Bericht an den Grossen Rat

2009

Tätigkeitsbericht des Datenschutzbeauftragten des Kantons Basel-Stadt

Inhaltsübersicht

Bilanz

Themen

Fälle

Anhang

Bilanz 2009

Das erste Jahr

Nach dem ersten Tätigkeitsjahr der durch die «Schengen-Revision» des Datenschutzgesetzes neu geschaffenen Datenschutzaufsicht wäre es vermessen, eine umfassende Bilanz ziehen zu wollen. Trotzdem: Durch die breit angelegte Beratungs- und Kontrolltätigkeit konnten erste Eindrücke gewonnen werden, die Hinweise auf künftigen Handlungsbedarf erlauben.

Erste Eindrücke

Sensibilisierung in der Verwaltung Positiv lässt sich festhalten, dass in vielen Verwaltungsstellen die Sensibilisierung für Fragen des Datenschutzes hoch ist; entsprechend gelangten diese Stellen mit zahlreichen Fragen an den Datenschutzbeauftragten. In anderen Stellen muss mit einer Verstärkung der Sensibilisierungsbemühungen der Schutz der Persönlichkeitsrechte der betroffenen Personen künftig noch intensiver thematisiert werden. Auch der Datenschutz-Audit (Seiten 20 ff.) dürfte zu einer besseren Verankerung des Themas beitragen.

Rechte der betroffenen Personen Zahlreicher als erwartet haben sich Private, die von staatlichem Datenbearbeiten betroffen sind, an den Datenschutzbeauftragten gewandt. Dabei standen zwei Themenbereiche im Vordergrund: einerseits die Frage, ob staatliches Datenbearbeiten rechtmässig und verhältnismässig ist, und anderseits Fragen zu den Rechten der betroffenen Personen, insbesondere zur Auskunft und Einsicht sowie zum Anspruch auf Berichtigung unrichtiger Daten.

Genügende gesetzliche Grundlagen? Personendaten dürfen bearbeitet werden, wenn dafür eine unmittelbare oder mittelbare gesetzliche Grundlage besteht (§ 5 Datenschutzgesetz/DSG*, § 9 Abs. 1 Entwurf zum Informations- und Datenschutzgesetz/E-IDG). Eine unmittelbare gesetzliche Grundlage regelt das konkrete Bearbeiten selber, mit der mittelbaren wird einem öffentlichen Organ eine gesetzliche Aufgabe zugewiesen, die es nur erfüllen kann, wenn es dazu Personendaten bearbeitet. Wenn besonders schützenswerte Personendaten bearbeitet werden sollen, muss die entsprechende Regelung in einem Gesetz im formellen Sinn, d.h. in einem vom Grossen Rat im ordentlichen Gesetzgebungsverfahren erlassenen Gesetz enthalten sein (§ 6 DSG, § 9 Abs. 2 E-IDG). Hier besteht ein Defizit: Erst für wenige Bearbeitungen von besonders schützenswerten Personendaten sind die notwendigen formellgesetzlichen Grundlagen in der erforderlichen Bestimmtheit vorhanden – beispielsweise im Harmonisierungsgesetz Sozialleistungen (SoHaG) und der dazugehörenden Verordnung. Viele andere Rechtsgrundlagen bleiben zu unbestimmt. Hier dürften wohl erst in Zukunft genügende Rechtsgrundlagen geschaffen werden, etwa durch den Erlass des geplanten Gesundheitsgesetzes oder durch die Schaffung eines Statistikgesetzes. Die neue Kantonsverfassung (KV) sieht als Formen der Rechtsetzung nur noch das Gesetz (§ 83 Abs. 1 KV) und die Verordnung (§ 105 Abs. 2 KV) vor – Regierungsratsbeschlüsse genügen den Anforderungen für die Einschränkung von Grundrechten nicht (mehr) (§ 36 Abs. 1 BV, § 13 Abs. 1 KV). Zu prüfen ist auch, ob – zum Beispiel für geplante Pilotanwendungen im Umfeld von eHealth (elektronisches Patientendossier, elektronische Medikamentenverschreibung) – eine gesetzliche Grundlage für Pilotversuche geschaffen werden müsste; der Bund hat das etwa in Art. 17a des Bundesdatenschutzgesetzes getan.

* *Die im Text erwähnten Rechtsnormen und Materialien werden in einem Verzeichnis am Schluss des Berichts detailliert aufgeführt.*

Datenschutzrechtliche Verantwortung Die im vergangenen Jahr bearbeiteten Geschäfte lassen vermuten, dass teilweise das Bewusstsein für die eigene Verantwortlichkeit fehlt. Das öffentliche Organ, das zur Aufgabenerfüllung Personendaten bearbeitet, ist für die Einhaltung des Datenschutzes verantwortlich (§ 7 DSG, § 6 E-IDG). Im Zusammenhang mit den rund 600 bestehenden Autorisierungen für Online-Zugriffe auf Daten anderer öffentlicher Organe (§ 10 Abs. 2 DSG) musste festgestellt werden, dass nicht selten die Angaben zur gesetzlichen Grundlage im Gesuch ungenügend sind; immerhin sollte die Dateneigentümerin aufgrund dieses Gesuches beurteilen können, ob sie verpflichtet oder mindestens berechtigt ist, die Daten bekannt zu geben bzw. den Online-Zugriff darauf zu gewähren. Manchmal fehlen die Stellungnahmen der Dateneigentümerinnen überhaupt. Und in sehr vielen Fällen musste auch festgestellt werden, dass die Autorisierungen – zum Teil seit etlichen Jahren – nicht mehr gültig sind. Das Autorisierungsverfahren nach § 10 Abs. 2 DSG hat offensichtlich dazu geführt, dass sich die Dateneigentümerinnen ihrer Verantwortung als «Hüterinnen ihrer Daten» nicht mehr bewusst waren. Auch im Bereich der Informationssicherheit bestehen offensichtlich Unsicherheiten darüber, wer wofür verantwortlich ist. Nach dem IDG-Entwurf sollen die Verantwortlichkeiten wieder entwirrt werden. In Zukunft wird zu prüfen sein, ob nicht für Informatikplattformen wie den Datenmarkt oder die Bewilligungsplattform eine gesetzliche Grundlage zu schaffen ist, damit die Verantwortlichkeiten klar abgegrenzt werden können.

Bilanz

Datenschutzbewusstsein Datenschutz ist nicht Selbstzweck, sondern dient dem Schutz der Grundrechte der Personen, über die der Staat Daten bearbeitet. Erfreulicherweise sind sich viele Verwaltungsstellen – oder genauer: viele Menschen, die in der Verwaltung arbeiten – dieser Herausforderung und ihrer Verantwortung bewusst. Anderen muss dieses Bewusstsein durch Sensibilisierungsbemühungen noch vermehrt vermittelt werden.

Ausdruck einer Haltung Datenschutz ist nicht freiwillige Zusatzleistung, sondern Teil der staatlichen Aufgabenerfüllung. Ihm zugrunde liegt die Forderung nach Achtung vor den Menschen, über die wir Daten bearbeiten. Die Art der Umsetzung ist nicht zuletzt ein Ausdruck der Haltung gegenüber diesen Menschen. An dieser Haltung gilt es weiter zu arbeiten – gerade auch im Hinblick auf die bevorstehende Einführung des Öffentlichkeitsprinzips. Mit diesem soll das staatliche Handeln für die Bürgerinnen und Bürger transparent und nachvollziehbar gemacht werden – einfach, weil sie als Betroffene das Recht haben, zu wissen, was ihr Staat tut. Wer seine Kundinnen und Kunden so sieht, braucht sich vor dem Öffentlichkeitsprinzip in keiner Weise zu fürchten.

Dank

Unsere Aufgabe könnten wir nicht erfüllen ohne die Unterstützung vieler Menschen und Organisationen. Ich bedanke mich deshalb bei allen, die ein waches Auge haben für Entwicklungen des Datenschutzes und sich für Datenschutzbelange einsetzen, bei allen Privaten, Mitarbeiterinnen und Mitarbeitern der Verwaltung, die sich vertrauensvoll mit Fragestellungen an uns gewandt haben, bei allen Mitarbeiterinnen und Mitarbeitern der Verwaltung, welche ein offenes Ohr für die von uns vertretenen Anliegen haben und kompetent mitgeholfen haben, datenschutzkonforme Lösungen zu finden und umzusetzen, bei den Präsidien und Mitgliedern des Grossen Rates, des Büros des Grossen Rates, der Datenschutz-Delegation des Büros, der Geschäftsprüfungskommission und der Justiz-, Sicherheits- und Sportkommission für ihr Interesse an unserer Arbeit und ihre Unterstützung, bei den Leitungen des Parlamentsdienstes, der Ombudsstelle und der Finanzkontrolle für die gute Zusammenarbeit und last but not least bei meinem Team, das mit grossem Engagement, spannenden Diskussionen und konstruktiven Anregungen unsere Arbeit bereichert und erleichtert hat.

Beat Rudin, Datenschutzbeauftragter

Themen

Thema 1 Aufbau der neuen Datenschutzaufsicht

Thema 2 Themen quer durch die gesamte Verwaltung

Thema 3 Auf dem Weg zum Informations- und Datenschutzgesetz

Thema 4 Videoüberwachung: Lösung oder Problem?

Thema 5 Neue Aufgabe: Anlassfreie Kontrolle der Datenbearbeitungen

Thema 1

Aufbau der neuen Datenschutzaufsicht

Am 1. Februar 2009 wurde die neue, mit der «Schengen-Revision» des Datenschutzgesetzes beschlossene Datenschutzaufsicht wirksam. Im ersten Jahr standen der Aufbau des neuen Teams, die Entwicklung der notwendigen neuen Strukturen und Prozesse sowie die Vernetzung mit anderen Datenschutzorganen im Vordergrund.

Aufbau

Vorgänger Per 31. Januar 2009 endete die Amtszeit von Jean-Louis Wanner. Er war Mitte 2005 vom Regierungsrat zum ersten Datenschutzbeauftragten des Kantons Basel-Stadt gewählt worden. Zuvor war er von 1989 bis 1993 Registerführer des Basler Zentralregisters der Datensammlungen. Anschliessend war er bis zu ihrer Abschaffung im Jahr 2005 Leiter der mit dem Datenschutzgesetz von 1992 geschaffenen Geschäftsstelle der Datenschutzkommission.

Der neue Datenschutzbeauftragte Am 1. Februar 2009 trat Beat Rudin das Amt als Datenschutzbeauftragter des Kantons Basel-Stadt an. Anders als sein Vorgänger war er – im Gefolge der «Schengen Revision» des Datenschutzgesetzes – nicht mehr vom Regierungsrat zu wählen, sondern vom Grossen Rat auf Antrag seiner Wahlvorbereitungskommission. Der Datenschutzbeauftragte ist ausserdem neu administrativ dem Büro des Grossen Rates zugeordnet; bisher war der Datenschutzbeauftragte fachlich dem Justizdepartement und administrativ der Staatskanzlei unterstellt. Beat Rudin, der am 10. Dezember 2008 vom Grossen Rat einstimmig gewählt wurde, ist promovierter Jurist, Advokat und seit 2003 Lehrbeauftragter für öffentliches Recht (mit Schwergewicht Datenschutzrecht) an der Juristischen Fakultät der Universität Basel. Von 1992 bis 2001 war er Datenschutzbeauftragter des Kantons Basel-Landschaft. Von 2001 an war er Geschäftsführer der Stiftung für Datenschutz und Informationssicherheit und selbständigerwerbender Datenschutzexperte; als solcher hat er etwa im Auftrag der Konferenz der Kantonsregierungen eine Wegleitung zur kantonalen Umsetzung der Schengen-Assoziierung im Bereich des Datenschutzes verfasst.

Der Datenschutzbeauftragte ist neu administrativ dem Büro des Grossen Rates zugeordnet.

