Bericht an den Grossen Rat

2011

Tätigkeitsbericht des Datenschutzbeauftragten des Kantons Basel-Stadt

Der Datenschutzbeauftragte erstattet der Wahlbehörde jährlich Bericht über seine Tätigkeit, Feststellungen und Erfahrungen; der Bericht wird veröffentlicht (§ 28 lit. d DSG).

Inhaltsübersicht

Einleitung

Themen

Fälle

Anhang

Einleitung

2011 – Konsolidierung und Aufbruch

Im vergangenen Jahr ging es einerseits um die Konsolidierung der im Vorjahr eingeführten Prozesse, andererseits war es das Jahr der Vorbereitung auf das neue Informations- und Datenschutzgesetz. Erfreulich war insbesondere, dass sich die öffentlichen Organe mit heiklen Themen vermehrt von sich aus an den Datenschutzbeauftragten wandten.

Ein Blick aufs vergangene Jahr

Brisante Themen Das Thema Datenschutz verliert in keiner Weise an Brisanz. Im vergangenen Jahr haben technologische und gesellschaftliche Entwicklungen ihre Spuren (auch) in der Verwaltung hinterlassen. Die fortschreitende Digitalisierung, die zunehmende Vernetzung, die immer stärker verbreitete Verwendung mobiler Geräte sind nur ein paar Stichworte, welche die technologische Entwicklung illustrieren. Outsourcing und Cloud Computing erscheinen unter dem Aspekt des anhaltenden Kostendrucks attraktiv, führen aber auch dazu, dass die Verantwortlichkeitsbereiche plötzlich nicht mehr so klar erkannt werden. Die teils unbedachte Verwendung von Social Media führt zu einer Ver schiebung im Wertesystem – was früher als privat galt und gehütet wurde, wird von einer zunehmenden Zahl von Menschen öffentlich gemacht. Der Sozialdruck kann dazu führen, dass Menschen Informationen über sich preisgeben, die sie noch vor kurzem lieber für sich behalten hätten. Private, ja intime Informationen werden zur Währung im Wettkampf um Aufmerksamkeit und «Freunde». Nur wenige können sich diesen Entwicklungen entziehen; nicht alle denken daran, dass die Information, die sie heute als «cooler» als andere erscheinen lässt, morgen von anderen verwendet werden können. Die Bilder der letzten feuchtfröhlichen Party oder des neuen Bikinis mögen zwar den 472 «Freunden» gefallen, aber vielleicht nicht der Personalabteilung des Arbeitgebers. Die Tatsache, dass Normsysteme – Gesetze, aber auch einfache gesellschaftliche Regeln – nicht mehr selbstverständlich beachtet werden, lässt den Ruf nach Überwachung laut werden, sei es an Hotspots in der Stadt oder bei der Internetnutzung am Arbeitsplatz. Und rasch wird schliesslich versucht, unerwünschte gesellschaftliche Entwicklungen mit neuen rechtlichen Regeln in den Griff zu bekommen ...

Achtung In diesem Spannungsfeld spielt sich «Datenschutz» ab. Dabei können gesellschaftliche und technologische Entwicklungen realistischerweise nicht aufgehalten oder ungeschehen gemacht werden. Der Datenschutzbeauftragte kann aber auf einen sorgsamen Umgang mit Informationen hinwirken. Es geht dabei auch um Achtung – um Achtung vor den Menschen, deren Informationen wir bearbeiten. Der Datenschutzbeauftragte ist dieser Aufgabe auch im vergangenen Jahr nachgekommen und will mit dem vorliegenden Tätigkeitsbericht in der Rubrik «Themen» (Seiten 4 ff.) Probleme und Lösungsansätze schildern. Zwei Themen werden herausgegriffen und vertieft behandelt: der 2011 vorbereitete Sprung zum Öffentlichkeitsprinzip (Seiten 12 ff.) und der Zugang zu den eigenen Personendaten (Seiten 17 ff.).

Geschäfte und ihre Herkunft 344 neue Geschäfte (2010: 323) wurden 2011 eröffnet. Die Initiant(inn)en verteilten sich wie folgt:

— 69 Fälle (20% / 2010: 22%) wurden von Privatpersonen initiiert; sie stellten meistens konkretes behördliches Datenbearbeiten in Frage;
— in 9 Fällen (3% / 2010: 4%) ging der Anstoss von öffentlichen Organen der Gemeinden aus;
— in 24 Fällen (7% / 2010: 4%) waren ausserkantonale Stellen die Initianten;
— in 11 Fällen (3% / 2010: 3%) kamen Anfragen von Medien;
— in 37 Fällen (11% / 2010: 12%) ging die Initiative vom Datenschutzbeauftragten selber aus; dazu gehörten insbesondere administrative Geschäfte, die Kontrollen und das Aktivwerden im Zusammenhang mit der Verlängerung von Videoüberwachungs-Autorisierungen und bei Feststellungen beispielsweise aufgrund von Medienberichten.
— In den übrigen 56% (2010: 55%) waren öffentliche Organe des Kantons (inkl. den öffentlich-rechtlichen Anstalten) die Initianten.

Personal In personeller Hinsicht hat sich im vergangenen Jahr einiges bewegt. Frau Paola Vassalli, MLaw, beendete ihr juristisches Volontariat per Ende Februar 2011; ihr folgten Frau Daniela Waldmeier, MLaw (1. April bis 31. Juli 2011) und Frau Alexandra Büche, MLaw (1. Oktober 2011 bis 31. März 2012). Mit den vom Grossen Rat bewilligten zusätzlichen Stellenprozenten konnte das Datenschutz-Team verstärkt werden: Zuerst konnte per 1. Juni 2011 die neue Stelle eines Informatikrevisors mit Herrn Markus Brönnimann besetzt werden (80%); er brachte von seiner früheren Tätigkeit in den Zentralen Informatikdiensten (ZID) fundierte Kenntnisse der kantonalen Informatik mit. Am 1. August 2011, direkt nach ihrem Volontariat, begann schliesslich Frau Daniela Waldmeier, MLaw, ihre Tätigkeit als juristische Mitarbeiterin (60%).

Bilanz

Erfreulich Ein Kernelement des Datenschutzrechts ist die Verantwortung. Für den Umgang mit Personendaten (oder künftig umfassender: für den Umgang mit Informationen) trägt dasjenige öffentliche Organ die Verantwortung, das die Informationen zur Erfüllung seiner gesetzlichen Aufgaben bearbeitet[1] oder bearbeiten lässt[2]. Der Datenschutzbeauftragte weist die öffentlichen Organe seit zwei Jahren aktiv auf diesen Umstand hin. Der Blick auf die von öffentlichen Organen im letzten Jahr dem Datenschutzbeauftragten unterbreiteten Fragen zeigt, dass sich die öffentlichen Organe heikler Themen zunehmend bewusster werden und sich vermehrt von sich aus an den Datenschutzbeauftragten wenden. Es ist daraus der erfreuliche Schluss zu ziehen, dass sich das Thema «datenschutzrechtliche Verantwortung» in der Verwaltung auszubreiten beginnt.

Erstaunlich Auf der anderen Seite ist es doch erstaunlich, dass sich gerade im Bereich der Informationssicherheit immer wieder öffentliche Organe erstaunt zeigen, dass sie als IT-Leistungsbezüger auch hier in der Verantwortung stehen. Allzu oft scheint noch das Gefühl zu herrschen, dass mit dem «Einkauf» von Leistungen auch gleich die gesamte Verantwortung delegiert wird. Das Thema Verantwortung – im grösseren Zusammenhang (IT-)Governance[3] – wird auf dem Radarschirm bleiben und bei der Beratungs- wie auch der Kontrolltätigkeit des Datenschutzbeauftragten auch in Zukunft beharrlich zur Sprache gebracht werden.

Zum Schluss

Danke! Unsere Aufgabe, darauf hinzuwirken, dass die Rechte der Personen, über die öffentliche Organe Daten bearbeiten, geachtet werden, könnten wir nicht erfolgreich erfüllen, wenn wir nicht die Unterstützung vieler Menschen und Institutionen bekämen. Mein Dank gilt deshalb:

— allen, die sich bewusst sind, dass sie selber dazu beitragen können, dass ihre Privatheit und die Privatheit der anderen Menschen, über die sie Informationen bearbeiten und weitergeben, geschützt bleibt;

— Privaten und Mitarbeiterinnen und Mitarbeitern der Behörden von Kanton und Gemeinden, die sich vertrauensvoll mit ihren Datenschutzfragen an uns wenden;

— allen Mitarbeiterinnen und Mitarbeitern der Verwaltung, der öffentlichrechtlichen Anstalten und der Gerichte, die auch dieses Jahr wieder mitgeholfen haben, datenschutzkonforme Lösungen zu finden und umzusetzen;

— den Kolleginnen und Kollegen der Ombudsstelle, der Finanzkontrolle und des Parlamentsdienstes für die unkomplizierte Kooperation;

— den Präsidien und Mitgliedern des Grossen Rates, des Büros des Grossen Rates, der Datenschutz-Delegation des Büros und der Geschäftsprüfungskommission des Grossen Rates für ihr Interesse an unserer Arbeit und ihre wertvolle Unterstützung;

— den juristischen Volontärinnen für ihre kritische Neugier und aktive Mitarbeit

— und last but not least meinem Team – Carmen Lindner, Sandra Husi, Daniela Waldmeier, Barbara Widmer und Markus Brönnimann –, das unsere Arbeit mit unermüdlichem Engagement, mit spannenden Diskussionen und konstruktiven Anregungen bereichert und vorangebracht hat.

Beat Rudin, Datenschutzbeauftragter

1 § 6 Abs. 1 IDG
2 § 7 Abs. 2 IDG
3 TB 2010, 19 ff.

Themen

Thema 1 Von A (Autorisierungen) bis Z (Zusammenarbeit)

Thema 2 Auf dem Sprung zum Öffentlichkeitsprinzip

Thema 3 Zugang zu den eigenen Personendaten

Thema 1

Von A (Autorisierungen) bis Z (Zusammenarbeit)

344 neue Geschäfte, 18 Autorisierungen von Online-Zugriffen, 12 durchgeführte Schulungen und 2 abgeschlossene Audits: das zeigt der Blick in die Geschäftskontrolle 2011 des Datenschutzbeauftragten. Auf den folgenden Seiten präsentieren wir einen kleinen Querschnitt der Datenschutzthemen, die aktuell die staatliche Verwaltung beschäftigen.

Vorabkontrolle

Ziel Vorabkontrollen sollen sicherstellen, dass sowohl datenschutzrechtliche Grundlagen wie auch die daraus abgeleiteten Anforderungen an die Informationssicherheit bereits in einem frühen Projektstadium berücksichtigt werden. Mit der Schengen-/Dublin-Revision des DSG im Jahr 2008[1] wurden die öffentlichen Organe verpflichtet, Bearbeitungen von Personendaten, die aufgrund der Art der Bearbeitung oder der zu bearbeitenden Daten geeignet sind, besondere Risiken für die Rechte und Freiheit der betroffenen Personen mit sich zu bringen, dem Datenschutzbeauftragten zur Vorabkontrolle vorzulegen. Gemeinsam mit den jeweiligen Amtsstellen soll ein konstruktiver Austausch über Chancen und Risiken neuer Projekte gepflegt und gestützt darauf eine unabhängige datenschutzrechtliche Beurteilung abgegeben werden. Das IDG übernimmt die Regelung in § 13.

