte dazu, dass auf bestimmte oder bestimmbare Personen zurückgeschlossen werden konnte.

Eine Person ist dann bestimmbar, wenn die Möglichkeit besteht, sie zu identifizieren. Bei der Bearbeitung von Personendaten zu nicht personenbezogenen Zwecken darf keine Möglichkeit vorhanden sein, welche es erlaubt, betroffene Personen zu bestimmen.

Bei den Befragungen der Absolvierenden wurde den auskunftgebenden Personen Anonymität zugesichert. Somit ist sie diesen Personen gegenüber zu garantieren. Der Datenschutzbeauftragte kann nicht abschliessend beurteilen, wie es sich bei den einzelnen Evaluationen verhält, wann einzelne Personen bestimmbar werden und wann nicht. Es kann deshalb keine allgemein geltende konkrete Zahl genannt werden. Diese Zahl ist durch die verantwortliche Stelle im Einzelfall je nach Projekt und Ausgangslage zu prüfen und festzulegen.

Sollten die Auftraggebenden detailliertere Auswertungen wünschen, welche unter Umständen Rückschlüsse auf bestimmte oder bestimmbare Personen zulassen, wäre ein anderes Vorgehen zu wählen: Den zu Befragenden müsste vor der Befragung unmissverständlich erklärt werden, dass auf sie zurückgeschlossen werden könne. Sind sie bereit, unter diesen veränderten Umständen bei der Befragung mitzuwirken, ist von ihnen im Voraus ihre ausdrückliche Einwilligung zu diesem Vorgehen einzuholen.

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

Beratung und Vermittlung
lic. iur. Beda Harb, Stv. Datenschutzbeauftragter
lic. iur. Barbara Mathis
lic. iur. Beatrice Glaser
lic. iur. Karin Brunner Steib
lic. iur., RA Claudio Fäh

Aufsicht und Kontrolle
lic. iur. Veronica Blattmann
lic. iur., RA Raphael Weiss
Andrea C. Mazzocco, CISA

Kommunikation / Aus- und Weiterbildung
Dr. phil. Andrea Ruf

Dienstleistungen
Martina Richard
Susanne Brüngger

Tätigkeitsbericht Nr. 14 (1.–9.2008)
ISSN 1422-5816

Gestaltung
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