Den Kanton Basel-Stadt kennt er aus eigener Erfahrung: Von 1990-1992 war er als akademischer Adjunkt und stellvertretender Departementssekretär im Wirtschafts- und Sozialdepartement tätig. Ausserdem hat er im Auftrag der beiden Basel den Entwurf zum neuen Informations- und Datenschutzgesetz erarbeitet und den baselstädtischen Entwurf im Auftrag des Justizdepartements auch bis zur Ratschlags-Reife gebracht. Sein Pensum beträgt 85%, um weiterhin die Wahrnehmung des Lehrauftrags an der Universität zu ermöglichen. Zudem ist er Herausgeber von digma, der Zeitschrift für Datenrecht und Informationssicherheit und Co-Organisator des Symposium on Privacy and Security an der ETH Zürich.

Neues Team – neuer Standort

Stellenausschreibung und Bürosuche Um die Wirksamkeit der Datenschutzaufsicht zu erhöhen, hatte der Grosse Rat für das erste Budget des Datenschutzbeauftragten aufgrund einer groben Abschätzung des Büros des Grossen Rates vorerst 300 Stellenprozente bewilligt. Deshalb musste der neue Datenschutzbeauftragte möglichst rasch die Stellen ausschreiben und Büroräumlichkeiten suchen. Diese sollten, um die Unabhängigkeit von der Verwaltung auch gegen aussen, gegenüber den Bürgerinnen und Bürgern, sichtbar zu machen, wie bei der Ombudsstelle nicht in einer bereits von der Verwaltung genutzten Liegenschaft sein. Schon am 1. Mai 2009 konnte er mit seinem neuen Team die Büroräumlichkeiten an der Henric Petri-Strasse 15 beziehen.

Neues Team Im Team des Datenschutzbeauftragten teilen sich drei Juristinnen 200 Stellenprozente:
—— lic. iur. Carmen Lindner, welche zuvor im Rechtsdienst des Gesundheitsdepartements tätig war, ist zuständig für die Belange des Gesundheitsdepartements, des Departements für Wirtschaft, Soziales und Umwelt sowie des Finanzdepartements. Mit ihrer Zusatzausbildung in Kommunikation betreut sie ausserdem die Öffentlichkeitsarbeit.
—— Dr. Sandra Stämpfli hat an der Universität Basel zum Thema Schengener Informationssystem und informationelle Selbstbestimmung promoviert. Sie ist zuständig für die Geschäfte des Präsidialdepartments, des Justiz- und Sicherheitsdepartements, des Bau- und Verkehrsdepartements sowie des Erziehungsdepartements.
—— lic. iur. Barbara Widmer, LL.M., war zuvor in verschiedenen Projekten in der Verwaltung des Kantons Basel-Stadt tätig. Sie besitzt neben dem juristischen einen Abschluss als interne Revisorin (Certified Internal Auditor, CIA) und ist deshalb schwergewichtig für den Bereich der Kontrollen und – solange das Informations- und Datenschutzgesetz noch nicht beschlossen und in Kraft gesetzt ist – für die Autorisierungen nach § 10 Abs. 2 DSG zuständig.

Volontariat Ausserdem bietet der Datenschutzbeauftragte eine Ausbildungsmöglichkeit für Juristinnen und Juristen: Seit Oktober 2009 wird eine Volontariatsstelle angeboten. Erste Volontärin war (bzw. ist noch bis Ende März 2010) Andrea Klüser, MLaw.

Strukturen und Prozesse Nach dem bisherigen Einmannbetrieb waren die notwendigen Strukturen und Prozesse zu entwickeln und einzuführen. Insbesondere bestand auch keine Geschäftskontrolle. Dank enger Zusammenarbeit mit dem Parlamentsdienst und der Ombudsstelle konnte teilweise auf bestehenden Lösungen aufgebaut werden.

Blick über den Zaun

Interkantonale und internationale Zusammenarbeit Das Datenschutzgesetz verpflichtet ausdrücklich zur Kooperation mit den Organen der anderen Kantone, des Bundes und des Auslandes, welche die gleichen Aufgaben erfüllen (§ 28 lit. i DSG, künftig § 49 E-IDG). Der Datenschutzbeauftragte pflegt diese Zusammenarbeit sehr intensiv, da er dabei auch von den Aktivitäten anderer Kantone profitieren kann. Auf dieser Basis findet etwa die Kooperation mit dem Datenschutzbeauftragten des Kantons Zürich bezüglich der Datenschutz-Audits statt (Seiten 20 f.). Auch mit den anderen Nordwestschweizer Kantonen findet nicht zuletzt aufgrund von thematischen Berührungspunkten etwa im Bildungsbereich eine regelmässige Kooperation statt.

Mitarbeit in Gremien Beat Rudin wurde gleich nach seinem Amtsantritt in das Büro von privatim, der Vereinigung der schweizerischen Datenschutzbeauftragten, berufen – quasi als «Rückkehrer», denn er war als Baselbieter Datenschutzbeauftragter bereits der erste Präsident der Vereinigung. Ausserdem wurde er vom Eidgenössischen Departement des Innern in die Expertenkommission eHealth berufen und vertritt privatim in der Arbeitsgruppe Diagnoseregister des Bundesamtes für Gesundheit.

Der Datenschutzbeauftragte pflegt die interkantonale und internationale Zusammenarbeit intensiv.

Auch die Juristinnen aus dem Team des Datenschutzbeauftragten wirken entsprechend den von ihnen betreuten Sachgebieten in Arbeitsgruppen von privatim mit: Carmen Lindner ist Mitglied der Arbeitsgruppe Gesundheit, Sandra Stämpfli Mitglied der Arbeitsgruppe Innere Sicherheit und Barbara Widmer Mitglied der Arbeitsgruppe ICT (Information and Communication Technologies). Ausserdem soll der Datenschutzbeauftragte des Kantons Basel-Stadt im Turnus die Schweizer Kantone in der Joint Supervisory Authority (der Datenschutzaufsicht) für Schengen vertreten. Er wird dort Nachfolger des Datenschutzbeauftragten des Kantons Zürich, welcher künftig den Kanton Basel-Landschaft in der (arbeitsintensiveren) Working Party on Police and Justice (WPPJ) ablöst.
——

Thema 2

Themen quer durch die gesamte Verwaltung

Datenschutz ist eine Querschnittsmaterie. Kaum eine öffentliche Aufgabe kann erfüllt werden, ohne dass dazu Personendaten bearbeitet werden müssen. Entsprechend breit ist das Themenspektrum, mit dem sich das Team des Datenschutzbeauftragten bereits im ersten Jahr auseinanderzusetzen hatte.

Neuanfang

Kurze Einarbeitungszeit Im ersten Jahr ging es darum, die neue Datenschutzaufsicht operativ werden zu lassen. Dank dem Erfahrungsschatz des Datenschutzbeauftragten und seines Teams konnte der Datenschutz rasch eine wirkungsvolle Aktivität entwickeln. Die bei einem Neuanfang notwendige Einarbeitungszeit fiel deshalb sehr kurz aus.

Beratung in Fragen des Umgangs mit Informationen In der Verwaltung war der Bedarf nach datenschutzrechtlicher Beratung ausserordentlich gross. Zwar bestand zum Teil die Befürchtung, dass die neue Datenschutzaufsicht nach der «Schengen-Revision» des Datenschutzgesetzes nicht mehr beraten, sondern nur noch kontrollieren würde. Diese Ängste konnten vertrieben werden: Für die Verbesserung des Datenschutzes ist es ebenso wichtig, die datenbearbeitenden Behörden optimierend bei der datenschutzkonformen Aufgabenerfüllung zu unterstützen, wie sie bezüglich der Einhaltung der minimalen gesetzlichen Anforderungen zu kontrollieren. Deshalb sieht der Entwurf zum Informations- und Datenschutzgesetz – wie das geltende Datenschutzgesetz bisher – vor, dass der Datenschutzbeauftragte die datenbearbeitenden öffentlichen Organe in Fragen des Umgangs mit Informationen zu beraten hat (§ 45 lit. c E-IDG, § 28 lit. a DSG).

Blick auf die Themenpalette Der Datenschutzbeauftragte wurde von kantonalen und kommunalen Verwaltungsbehörden zu sehr vielen – grösseren und kleineren – Geschäften beigezogen. Ein Auszug aus den wichtigsten Themen soll hier kurz erwähnt werden (alphabetisch).

Geschäfte

Informations- und Datenschutzgesetz Der Datenschutzbeauftragte wurde zur Behandlung des IDG-Entwurfs durch die Justiz-, Sicherheits- und Sportkommission des Grossen Rates (JSSK) beigezogen; ausserdem beschäftigte er sich intensiv mit der Vorbereitung der Umsetzung des IDG. Das Thema wird in diesem Bericht separat behandelt (Seiten 13 ff.).

Informationssicherheit In einer digitalen Umgebung gibt es keinen Datenschutz ohne Informationssicherheit. Die Anforderungen bezüglich Vertraulichkeit, Integrität / Nachvollziehbarkeit, Zurechenbarkeit und Verfügbarkeit können nur durch entsprechende Sicherheitsmassnahmen gewährleistet werden. Sowohl das Datenschutzgesetz als auch der IDG-Entwurf verlangen, dass Informationen durch angemessene organisatorische und technische Massnahmen geschützt werden (§ 17 DSG, § 8 E-IDG). Seit 2002 regelt die Informatiksicherheitsverordnung (ISV) die Verantwortlichkeiten.

In einer digitalen Umgebung gibt es keinen Datenschutz ohne Informationssicherheit.

Es musste festgestellt werden, dass sich die Verwaltungsorgane als Leistungsbezüger ihrer Verantwortung oft nicht bewusst sind und den Schutzbedarf ihrer Datenbestände nicht bestimmt haben oder nicht als «Bestellung von Sicherheit» an die Leistungserbringer weitergegeben haben. Verbesserungen sind inzwischen in mehrfacher Hinsicht aufgegleist: Die Informatikkonferenz hat auf Antrag des Datenschutzbeauftragten ein Konzept für den Schutz besonders schützenswerter Personendaten erstellen lassen. Beim Projekt Datenklassifikation wurde der Datenschutzbeauftragte von der Staatsschreiberin und der

Fachstelle Informatik und Organisation (FIO) beigezogen; das für die Klassifikation entwickelte Tool wird bereits im Rahmen des Datenschutz-Pilotaudits (Seite 21) eingesetzt. Mit dem Datenschutz-Audit wird das Thema Informationssicherheit bei den kontrollierten öffentlichen Organen mit Nachdruck «platziert»; vorerst konzentriert sich der Teil «Informationssicherheit» schwergewichtig auf die organisatorischen Massnahmen bei den Leistungsbezügern.

Rechte der betroffenen Personen Wenn Daten einer Person von staatlichen Behörden bearbeitet werden, kommen dieser Person aus dem Datenschutzgesetz (und künftig aus dem Informations- und Datenschutzgesetz) bestimmte Rechte zu. Insbesondere das Recht auf Auskunft über und Einsicht in die eigenen Daten sowie das Recht auf Berichtigung unrichtiger Daten bilden regelmässig Anlass für Auseinandersetzungen zwischen Amtsstellen und betroffenen Personen, zu welchen der Datenschutzbeauftragte beigezogen wird.

Die Rechte der betroffenen Personen bilden regelmässig Anlass für Auseinandersetzungen zwischen Amtsstellen und Betroffenen.

Betroffenen Personen musste teilweise klar gemacht werden, dass z.B. Einschränkungen zum Schutz von überwiegenden Interessen von Drittpersonen nicht nur zulässig, sondern sogar geboten sind. In Einzelfällen musste umgekehrt gegenüber Verwaltungsstellen deutlich gemacht werden, dass die Ansprüche innert angemessener Frist zu erfüllen und Einschränkungen nur unter den im DSG vorgesehenen Voraussetzungen zulässig sind. Dabei hat sich aber gezeigt, dass im Falle eines Nichthandelns der Verwaltung das Hauptinstrument des Datenschutzbeauftragten, die Empfehlung, von beschränkter Wirksamkeit ist – auch die Weisung, die im konkreten Fall nicht mehr nötig war, hätte faktisch nicht weitergeführt.