Umfang und Durchführung Die IDV konkretisiert die «besonderen Risiken für die Rechte und Freiheit der betroffenen Personen»[2]. Sie sind gegeben bei Vorhaben zur Bearbeitung von Personendaten, welche a) ein Online-Abrufverfahren vorsehen; b) besondere Personendaten betreffen; c) den Einsatz einer neuen Technologie vorsehen oder d) eine grosse Anzahl Personen betreffen. Ferner kann auch ein Gesetz oder eine Verordnung die Vorabkontrolle vorsehen. Das Verfahren der Vorabkontrolle bestimmt sich im Wesentlichen nach dem konkret vorgelegten Projekt. In der Regel basiert die Beurteilung auf der Prüfung (bereits) vorhandener Dokumente[3] und auf Gesprächen mit den Verantwortlichen. Eine Vorabkontrolle kann zu unterschiedlichen Zeitpunkten, an sogenannten Meilensteinen, sowie je nach Projektverlauf einmalig oder in mehreren Schritten erfolgen[4]. Die Erfahrung hat gezeigt, dass der frühzeitige Beizug aller «Interessensgruppen» ebenso essentiell ist wie die Berücksichtigung der diversen (datenschutz)rechtlichen, Geschäfts-, Rechnungslegungs- und Informationssicherheits-Anforderungen.

Unterstützung bei Projekten

Projektbegleitung Keine Pflicht zur Vorabkontrolle besteht, wenn der Datenschutzbeauftragte bereits in der Projektorganisation eines Vorhabens mitwirkt[5]. Auch auf diese Weise können Datenschutzanliegen laufend und insbesondere frühzeitig eingebracht werden.

Wahrung der Unabhängigkeit Die Einbindung des Datenschutzbeauftragten muss so erfolgen, dass seine Unabhängigkeit gewahrt bleibt. Wird der Datenschutzbeauftragte zu stark in die Ausarbeitung eines Projekts involviert, hat er insbesondere bei Beschlüssen mitzuwirken, so kann er die Möglichkeit verlieren, nach Beendigung des Projekts die laufenden Datenbearbeitungen unvoreingenommen zu kontrollieren.

Beispiel IAM Derzeit ist der Datenschutzbeauftragte (u.a.) in der Begleitgruppe zum Projekt Identity & Access Management (IAM) aktiv vertreten. Das Projekt IAM greift ein zentrales Thema im Bereich der Informationssicherheit auf: Der Zugriff auf Informationen innerhalb der Verwaltung muss zuverlässig und nachvollziehbar gesteuert werden bzw. erfolgen. Mit der in diesem konkreten Projekt gewählten Vertretung in der Begleitgruppe (statt beispielsweise im Kernteam) wird die Unabhängigkeit gewahrt.

Datenschutz-Audits

Ziel Mit dem Datenschutz-Audit soll erreicht werden, dass die öffentlichen Organe des Kantons ihre Leistungen unter Berücksichtigung der datenschutzrechtlichen Vorgaben erbringen, d.h. unter Wahrung der Persönlichkeitsrechte der betroffenen Personen sowie unter Einhaltung der Vorgaben der Informationssicherheit. Gleichzeitig sind aber auch Überlegungen

der Effizienz und Praktikabilität zu berücksichtigen. Ein «Standard-Datenschutz-Audit» besteht daher aus zwei Bereichen und berücksichtigt die genannten Themenkreise jeweils im spezifischen Kontext:

— Im rechtlichen Teil des Audits wird geprüft, ob eine (unmittelbare oder mittelbare) gesetzliche Grundlage für die einzelnen Datenbearbeitungen besteht, ob die in den Normen enthaltenen rechtlichen Voraussetzungen eingehalten werden und ob die Datenbearbeitung verhältnismässig, d.h. für die Erfüllung des Bearbeitungszwecks geeignet und erforderlich sowie für die Betroffenen zumutbar ist.

— Im Informationssicherheits-Teil des Audits wird geprüft, ob angemessene organisatorische und technische Massnahmen ergriffen wurden, um die genutzten Personendaten vor unrechtmässiger Kenntnisnahme, mangelnder Richtigkeit und Vollständigkeit sowie vor unzureichender Verfügbarkeit zu bewahren[6]. Die Daten müssen ferner einer Person zugerechnet werden können und Veränderungen sowie Zugriffe der Informationen müssen nachvollziehbar sein[7]. Gleichzeitig muss die Balance zwischen Informationssicherheit und effektiver und effizienter Erfüllung der Aufgaben der öffentlichen Organe sichergestellt werden.

(IT-)Governance, Internes Kontrollsystem (IKS) und unternehmensweites Risikomanagement – diesen Themen kann sich die Basler Verwaltung nicht verschliessen.

Erfahrungen Der rechtliche Teil der Audits konnte grösstenteils ordnungsgemäss durchgeführt werden. Hingegen war im Informationssicherheitsteil festzustellen, dass die Anforderungen für einen erfolgreichen Audit offenbar zu hoch angesetzt waren und nicht erfüllt werden konnten[8]. Erstaunlich war dies insbesondere aufgrund des Umstandes, dass das aktuelle Standard-Prüf-Programm mehrheitlich Punkte umfasst, welche dem organisatorischen Bereich zuzuordnen sind. Der Datenschutzbeauftragte ist trotz Anpassungen beim Vorgehen davon überzeugt, dass das Prüfprogramm, das sich auf etablierte Standards abstützt, einem absoluten Minimum entspricht, damit die öffentlichen Organe die Verantwortung, die sie nach § 6 IDG und, wenn sie Informationen bearbeiten lassen, nach § 7 Abs. 2 IDG zu übernehmen haben, auch tatsächlich tragen können. Die Verantwortlichen bei den Organisationseinheiten, bei denen 2011 Audits durchgeführt oder begonnen werden konnten, haben erkannt, dass solche Kontrollen sie in ihrer Aufgabenerfüllung unterstützen.

Anpassung Die Erfahrungen zeigen, dass offensichtlich ein grösserer Handlungsbedarf im Bereich der Informationssicherheit besteht und ein Standard-Audit nicht sinnvoll durchgeführt werden kann. Der Datenschutzbeauftragte hat daher damit begonnen, den Audit auf die jeweilige Situation des öffentlichen Organs anzupassen. In einem ersten Schritt wird gemeinsam mit dem jeweiligen öffentlichen Organ eine Auslegeordnung erstellt und gestützt darauf die Durchführung des Audits individuell geplant. Wenn sich bereits hier herausstellt, dass grundlegende Fragen nicht geklärt sind (wie etwa die Verantwortlichkeit) oder elementare Dokumentationen nicht vorhanden sind, macht es keinen Sinn, mit einer vertieften Prüfung weiterzufahren.

Governance – ein Buch mit sieben Siegeln?

Aktuelle Diskussionen Begriffe wie (IT-)Governance, Internes Kontrollsystem (IKS) und unternehmensweites Risikomanagement prägen zur Zeit die Diskussionen auf den Chefetagen – nicht nur von privaten Unternehmen, sondern auch in öffentlichen Verwaltungen. Kann sich die Basler Verwaltung vor diesen Themen verschliessen?

Fragen aus der Praxis Der Datenschutzbeauftragte wurde im Jahr 2011 von Verantwortlichen aus der kantonalen und kommunalen Verwaltung mit zahlreichen ganz praktischen Fragen konfrontiert: «Rechtfertigt der Datenschutz die Sperrung der USB-Schnittstellen an PCs?», «Gibt es im Bereich Datenschutz eine Grundlage, um das erzwungene Sperren des Bildschirms zu rechtfertigen?», «Gibt es eine Einschränkung oder eine Rechtsgrundlage, dass bei einem Outsourcing die Daten in der Schweiz bleiben müssen?» oder «Gibt es eine gesetzliche Grundlage dafür, dass das Passwort mindestens sechs Zeichen, eine Zahl und ein Sonderzeichen enthalten muss?» In der Regel stellen sich Mitarbeiter(innen) technischer oder techniknaher Stellen diese Fragen, wenn sie mit der Umsetzung des Datenschutzrechts in den jeweiligen Bereichen betraut werden, manchmal sind es aber auch Anwender(innen), welche die diversen Massnahmen der Informationssicherheit als hinderlich für ihre Aufgabenerfüllung auffassen. >

Handlungsbedarf Diese und ähnliche Fragen können nicht allein gestützt auf das IDG beantwortet werden. Denn letztlich geht es um die Grundentscheidung, welche Risiken im Bereich der Informationssicherheit durch wen mit welchen Massnahmen ausgeschaltet und welches Restrisiko vom öffentlichen Organ bzw. seinen verantwortlichen Leitungsorganen getragen werden sollen. Dazu braucht es einen weiteren Rahmen, in welchem Zuständigkeiten, Verantwortlichkeiten, Organisation und Verfahren geregelt sind. Auch der Kanton Basel-Stadt kommt nicht darum herum, sich entsprechend auszurüsten[9]. Dabei ist zu berücksichtigen, dass sich das Umfeld dynamisch entwickelt. Die Durchdringung der Leistungserbringungsprozesse durch die Informatik und die zunehmende Vernetzung über die Organisationsgrenzen hinweg schaffen neue Abhängigkeiten und Risiken. Aufgrund der Abhängigkeit von den Systemen der Informations- und Kommunikationstechnologie (IKT-Systeme) steigen die qualitativen Anforderungen an Informatik-Leistungen. Gleichzeitig zwingt der Kostendruck zu Konsolidierungs-, Zentralisierungs- oder Outsourcing-Überlegungen. Von den Verantwortlichen werden weit reichende strategische Entscheidungen erwartet: Was gehört zu den Kernkompetenzen, was kann oder soll selbst oder durch Dritte gemacht werden und in welcher Qualität muss die Leistung zur Verfügung gestellt werden? Wie kann sichergestellt werden, dass die Informatik die öffentlichen Organe möglichst optimal unterstützt? Ohne Unterstützung durch Regelwerke (Frameworks) kann nicht mit ausreichender Zuverlässigkeit garantiert werden, dass die Anforderungen genügend berücksichtigt und die Entscheidungsprozesse möglichst strukturiert, nachvollziehbar und auf Fakten basierend erfolgen.