Schengen: Koordinierte Kontrollen Bund und Kantone Aufgrund der Schengen-Assoziierung der Schweiz sind Bund und Kantone auch verpflichtet, regelmässig die schengen-spezifischen Datenbearbeitungen zu kontrollieren. Der Datenschutzbeauftragte des Kantons Basel-Stadt engagiert sich auch gemeinsam mit denjenigen der Kantone Freiburg, Waadt und Zürich und dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten bei der Entwicklung einer Kontrollmethodologie für die koordinierten Schengen-Kontrollen ab 2011.

Schule und Datenschutz Während in anderen Kantonen Datenschutz in der Schule längst zum Thema geworden ist und Wegleitungen den Lehrpersonen Hilfestellung für die entsprechenden Fragen im schulischen Alltag bieten, fehlt eine solche Anleitung bisher in Basel-Stadt. Nach zahlreichen Anfragen von Lehrpersonen an den Datenschutzbeauftragten nahm dieser mit dem Bereich Bildung des Erziehungsdepartements Kontakt auf und konnte belegen, dass auch hier aktueller Handlungsbedarf besteht. Daraufhin wurde die Arbeit an einem Leitfaden «Schule und Datenschutz» aufgenommen; in direkten Gesprächen mit verschiedensten Gremien konnten die spezifischen Problemfelder eruiert und Lösungsansätze diskutiert werden. Mit den Landgemeinden konnten Fragen im Zusammenhang mit der Übernahme der Primarschul-Schülerdossiers geklärt werden.

Sozialversicherungsnummer Der Bundesgesetzgeber hat nach dem Hinweis auf die Verfassungswidrigkeit eines generellen Eidgenössischen Personenidentifikators auf dessen Einführung verzichtet, aber gleichzeitig im Hinblick auf die registergestützte Volkszählung die Verwendung der neuen Sozialversicherungsnummer für gewisse Bereiche vorgeschrieben (Sozialversicherung, Prämienverbilligung in der Krankenversicherung, Sozialhilfe, Steuerwesen, Bildungswesen). Darüber hinaus darf die Nummer nur verwendet werden, wenn ein kantonales Gesetz dies vorsieht. Der Entwurf zum IDG sieht – im «provisorischen Statistik-Paragrafen» (§ 10 Abs. 2 E-IDG) – vor, dass das Statistische Amt die Sozialversicherungsnummer zum Zweck der Verknüpfung von Personendaten verwenden darf; das heisst aber ebenso klar, dass diese Bestimmung anderen als im Bundesrecht genannten öffentlichen Organen nicht das Recht gibt, die Sozialversicherungsnummer zu verwenden – und das ist auch gut so, da sonst der Verknüpfbarkeit von Personendaten Tür und Tor geöffnet würde.

Staatsschutz Die Auswirkungen der Vorkommnisse im Bereich des Staatsschutzes (einerseits Aufnahme von türkischstämmigen Grossrätinnen und Grossräten ins ISIS, das Staatsschutzinformationssystem des Bundes, anderseits Aufnahme von Mitgliedern des Grossen Rates im Zusammenhang mit der Anti-WEF-Demo ins ISIS) führten zum Versuch, die Aufsicht über die Staatsschutztätigkeiten im Kanton Basel-Stadt in einer kantonalen Verordnung zu regeln.

>

Vom Vorsteher des Justiz- und Sicherheitsdepartements wurde auch der Datenschutzbeauftragte zur Mitwirkung in der Arbeitsgruppe eingeladen. Der Datenschutzbeauftragte hatte ausserdem geplant, die rechtlichen Möglichkeiten auszuschöpfen, um auszuloten, ob der Dienst für Analyse und Prävention ihm nicht doch noch die Einsicht in die Daten bei der Fachgruppe 9 gewähren würde. Nach den Erfahrungen mit der vom Regierungsrat beschlossenen Verordnung wurde mangels Aussicht auf Erfolg darauf verzichtet.

Videoüberwachung Das Thema Videoüberwachung beschäftigte den Datenschutzbeauftragten im ersten Jahr in grossem Masse; es wird in diesem Bericht separat dargestellt (Seiten 17 ff.).

Volkszählung und Registerharmonisierung Die im Dezember 2010 fällige Volkszählung soll erstmals nicht mehr als klassische Volks«zählung» mit Fragebogen, die von allen Einwohnerinnen und Einwohnern ausgefüllt werden müssen, durchgeführt werden. Der Bund hat die gesetzlichen Grundlagen für eine registergestützte Volkszählung geschaffen. Als Voraussetzung dafür müssen aber die vielen staatlichen Register – allen voran die Einwohnerkontrollen – harmonisiert werden. Der Bund hat die Einführung einer Wohnungsnummer vorgeschrieben, so dass der Staat erstmals flächendeckend weiss, wer mit wem in welcher Wohnung zusammen wohnt.

> Mit der Einführung einer Wohnungsnummer weiss der Staat erstmals flächendeckend, wer mit wem in welcher Wohnung zusammen wohnt.

Auf kantonaler Ebene bedarf es einerseits der rechtlichen Umsetzung der Bundesvorgaben, die mit der Revision des Aufenthaltsgesetzes vorgenommen werden sollen; dabei sind Berührungspunkte entstanden mit der Vorlage zum Informations- und Datenschutzgesetz, zu deren Abstimmung der Datenschutzbeauftragte vom federführenden Justiz- und Sicherheitsdepartement und von der Justiz-, Sicherheit- und Sportkommission beigezogen wurde. Anderseits müssen die Register auch inhaltlich angepasst werden, etwa durch die Zuweisung der Einwohnerinnen und Einwohner zu den einzelnen Wohnungen; in dieses Outsourcingprojekt wurde der Datenschutzbeauftragte einbezogen und konnte dazu beitragen, dass das bundesrechtliche Weiterbearbeitungsverbot auch durchgesetzt wurde. In diesem Zusammenhang ist auch weiterhin ein strenges Auge auf die Verwendung der neuen Sozialversicherungsnummer (AHVN13) zu werfen (Seite 11).

Thema 3

Auf dem Weg zum Informations- und Datenschutzgesetz

Mit dem Amtsantritt des neuen Datenschutzbeauftragten trat die «Schengen-Revision» des kantonalen Datenschutzgesetzes vollständig in Kraft. In Kürze hat der Grosse Rat aber bereits über ein Informations- und Datenschutzgesetz zu beschliessen, welches das Öffentlichkeitsprinzip und den Datenschutz als zwei Seiten derselben Medaille vereinigt.

Die «Schengen-Revision» des Datenschutzgesetzes

Anpassungsbedarf Am 16. April 2008 hat der Grosse Rat Anpassungen am kantonalen Datenschutzgesetz beschlossen. Mit der Revision des Gesetzes sollte sichergestellt werden, dass die Anforderungen erfüllt werden, welche einerseits durch die Assoziierung der Schweiz an Schengen und anderseits aufgrund der schweizerischen Ratifizierung des Zusatzprotokolls zur Europarats-Konvention 108 (ZP zur ER-Konv 108) in materieller und institutioneller Hinsicht an das kantonale Datenschutzrecht gestellt werden.

Materielle Änderungen In inhaltlicher Hinsicht mussten im Bereich des Geltungsbereichs (§ 4 DSG), bezüglich der Erkennbarkeit der Datenbearbeitungen (§ 9 DSG) und des Rechts der betroffenen Personen, die Bekanntgabe von Daten über sie sperren zu lassen (§ 13 DSG), sowie bezüglich der grenzüberschreitenden Datenbekanntgabe (§ 14 DSG) Anpassungen vorgenommen werden. Ausserdem wurde das Instrument der Vorabkontrolle (neuer § 18a DSG) eingeführt.

Sicherstellung der Unabhängigkeit Grössere Änderungen waren in institutioneller Hinsicht notwendig: In diesem Bereich ging es primär darum, die Unabhängigkeit und Wirksamkeit der Datenschutzaufsicht zu stärken. Schon seit geraumer Zeit hatte vor allem die Geschäftsprüfungskommission hierzu Defizite ausgemacht. Gegenüber dem regierungsrätlichen Entwurf (Ratschlag 05.1024.01) wurden verschiedene Änderungen vorgenommen, um die verlangte «völlige Unabhängigkeit» zu gewährleisten. So wird die oder der Datenschutzbeauftragte nicht vom Regierungsrat unter Vorbehalt der Genehmigung durch den Grossen Rat auf eine Amtsdauer von vier Jahren gewählt, sondern vom Grossen Rat selbst auf Antrag seiner Wahlvorbereitungskommission auf eine Amtsdauer von sechs Jahren – wie die Ombudsleute und die Leiterin/der Leiter der Finanzkontrolle. Um Interessenkollisionen zu vermeiden, wurden auch die Unvereinbarkeitsregeln verstärkt. Die Aufsichtsstelle verfügt über ein eigenes Budget und ist organisatorisch dem Büro des Grossen Rates statt der Staatskanzlei zugeordnet.

Verstärkung der Wirksamkeit Um die Wirksamkeit zu verbessern, hat die oder der Datenschutzbeauftragte – wie vom Regierungsrat beantragt – künftig das Recht, gegenüber öffentlichen Organen, welche die an sie gerichteten Empfehlungen nicht einhalten, Weisungen in der Form von Verfügungen zu erlassen, soweit das Interesse an der Durchsetzung der Empfehlung schwer wiegt (§ 29 Abs. 5 DSG). Das öffentliche Organ, an welches die Weisung gerichtet ist, kann die Weisung mit einem Rekurs – nicht wie ursprünglich vorgeschlagen beim Regierungsrat –, sondern beim Verwaltungsgericht anfechten (§ 29 Abs. 6 DSG).

Bei der «Schengen-Revision» ging es darum, die Unabhängigkeit und Wirksamkeit der Datenschutzaufsicht zu stärken.

Ausserdem beschloss der Grosse Rat, dass der Datenschutzaufsicht die nötigen Ressourcen zugeteilt werden sollen, damit sie die neuen Aufgaben auch wirksam erfüllen kann: Vorerst sollten im Budget 2009, welches auf einer groben Abschätzung durch das Büro des Grossen Rates basiert, drei Stellen zur Verfügung stehen; dabei wurde aber bereits darauf hingewiesen, dass das geplante neue IDG der Datenschutzaufsichtsstelle voraussichtlich zusätzliche Aufgaben zuweisen werde.

>

Öffentlichkeitsprinzip

Neue Kantonsverfassung Erstmals enthält die neue KV, welche 2006 die alte Verfassung von 1889 abgelöst hat, eine Grundrechtsgarantie im Datenschutzbereich: § 11 lit. j KV gewährleistet «den Schutz personenbezogener Daten sowie des Rechts auf Einsichtnahme und auf Berichtigung falscher Daten». Damit erhielt das Datenschutzrecht eine verfassungsrechtliche Grundlage auf kantonaler Ebene. Einschneidender für den Umgang mit behördlichen Informationen dürfte allerdings die Einführung des Öffentlichkeitsprinzips in § 75 KV sein: Neu hat nach diesem Prinzip jede Person das Recht auf Zugang zu den bei einem öffentlichen Organ vorhandenen Informationen, soweit nicht überwiegende öffentliche oder private Interessen entgegenstehen. Das Nähere zur Umsetzung dieses Paradigmenwechsels vom Geheimhaltungsprinzip mit Öffentlichkeitsvorbehalt zum Öffentlichkeitsprinzip mit Geheimhaltungsvorbehalt ist in einem Gesetz zu regeln.

Vorbereitung gemeinsam mit Basel-Landschaft Ursprünglich war vorgesehen, die Umsetzung des Öffentlichkeitsprinzips in einem Informationsgesetz zu regeln und dieses Gesetz gemeinsam mit dem Kanton Basel-Landschaft vorzubereiten. Das Mitberichtsverfahren zu einem ersten Entwurf zeigte aber Schwächen in der Abstimmung mit den in beiden Kantonen bereits bestehenden Datenschutzgesetzen. Die Kantone beschlossen daher, mit der Überarbeitung einen externen Experten zu beauftragen. Auf dessen Vorschlag hin sollten die Themen Öffentlichkeitsprinzip und Datenschutz in einem Gesetz gemeinsam geregelt werden, weil sie beide dasselbe zum Gegenstand haben: Information. Personendaten sind nichts anderes als Informationen mit Personenbezug. Aus diesem Grund entstand in der Folge der Entwurf zum Informations- und Datenschutzgesetz.

Informations- und Datenschutzgesetz

Gesetzesentwurf Die Ergebnisse der Mitberichtsverfahren in den beiden Kantonen Basel-Stadt und Basel-Landschaft zeigten, dass man im Datenschutzbereich an jeweils bewährten Regelungen festhalten wollte. Aus diesem Grund war im Vernehmlassungsentwurf zwar der ‹Informationsteil› noch weitgehend identisch; die ‹Datenschutzteile› unterschieden sich aber in einigen Regelungen.

Mit der neuen Kantonsverfassung erhielt das Datenschutzrecht eine verfassungsrechtliche Grundlage.

Die zuständigen Departemente der beiden Kantone, das Justizdepartement des Kantons Basel-Stadt und die Justiz-, Polizei- und Militärdirektion (später: Sicherheitsdirektion) des Kantons Basel-Landschaft, eröffneten noch gemeinsam die Vernehmlassungsverfahren. Die Vernehmlassungsantworten beendeten aber das partnerschaftliche Geschäft: Im Kanton Basel-Stadt war die Einführung des Öffentlichkeitsprinzips aufgrund der bestehenden Verfassungsregelung unbestritten; im Partnerkanton bestand eine solche Verfassungsbestimmung aber noch nicht. Aufgrund des Zeitdrucks in unserem Kanton – der Grosse Rat hatte bei der vorletzten Revision des Datenschutzgesetzes 2005 eine Befristung bis Ende 2008 eingeführt, um seiner Forderung nach einer Verstärkung des Datenschutzes Nachdruck zu verleihen – hat der Regierungsrat am 10. Februar 2009 den Ratschlag für das IDG (Ratschlag 08.0637.01) verabschiedet und dem Grossen Rat zugestellt, ohne auf den entsprechenden Schritt im Baselbiet zu warten.

Behandlung in der JSSK Im Berichtsjahr hat sich die Justiz-, Sicherheits- und Sportkommission des Grossen Rates (JSSK) des Geschäftes angenommen. Zu ihren Sitzungen, in welchen das IDG behandelt wurde, hat sie jeweils auch den Datenschutzbeauftragten, der vor seiner Wahl als externer Experte im Auftrag der beiden Kantone den Entwurf ausgearbeitet hatte, beigezogen. Im Auftrag der JSSK und in Abstimmung mit dem federführenden Justiz- und Sicherheitsdepartement hat er auch diverse Formulierungsvorschläge ausgearbeitet, insbesondere zur Abstimmung mit dem sich gleichzeitig in Revision befindenden Aufenthaltsgesetz (Ratschlag 09.0298.01).

Ausblick

Auswirkungen Wird das Informations- und Datenschutzgesetz vom Grossen Rat ohne grosse Änderungen verabschiedet und vom Regierungsrat in Kraft gesetzt, wird sich für die Verwaltung im Umgang mit Informationen einiges ändern.

Änderungen im ‹Datenschutzteil› Nicht sehr einschneidend werden die Änderungen im ‹Datenschutzteil› sein, weil das Grundkonzept (gesetzliche Grundlage, Verhältnismässigkeit, Rechte der betroffenen Personen) unverändert bleibt. Klärungen gibt es beim Geltungsbereich des Gesetzes (§ 2 E-IDG) und bei den Voraussetzungen für das Bearbeiten und für das Bekanntgeben von Personendaten (§§ 9 und 21 E-IDG). Auch das Zweckbindungsgebot (§ 12 E-IDG) wird klarer als bisher umschrieben. Künftig soll für neue IT-Systeme das Prinzip der Datenvermeidung und Datensparsamkeit verankert werden (§ 14 E-IDG). Verstärkt wird auch die Transparenz für die betroffenen Behörden, indem – wie im Bundesrecht – eine Informationspflicht bei der Beschaffung von besonderen Personendaten eingeführt wird (§ 15 Abs. 3 E-IDG). Neu geregelt wird die Videoüberwachung (§§ 17 f. E-IDG, vgl. die ausführlichere Darstellung auf Seite 18). Das bisher von der oder dem Datenschutzbeauftragten zu führende zentrale Register der Datensammlungen wird abgelöst durch ein dezentral von den verantwortlichen Organen gepflegtes, aber zentral veröffentlichtes Verzeichnis der Verfahren, bei welchen Personendaten bearbeitet werden (§ 24 E-IDG).

Mit dem Informations- und Datenschutzgesetz wird sich für die Verwaltung im Umgang mit Informationen einiges ändern.

Wichtigste Eckpunkte im ‹Informationsteil› Einschneidender wird sich der neue ‹Informationsteil› auswirken, mit welchem die von § 75 KV verlangte Detailregelung für das Öffentlichkeitsprinzip geschaffen wird. Die Verwaltung verliert die bisherige Informationshoheit, weil nicht mehr sie allein bestimmen kann, welche Informationen sie der Öffentlichkeit zugänglich machen will. Zwar ist sie wie bis anhin auch weiter zuständig für die aktive Informationstätigkeit («Informieren von Amtes wegen»). Neu aber erhält jede Person das Recht auf Zugang zu den bei einem öffentlichen Organ vorhandenen Informationen (§ 25 E-IDG). Dieser Anspruch kann voraussetzungslos geltend gemacht werden; die gesuchstellende Person muss also keinerlei Interessennachweis erbringen. Der Zugang zu Informationen darf – wie auch die Bekanntgabe von Informationen zur Aufgabenerfüllung eines öffentlichen Organs – nur eingeschränkt werden, wenn eine besondere Geheimhaltungspflicht (wie z.B. das Steuergeheimnis oder das ärztliche Berufsgeheimnis) dies vorsieht oder wenn ein überwiegendes öffentliches oder privates Interesse entgegensteht (§ 29 Abs. 1 E-IDG). Welche öffentlichen oder privaten Interessen dies namentlich sein können, führen die Abs. 2 und 3 von § 29 E-IDG auf. Weil die transparente Verwaltung das Ziel der Einführung des Öffentlichkeitsprinzips ist, nicht aber die gläserne Bürgerin oder der gläserne Bürger, müssen Personendaten vor der Zugangsgewährung anonymisiert werden, falls der Zugang nicht schon wegen eines überwiegenden privaten Interesses überhaupt zu verweigern ist (§ 29 Abs. 4 E-IDG). Das Gesetz setzt der Verwaltung eine Frist von 30 Tagen, innert welcher sie das Zugangsgesuch spätestens beantworten muss. Innerhalb dieser Zeitspanne hat sie entweder den Zugang zu gewähren, mitzuteilen, dass sie eine Abweisung des Gesuchs in Betracht zieht, oder zu erklären, warum sie noch nicht entscheiden kann und bis wann der Entscheid vorliegen wird (§ 36 E-IDG). Kontrovers ist, ob – wie es der Regierungsrat beantragt hat – bei Ablehnung des Gesuchs oder der Nichtberücksichtigung von Einwänden gegen die Zugangsgewährung ein Schlichtungsverfahren vor der Ombudsstelle verlangt werden kann (§ 34 E-IDG). Nicht bestritten ist hingegen, dass nur in Ausnahmefällen (bei aufwändigen Verfahren und für die Anfertigung von Kopien) Gebühren verlangt werden dürfen (§ 37 E-IDG).

Paradigmenwechsel Wird in dem Moment, in welchem das Informations- und Datenschutzgesetz in Kraft gesetzt wird, ein Paradigmenwechsel stattfinden? Kaum. Mit dem Informations- und Datenschutzgesetz werden zwar die Rechtsgrundlagen für den Paradigmenwechsel geschaffen. Ein solcher ist aber auch abhängig von einem Kulturwechsel, vom Wechsel des Verständnisses von Staat und Bürgerin/Bürger in den Köpfen der Verwaltungsmitarbeiterinnen und -mitarbeiter. Dies wird eine gewisse Zeit in Anspruch nehmen – so wie es heute schon Departemente gibt, die aktiver und offener informieren als andere.

>

Immerhin bietet das IDG einen «Schuhlöffel» für den Einstieg in eine offenere Verwaltung: Auf ein Zugangsgesuch muss ein öffentliches Organ nicht eintreten, wenn es die gewünschte Information bereits öffentlich zugänglich gemacht hat (§ 32 Abs. 1 E-IDG). Die Verwaltungsstelle, welche umfassender aktiv informiert, also die interessanten Informationen von sich aus veröffentlicht, spart sich das aufwändigere individuelle Zugangsverfahren.

Ziel der Einführung des Öffentlichkeitsprinzips ist nicht der gläserne Bürger, sondern die transparenten Verwaltung.

Informations- und Datenschutzverordnung

Ausserdem ist, selbst wenn das Informations- und Datenschutzgesetz ohne grosse Änderungen verabschiedet wird, noch offen, wie die Ausführungsbestimmungen in der erst noch auszuarbeitenden Informations- und Datenschutzverordnung aussehen werden. Der Datenschutzbeauftragte ist nicht (mehr) in die Vorbereitung involviert, wird sich aber in seiner Vernehmlassung dafür einsetzen, dass die gesetzlichen Bestimmungen nicht verwässert werden.

Thema 4

Videoüberwachung: Lösung oder Problem?

Wer erwartet hat, dass mit der Videoüberwachungs-Regelung im Datenschutzgesetz den Videoüberwachungs-Boom in den Griff zu bekommen ist, muss sich angesichts der Fakten fragen, ob dies gelungen ist. Der IDG-Entwurf sieht eine differenziertere Lösung vor. Eine Evaluation der Wirkungen von Videoüberwachung bleibt aber in Zukunft – mindestens bei grösseren Videoüberwachungsprojekten – unverzichtbar.

Ausgangslage

Regelung im Datenschutzgesetz Die Sorge, dass mit Videoüberwachung immer mehr Bereiche unseres Lebens kontrolliert werden, hat den Grossen Rat 2004 veranlasst, das DSG durch «Besondere Voraussetzungen für das Bearbeiten der technischen Überwachung mittels Bildübermittlungs- und Bildaufzeichnungsgeräten (Videoüberwachung)» (§ 6a DSG) zu ergänzen. Zur Anwendung kommen diese Regelungen nur dann, wenn kantonale oder kommunale Behörden Videoüberwachungsanlagen betreiben, nicht aber, wenn Privatpersonen wie z.B. Vermieter oder private Unternehmen wie Banken oder Hotels dasselbe tun – dann gilt das Bundesdatenschutzgesetz und der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte ist für die Aufsicht zuständig.

> Derzeit bestehen Bewilligungen für den Betrieb von über 1500 Kameras durch öffentliche Organe.

Dem Videoüberwachungs-Boom sollten vor allem mit folgenden Vorgaben Grenzen gesetzt werden:

—— Der Betrieb einer Videoüberwachungsanlage bedarf einer gesetzlichen Grundlage (Verweis in § 6a Abs. 1 auf § 5 DSG); die rechtliche Grundlage findet sich also nicht im DSG, sondern muss im Sachrecht (z.B. im Polizei-, Schul- oder Personalgesetz) enthalten sein.

—— Videoüberwachung darf einzig zum Schutz von Personen und Sachen vor strafbaren Handlungen eingerichtet werden (§ 6a Abs. 2 DSG).

—— Aufzeichnungen sind nach sehr kurzer Zeit zu vernichten (nächster Arbeitstag plus 24 Stunden) (§ 6a Abs. 4 DSG).

—— Das Einrichten einer Videoüberwachungsanlage bedarf einer Autorisierung durch den Datenschutzbeauftragten (§ 6a Abs. 1 DSG), der damit vorgängig zu prüfen hat, ob die Voraussetzungen erfüllt sind; die Bewilligung ist zu befristen.

Der Regierungsrat erliess dazu in der Videoüberwachungsverordnung detaillierte Ausführungsbestimmungen. Darin wird etwa der Inhalt der Gesuche festgelegt; ausserdem werden die Betreiber von bewilligten Videoüberwachungsanlagen verpflichtet, rechtzeitig vor Ablauf der Frist um die Verlängerung nachzusuchen.