Frameworks Mittels Frameworks kann auf das Wissen und die Erfahrung einer Vielzahl von Experten zugegriffen werden. Gerade in Bezug auf das interdisziplinäre Umfeld, das wir im Bereich der Governance – also der «gesamtheitlichen» Führung – vorfinden, ist auch die Etablierung einer «einheitlichen Sprache» ein gewichtiges Argument für die Einführung eines (oder mehrerer aufeinander abgestimmter) Frameworks. Einige der etablierten Frameworks sind so ausgelegt, dass sie sich ergänzen. Zu den aktuell weitverbreiteten Vertretern gehören hier COBIT[10] (IT-Governance), ITIL[11] (IT-Service-Management) und Standards aus ISO/IEC 2700x[12] und vom BSI[13] (Informationssicherheit).

Festlegung und Umsetzung Der Einsatz von Frameworks erscheint ausserordentlich sinnvoll, wenn man nicht alles neu erfinden will. Es braucht aber eine Festlegung, welche Frameworks beigezogen werden sollen. Ausserdem geben sie nur einen Rahmen ab; jede Organisation (z.B. der Kanton Basel-Stadt) hat den Inhalt und die genaue «Auslegung» selbst zu erarbeiten und zu bestimmen – angepasst an seine Grösse, seine Organisation, den spezifischen Risiken, die Komplexität seiner Geschäftstätigkeit und der Informatik. Es gilt etwa, die «Risikobereitschaft» festzulegen – und dann auch politisch und rechtlich zu verantworten. Frameworks sind beileibe kein Wunderheilmittel, sie können aber einen wertvollen Beitrag dazu leisten, dass die Verwaltung ihre Aufgaben geordnet, zuverlässig, effizient und zielgerichtet erfüllen und die bestehenden Chancen und Risiken identifizieren und damit verantwortungsvoll umgehen kann. Der Handlungsbedarf dürfte erkannt sein; der Datenschutzbeauftragte ist bereit aktiv mitzuwirken.

Es geht um die Grundentscheidung, welche Risiken im Bereich der Informationssicherheit mit welchen Massnahmen ausgeschaltet sollen und welches Restrisiko getragen werden soll.

Autorisierung von Online-Zugriffen

Nach DSG Bis Ende 2011 hatte der Datenschutzbeauftragte Online-Zugriffe von öffentlichen Organen auf Datenbestände anderer öffentlicher Organe zu «autorisieren». 19 solcher Zugriffe (2010: 24) wurden in diesem Jahr bewilligt. Dabei hat sich gezeigt, dass die Dateneigner(innen), auf deren Daten zugegriffen werden soll, sorgfältiger als früher prüften, ob die gesetzlichen Voraussetzungen für den Online-Zugriff erfüllt sind. Früher wurde dieser Entscheid zum Teil faktisch an die Datenschutzkommission bzw. an den Datenschutzbeauftragten «delegiert», indem die Dateneigner(innen) ohne Prüfung der (manchmal nicht einmal angeführten) Rechtsgrundlagen ihr Einverständnis zur Einräumung der Online-Zugriffsmöglichkeit gegeben haben.

Nach IDG Das IDG kennt diese Online-Zugriffs-Autorisierung nicht mehr. Der Entscheid über die Datenbekanntgabe an ein anderes öffentliches Organ ist ganz normaler Inhalt der Verantwortung der Dateneigner(innen) nach § 7 IDG. Der Unterschied zur Einzelbekanntgabe liegt darin, dass mit der Einräumung der Online-Zugriffsmöglichkeit die Prüfung, ob die Bekanntgabe gesetz- und verhältnismässig ist, im konkreten Anwendungsfall nicht mehr möglich ist; das andere öffentliche Organ kann sich einfach «bedienen». Aus diesem Grund müssen die Dateneigner(innen), in deren Verantwortung der Entscheid bleibt, die generelle Öffnung für solche Dritte sorgfältig prüfen. Unterstützt werden sie darin durch den Datenschutzbeauftragten: Nach § 2 Abs. 1 lit. a IDV sind ihm beabsichtigte Online-Abrufverfahren zur Vorabkontrolle vorzulegen. Er nimmt damit Stellung zum Vorhaben – der Entscheid obliegt aber den Dateneigner(inne)n.

Umbau Ende 2011 wurde damit begonnen, das bisherige Autorisierungsverfahren in Zusammenarbeit mit den Zentralen Informatikdiensten (ZID) und der Fachstelle Informatik und Organisation (FIO) «umzubauen», damit es den neuen Anforderungen zu genügen vermag. Ebenfalls sollen neu vereinfachte Verfahren geschaffen werden für die Verlängerung bzw. Erweiterung von bestehenden Autorisierungen, soweit sie bereits mit dem seit Mitte 2009 verwendeten detaillierten Gesuchsformular begründet worden sind.

Videoüberwachung

Aufbruch Das Jahr 2011 war auch im Bereich der Videoüberwachung geprägt von der Übergangsphase von DSG zu IDG. 24 Anfragen zur Videoüberwachung beschäftigten den Datenschutzbeauftragten in diesem Jahr. Die Fragestellungen reichten von Anrufen aus der Bevölkerung zu privaten Anlagen[14] und Kameras von öffentlichen Organen über Fragestellungen öffentlicher Organe zum sinnvollen Einsatz von Videoüberwachungsanlagen bis hin zu Verlängerungsgesuchen für bestehende Anlagen. Der Datenschutzbeauftragte hat all diese Anfragen sowohl im Hinblick auf das noch geltende DSG wie auch auf die neue Rechtslage nach dem Inkrafttreten des IDG beantwortet.

Verlängerungen Videoüberwachungsanlagen, deren Betriebsbewilligung im Jahr 2011 auslief, wurden zwar wieder vom Datenschutzbeauftragten bewilligt, jedoch wurden die zuständigen Stellen angehalten, im Hinblick auf das Inkrafttreten des IDG ein Reglement für den Betrieb der Kameras auszuarbeiten, welches den Erfordernissen des § 18 IDG und insbesondere des § 5 IDV genügt, d.h. auch Bestimmungen zur Evaluation enthält. Diese Umstellung nahmen die Universität Basel und das Erziehungsdepartement zum Anlass, die diversen Videoüberwachungsanlagen in einem Reglement zusammenzufassen und einheitlichen Betriebsbestimmungen zu unterwerfen.

Der Datenschutzbeauftragte hat bei der «grossen Innenstadtüberwachung» vorgängig auf wichtige Fragen wie die Notwendigkeit einer wissenschaftlichen Begleitevaluation hingewiesen.

Zuständigkeit Ebenfalls thematisiert wurde die Zuständigkeit zur Kontrolle der Videoüberwachungsanlagen der Rheinhäfen sowie der Fachhochschule Nordwestschweiz. Zwar gründen beide Institutionen auf einem interkantonalen Vertrag, das anwendbare (Datenschutz-)Recht ist jedoch in beiden Fällen nur sehr rudimentär geregelt. Entsprechend problematisch gestaltet sich die Klärung der Frage, unter welches Recht und damit verbunden in wessen Zuständigkeitsbereich die Videoüberwachungskameras an den unterschiedlichen Standorten fallen. Die Datenschutzbeauftragten der betroffenen Kantone stehen in diesen Fragen in kontinuierlichem Austausch und sind um möglichst praktikable Lösungen bemüht.

Absage Mit 50 zu 41 Stimmen ist der Grosse Rat im Oktober 2011 auf den Ausgabenbericht zur «grossen Innenstadtüberwachung»[15] nicht eingetreten. Geplant war, die Achse Bahnhof SBB – Badischer Bahnhof mittels an strategisch günstigen Orten positionierter Kameras zu überwachen. Der Datenschutzbeauftragte hat sich seiner Aufgabe entsprechend nicht an der politischen Diskussion über die Wünschbarkeit einer solchen Installation beteiligt. Hingegen war er vorgängig von der Kantonspolizei und vom Vorsteher des Justiz- und Sicherheitsdepartements beigezogen worden und hatte auf wichtige Fragen rund um die Videoüberwachung hingewiesen[16].

Studien und Umfragen

Zunahme Gleich mehrfach tauchten im Jahr 2011 Fragestellungen zur Durchführung von Studien und Befragungen auf. Quartiervereine, Universitätsinstitute und Abteilungen der FHNW, aber auch Organe des Kantons Basel-Stadt wollten anhand konkreter Fragestellungen wissenschaftlich verwert- bzw. für das weitere Qualitätsmanagement nutzbare Informationen gewinnen. Die Durchführung solcher Studien wirft zahlreiche Fragen auf, welche von Fall zu Fall unterschiedlich beantwortet werden müssen. >

Gesetzliche Grundlage Das IDG hält in § 10 fest, dass Organe, welche Personendaten zur Erfüllung ihres jeweiligen gesetzlichen Auftrags bearbeiten (§ 9 IDG), diese Daten auch ohne Personenbezug nutzen dürfen. Ebenso regelt das IDG, dass Personendaten an andere öffentliche Organe oder Privatpersonen zum Zweck nicht personenbezogener Bearbeitung bekannt gegeben werden dürfen (§ 22). Die wenigsten Umfragen und Studien werden gestützt auf eine unmittelbare gesetzliche Grundlage durchgeführt, sondern basieren auf einer, zum Teil nur mit viel innovativer Auslegung auffindbaren, mittelbaren gesetzlichen Grundlage. Immerhin – für den grössten Datenbearbeiter in diesem Gebiet, für das Statistische Amt, wird an einer gesetzlichen Grundlage gearbeitet; der Datenschutzbeauftragte wurde in die Vorbereitungsarbeiten einbezogen. Allein, dass eine gesetzliche Grundlage das Erheben von Personendaten zu einem nicht personenbezogenen Zweck erlaubt, heisst noch lange nicht, dass die befragten Personen auch Auskunft geben müssen. Wenn nicht auch dafür ausdrücklich eine gesetzliche Grundlage besteht, ist die Teilnahme an einer Umfrage oder Studie grundsätzlich freiwillig.

Studien sind wenn immer möglich mit pseudonymisierten oder anonymisierten Daten durchzuführen, weil damit die Gefahr einer Persönlichkeitsverletzung vermieden oder erheblich reduziert wird.

Einwilligung Aufgrund der Freiwilligkeit der Teilnahme ist bei jeder Befragung zu klären, wer sein Einverständnis in die Partizipation wie geben muss: Bei mündigen Teilnehmer(inne)n ist dies weitaus weniger problematisch als bei Minderjährigen; es stellt sich vor allem die Frage nach dem «informed consent»: Wie viele Informationen über die Studie müssen den Befragten bekannt gegeben werden und von welcher Qualität müssen die Informationen sein, damit die Teilnehmer(innen) die Reichweite ihrer Einwilligung abschätzen können? Bei Minderjährigen, die befragt werden sollen, stellen sich weitere Fragen: Haben die Eltern einzuwilligen? Anstelle der Minderjährigen oder zusätzlich zu ihnen? Dabei spielt das Alter der zu Befragenden ebenso eine Rolle wie der Inhalt der Studie. Auch hier stellt sich die Frage nach Quantität und Qualität der (Eltern-)Information. In aller Regel hat die Einwilligung in Form eines Opt-in (ausdrückliche Einwilligung) zu erfolgen[17]. Ein Opt-out (Annahme einer Einwilligung, wenn die betroffene Person nicht ausdrücklich widerspricht) kann höchstens genügen, wenn es sich nicht um besondere Personendaten handelt und die Fragen keine heiklen Bereiche betreffen. Das hat vor allem Konsequenzen, wenn die Personen, die um ihre Einwilligung gebeten werden, nicht antworten: Bei einem Opt-in fehlt damit die notwendige Einwilligung, bei einem Opt-out würde damit eine stillschweigende Einwilligung angenommen.

Pseudonymisierung und Anonymisierung Umfragen und Studien sind wenn immer möglich mit pseudonymisierten oder anonymisierten Daten durchzuführen, weil damit die Gefahr einer Persönlichkeitsverletzung ganz vermieden oder doch erheblich reduziert wird. Pseudonymisierung bedeutet, dass Personendaten aufgrund eines Musters verschlüsselt werden und nur noch die daraus entstehende Nummer oder Buchstaben-Zahlen-Zeichen-Kombination genutzt wird. Eine Pseudonymisierung ist nicht definitiv, sondern kann, eben anhand des ursprünglich genutzten Schlüssels, wieder rückgängig gemacht werden. Bei einer Anonymisierung wird die Personenbeziehbarkeit definitiv beseitigt; auch hier werden die Daten verschlüsselt, allerdings wird der Schlüssel vernichtet, so dass eine Rückgängigmachung (d.h. eine Wiederherstellung der identifizierenden Angaben) verunmöglicht wird. Ob bereits von Anfang an auf Personendaten verzichtet und die Studie mit anonymisierten Informationen durchgeführt oder ob lediglich eine Pseudonymisierung vorgenommen werden kann, ist von der jeweiligen Studienplanung abhängig.

Fall-zu-Fall-Lösungen Jede Studie und Umfrage wirft aufgrund ihrer Ausrichtung diverse Variationen und Kombinationen dieser Fragestellungen auf. Der Datenschutzbeauftragte prüft daher die jeweiligen Studien-Konzepte, die ihm vorgängig vorgelegt werden, in enger Zusammenarbeit mit den durchführenden Stellen und wird auch weiterhin darum bemüht sein, gemeinsam mit den Projekt-Teams eine datenschutzkonforme Durchführung der Studien und Befragungen zu erreichen. Im Jahr 2011 wurde (u.a.) in Basler Schulen eine grössere Studie der Pädagogischen Hochschule (PH) der FHNW durchgeführt. Dabei wurde vorab weder eine datenschutzrechtliche noch eine ethische Beurteilung vorgenommen. Als sich eine von den Schilderungen ihrer 11jährigen Tochter aufgeschreckte Mutter an den Datenschutzbeauftragten wandte, wurde die Befragung unterbrochen. Gemeinsam mit der Datenschutzaufsicht des

Kantons Aargau wurde daraufhin eine Verbesserung verlangt. Die Projektleitung hat in der Folge auf zu heikle Fragestellungen verzichtet, die Elterninformationen deutlich verbessert und verlangt künftig ein Opt-in der Eltern.

Staatsschutzkontrolle

Verstärkung der Dienstaufsicht Mit der «Staatsschutzvollzugsverordnung» (VV-BWIS)[18] hat der Kanton Basel-Stadt die Dienstaufsicht über das Staatsschutzorgan (Fachgruppe 9 des Kriminalkommissariats, FG9) verstärkt. Insbesondere hat er dazu ein Kontrollorgan eingesetzt (Ständerätin Anita Fetz, Prof. Dr. Heinrich Koller, Prof. Dr. Markus Schefer), welches die Dienstaufsicht in allen Bereichen unterstützt, die in der Kompetenz des Kantons liegen[19]. Es überprüft insbesondere,

— ob die kantonalen Verwaltungsabläufe den massgebenden Rechtsvorschriften entsprechen;

— ob die Staatsschutzbehörde die datenschutzrechtlichen Anforderungen (Datensicherheit, Persönlichkeitsschutz) einhält und ob es die Daten zur Wahrung der inneren Sicherheit von den übrigen polizeilichen Informationen getrennt bearbeitet;

— wo und wie die Staatsschutzbehörde Informationen beschafft und

— wie die Staatsschutzbehörde die vom Bund erteilten Aufträge erledigt, wobei es sich dabei auf die Liste des Bundes stützt[20].

Überschneidungen Aus dieser Aufgabenumschreibung ergibt sich, dass sich ein Grossteil der Kontrolltätigkeit des Staatsschutzkontrollorgans auf Datenbearbeitungen bezieht. Damit überschneiden sich die Aufsichtsbereiche dieser Dienstaufsicht mit der Datenschutzaufsicht durch den Datenschutzbeauftragten. Wie ist damit umzugehen? Auch wenn die Dienstaufsicht – anders als die Datenschutzaufsicht – nicht unabhängig ist, ist die Kontrolle über das Staatsschutzorgan dank der Einsetzung des Kontrollorgans und der Wahl der drei Persönlichkeiten aus Politik und Wissenschaft doch erheblich «unabhängiger» als in den anderen Kantonen. Ausserdem verfügt das Kontrollorgan bisher über weitgehenden Zugang zu den beim Vollzug des BWIS anfallenden Informationen, während dies beim Datenschutzbeauftragten nicht der Fall ist – ein Streitpunkt, der zwischen den kantonalen Datenschutzbehörden und dem Bund noch nicht geklärt ist.

Abgrenzung Es wäre nicht zielführend, wenn Dienstaufsicht und Datenschutzaufsicht bezüglich des gleichen Sachverhalts zu unterschiedlichen datenschutzrechtlichen Beurteilungen kämen. Datenschutzbeauftragter und Staatsschutzkontrollorgan haben deshalb den folgenden «modus cooperandi»[21] vereinbart:

— Das Staatsschutzkontrollorgan beaufsichtigt die Tätigkeiten der FG9 und der Kantonspolizei im Staatsschutzbereich, sowohl jeweils innerhalb der beiden öffentlichen Organe als auch im Verkehr zwischen den beiden. Das betrifft auch datenschutzrechtliche Fragestellungen, wobei das Kontrollorgan bei solchen Fragestellungen (ausser in eindeutigen Fällen) den Datenschutzbeauftragten – unter Wahrung der für das Kontrollorgan geltenden Geheimhaltungspflicht – konsultiert.

— Der Datenschutzbeauftragte beaufsichtigt die Datenbearbeitungen aller anderen öffentlichen Organe, auch wenn sie Staatsschutzbelange betreffen (und natürlich die Datenbearbeitungen der Kantonspolizei ausserhalb des Staatsschutzbereichs). Stösst das Staatsschutzkontrollorgan bei der FG9 und/oder der Kantonspolizei auf Hinweise, die eine nähere Abklärung auf Seiten eines solchen anderen öffentlichen Organs nahe legen, teilt es dies – unter Wahrung der für das Kontrollorgan geltenden Geheimhaltungspflicht – dem Datenschutzbeauftragten mit, der dann über das weitere Vorgehen entscheidet. Stösst der Datenschutzbeauftragte seinerseits bei einem solchen öffentlichen Organ auf Hinweise, die eine Abklärung auf Seiten der FG9 und/oder der Kantonspolizei nahe legen, teilt er dies dem Kontrollorgan mit. Ausserdem konsultiert er das Kontrollorgan in staatsschutzrechtlichen Fragen im Zusammenhang mit seiner Tätigkeit.

Datenschutzbeauftragter und Staatsschutzkontrollorgan haben einen «modus cooperandi» vereinbart.

Zwischenfazit Mit diesem Kooperationsmodus kann die kantonale Aufsicht über die Staatsschutztätigkeiten der kantonalen öffentlichen Organe sichergestellt werden. Die im interkantonalen Vergleich wesentlich stärkere Dienstaufsicht und die gegenseitige Konsultation rechtfertigen unseres Erachtens vorläufig auch den Verzicht auf die eigene Kontrolltätigkeit des Datenschutzbeauftragten bei der FG9 und – im Staatsschutzbereich – bei der Kantonspolizei. Der regelmässige Erfahrungsaustausch zwischen Kontrollorgan und Datenschutzbeauftragtem stellt auch sicher, >

dass bei veränderter Ausgangslage die Kooperationsregelung angepasst werden kann. Beim Datenschutzbeauftragten ermöglicht die Aufgabenteilung, dass die begrenzten Kontrollkapazitäten nicht dort eingesetzt werden, wo eine anderweitige und – nach unserer Beurteilung – wirksame Kontrolle bereits stattfindet.

Outsourcing

Grundsätzliches Aus datenschutzrechtlicher Sicht ist es bedeutsam zwei Arten der «Auslagerung» zu unterscheiden:

— *Aufgabenübertragung:* Bei der ersten Variante bearbeitet die externe Drittperson Personendaten zur Erfüllung einer ihr, also der Externen, übertragenen öffentlichen Aufgabe, womit diese selbst zu einem öffentlichen Organ wird und den kantonalen Datenschutzbestimmungen untersteht[22]. Diese Variante verursacht bei der Umsetzung datenschutzrechtlicher Vorgaben keine besonderen Probleme, da sowohl die Datenbearbeitung als auch die Verantwortung für die Datenbearbeitung bei ein und derselben Stelle liegen: bei der Drittperson, der die Aufgabe übertragen wurde.

Lässt ein öffentliches Organ Informationen durch einen Dritten bearbeiten, bleibt es für die Einhaltung der kantonalen Datenschutzbestimmungen verantwortlich.

— *Datenbearbeitung im Auftrag:* Bei dieser zweiten Variante lässt ein öffentliches Organ eine externe Drittperson Personendaten bearbeiten, um seine, also des öffentlichen Organs eigene Aufgabe zu erfüllen. In diesem Fall handelt es sich datenschutzrechtlich aus Sicht der beauftragten Drittperson um ein Datenbearbeiten im Auftrag[23] bzw. aus Sicht des auftraggebenden öffentlichen Organs um ein Bearbeitenlassen von Personendaten. Hier bleibt das auftraggebende öffentliche Organ für die Einhaltung der kantonalen Datenschutzbestimmungen verantwortlich[24], obwohl es die «Sachherrschaft» über die gelieferten Daten verliert. Als Beispiele sind etwa die Zuweisung von Wohnungsnummern zu den Einwohner(inne)n im Vorfeld der Volkszählung 2010 durch die Post, die Wartung von produktiven IT-Systemen durch eine externe IT-Firma oder die Verlustscheinbewirtschaftung durch ein privates Inkassobüro zu nennen.