Ziel erreicht? Ob mit der Regelung das Ziel nach fünf Jahren erreicht wurde, muss angesichts der folgenden Feststellungen bezweifelt werden:

—— Derzeit bestehen Bewilligungen für den Betrieb von über 1500 Kameras durch öffentliche Organe im Kanton Basel-Stadt. Neu bewilligt wurden im Jahr 2009 einzig die Videoüberwachungsanlage eines noch nicht überwachten Fahrzeugdepots der Basler Verkehrs-Betriebe (BVB) sowie eine Erweiterung der bereits bewilligten Videoüberwachungsanlage der Steuerverwaltung. Ausserdem wurde den BVB ein Pilotversuch für eine Haltestellen-Überwachung bewilligt – mit Auflagen, damit die Anlage verhältnismässig ist und den Zweck eines Pilotversuches (Prüfung des technischen Geräts, Evaluation möglicher Einsatzoptionen) erfüllen kann. Die BVB teilten daraufhin mit, dass sie die Strategie betreffend die Videoüberwachung an den Haltestellen neu überdenken wollen.

—— Lediglich für rund 60% der Kameras besteht eine gesetzliche Grundlage; der grösste Teil von ihnen wird von der Kantonspolizei betrieben, die sich dafür auf ihre im Polizeigesetz erwähnten Aufgaben stützen kann; ohne die Kameras der Kantonspolizei wäre der Anteil ohne gesetzliche Grundlage deutlich höher.

>

—— Eine Kontrolle Ende 2009 ergab, dass nur noch für rund 65% der Anlagen eine gültige Autorisierung vorlag; bei den restlichen Autorisierungen war die Geltungsdauer abgelaufen. Einzig die Kantonspolizei und die BVB reichten 2009 auf eigene Initiative Gesuche um Verlängerung der Bewilligungen ein.

Ausserdem liess sich feststellen, dass nur sehr wenige Behörden über interne Regelungen für den Betrieb ihrer Videoüberwachungsanlagen verfügen. Nur für rund einen Sechstel der Kameras – darunter die Anlagen der Basler Verkehrs-Betriebe BVB – enthielten die Dossiers beim Datenschutzbeauftragten schriftliche Dokumente, welche Zugriff, Speicherdauer und den allgemeinen Umgang mit den Anlagen regelten.

Beantragte Neuregelung

Gesetzliche Grundlage im IDG Der Regierungsrat hat die Mängel in der geltenden Praxis zum Anlass genommen, im E-IDG eine Neuregelung zu beantragen. Die formalgesetzliche Grundlage für die Videoüberwachung generell soll im IDG geschaffen werden (§ 17 E-IDG). Für jede Anlage, bei deren Aufnahmen Personen identifizierbar sind, wird aber neu zusätzlich ein Reglement verlangt. Es muss den Zweck möglichst konkret festlegen und die wichtigsten Eckpunkte des Einsatzes (wie z.B. die verantwortliche Behörde, die erfassten Orte und Personen, die Betriebszeiten, die Aufzeichnungen, die Speicherfrist und den Zugriff auf die Aufzeichnungen) verbindlich regeln. Es ist von hoher Stelle zu erlassen – in der kantonalen Verwaltung z.B. durch das Departement (§ 18 E-IDG).

Flexibler– aber kontrolliert Auf der anderen Seite sollen zu starre Bestimmungen zweckkonform flexibler ausgestaltet werden: Die extrem knappe Aufbewahrungsfrist hat sich für viele Anlagen als zu kurz herausgestellt; neu soll sie in der Regel eine Woche betragen (§ 17 Abs. 4 E-IDG). Die Kontrolle durch den Datenschutzbeauftragten erfolgt in Form der Vorabkontrolle. Das Reglement muss ihm vor dem Erlass und vor der Verlängerung zur Stellungnahme vorgelegt werden. Die Departementsleitung, welche das Reglement zu erlassen hat, kann wohl von seiner Empfehlung abweichen, muss dafür aber die rechtliche und politische Verantwortung übernehmen. Der Datenschutzaufsicht ist es unbenommen, mit einer nachträglichen Kontrolle zu prüfen, ob die minimalen rechtlichen Anforderungen eingehalten sind, und mit ihren Einwirkungsmöglichkeiten auf eine nötige Verbesserung hinzuwirken. Ausserdem muss, bevor ein ablaufendes Reglement verlängert werden darf, eine Evaluation stattfinden. D.h. nur wenn Videoüberwachung notwendig und wirksam ist, darf eine Verlängerung vorgenommen werden. Mit dieser Regelung wird eine Klärung der Verantwortlichkeiten erreicht.

Übergang von der DSG- zur IDG-Regelung Nach der Behandlung der Videoüberwachungsparagrafen in der JSSK hat der Datenschutzbeauftragte begonnen, bei Verlängerungsgesuchen darauf hinzuwirken, dass die künftig verlangten Voraussetzungen bereits heute eingehalten werden. Ausserdem werden die Verlängerungen so befristet, dass die beantragten IDG-Regelungen möglichst rasch nach ihrem Inkrafttreten auch wirksam werden.

Herausforderungen

Bundesgerichtspraxis Der Entscheid des Bundesgerichts zur Regelung der Videoüberwachung im Polizeigesetz des Kantons Zürich (Urteil 1C_179/2008 vom 30. September 2009) wirft Fragen im Hinblick auf die vorgeschlagene Regelung auf. Die Zürcher Bestimmung wurde als zu unbestimmt bewertet, um eine genügende gesetzliche Grundlage für den Betrieb von Videoüberwachungsanlagen darzustellen. Die baselstädtische Lösung enthält zwar eine verhältnismässig weit gefasste Zweckbestimmungs-Regelung, geht aber gleichwohl weniger weit als die Zürcher Norm. Ausserdem – und das ist unseres Erachtens der entscheidende Unterschied – verlangt das IDG, dass für jede Anlage der Zweck in einem Reglement konkretisiert wird, so dass anhand dieser Zweckbestimmung die Verhältnismässigkeit der Anlage beurteilt werden kann.

Videoüberwachung ist kein Wundermittel, auch wenn mit ihrer Installation oft Wunder erwartet werden.

«Zu Ihrer Sicherheit»? Videoüberwachung ist kein Wundermittel, auch wenn mit ihrer Installation oft Wunder erwartet werden. Gefährlich wird es, wenn Erwartungen geweckt werden, aber nicht erfüllt werden können. Wenn «Videoüberwachung zu Ihrer Sicherheit» versprochen wird, darf jemand auch erwarten, dass eine bestimmte Sicherheit geboten wird: Der überfallenen Frau ist nur gedient, wenn die Aufnahmen in einer Überwachungszentrale in Echtzeit aus-

gewertet werden und sofort eine Intervention ausgelöst werden kann – nicht aber, wenn Stunden später bei der Visionierung der Aufzeichnungen bloss festgestellt werden kann, dass der Täter eine schwarze Gesichtsmaske getragen hat. Wenn Videoüberwachung abhaltend (dissuasiv) wirken soll, indem der Täter damit rechnen muss, dass er – wie beim Schlägerangriff im BVB-Bus von März 2009 – identifiziert und strafrechtlich verfolgt werden kann, dann ist es für die Abhaltewirkung natürlich verheerend und der Betreiber kommt in mehr als nur einen Erklärungsnotstand, wenn sich herausstellt, dass die vermeintlichen Überwachungskameras bloss Attrappen sind.

In der Schweiz existieren praktisch keine Untersuchungen über die tatsächlichen Wirkungen von Videoüberwachung.

Der staatliche Videoüberwacher muss sich die Frage gefallen lassen, wie stark er Sicherheitserwartungen schüren darf, ohne sie wirklich zu erfüllen – und ob er nicht irgendwann Gefahr läuft, aufgrund einer Art Garantenstellung mit Haftungsansprüche konfrontiert zu werden. Damit wird klar, dass die «billigen» Lösungen – Verzicht auf Echtzeit-Auswertung in einer Überwachungszentrale sowie Attrappen – keine günstigen Lösungen sind. Videoüberwachung schafft ein gefährliches und unentschuldbares Sicherheitsdefizit, wenn sie als Sparmassnahme konzipiert ist.

Wirkung und Evaluation

Wirkung Vor der Installation verspricht man sich viel von Videoüberwachung – die Erhöhung der Sicherheit, die Verbesserung der Sauberkeit eines Areals usw. Doch was kann Videoüberwachung tatsächlich bewirken? Untersuchungen aus England lassen erkennen, dass Videoüberwachung an gewissen Orten (z.B. in Parkhäusern) und gegen bestimmte Delikte dissuasive Wirkung entfalten, dass aber in anderen Bereichen und bei anderen Deliktsarten höchstens eine Verlagerungswirkung erreicht wird. In der Schweiz existieren praktisch keine Untersuchungen über die tatsächlichen Wirkungen von Videoüberwachung. Zwar wird häufig argumentiert, es gehe darum, der «gefühlten Unsicherheit» in der Bevölkerung zu begegnen. Doch ist auch die durch Videoüberwachung geschaffene «gefühlte Sicherheit» wohl in vielen Fällen trügerisch.

Evaluation § 18 Abs. 3 E-IDG sieht vor, dass die Videoüberwachungsanlagen vor einer allfälligen Bewilligungsverlängerung auf deren Wirksamkeit hin evaluiert werden müssen. Damit trägt das Gesetz der erwähnten Unsicherheit über die Wirksamkeit Rechnung. Auch in Basel-Stadt wurden bislang die wenigsten Kameras nach Ablauf der Bewilligungsfrist auf ihre Wirksamkeit hin unter die Lupe genommen. Konnte der mit der Installation verfolgte Zweck erreicht werden? Hat eventuell bloss eine Verlagerung stattgefunden, haben also die Kameras die unerwünschten Tätigkeiten bloss an nicht überwachte Orte verdrängt? Je nach Beantwortung dieser Fragen sind die Videoüberwachungsanlagen zu modifizieren oder unter Umständen gar ausser Betrieb zu nehmen. Möglicherweise kann bereits ein Pilotversuch wertvolle Erkenntnisse vermitteln. Deshalb ist darauf zu achten, dass auch solche Einrichtungen kompetent begleitet werden.

Gesellschaftliche Auswirkungen Letztlich steht die Frage im Raum, wie sich Videoüberwachung auf die überwachten Menschen, auf ihr Verhalten und ihre Freiheitsrechte auswirkt. Deshalb lässt etwa die Sicherheitsdirektion der Stadt Luzern die Videoüberwachung im öffentlichen Raum durch einen Forscher der Universität Basel (Department of Business and Economics) wissenschaftlich begleiten und auswerten. Mindestens für grössere Videoüberwachungsprojekte im öffentlichen Raum erscheinen solche Untersuchungen unverzichtbar.

———

Thema 5

Neue Aufgabe: Anlassfreie Kontrolle der Datenbearbeitungen

Mit der «Schengen-Revision» des Datenschutzgesetzes wurde der Datenschutzbeauftragte verpflichtet, das Datenbearbeiten öffentlicher Organe daraufhin zu kontrollieren, ob es die Datenschutzvorgaben einhält. Als Instrument für die Kontrolle wurde der «Datenschutz-Audit» entwickelt. Ende 2009 konnte mit einem Pilotaudit bei der Sicherheitsabteilung der Kantonspolizei begonnen werden.

Aufgaben des Datenschutzbeauftragten

Im «alten» Datenschutzgesetz Unter den Aufgaben der Datenschutzaufsicht war bis zur «Schengen-Revision» schon im «alten» Datenschutzgesetz erwähnt: «Die Aufsichtsstelle überwacht die Anwendung der Vorschriften über den Datenschutz fachlich selbständig und unabhängig» (§ 28 DSG Einleitungssatz vor der «Schengen-Revision»). Auch wenn das Hauptgewicht dieser Bestimmung wohl eher auf der fachlichen Selbständigkeit und Unabhängigkeit lag, liess sich daraus doch auch die Aufgabe «Überwachung» ableiten. In der Aufsichtswirklichkeit erlangte diese Aufgabe aber nie eine grosse Bedeutung – womit der Kanton Basel-Stadt freilich keine Ausnahmeerscheinung war. In der Schweiz waren bisher die Kantone, welche anlassfreie Kontrollen durchführen konnten, an einer Hand abzuzählen. Eine mehr als bloss punktuelle Kontrolltätigkeit entwickelte bis vor kurzem nur der Kanton Zürich. Mit den in Basel-Stadt vorhandenen Ressourcen war es undenkbar, neben der Beratungstätigkeit und den Autorisierungsverfahren auch noch an Kontrollen zu denken – eines der Defizite im Datenschutzbereich, die auch durch die 2005 vorgenommene Ablösung der Datenschutzkommission durch einen Datenschutzbeauftragten nicht behoben wurden.

Nach der «Schengen-Revision» Mit der Ratifizierung des Zusatzprotokolls zur Europarats-Konvention 108 (ZP zur ER-Konv 108) und vor allem mit der Schengen-Assoziierung der Schweiz, durch welche die EG-Datenschutzrichtlinie 95/46 mindestens bei Schengen-Datenbearbeitungen für die Schweiz verbindlich wurde, konnte dieses Defizit nicht mehr hingenommen werden. Eine Wegleitung der Konferenz der Kantonsregierungen zur Umsetzung von Schengen im Datenschutzbereich betonte ebenfalls die Wichtigkeit anlassfreier Kontrollen. Dementsprechend wurde mit der «Schengen-Revision» des Datenschutzgesetzes die Kontrollaufgabe ausdrücklich in die Aufgabenumschreibung aufgenommen: «Die Aufsichtsstelle kontrolliert nach einem durch sie autonom aufzustellenden Prüfprogramm die Anwendung der Bestimmungen über den Datenschutz» (§ 28 Einleitungssatz nach der «Schengen-Revision»). In den Entwurf zum Informations- und Datenschutzgesetz wurde diese Bestimmung unverändert übernommen.

Kontrollmethodik

Systematisches Vorgehen Eine wirksame Kontrolle verlangt ein methodisches Vorgehen. Eine eigentliche Kontrollmethodik hat bisher – soweit ersichtlich – kein Kanton ausser Zürich erarbeitet und regelmässig angewandt. Mehrere andere Kantone liessen Kontrollen jeweils durch externe Unternehmen durchführen. Aus diesem Grund wurde von Anfang an die Zusammenarbeit mit dem Datenschutzbeauftragten des Kantons Zürich (dsb zh) gesucht. Allerdings war auch der «Datenschutz-Review Typ ‹Standard›», den der dsb zh bei kleinen und mittleren Gemeinden durchführt, nicht geeignet zur Übernahme für den Kanton Basel-Stadt. Zu unterschiedlich sind die Strukturen, insbesondere auch im Bereich der Informatik.

In der Schweiz waren bisher die Kantone, welche anlassfreie Kontrollen durchführen konnten, an einer Hand abzuzählen.

Der Datenschutz-Audit, mit welchem die Einhaltung der datenschutzrechtlichen Vorschriften durch Dienststellen bzw. Abteilungen kontrolliert werden soll, musste deshalb erst entwickelt werden. Da die für dieses Projekt verantwortliche juristische Mitarbeiterin auch einen Abschluss als interne Revi-

sorin (Certified Internal Auditor, CIA) hat und in einer der grossen Revisionsgesellschaften tätig war, konnte auf Erfahrungen aus der Privatwirtschaft zurückgegriffen werden. Für die Vorbereitung der Prüfung der Informationssicherheit konnte ausserdem auf kompetente Fachleute bei der Fachstelle für Informatik und Organisation gezählt werden.

Ziel der Kontrolltätigkeit Es geht bei der Kontrolltätigkeit nicht darum, «Schuldige» zu identifizieren und an ihnen ein Exempel zu statuieren. Vielmehr soll – wie mit der Beratung – auch mit der Kontrolltätigkeit vor allem eine Verbesserung des Datenschutzes erreicht werden. Dies geschieht gerade auch im Interesse des öffentlichen Organs. Nach § 7 DSG (und § 6 E-IDG) trägt dasjenige öffentliche Organ die Verantwortung für die Einhaltung der gesetzlichen Vorschriften, welches Informationen zur Erfüllung seiner gesetzlichen Aufgabe bearbeitet oder bearbeiten lässt. In einer informatisierten Umgebung gibt es – wie erwähnt – keinen Datenschutz ohne Informationssicherheit, weshalb das DSG wie auch der IDG-Entwurf entsprechende Vorgaben machen (§ 17 DSG, § 8 E-IDG). Darum umfasst die Verantwortung der Dienststellenleitung ebenso die Informationssicherheit, auch wenn sie die Daten durch eine andere Stelle bearbeiten lässt, also z.B. Informatikdienstleistungen bei den Zentralen Informatikdiensten oder externen Dienstleistern bezieht.

Ablauf des Datenschutz-Audits Mit dem Instrument des nun entwickelten Datenschutz-Audits wird ein öffentliches Organ einer systematischen Datenschutzkontrolle unterzogen. Der Datenschutz-Audit besteht aus zwei Teilen: Im Teil ‹Recht› werden die ausgesuchten Datenbearbeitungsprozesse auf ihre Übereinstimmung mit den datenschutzrechtlichen Vorgaben hin untersucht; ausserdem werden prozessunabhängige Aspekte (u.a. die Gewährleistung der Rechte der betroffenen Personen) geprüft. Im Teil ‹Informationssicherheit› wird untersucht, ob die IT-seitige Umsetzung die rechtlichen Vorgaben einhält, insbesondere ob die Informationen angemessen vor Verlust, Entwendung, unbefugter Bearbeitung oder Kenntnisnahme durch Unberechtigte geschützt sind (§ 17 DSG, § 8 E-IDG und Informatiksicherheitsverordnung).

Für die Verantwortlichen des öffentlichen Organs wird eine Schulung angeboten und sie haben während einer bestimmten Zeit Gelegenheit, ihre Datenbearbeitungen einer Selbstüberprüfung zu unterziehen, wofür der Datenschutzbeauftragte zweckdienliche Tools zur Verfügung stellt. Anschliessend werden die beiden Teile ‹Recht› und ‹Informationssicherheit› durch Audit-Teams des Datenschutzbeauftragten – gestützt auf die eingeforderten Unterlagen und mittels Interviews – nach einem vorgegebenen Prüfprogramm unter die Lupe genommen. Danach haben die Beteiligten des kontrollierten öffentlichen Organs die Möglichkeit, zum Prüfergebnis Stellung zu nehmen. Allenfalls werden im Prüfbericht für die Umsetzung von Empfehlungen Fristen vorgegeben und ein Follow-up vorgesehen.

Mit dem Datenschutz-Audit wird ein öffentliches Organ einer systematischen Datenschutzkontrolle unterzogen.

Pilotaudit In einem Pilotversuch soll geprüft werden, ob die geplanten Abläufe, die vorbereiteten Unterlagen für die Selbstüberprüfung und die Prüfprogramme ‹Recht› und ‹Informationssicherheit› den Praxistest bestehen. Im Berichtsjahr konnte bei der Sicherheitsabteilung der Kantonspolizei mit diesem Pilotaudit begonnen werden.

Ausblick

Beginn der Kontrollen Es ist geplant, nach Abschluss der Pilotphase risikoorientiert mit den Kontrollen zu beginnen. Im Vordergrund sollen Bereiche stehen, bei welchen das Risiko von Persönlichkeitsverletzungen tendenziell grösser ist, etwa weil sensitive Daten bearbeitet werden. Allerdings hat sich bereits jetzt gezeigt, dass die Durchführung von Datenschutz-Audits, die mehr als blosse Scheinkontrollen sein sollen, auf Seiten der Audit-Teams äusserst ressourcenintensiv ist. Die Kadenz, mit welchen einzelne Dienststellen oder Abteilungen auditiert werden können, wird entscheidend davon abhängen, welche Personalressourcen für die Kontrolltätigkeit zur Verfügung stehen.

Fälle

Fall 1 Herausgabe des Lohnausweises an die Sozialhilfe?

Eine private Arbeitgeberin wurde von der Sozialhilfebehörde aufgefordert, den Lohnausweis eines Angestellten einzureichen, weil dieser Sozialhilfe bezog und die Herausgabe des Lohnausweises ablehnte. Die Sozialhilfebehörde wollte damit ermitteln, ob der betreffende Arbeitnehmer mit seinem Arbeitseinkommen über dem gesetzlichen Freibetrag liegt oder ob er zu Recht die vollen Sozialhilfeleistungen bezieht.

Die private Arbeitgeberin gelangte an den kantonalen Datenschutzbeauftragten mit der Frage, ob sie den Lohnausweis an die Sozialhilfebehörde weiterleiten dürfe.

Nach § 2 Abs. 1 DSG handelt es sich bei Angaben über eine natürliche oder juristische Person, soweit diese bestimmt oder bestimmbar ist, um Personendaten. § 2 Abs. 3 DSG statuiert, dass jeder Umgang mit Personendaten ein Bearbeiten darstellt, namentlich das Beschaffen, Verwenden und Bekanntgeben.

Lohnausweise haben einen auf die betroffene Person bezogenen Aussagegehalt und sind daher als Personendaten zu qualifizieren. Durch die Weitergabe an die Sozialhilfebehörde werden sie bekannt gegeben und daher bearbeitet.

Damit Personendaten rechtmässig bearbeitet werden dürfen, ist nach § 5 Abs. 1 DSG eine gesetzliche Grundlage notwendig. Diese kann die Bearbeitung konkret vorschreiben (unmittelbare gesetzliche Grundlage) oder eine gesetzliche Aufgabe statuieren, zu deren Erfüllung die Datenbearbeitung erforderlich ist (mittelbare gesetzliche Grundlage). Das Bearbeiten der Daten muss zudem nach § 5 Abs. 2 DSG verhältnismässig sein.

Hier ist die gesetzliche Grundlage im Sozialhilfegesetz zu finden. § 28 Abs. 3 schreibt vor, dass die Arbeitgeberin einer unterstützten Person gegenüber den Organen der öffentlichen Sozialhilfe zur mündlichen oder schriftlichen Auskunftserteilung verpflichtet ist. § 28 Abs. 3 Sozialhilfegesetz stellt somit eine unmittelbare gesetzliche Grundlage dar, die es den Sozialhilfebehörden erlaubt, den Lohnausweis eines Sozialhilfeempfängers direkt bei deren Arbeitgeberin einzufordern.

Damit die Datenbearbeitung verhältnismässig ist, muss sie geeignet, erforderlich und für den Betroffenen zumutbar sein. Der Lohnausweis ist ein taugliches Mittel, um die finanziellen Verhältnisse eines Sozialhilfeempfängers zu überprüfen. Die Datenerhebung beim Arbeitgeber erscheint für den angestrebten Zweck geeignet.

Um jedoch auch erforderlich zu sein, muss sie das mildeste mögliche Mittel darstellen, d.h. die Sozialhilfebehörde müsste zunächst die Information vom Sozialhilfeempfänger selbst beziehen. Doch wenn dieser – wie im vorliegenden Fall – die Auskunft verweigert, bleibt nur der direkte Weg über die Arbeitgeberin. Die Datenbearbeitung ist somit nicht nur geeignet, sondern auch erforderlich.

Ergebnis

Aufgrund von § 28 Abs. 3 Sozialhilfegesetz ist die Arbeitgeberin verpflichtet, auf Anfrage den Lohnausweis eines Angestellten der Sozialhilfebehörde auszuhändigen, damit diese die finanzielle Situation des Sozialhilfeempfängers korrekt ermitteln und gestützt darauf die ihm zustehenden Leistungen festlegen kann.

Fall 2 Daten aus dem Datenmarkt – privat «genutzt»

Die Mitarbeiter einer Verwaltungsstelle haben einen Online-Zugriff auf den Datenmarkt, weil sie die entsprechenden Einwohnerdaten zur Erfüllung ihrer gesetzlichen Aufgabe benötigen. Dürfen sie den Zugriff auch für private Recherchen nutzen?