Voraussetzungen Ein öffentliches Organ darf das Bearbeiten von Personendaten Drittpersonen übertragen, wenn keine rechtliche Bestimmung oder keine vertragliche Vereinbarung der Übertragung entgegensteht und sichergestellt ist, dass die Daten nur so bearbeitet werden, wie es das öffentliche Organ selbst tun dürfte[25]. Mit anderen Worten: Das öffentliche Organ muss – etwa durch klare Regelung im Vertrag – dafür sorgen, dass die beauftragte Drittperson genau weiss, was sie tun muss und tun darf bzw. nicht tun darf. Ausserdem empfiehlt es sich, diese Regelung durch Androhung geeigneter Massnahmen im Zuwiderhandlungsfall zu verstärken, z.B. durch eine hohe Konventionalstrafe. Das öffentliche Organ hat jedes Interesse daran, diese Einbindung klar und verbindlich vorzunehmen, da es gegenüber einem geschädigten Dritten – etwa wenn Informationen widerrechtlich verwendet oder weitergegeben werden – haftbar ist. Das IDG sieht für die Zukunft vor, dass mit Busse bestraft wird, wer als beauftragte Drittperson ohne ausdrückliche Ermächtigung des auftraggebenden öffentlichen Organs vorsätzlich oder fahrlässig Personendaten für sich oder andere verwendet oder anderen bekannt gibt[26]. Einfacher und wirksamer, weil nicht nur Busse angedroht würde, wäre es, das Amtsgeheimnis auf die Drittperson zu übertragen[27]. Allerdings ist rechtlich nicht abschliessend geklärt, ob ein gesetzliches Geheimnis per Vertrag gültig übertragen werden kann.

Schengen

Schengen-Kontrolle Im Jahr 2011 konnte die 2010 begonnene, durch eine externe Revisionsgesellschaft durchgeführte Schengen-Kontrolle abgeschlossen werden. Es ist vorgesehen, im Jahr 2012 eine weitere Kontrolle vorzunehmen. Sandra Husi-Stämpfli vertritt auch weiterhin die Schweizer Kantone im Datenschutzaufsichtsorgan für Schengen (Joint Supervisory Authority, JSA). Die seit 2009 bestehende Koordinationsgruppe der schweizerischen Datenschutzbeauftragten tagt unter dem Vorsitz des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) ein- bis zweimal jährlich. Eine in allen Kantonen gleichzeitig durchgeführte und mit dem Bund koordinierte Kontrolle des Schengener Informationssystems (SIS) fand noch nicht statt.

Hotelmeldescheine Die JSA hat in einer Stellungnahme darauf hingewiesen, dass die in verschiedenen Schweizer Kantonen (und anderen Staaten) automatisch und damit verdachtsunabhängig vorgenommene Abgleichung von Hotelmeldescheinen mit dem Schengener Informationssystem (SIS) keine Rechtsgrundlage im Schengen-Durchführungsübereinkommen (SDÜ) findet. Die Kantonspolizei Basel-Stadt hat

auf Intervention des Datenschutzbeauftragten den Abgleich eingestellt. Die Frage, inwieweit ein automatischer Abgleich aller Hotelmeldescheine mit dem schweizerischen Fahndungsregister RIPOL zulässig ist, ist in Abklärung. Im Kanton Zürich soll eine spezifische Gesetzesgrundlage dafür geschaffen werden.

Durch die Mitarbeit in privatim kann der Datenschutzbeauftragte auch von den Arbeiten der anderen Datenschutzbehörden profitieren.

Zusammenarbeit

Vernetzung Neben der kantonsinternen Zusammenarbeit [28] arbeitet der Datenschutzbeauftragte auch weiterhin regelmässig mit den Datenschutzbehörden derjenigen Kantone zusammen, mit denen – beispielsweise durch die FHNW – Berührungspunkte bestehen, also v.a. mit Aargau, Basel-Landschaft und Solothurn. Auch die Zusammenarbeit mit dem Datenschutzbeauftragten des Kantons Zürich war unverändert intensiv, etwa im Bereich der Datenschutz-Audits. Der grösste Teil der interkantonalen Zusammenarbeit findet aber weiterhin im Rahmen von privatim, der Vereinigung der schweizerischen Datenschutzbeauftragten, statt. Durch die Mitarbeit im Büro von privatim und in den privatim-Arbeitsgruppen kann der Datenschutzbeauftragte auch von den Arbeiten der anderen Datenschutzbehörden profitieren. So wurden u.a. Themen im Bereich Swiss-DRG, elektronisches Patientendossier (ePatientendossier), eGovernment, Personenidentifikator im Zusammenhang mit eHealth und eGovernment wie auch Vernehmlassungen zu Bundesgesetzgebungsvorhaben im Rahmen der privatim-Kooperation behandelt.

—

1 Neuer § 18a DSG.
2 § 2 IDV.
3 § 4 IDV.
4 § 3 IDV.
5 § 2 Abs. 2 IDV.
6 § 8 Abs. 2 lit. a bis c IDG.
7 § 8 Abs. 2 lit. d und e IDG.
8 Vgl. TB 2010, 11 f.
9 Siehe TB 2010, 19 ff., insb. 20-22.
10 Control Objectives for Information and Related Technology von Information Systems Audit and Control Association (ISACA).
11 IT Infrastructure Library des Cabinet Office (Teil einer Regierungsbehörde Grossbritanniens).
12 Internationale Organisation für Normung.
13 Bundesamt für Sicherheit in der Informationstechnik (Deutschland).
14 Hier wurden den Anfragenden zwar allgemeine Fragen beantwortet; sie wurden aber für detailliertere Abklärungen an den Eidgenössischen Datenschutzbeauftragten verwiesen.
15 Ausgabenbericht 11.0637.01 vom 19. April 2011 betreffend Installation und Betrieb einer Videoüberwachungsanlage für die Kantonspolizei Basel-Stadt; Bericht 11.0637.02 der JSSK vom Bericht 11.0637.02 der Justiz-, Sicherheits- und Sportkommission vom 14. September 2011 zum Ausgabenbericht betreffend Installation und Betrieb einer Videoüberwachungsanlage für die Kantonspolizei Basel-Stadt sowie Bericht der Kommissionsminderheit;
16 Z.B. auf den Bedarf nach einer wissenschaftlichen Begleitevaluation, um herauszufinden, ob die Videoüberwachung die erwünschten Wirkungen oder unerwünschte Nebenwirkungen (wie etwa die blosse Verdrängung unerwünschter Aktivitäten in nicht überwachte Gebiete) zeitigt; vgl. dazu auf TB 2010,10.
17 Das Bundesdatenschutzgesetz lässt in seinem Geltungsbereich bei besonders schützenswerten Personendaten ausschliesslich eine ausdrückliche Einwilligung gelten.
18 Verordnung vom 21. September 2010 über den Vollzug des Bundesgesetzes zur Wahrung der inneren Sicherheit (VV-BWIS, SG 123.200).
19 § 10 Abs. 1 VV-BWIS.
20 § 10 Abs. 2 VV-BWIS.
21 Vgl. dazu auch Tätigkeitsbericht des Kontrollorgans über den Staatsschutz im Kanton Basel-Stadt 2011, 20 f.
22 § 2 Abs. 5 DSG bzw. § 3 Abs. 1 lit. IDG.
23 § 16 DSG bzw. § 7 IDG.
24 § 16 Abs. 1 DSG bzw. § 7 Abs. 2 IDG.
25 § 16 Abs. 1 DSG bzw. § 7 Abs. 1 IDG.
26 § 51 Abs. 1 IDG.
27 Was nach einer funktionalen Auslegung automatisch passieren soll, weil die Drittperson nun auch eine öffentliche Aufgabe erfüllt (Basler Kommentar StGB, 2. Aufl., Basel 2007, Niklaus Oberholzer, Art. 320 N 5).
28 Vgl. TB 2010, 12.

Thema 2

Auf dem Sprung zum Öffentlichkeitsprinzip

Im August 2011 hat der Regierungsrat die Informations- und Datenschutzverordnung (IDV) beschlossen. Damit stand auch fest, dass per 1. Januar 2012 das Informations- und Datenschutzgesetz (IDG) und die IDV in Kraft treten würden. Die Vorbereitungskurse zeigten auch schon, welche IDV-Bestimmungen in der Praxis schwierig umzusetzen sein dürften.

Übergang

Ende der DSG-Geltungszeit Mit dem Jahr 2011 endet auch die Geltungszeit des Datenschutzgesetzes von 1992. Was vor rund sechs Jahren mit dem Inkrafttreten der neuen Kantonsverfassung seinen Anfang genommen hat, die Verankerung des Öffentlichkeitsprinzips, beginnt anfangs 2012 zu wirken. Dabei folgt der Kanton Basel-Stadt der jüngeren Tradition kantonaler Rechtsetzung, indem er Öffentlichkeitsprinzip und Datenschutz im selben Gesetz regelt. Schliesslich geht es bei beiden Themen um den Zugang und Nichtzugang zu Informationen als zwei Seiten derselben Medaille.

Informations- und Datenschutzgesetz Im Februar 2009 hat der Regierungsrat dem Grossen Rat den Ratschlag und Entwurf zu einem neuen Informations- und Datenschutzgesetz (IDG) unterbreitet. Die Justiz-, Sicherheits- und Sportkommission des Grossen Rates (JSSK) hat die Vorlage intensiv behandelt und ihren Bericht im Frühjahr 2010 dem Plenum vorgelegt. Am 9. Juni 2010 hat der Grosse Rat das neue Gesetz einstimmig verabschiedet. Am 24. Juli 2010 lief die Referendumsfrist ungenutzt ab.

Informations- und Datenschutzverordnung Damit hätte das IDG bereits im Sommer 2010 in Kraft treten können. Es war allerdings klar, dass es dazu Ausführungsbestimmungen in Form einer Verordnung brauchte. Bereits ein Jahr zuvor hatte eine verwaltungsinterne Arbeitsgruppe mit den Vorarbeiten zur Informations- und Datenschutzverordnung (IDV) begonnen. Die Diskussionen verliefen – offensichtlich – sehr kontrovers. Dementsprechend zogen sich die Arbeiten lange dahin. Ein erster interner Vernehmlassungsentwurf fand im Herbst 2010 keine Gnade. Nach der Behandlung in einer Klausurtagung des Regierungsrates folgte eine längere Überarbeitungsphase. Zum Entwurf, der dem Regierungsrat vorgelegt wurde, nahm der Datenschutzbeauftragte nochmals Stellung. Erklärtes Ziel[1] war es, den Eindruck zu vermeiden, dass mittels der Verordnung versucht werde, den von der Verfassung vorgegebenen und im IDG umgesetzten Paradigmenwechsel vom Geheimhaltungsprinzip mit Öffentlichkeitsvorbehalt zum Öffentlichkeitsprinzip mit Geheimhaltungsvorbehalt abzuschwächen. Mit zwei Ausnahmen[2] wurden seine Vorschläge und Einwände vom Regierungsrat nicht berücksichtigt.