Ein Dienststellenleiter hat mitbekommen, dass Mitarbeiter eine neue Kollegin im Datenmarkt recherchiert hatten. Sie haben dabei herausgefunden, dass unter derselben Adresse eine weitere Arbeitskollegin gemeldet ist. Diese «Erkenntnis» wurde dann intern weiterverbreitet und zu Klatsch umfunktioniert («die beiden sind lesbisch!»). Wie ist diese Nutzung aus datenschutzrechtlicher Sicht zu beurteilen?

Nach dem Datenschutzgesetz sind Personendaten Angaben, die sich auf eine Person beziehen oder auf eine Person beziehbar sind; die Person muss bestimmt oder mindestens bestimmbar sein. Hier handelt es sich unzweifelhaft um Personendaten.

Personendaten dürfen nach § 5 DSG bearbeitet werden, wenn eine gesetzliche Grundlage zum konkreten Datenbearbeiten verpflichtet oder ermächtigt (unmittelbare gesetzliche Grundlage) oder das Bearbeiten zur Erfüllung einer gesetzlichen Aufgabe erforderlich ist (mittelbare gesetzliche Grundlage). Ausserdem muss das Datenbearbeiten verhältnismässig, d.h. zur Zweckerreichung geeignet und erforderlich und der betroffenen Person zumutbar sein. Erforderlich ist es, wenn die gesetzliche Aufgabe ohne das Bearbeiten der Daten nicht erfüllt kann.

Der Online-Zugriff auf den Datenmarkt stellt datenschutzrechtlich ein Bekanntgeben dar. Damit ein Bekanntgeben an eine andere Behörde zulässig ist, muss es die gleichen Voraussetzungen erfüllen (und darf nicht durch eine besondere gesetzliche Geheimhaltungspflicht verboten sein). Die rechtliche Rechtfertigung liegt also in der Erfüllung einer gesetzlichen Aufgabe. Den Mitarbeitern ist es deshalb erlaubt, zur Aufgabenerfüllung – aber auch nur zur Aufgabenerfüllung – mittels Online-Zugriff Daten aus dem Datenmarkt zu beziehen. Dasselbe gilt logischerweise auch für den Zugriff beispielsweise auf Steuerdaten, wobei hier mit dem Steuergeheimnis noch eine gesetzliche Verschwiegenheitspflicht hinzutritt.

Wer Personendaten, auf die er kraft seiner gesetzlichen Aufgabe zugreifen kann, für andere Zwecke verwendet, verletzt das Datenschutzgesetz und die Persönlichkeitsrechte der betroffenen Personen. Die Vertrauenswürdigkeit von Mitarbeitern, welche amtliche Zugriffsberechtigungen für private Zwecke missbrauchen, ist mehr als bloss fraglich. Die Rechtsverletzung kann arbeitsrechtliche Konsequenzen zur Folge haben, abgesehen davon, dass allenfalls auch die Betroffenen Rechtsansprüche erheben können. Der Datenschutzbeauftragte ist daran, Kontrollen vorzubereiten, bei welchen anhand von Systemaufzeichnungen die Berechtigung von Zugriffen einzelner Mitarbeiter geprüft werden kann.

Ergebnis

Wer Personendaten, auf die er kraft seiner gesetzlichen Aufgabe zugreifen kann, für andere Zwecke verwendet, verletzt das Datenschutzgesetz und die Persönlichkeitsrechte der betroffenen Personen. Er muss mit arbeitsrechtlichen Konsequenzen rechnen und kann unter Umständen von den Betroffenen belangt werden. Vorgesetzte dürfen solche Rechtsverletzungen auf keinen Fall tolerieren.

Fall 3 Informationsrechte der Eltern

Wenn Schulkinder das Angebot eines pädagogischen Dienstes in Anspruch nehmen (müssen), so fühlen sich Eltern oftmals im Unklaren darüber, was «hinter den verschlossenen Türen» mit dem oder über das Kind besprochen wird, welche Entscheide gefällt werden und wie diese Entscheide die weitere Laufbahn des Kindes beeinflussen könnten.

Wenn Schülerinnen oder Schüler Angebote des logopädischen oder schulpsychologischen Dienstes in Anspruch nehmen, so entsteht bei erziehungsberechtigten Personen manchmal das Gefühl einer fehlenden Aufklärung über die einzelnen Schritte und Therapiesitzungen. Das Datenschutzrecht verlangt Transparenz gegenüber den betroffenen Personen – besser schon während des laufenden Verfahrens und nicht erst, wenn die Eltern ihr Recht auf Auskunft geltend machen und möglicherweise die Zusammenarbeit zu verweigern drohen. Die zwischen Behörden und Eltern mindestens notwendigen Informationsflüsse lassen sich exemplarisch anhand des Logopädischen Dienstes (LPD) illustrieren:

—— Die Eltern melden sich beim LPD und bitten um eine Abklärung. Der LPD lässt den Eltern ein Formular «Anmeldung zur Abklärung» zukommen. Auf diesem Formular haben die Eltern die Möglichkeit, den Informationsaustausch zwischen dem LPD und anderen Stellen zu erlauben (Einverständnis-Erklärung). Die Einwilligung kann für jeden Dienst einzeln abgegeben werden – die Eltern können also den Informationsaustausch mit dem behandelnden Kinderarzt zulassen, nicht aber mit der Klassenlehrerin usw.

—— Haben die Eltern das Formular ausgefüllt, so wird eine Abklärung vorgenommen. Die Eltern werden über das Resultat der Abklärung und das weitere Vorgehen schriftlich informiert.

—— Die Eltern haben jederzeit die Möglichkeit, Akteneinsicht zu verlangen. In der Regel wird diese vor Ort gewährt, da aufgrund der Komplexität und der zahlreichen Fachausdrücke die Anwesenheit eines Logopäden/einer Logopädin sinnvoll ist. Mit der so erfolgenden Erläuterung können Missverständnisse aus dem Weg geräumt werden.

—— Haben die Eltern eingewilligt, so erhalten die Lehrpersonen usw. lediglich die Information, dass eine Abklärung stattgefunden hat und ob eine Therapie angeordnet wurde. Erscheint es für den Unterricht und die Förderung des Kindes sinnvoll, so kann der LPD auch nähere Informationen weitergeben (z.B. Vorschläge für Übungen im Deutschunterricht usw.).

—— Wird die Therapie schliesslich aufgenommen, so werden Lehrpersonen usw. darüber informiert, sofern die Eltern eingewilligt haben.

Werden diese Schritte eingehalten bzw. werden bereits zu Beginn einer Therapie die allenfalls in Frage kommenden Informationsflüsse transparent gemacht und mit den Erziehungsberechtigten besprochen, so wird die für eine erfolgreiche Zusammenarbeit sämtlicher Beteiligten notwendige Transparenz geschaffen.

Ergebnis

Das Datenschutzrecht garantiert Transparenz gegenüber den betroffenen Personen, spätestens dann, wenn sie ihr Auskunfts- und Einsichtsrecht nach § 19 DSG geltend machen – oft ist im Interesse einer erfolgreichen Zusammenarbeit eine aktive und offene Kommunikation während des laufenden Verfahrens unabdingbar.

Fall 4 Kantonale (Prä-)Hooligan-Datenbank

Die Kantonspolizei führte während mehreren Jahren eine Datenbank, in der sie Personen, welche im Umfeld von Fussballspielen auffällig geworden waren, verzeichnete. Diese Personen wurden noch nicht als Hooligans klassifiziert, zeichneten sich aber durch ein erhöhtes Gewaltpotential aus.

In der Stadt Zürich wurde über die Schaffung einer Rechtsgrundlage für eine Datenbank Gamma (griechisch «G» für Gewalt) abgestimmt. In dieser Datenbank sollten Personen erfasst werden, welche am Rande von Sportanlässen die Nähe zur Gewalt suchen und Gewaltbereitschaft zeigen, ohne selbst schon gewalttätig zu werden. Im Vorfeld der Abstimmung stellte ein Medienschaffender die Frage nach dem Bestehen einer derartigen Fussball-Fan-Datenbank in Basel-Stadt. Die Vermutung bestätigte sich – auch die Kantonspolizei Basel-Stadt unterhielt eine Datenbank, in welcher im erwähnten Sinne auffällige Fussballfans verzeichnet wurden. Die gesamtschweizerische Hooligan-Datenbank «Hoogan» gab es zum Zeitpunkt der Schaffung der kantonalen (Prä-)Hooligan-Datenbank noch nicht, und auch nach der Inbetriebnahme von «Hoogan» erachtete die damalige Polizeileitung den Betrieb der kantonalen Datenbank für notwendig, da in «Hoogan» keine potentiellen Hooligans verzeichnet werden. Mit der Schaffung der gesamtschweizerischen Hooligan-Datenbank «Hoogan» stellte sich die Frage, ob und wenn ja auf welcher Rechtsgrundlage basierend die kantonale (Prä-)Hooligan-Datenbank weiterhin betrieben werden könne.

Datenbearbeitungen durch kantonale Behörden bedürfen einer gesetzlichen Grundlage (§ 5 Abs. 1 DSG). In diesem Fall stützte die Kantonspolizei den Betrieb der (Prä-)Hooligan-Datenbank auf die polizeiliche Generalklausel. Die polizeiliche Generalklausel dient als Rechtgrundlage für die Abwehr von unmittelbar drohenden und nicht voraussehbaren Gefahren, welche ein Eingreifen der Polizei erforderlich machen. Das Auftreten von gewaltbereiten Personen im Umfeld von Fussballspielen ist zweifelsohne kein solches nicht voraussehbares Ereignis, das mit solcher zeitlicher Dringlichkeit das Führen eines Registers verlangt, dass keine ordentliche Rechtsgrundlage geschaffen werden könnte. Davon abgesehen sieht das Polizeigesetz vor, dass gestützt auf die polizeiliche Generalklausel nur «im Einzelfall» unaufschiebbare Massnahmen getroffen werden dürfen (§ 9 PolG), was bei einer Registrierung klarerweise nicht der Fall ist. Aus diesen Gründen kann die polizeiliche Generalklausel nicht zur Anwendung gelangen, weshalb ja auch in der Stadt Zürich eine Rechtsgrundlage geschaffen wurde.

Der Datenschutzbeauftragte hätte nach dem Bekanntwerden dieser Umstände der Polizeileitung in einer Empfehlung zur Einstellung der Datenbearbeitung geraten und im Falle einer Ablehnung der Empfehlung eine verbindliche Weisung im Sinne von § 29 Abs. 5 DSG erlassen. Der neue Polizeikommandant anerkannte das Fehlen einer gültigen Rechtsgrundlage und ordnete sofort an, die Datenbank ausser Betrieb zu nehmen. Auch der Datenschutzbeauftragte begrüsste dieses Vorgehen.

Ergebnis

Die polizeiliche Generalklausel dient als Rechtgrundlage für die Abwehr von unmittelbar drohenden und nicht voraussehbaren Gefahren, welche ein Eingreifen der Polizei erforderlich machen. Das Auftreten gewaltbereiter Fussball-Fans ist nicht derart unvorhersehbar, dass nicht eine ordentliche Rechtsgrundlage für eine Registrierung geschaffen werden könnte. Der (Prä-)Hooligan-Datenbank fehlt deshalb die nötige rechtliche Grundlage, weshalb ihr Betrieb einzustellen ist.

Fall 5 Adressbekanntgabe trotz Sperrung?

Immer wieder wenden sich Personen an das Einwohneramt mit der Bitte, Name, Adresse oder Geburtsdatum einer bestimmten Person bekannt zu geben. Gestützt auf § 12 DSG ist diese Auskunfterteilung zulässig. Was aber, wenn die betreffende Person die Bekanntgabe ihrer Daten beim Einwohneramt hat sperren lassen?