Stellungnahme des DSB zur IDV

Bearbeitenlassen von Personendaten § 1 IDV ist bloss noch ein Überbleibsel der entsprechenden Bestimmung im früheren Entwurf. Es wird nur noch festgehalten, dass ein Auftrag für das Bearbeiten von Personendaten durch Organisationseinheiten oder Private, die dem IDG nicht unterstehen, schriftlich erteilt werden muss, hingegen nicht mehr, was darin geregelt werden muss. Es wird auf anderem Weg, etwa durch die Ausarbeitung von kantonsweit geltenden AGB oder Musterverträgen für das Outsourcing, sicherzustellen sein, dass die zur Umsetzung von § 7 IDG notwendigen Regelungen tatsächlich getroffen werden.

Nichtpersonenbezogenes Bearbeiten In § 10 IDV (Bekanntgabe von Personendaten zu einem nicht personenbezogenen Zweck) wurde ein früherer Abs. 1 gestrichen; er hatte klar ausgedeutscht, wie der Regierungsrat die in § 22 IDG getroffene Regelung laut Ratschlag[3] verstanden hat: Nicht-anonymisierte und nicht-pseudonymisierte Personendaten darf ein öffentliches Organ zu einem nicht personenbezogenen Zweck an Dritte (andere öffentliche Organe oder Private) nur herausgeben, wenn der Zweck (Statistik, Planung, Wissenschaft, Forschung) mit anonymisierten oder pseudonymisierten Personendaten nicht

erreicht werden kann. Das ist etwa dann der Fall, wenn Daten aus verschiedenen Quellen zusammengeführt («gematcht») werden müssen. Die Bekanntgabe von Personendaten braucht als Eingriff in das verfassungsrechtliche Grundrecht auf Datenschutz[4] eine hinreichend bestimmte gesetzliche Grundlage und muss verhältnismässig sein[5]. Verhältnismässig ist eine Datenbekanntgabe, wenn (u.a.) der Zweck, zu dem die Daten bekannt gegeben werden, ohne die Personendaten nicht erreicht werden kann (Aspekt der Erforderlichkeit). Kann der Bearbeitungszweck auch mit anonymisierten oder pseudonymisierten Daten erreicht werden, dann ist die Bekanntgabe von nicht-anonymisierten und nicht-pseudonymisierten Personendaten gerade nicht erforderlich. Folglich ist eine solche Bekanntgabe nicht verhältnismässig und damit unzulässig. Verantwortlich für die Einhaltung ist das öffentliche Organ, das die Daten bekannt gibt. Um die Gefahr einer versehentlichen Rechtsverletzung («aus Nichtwissen») zu minimieren und das öffentliche Organ in seinem Entscheid, nur anonymisierte oder pseudonymisierte Personendaten herauszugeben, zu stärken, wäre es notwendig gewesen, Abs. 1 in der früheren Fassung («Kann der Bearbeitungszweck auch mit anonymisierten oder pseudonymisierten Daten erreicht werden, sind die Personendaten vor der Bekanntgabe zu anonymisieren oder zu pseudonymisieren») wieder aufzunehmen. Der Regierungsrat hat jedoch leider darauf verzichtet.

Sperrrecht Auch in § 14 IDV (Sperrrecht) wurde ein früherer Abs. 1 gestrichen; danach hätte ein öffentliches Organ der gesuchstellenden Person mitgeteilt, dass es die Sperrung vollzogen hat. Diese Pflicht ist zwar datenschutzrechtlich nicht zwingend, aber es erscheint wenig bürgerfreundlich, sie zu streichen. Wenn die antragstellende Person es verlangt, muss die Bestätigung ohnehin zugestellt werden. Eine standardisierte Mitteilung wäre bestimmt weniger aufwändig als die Beantwortung von Nachfragen, ob die beantragte Sperrung nun vollzogen sei. Ausserdem muss das öffentliche Organ den Vorgang ohnehin dokumentieren, um sich später gegen den allfälligen Vorwurf, eine Sperrung unrechtmässigerweise nicht vollzogen zu haben, wehren zu können.

Verzeichnis Nach dem bisher geltenden Datenschutzgesetz musste ein Register aller *Datensammlungen* erstellt werden. Der Regierungsrat hat diese Regelung in den IDG-Entwurf übernommen. Der Grosse Rat hat das Verzeichnis (§ 24 IDG) gegenüber dem regierungsrätlichen Entwurf reduziert: Es sind nicht mehr alle Datensammlungen zu melden, sondern nur noch die *Verfahren, in welchen Personendaten bearbeitet werden.* Damit ist – gerade auch im Vergleich zur Regelung von § 8 DSG – eine erheblich kleinere Zahl von Eintragungen absehbar. Das Verzeichnis dient zwei Zwecken:

— Die betroffenen Personen haben das Recht zu wissen, welche Datenbearbeitungen im Kanton erfolgen; dieses Wissen ist die notwendige Grundlage für die Wahrnehmung der Rechte der betroffenen Personen (§§ 26 f. IDG).

— Die Verantwortlichen aller Stufen sollen einen Überblick erhalten, über alle Verfahren, die in ihrem Verantwortungsbereich ablaufen. Nur so können sie ermessen, wofür sie die Verantwortung tragen, und angemessen handeln.

Der Entwurf sah vor, dass für jedes Verfahren die folgenden Angaben aufgenommen werden sollten: a) die Bezeichnung des Verfahrens, b) die Rechtsgrundlage für die Datenbearbeitung, c) das verantwortliche öffentliche Organ, d) der Zweck der Datenbearbeitung, e) andere am Verfahren beteiligte öffentliche Organe oder Private, f) die Herkunft der Daten, g) die regelmässigen Empfängerinnen und Empfänger der Daten (inkl. Angaben über einen allfälligen Online-Zugriff anderer öffentlicher Organe oder Privater), h) die erfassten Personengruppen, i) die Anzahl der erfassten Personen, j) die Angabe, ob besondere Personendaten bearbeitet werden und k) die Angabe, ob das Bearbeiten ganz oder teilweise an Dritte übertragen ist. Mit Ausnahme der letzten beiden Punkte sind dies dieselben Angaben, die bisher nach dem DSG erfasst wurden. Leider hat der Regierungsrat die Buchstaben e) bis k), welche gemeinsam mit der Fachstelle für Informatik und Organisation als Stabs- und Planungsstelle der Informatik-Konferenz Basel-Stadt vorgeschlagen wurde, gestrichen. Damit wird den verantwortlichen Stellen aller Stufen ein Instrument verweigert, das sie bei der Wahrnehmung ihrer Verantwortung unterstützt. Es ist wenig verständlich, wieso in der Verordnung zu einem Gesetz, welches das Öffentlichkeitsprinzip einführt, gerade diese Transparenz unterbunden werden soll – insbesondere wenn der Nutzen gross und der Aufwand gering wäre. Und der Aufwand wäre tatsächlich minim: >

— Die Angaben mussten entweder bereits bis anhin nach § 8 DSG gemeldet werden (am Verfahren beteiligte öffentliche Organe, regelmässige Empfänger[innen], Datenherkunft) oder
— die Angaben sind eine einmalig vorzunehmende knappe Beschreibung (erfasste Personengruppen[6]), oder
— sie verlangen bloss ein Kreuzchen (×) in einer Auswahl (Anzahl der erfassten Personen [in Kategorien], besondere Personendaten [ja/nein], Outsourcing [ja/nein]).

In vielen Gesprächen kam zum Ausdruck, dass die Klassifizierungsregelung von der Verwaltung als wenig hilfreich und kaum umsetzbar erachtet wird – unseres Erachtens zu Recht.

Klassifizierung Zur Regelung einer Klassifizierung (§§ 18-22 IDV) ist aus datenschutzrechtlicher Sicht anzumerken, dass diese zwar ein Hilfsmittel sein kann für die praktische Umsetzung im Alltag, dass sie aber die Interessenabwägung im konkreten Fall eines Zugangsgesuches, wie sie § 29 IDG vorsieht, nicht ersetzen kann. Eine Bestimmung, die dies klargestellt hätte («Wird gestützt auf § 25 IDG ein Gesuch um Zugang zu klassifizierten Informationen gestellt, hat das öffentliche Organ ungeachtet der Klassifizierung im konkreten Fall zu prüfen, ob der Zugang nach § 29 IDG ganz oder teilweise zu verweigern oder aufzuschieben ist»), wurde leider vom Regierungsrat nicht in die Verordnung aufgenommen. Sie hätte für gesuchstellende Personen wie auch für die öffentlichen Organe, die mit einem Zugangsgesuch konfrontiert sind, Rechtssicherheit geschaffen.

Vorbereitung auf das Öffentlichkeitsprinzip

Einführungskurse Gemeinsam mit der Staatskanzlei (Koordinationsstelle Öffentlichkeitsprinzip und Abteilung Kommunikation) wurden im November und Dezember 2011 sechs Kurse «Datenschutz und Öffentlichkeitsprinzip – kurz erklärt» durchgeführt. Sie richteten sich an Kadermitarbeitende aller Stufen sowie an Personen mit Projektleitungs-, Produkt- oder Prozessverantwortung, welche mit Informationen und Personendaten umzugehen haben. Rund 100 Personen wurden die Neuerungen vorgestellt, die das IDG mit sich bringt:
— Was bedeutet das neue Gesetz für die Verwaltung?
— Wie muss mit Daten und Informationen umgegangen werden, um den gesetzlichen Erfordernissen Rechnung zu tragen?
— Wo besteht Handlungsbedarf, damit aus den ersten Fällen nicht Fallen werden?

Schwerpunkte Logischerweise wurde das Gewicht in diesen Kursen mehr auf das Öffentlichkeitsprinzip gelegt als auf die mehr oder weniger gleich bleibenden Datenschutzbestimmungen. Immerhin konnte in diesem Bereich aber auf das im Vergleich zu früher grössere Gewicht der Verantwortung der datenbearbeitenden Stellen und auf das neue Instrument der Vorabkontrolle hingewiesen werden. Im Vordergrund standen aber der Zugang zu Informationen, die bei einem öffentlichen Organ vorhanden sind, sowie die zulässigen Einschränkungen. Dabei konnte den öffentlichen Organen eine ausführliche Checkliste abgegeben werden. In den Diskussionen zeigte sich der grosse Respekt vor der unbekannten Entwicklung.

Optimierungspotenzial

Klassifizierung Die IDV regelt – wie oben erwähnt – die Klassifizierung von Informationen. Schutzwürdige Informationen – ein neuer Begriff, den das IDG nicht verwendet – sollen nach dem Grad ihrer Schutzwürdigkeit als «geheim» oder «vertraulich» klassifiziert werden; nicht klassifizierte Informationen gelten demnach als nicht schutzwürdig. In den Vorbereitungskursen und in vielen Gesprächen kam zum Ausdruck, dass diese Regelung von der Verwaltung als wenig hilfreich und kaum umsetzbar erachtet werde – unseres Erachtens zu Recht:
— Wenn Informationen klassifiziert werden, heisst das nicht, dass sie nicht veröffentlicht oder zugänglich gemacht werden können; Swisslos-Entscheide sind beispielsweise nach der Umschreibung in der IDV[7] «vertraulich», werden aber weiterhin publiziert, weil die Unterstützung als Angelegenheit von allgemeinem Interesse[8] beurteilt wird.
— Wenn Informationen nicht klassifiziert werden, heisst das nicht, dass sie veröffentlicht oder zugänglich gemacht werden dürfen. Nur besondere Personendaten führen zur Klassifikation «vertraulich»[9], «gewöhnliche» Personendaten hingegen nicht. Das IDG sieht aber vor, dass bei einem überwiegenden privaten Geheimhaltungsinteresse der Zugang zu verweigern ist[10], und selbst wenn das private Geheimhaltungsinteresse nicht überwiegt, müssen Personendaten vor der Zugangsgewährung anonymisiert werden[11].
— Eine Klassifizierung ersetzt – wie oben bereits erwähnt – in keinem Fall die Interessenabwägung, die nach § 29 IDG vorzunehmen ist, wenn der Zugang eingeschränkt werden soll. Eine Interessenabwägung muss immer im Einzelfall stattfinden – eine Klassifizierung ist höchstens ein Hinweis darauf, dass hier Geheimhaltungsinteressen bestehen können.

— Die Umschreibung der Inhalte, die zu einer Klassifizierung führen, sind mit den Vorgaben von § 29 IDG nicht deckungsgleich; sie bilden sie nicht vollständig ab und ergänzen sie zum Teil um nicht vorgesehene Sachverhalte.
— Wesentliche Fragen zum Umgang mit klassifizierten Informationen werden nicht beantwortet. Während im Bund [12] ausführlich geregelt wird, wie mit solchen Informationen umzugehen ist, hat die IDV gerade eine einzige Bestimmung daraus übernommen, die für sich allein nichts anderes sagt, als was nach den allgemeinen Regeln für den Umgang mit Informationen ohnehin schon gilt: «Klassifizierte Informationen dürfen nur jenen Personen bekannt gegeben werden oder zugänglich gemacht werden, die davon Kenntnis haben müssen» [13].

Anpassungsbedarf Nachdem in den gemeinsam mit der Staatskanzlei durchgeführten Vorbereitungskursen festgestellt worden ist, dass die bestehende Klassifizierungsregelung kaum umsetzbar ist, ist davon auszugehen, dass über kurz oder lang eine Anpassung der Verordnung vorgenommen wird. Eine entsprechende Regelung macht wohl Sinn für Regierungsgeschäfte; dafür wurde sie ja von der Staatskanzlei ursprünglich auch vorgeschlagen und dafür haben auch andere Gemeinwesen wie etwa die Stadt Zürich praktisch umsetzbare Regelungen.

Der Anspruch der Bürger(innen) auf Informationen soll nicht als Störung angesehen werden, sondern als willkommene Gelegenheit, auszuweisen, was die Verwaltung mit den Steuergeldern anfängt.

Paradigmenwechsel Mit dem Wirksamwerden des IDG wird ein Paradigmenwechsel angestrebt. Dieser wird nicht stattfinden, nur weil das Gesetz in Kraft tritt. Der Paradigmenwechsel muss in den Köpfen stattfinden, indem der Anspruch der Bürgerinnen und Bürger auf Informationen nicht als Störung angesehen wird, sondern als willkommene Gelegenheit, auszuweisen, was die Verwaltung mit den Steuergeldern anfängt. Es darf auf keinen Fall der Eindruck entstehen, die Verwaltung drücke sich um die Umsetzung des Öffentlichkeitsprinzips. Mit dem IDG ist dafür gesorgt worden, dass berechtigte Geheimhaltungsinteressen angemessen berücksichtigt werden können – die Handlungsfähigkeit der Regierung wird keineswegs beeinträchtigt, die Verwaltung in keiner Weise lahmgelegt. Entsprechende Ängste sind – mit Blick auf die Erfahrungen, welche die Kantone Bern (1995), Solothurn (2003), Aargau und Zürich (2008) sowie der Bund (2006) bei der Einführung des Öffentlichkeitsprinzips gemacht haben – unberechtigt; es gibt keine Anhaltspunkte dafür, dass das in Basel-Stadt anders sein sollte.

Sichtbarkeit Wenn die ersten Erfahrungen die Ängste vertrieben haben, dann kann sich auch dort die Haltung der Verwaltung gegenüber Gesuchstellenden entspannen, wo heute noch Befürchtungen bestehen. Die Art, wie Amtsstellen und Departemente mit Zugangsgesuchen umgehen, wird künftig auch ein Teil des Bildes sein, das die Verwaltung in der Öffentlichkeit abgibt. Die Information über das Öffentlichkeitsprinzip muss dann nicht mehr auf der Website des Kantons verborgen werden, sondern kann «entgegenkommender» platziert werden wie etwa im Kanton Zürich, wo bereits auf der Startseite der direkte Link «Öffentlichkeitsprinzip» angebracht ist …

Unterstützung Gleiches gilt bei der Behandlung von Personen, die ein nicht perfektes Gesuch stellen: Dabei geht es nicht darum, «fishing for information» zu ermöglichen, sondern um die Reduktion des Verwaltungsaufwandes und um das Bild, das die Verwaltung der Öffentlichkeit von sich vermittelt. Es ist sicher weniger aufwändig, das Gespräch mit einer gesuchstellenden Person zu suchen, um mit ihr zu klären, welche Information sie erhalten will, oder ihr aufzuzeigen, welche Informationen sie rasch und ohne Kosten erhalten kann, als das (u.U. mehrfache) Nichteintreten auf Gesuche, in denen auf den ersten Blick die erwünschte Information nicht hinreichend genau bezeichnet ist [14]. Wenn Bürgernähe das Ziel ist, dann wird dies sicher mit freundlicher Unterstützung besser erreicht als mit formalistischem Nichteintreten [15].

Open Government Data Ist die Einführung des Öffentlichkeitsprinzips das Ende einer langjährigen Entwicklung hin zu mehr Transparenz und Rechtssicherheit? Nein. Open Government Data (OGD) heisst eine Entwicklung, die insbesondere im angelsächsischen Raum, aber auch in Schweden, Deutschland und Österreich stattfindet. Das Thema ist inzwischen auch in der Schweiz angekommen. Mit OGD soll der Umgang mit Daten, die von staatlicher Seite generiert werden, vereinfacht werden. Insbesondere die Prinzipien der Maschinenlesbarkeit und der Kostenlosigkeit gehen über das hinaus, was zur Umsetzung des Öffentlichkeitsprinzips bereits geregelt ist. Der Grosse Rat hat im November 2011 einen wichtigen Entscheid dazu bei der Behandlung der kantonalen Geoinformationsgesetzes gefällt [16]: >

Die Nutzung von Geoinformationen soll gebührenfrei erfolgen können. Gemeinsam mit der Staatskanzlei hat der Datenschutzbeauftragte eine Tagung zum Thema «Öffentliche Informationen und offene Daten – wie viel Transparenz dank Öffentlichkeitsprinzip und Open Government Data» vorbereitet.

Bestimmte Bereiche staatlichen Handelns werden transparenter und damit kontrollierbarer werden – genau das hat der Verfassungsgeber gewollt.

Fazit und Ausblick

Positive Grundhaltung Aus den Vorbereitungskursen lässt sich das folgende Fazit ziehen: Die betroffenen Mitarbeiter(innen) der Verwaltung schauen der Einführung des Öffentlichkeitsprinzips mit positiver Erwartungshaltung entgegen, wenn auch da und dort die Ungewissheit über Zahl der Gesuche unsicher macht. Offenbar hat die Auseinandersetzung mit den konkreten Fragen etwas bewirkt: Die übertriebenen Ängste, die zum Teil bei der Vorbereitung der IDV zum Ausdruck kamen, waren bei den Teilnehmer(inne)n der Kurse nicht mehr vorhanden. Kritisch standen diese vielmehr den Klassifizierungsvorschriften gegenüber, die wohl gut gemeint sind, aber mit der Ausdehnung über die Regierungsgeschäfte hinaus auf alle Informationen in der Verwaltung kaum sinnvoll und mit vernünftigem Aufwand-/Ertrags-Verhältnis umsetzbar sind.

Ausblick Es ist davon auszugehen, dass die nähere Zukunft auch die letzten Befürchtungen beseitigen wird, der Kanton Basel-Stadt werde durch das Öffentlichkeitsprinzip lahm gelegt. Auf der anderen Seite wird seine Einführung aber sicher gewisse Veränderungen bringen: Bestimmte Bereiche staatlichen Handelns werden transparenter und damit kontrollierbarer werden – genau das hat der Verfassungsgeber gewollt.

—

1 Schreiben vom 19. April 2011 an alle Mitglieder des Regierungsrates, Vorbemerkung.
2 Streichung eines Abs. 2 in § 16 IDV, wonach für die öffentlichen Spitäler das Gesundheitsdepartement zu regeln hätte, wie die Transparenz herzustellen sei (anstelle der «normalen» Aufnahme der Verfahren, bei denen Personendaten bearbeitet werden, ins Verzeichnis nach § 24 IDG), und Wiederaufnahme des § 24 Abs. 2 IDV (Einschränkung zum Schutz des Kollegialitätsprinzips nicht nur für die kantonale, sondern auch für die kommunale Exekutive).
3 Ratschlag 08.0637.01, 39.
4 Recht auf informationelle Selbstbestimmung nach Art. 13 Abs. 2 BV, § 11 lit. j KV.
5 Art. 36 BV, § 15 KV.
6 Z.B. «alle Gesuchsteller(innen)», «in den letzten zwei Jahren in polizeilichen Rapporten erfasste Personen (Anzeiger, Beschuldigte, Geschädigte, Zeugen)», «aktuelle und ehemalige Mitarbeiter[innen]».
7 § 20 Abs. 1 lit. e IDV: «finanzielle Beiträge an Private (...), auf die kein Rechtsanspruch besteht».
8 § 20 Abs. 1 IDG.
9 § 20 Abs. 1 lit. d IDV.
10 § 29 Abs. 1 und Abs. 3 lit. a IDG.
11 § 30 Abs. 1 IDG.
12 Verordnung vom 4. Juli 2007 über den Schutz von Informationen des Bundes (Informationsschutzverordnung, ISchV), SR 510.411.
13 § 22 IDV.
14 § 31 Abs. 1 IDG.
15 Eine entsprechende Bestimmung («Das öffentliche Organ unterstützt Personen, die ein Gesuch um Zugang zu Informationen stellen wollen, im Hinblick darauf, die gewünschten Informationen hinreichend genau zu bestimmen») wurde leider nicht in die IDV aufgenommen.
16 Bericht 11.0028.2 der BRK vom 28. September 2011 zum Ratschlag 11.0028.1, Ziffer 3.b (Gebührenfreiheit der Nutzung von Geodaten, § 16 KGeoIG); Grossratsbeschluss vom 16. November 2011, Protokoll S. 953 ff.