Folgender fiktiver, aber aus verschiedenen Begebenheiten zusammengestellter Sachverhalt verdeutlicht die Problematik, mit welcher sich die Mitarbeiterinnen und Mitarbeiter des Einwohneramtes nicht selten konfrontiert sehen: Herr X wendet sich an das Einwohneramt mit der Bitte, ihm die aktuelle Adresse von Frau Y bekannt zu geben. Er habe noch eine Forderung aus einem gemeinsamen Mietvertrag gegenüber Frau Y – diese habe sich aber scheinbar in Luft aufgelöst und er könne ihre Adresse nirgendwo in Erfahrung bringen.

Gemäss § 12 Abs. 1 DSG darf die Einwohnerkontrolle einer privaten Person auf Gesuch hin Namen, Adresse und Geburtsdatum von einzelnen Personen bekanntgeben. Herr X hat also grundsätzlich das Recht, die Adresse von Frau Y zu erfahren. Hat Frau Y jedoch ihr Sperrrecht ausgeübt und die Bekanntgabe ihrer Daten sperren lassen, so ist die Bekanntgabe gemäss § 13 DSG nur dann zulässig, wenn eine gesetzliche Verpflichtung zur Bekanntgabe besteht bzw. die Bekanntgabe zur Erfüllung einer gesetzlichen Aufgabe erforderlich ist oder wenn im Gesuch glaubhaft gemacht wird, dass die Daten zur Durchsetzung von Rechtsansprüchen erforderlich sind. Da Herr X ja bereits dargelegt hat, dass eine Forderung aus einem Mietvertrag gegenüber Frau Y bestehe, könnte grundsätzlich ein Fall von § 13 lit. c DSG bejaht und die Datensperre durchbrochen werden.

Doch reicht das? Immerhin könnte Herr X lediglich «seinen Teil der Geschichte» erzählen. Besteht die behauptete Forderung überhaupt noch? Vielleicht hat Frau Y ihre Schuld längst bezahlt oder ein Gericht hat die Forderung abgewiesen. Vielleicht ist Herr X der Ex-Partner von Frau Y, der ihr nachstellt oder droht, ihr und den Kindern Gewalt anzutun; möglicherweise hat Frau Y genau deswegen ihr Sperrrecht ausgeübt. Lauter Hintergründe, welche das Einwohneramt nicht kennt und für seine «normale» Aufgabenerfüllung auch nicht zu kennen braucht. Das Einwohneramt kommt nur in den Besitz dieser Informationen, wenn es Frau Y fragt – aus dem Gesuch werden sie nicht hervorgehen. Soll also die Durchbrechung einer Datensperre bewirkt werden, so muss zwingend der betroffenen Person, welche die Bekanntgabe ihrer Daten hat sperren lassen, das rechtliche Gehör gewährt werden. Vorher darf das Einwohneramt die Adressen nicht herausgeben – anders als z.B. Geld, das wieder zurückverlangt werden kann, sind Informationen, die einmal herausgegeben worden sind, nicht zurückzuholen.Telefonische Anfragen zu Adressen, welche gesperrt wurden, sind daher zwingend auf den schriftlichen Weg zu verweisen.

Der Datenschutzbeauftragte hat im Rahmen der Beratung des IDG-Entwurfs der JSSK vorgeschlagen, dieses Vorgehen ausdrücklich im Gesetz zu verankern. Die Problematik betrifft übrigens seit der Revision von § 13 DSG (künftig § 28 E-IDG) nicht mehr nur das Einwohneramt, sondern alle öffentlichen Organe, welche aufgrund einer spezialgesetzlichen Bestimmung Personendaten voraussetzungslos bekannt geben dürfen.

Ergebnis

Keine Durchbrechung der Bekanntgabesperre nach § 13 DSG ohne rechtliches Gehör der betroffenen Person.

Fall 6

Umgang mit Patientendaten

Wer eine Bewilligung für eine selbständige Tätigkeit im medizinischen Bereich erlangen will, muss eine bestimmte Anzahl Praktika absolvieren. Im Rahmen der Praktika wird ein Praktikumsprotokoll erstellt, welches von der Bewilligungsbehörde kontrolliert wird. Die Bewilligungsbehörde verlangt nun im besagten Protokoll die Angaben der Initialen des Patienten. Ist das zulässig?

Wer im Kanton Basel-Stadt für die Ausübung einer selbständigen Tätigkeit eine Bewilligung nach Medizinalpersonengesetz erlangen will, muss bestimmte Voraussetzungen erfüllen. So wird im Rahmen dieses Bewilligungsverfahrens von den Kandidaten die Absolvierung von Praktika verlangt. Bei diesen Praktika wird ein Praktikumsprotokoll erstellt, das es der Bewilligungsbehörde (Gesundheitsdepartement) ermöglicht, die Praktikumstätigkeit zu überprüfen und – unter anderem – gestützt darauf zu entscheiden, ob die Voraussetzungen für die Erlangung einer Berufsausübungsbewilligung erfüllt sind oder nicht.

Der Vertreter eines privaten Instituts, welches Praktikanten ausbildet, hat sich an den kantonalen Datenschutzbeauftragten gewandt, weil er der Ansicht ist, dass mit der Angabe der Initialen der Patienten im Praktikumsprotokoll die Datenschutzbestimmungen nicht eingehalten werden:

Bei den Patientendaten, welche von den Praktikanten im Praktikumsprotokoll aufgezeichnet werden, handelt es sich um Personendaten im Sinne von § 2 Abs. 1 DSG. Auch wenn bloss Initialen, Geschlecht und Geburtsdatum anzugeben sind, sind die Patienten – über den Beizug des Patientendossiers – bestimmbar. Dies muss auch so sein, wenn eine Kontrolle über die Absolvierung der erforderlichen Behandlungen möglich sein soll. Weil es um Angaben im Kontext mit einer medizinischen Behandlung geht, handelt es sich sogar um besonders schützenswerte Personendaten im Sinne von § 2 Abs. 2 DSG. Die verlangte Bekanntgabe von Initialen, Geschlecht und Geburtsdatum der Patienten im Praktikumsprotokoll stellt ein Bekanntgeben und damit ein Bearbeiten von Personendaten dar (§ 2 Abs. 3 DSG).

Personendaten dürfen nach § 5 Abs. 1 DSG nur bearbeitet werden, wenn entweder eine gesetzliche Grundlage das Bearbeiten selber vorsieht oder das Bearbeiten zur Erfüllung einer gesetzlichen Aufgabe erforderlich ist. Nach § 6 DSG dürfen besonders schützenswerte Personendaten nur bearbeitet werden, wenn ein Gesetz dies ausdrücklich vorsieht oder wenn das Bearbeiten von besonders schützenswerten Personendaten für eine klar umschriebene gesetzliche Aufgabe zwingend notwendig ist.

Der Bewilligungsbehörde obliegen im hier relevanten Zusammenhang zwei Aufgaben: generell die Aufsicht über die Ausübung der medizinischen Berufe im Kanton Basel-Stadt und im Besonderen die Erteilung der Bewilligung für eine selbständige oder unselbständige Tätigkeit im medizinischen Bereich.

Im Rahmen ihrer Aufsichtspflicht muss es der Bewilligungsbehörde möglich sein, bei der Institution, bei welcher die Praktikanten ihre Behandlungen durchführen, zu kontrollieren, ob die Behandlungen den Anforderungen entsprechen und tatsächlich durchgeführt worden sind, etwa durch einen Rückgriff auf die entsprechenden Patientendossiers.

Die Erhebung der Initialen der Patienten können zwar diesen Rückgriff erleichtern, sind aber nicht erforderlich (und erst recht nicht zwingend erforderlich): Wenn nämlich die Institution gewährleisten kann, dass die Patientendossiers auch ohne Initialen gefunden werden können – etwa indem über das Behandlungsdatum und das Geburtsdatum der Zugriff auf das richtige Dossier möglich ist –, ist eine Kontrolle ohne die Initialen möglich. Die Verwendung der Initialen erhöht markant die Wahrscheinlichkeit, dass Personen erkannt werden, ohne dass dies zur Aufgabenerfüllung erforderlich ist.

Ergebnis

Da der kantonale Datenschutzbeauftragte gegenüber Privaten keine Empfehlung abgeben kann (in diesem Bereich ist der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte zuständig), empfahl er der Bewilligungsbehörde, auf die Erhebung der Initialen auf dem Praktikumsprotokoll zur Erlangung einer Berufsausübungsbewilligung im Kanton Basel-Stadt zu verzichten. Im Gegenzug empfahl er, die Bewilligungsbehörde solle die Institutionen, bei welchen Praktika zur Erlangung einer Berufsausübungsbewilligung durchgeführt werden können, ausdrücklich verpflichten, die Patientenadministration so zu führen, dass die für die Kontrolle relevanten Patientendossiers auch ohne Initialen gefunden werden können.

Anhang

Verzeichnis der zitierten Gesetze und Materialen

Basel-Stadt

DSG Gesetz über den Schutz von Personendaten (Datenschutzgesetz) vom 18. März 1992, SG153.260

E-IDG Entwurf zum Gesetz über die Information und den Datenschutz (Informations- und Datenschutzgesetz) vom 10. Februar 2009

ISV Verordnung zur Informatiksicherheit vom 9. April 2002, SG 153.320

KV Verfassung des Kantons Basel-Stadt vom 23. März 2005, SG 111.100

Medizinalberufegesetz Gesetz betreffend Ausübung der Berufe der Medizinalpersonen und der Komplementärmedizin (Medizinalberufegesetz) vom 26. Mai 1879, SG 310.100

PolG Gesetz betreffend die Kantonspolizei des Kantons Basel-Stadt (Polizeigesetz) vom 13. November 1996, SG 510.100

Ratschlag 05.1024.01 Ratschlag und Entwurf Nr. 05.1024.01 vom 25. September 2007 betreffend Teilrevision des Gesetzes über den Schutz von Personendaten (Datenschutzgesetz) vom 18. März 1992 (SG 153.260): Anpassung an Schengen/Dublin

Ratschlag 08.0637.01 Ratschlag Nr. 08.0637.01 vom 10. Februar 2009 betreffend Gesetz über die Information und den Datenschutz (Informations- und Datenschutzgesetz)

Ratschlag 09.0298.01 Ratschlag Nr. 09.0298.01 vom 24. März 2009: Änderung des Gesetzes über das Aufenthaltswesen vom 16. September 1998 (Aufenthaltsgesetz), SG 122.200

Sozialhilfegesetz Sozialhilfegesetz vom 29. Juni 2000, SG 890.100

SoHaG Gesetz über die Harmonisierung und Koordination von bedarfsabhängigen Sozialleistungen (Harmonisierungsgesetz Sozialleistungen, SoHaG) vom 25. Juni 2008, SG 890.700

Videoüberwachungsverordnung Verordnung über die Videoüberwachung (Videoüberwachungsverordnung) vom 4. Januar 2005, SG 153.290

Bund, international

DSG-Bund Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG) (Stand am 1. Januar 2008), SR 235.1

EG-DSRL Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EG Datenschutzrichtlinie), ABl L 281 vom 23.11.1995, 31 ff.

ER-Konv 108 Übereinkommen vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, SR 0.235.1

ZP zur ER-Konv 108 Zusatzprotokoll vom 8 November 2001 zum Übereinkommen des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Datenbezüglich Aufsichtsbehörden und grenzüberschreitende Übermittlung, SR 0.235.11

Datenschutzbeauftragter
des Kantons Basel-Stadt
Postfach 205, 4010 Basel
Tel. 061 201 16 40
Fax 061 201 16 41
datenschutz@dsb.bs.ch
www.dsb.bs.ch

Datenschutzbeauftragter
Dr. iur. Beat Rudin, Advokat

Team
lic. iur. Carmen Lindner
Dr. iur. Sandra Stämpfli
lic. iur. Barbara Widmer, LL.M., CIA

Bericht an den Grossen Rat
Tätigkeitsbericht des Daten-
schutzbeauftragten des Kantons
Basel-Stadt
ISSN 1664-1868

Bezug
Datenschutzbeauftragter
des Kantons Basel-Stadt
Postfach 205, 4010 Basel
Tel. 061 201 16 40
Fax 061 201 16 41
datenschutz@dsb.bs.ch
www.dsb.bs.ch

Gestaltung
Andrea Gruber,
Visuelle Gestaltung, Basel

Druck
Gremper AG