Thema 3

Zugang zu den eigenen Personendaten

Zu wissen, ob die öffentliche Verwaltung über einen Daten bearbeitet und, wenn ja, welche, das gehört zu den grundlegenden Rechten der Bürgerinnen und Bürger. Deshalb hält die Basler Verfassung dies auch ausdrücklich fest. Was heisst das für die öffentlichen Organe? Wie haben sie mit Gesuchen um Zugang zu den eigenen Personendaten umzugehen?

Allgemeines

Kantonsverfassung Die neue Kantonsverfassung zählt die Grundrechte der Bürgerinnen und Bürger auf[1]. Namentlich garantiert ist «der Schutz personenbezogener Daten sowie des Rechts auf Einsichtnahme und auf Berichtigung falscher Daten»[2]. Das entspricht weitestgehend dem im bisher geltenden Datenschutzgesetz vorgesehenen Recht auf Auskunft und Einsicht. Das neue Informations- und Datenschutzgesetz nennt dies das Recht auf Zugang zu den eigenen Personendaten.

Abgrenzungen Vorweg müssen drei Informationszugangsrechte voneinander unterschieden werden:

— Der allgemeine Anspruch auf *Zugang zu Informationen*[3] ergibt sich aus dem *Öffentlichkeitsprinzip* und stützt sich demgemäss auf § 75 KV. Dieses Prinzip hat zum Ziel, das Handeln der öffentlichen Organe transparent zu gestalten, das staatliche Handeln nachvollziehbar und kontrollierbar zu machen, die freie Meinungsbildung und die Wahrnehmung der demokratischen Rechte zu fördern und damit das Vertrauen der Öffentlichkeit in die Verwaltung zu stärken[4].

— Der datenschutzrechtliche Anspruch auf *Zugang zu den eigenen Personendaten*[5] leitet sich aus dem verfassungsrechtlichen Persönlichkeitsrecht[6] ab. Er soll den Schutz der betroffenen Person in ihren Persönlichkeitsrechten gewährleisten und umfasst den Zugang zu allen Informationen über die gesuchstellende Person. Der Anspruch auf Zugang zu den eigenen Personendaten entspricht dem bisherigen datenschutzrechtlichen Recht auf Auskunft und Einsicht[7].

— Das verfahrensrechtliche *Recht auf Akteneinsicht*[8] leitet sich aus dem verfassungsrechtlichen Anspruch auf rechtliches Gehör ab[9]. Es dient in Verfahren (oder im Hinblick auf Verfahren) der Sachgerechtigkeit der behördlichen Entscheidung und will dem Verfahren durch die Mitwirkungsmöglichkeit der Betroffenen eine höhere Legitimation verschaffen.

Anspruch auf Zugang zu den eigenen Personendaten

Gegenstand Der Anspruch nach § 26 IDG bezieht sich auf die Personendaten, die ein öffentliches Organ über eine Person bearbeitet. Er umfasst zuerst einmal den Anspruch zu wissen, *ob* über die gesuchstellende Person Daten bearbeitet werden, und wenn ja, *welche.*

Berechtigte Das Recht auf Zugang zu ihren eigenen Daten steht jeder Person zu, unabhängig von Alter, Wohnsitz, Nationalität oder anderen Eigenschaften. Die Person, die ein Gesuch auf Zugang zu den eigenen Personendaten stellt, muss sich über ihre Identität ausweisen, ausser wenn ihre Identität für das ersuchte öffentliche Organ zweifelsfrei feststeht[10] – etwa wenn ein Sozialhilfeklient bei seiner Sozialarbeiterin, die ihn seit Jahren betreut, mündlich Zugang verlangt. Das öffentliche Organ nimmt eine Kopie des Identitätsnachweises zu den Akten[11], um sich allenfalls später gegen den Vorwurf wehren zu können, einer anderen als der berechtigten Person Zugang gewährt zu haben.

Verpflichtete Verpflichtet zur Zugangsgewährung ist jedes öffentliche Organ. Anders als beim allgemeinen Zugang zu Informationen nach dem Öffentlichkeitsprinzip[12] fallen hier auch die Privaten darunter, die zum öffentlichen Organ geworden sind, weil ihnen von Kanton oder Gemeinden die Erfüllung öffentlicher Aufgaben übertragen ist.

Voraussetzungen Der Anspruch besteht voraussetzungslos. Es müssen keine Gründe angeführt werden, warum eine Person von diesem Zugangsrecht Gebrauch machen will. Insbesondere ist der Anspruch nicht an den Nachweis eines Interesses gebunden. >

Form Grundsätzlich hat die gesuchstellende Person die Möglichkeit, ihr Begehren mündlich oder schriftlich zu stellen [13]. Auch auf elektronischem Weg kann ein Zugangsgesuch gestellt werden, sofern die gesuchstellende Person identifiziert werden kann.

Einschränkungen

Grundsatz Der Zugang zu den eigenen Personendaten darf – wie schon unter der Geltung des DSG [14] – nur unter bestimmten Voraussetzungen eingeschränkt werden. Das öffentliche Organ hat den Zugang zu Informationen – auch zu den eigenen Personendaten – im Einzelfall ganz oder teilweise zu verweigern oder aufzuschieben, wenn eine besondere gesetzliche Geheimhaltungspflicht oder ein überwiegendes öffentliches oder privates Interesse entgegensteht [15].

Besondere gesetzliche Geheimhaltungspflicht Eine Geheimhaltungspflicht, die den Zugang der gesuchstellenden Person zu ihren eigenen Personendaten untersagt, gibt es im kantonalen Recht nicht [16].

Überwiegendes öffentliches Interesse Hingegen sind überwiegende öffentliche Interessen denkbar, die eine Einschränkung rechtfertigen können: Der Zugang zur Information, dass polizeiliche Ermittlungen laufen oder wann bei einem Restaurationsbetrieb eine lebensmittelpolizeiliche Kontrolle durchgeführt werden soll, könnte etwa die zielkonforme Durchführung konkreter behördlicher, insbesondere polizeilicher Massnahmen beeinträchtigen [17].

Überwiegendes privates Interesse Auch private Geheimhaltungsinteressen können gegenüber dem Zugangsinteresse überwiegen. Denkbar ist dies beispielsweise in folgenden Fällen:

— Bei sog. «gemischten Dossiers», in welchen Personendaten über verschiedene Personen gemeinsam bearbeitet werden, sind die Daten sorgfältig den einzelnen Personen zuzuordnen; der Zugang zu fremden Daten ist z.B. durch Abdecken oder Schwärzen auszuschliessen.

— Die Aussage einer Person über eine andere Person sagt über beide Personen etwas aus: über die Informantin wie auch die über von der Aussage direkt betroffene Person. Hier sind das Zugangsinteresse der gesuchstellenden (betroffenen) Person und das Geheimhaltungsinteresse der anderen Person (Informantin) sorgfältig gegeneinander abzuwägen. Wenn im konkreten Fall Anhaltspunkte dafür bestehen, dass der Informantin rechtswidrige Beeinträchtigungen durch die betroffene Person drohen, kann die Geheimhaltung gerechtfertigt sein. Denkbar sind solche Beeinträchtigungen insbesondere dann, wenn die betroffene Person schon zu einem früheren Zeitpunkt gegen die Informantin (oder andere Informanten) rechtswidrig vorgegangen ist oder wenn der Informant in einem Abhängigkeitsverhältnis zur betroffenen Person steht und anzunehmen ist, dass diese ihre Machtstellung rechtsmissbräuchlich ausnützen würde. Umgekehrt ist ein überwiegendes Interesse bei Gefahr blosser Unannehmlichkeiten zu verneinen.

Der Zugang zu den eigenen Personendaten darf – wie schon unter der Geltung des Datenschutzgesetzes – nur unter bestimmten Voraussetzungen eingeschränkt werden.

Spezialfall Offenbarungsschaden Der Zugang zu den eigenen Personendaten kann ausserdem eingeschränkt werden, wenn der betroffenen Person durch die Zugangsgewährung offensichtlich ein schwerer Nachteil droht (sog. Offenbarungsschaden) [18]. Würde also der Zugang zu den eigenen Personendaten im medizinischen oder psychiatrischen Bereich nach der Beurteilung des öffentlichen Organs die betroffene Person zu stark belasten, kann der Zugang einer Person ihres Vertrauens (z.B. Hausarzt) gewährt werden. Sofern die betroffene Person es indes ausdrücklich wünscht, ist ihr direkt und umfassend Zugang zu ihren Personendaten zu gewähren.

Zugangsgewährung

Gewährung des Zugangs zu den eigenen Personendaten Das öffentliche Organ gewährt den Zugang zu den eigenen Personendaten [19], indem es

— die Information schriftlich, in Form von Kopien oder auf Datenträgern aushändigt oder

— mit dem Einverständnis der gesuchstellenden Person die Information mündlich mitteilt oder

— vor Ort Einsicht in die Akten gewährt.

Ist das Zugangsgesuch mündlich gestellt worden, kann das öffentliche Organ auf jeden Fall – d.h. auch ohne das Einverständnis der gesuchstellenden Person – die Information mündlich mitteilen [20].

Verständlichkeit Die Auskunft muss so erteilt werden, dass sie allgemein verständlich ist. Das klingt selbstverständlich – es gab früher beispielsweise eine Einwohnerkontrollsoftware, in welcher im Feld «Kinder» der Eintrag «$^3/_2$» stehen konnte. Nun hat niemand drei halbe Kinder. Damit der Eintrag verständlich war, musste die Erklärung mitgeliefert werden: Anzahl Kinder / davon weiblich ...

Verfahren und Kosten

Verfahren Das Verfahren auf Zugang zu Informationen beginnt damit, dass eine Person bei einem öffentlichen Organ schriftlich oder mündlich ein Gesuch auf Zugang zu den eigenen Personendaten stellt[21]. Das öffentliche Organ prüft das Gesuch. Wird bei der Prüfung klar, dass aufgrund überwiegender privater oder öffentlicher Interessen der Zugang eingeschränkt werden muss, wird der gesuchstellenden Person mitgeteilt, dass eine Einschränkung des Zugangsgesuchs in Betracht gezogen wird. Diese Mitteilung sollte kurz begründet werden und mit dem Hinweis versehen sein, dass die gesuchstellende Person innert 30 Tagen nach Eingang der Mitteilung vom öffentlichen Organ verlangen kann, dass es eine anfechtbare Verfügung erlässt[22]. Die gesuchstellende Person kann die Einschränkung akzeptieren oder, wenn sie den Rechtsweg beschreiten will, den Erlass einer Verfügung verlangen. Das öffentliche Organ kann, wenn beispielsweise aufgrund der Vorgeschichte klar abzusehen ist, dass eine Einschränkung nicht akzeptiert wird, auch direkt eine Verfügung erlassen.

Das Recht auf Zugang zu den eigenen Daten gehört zum Kerngehalt des Grundrechts auf informationelle Selbstbestimmung und darf nicht durch eine Gebührenpflicht ausgehöhlt werden.

Kosten Nach IDG[23] darf für die Bearbeitung von Gesuchen, welche die eigenen Personendaten betreffen, keine Gebühr erhoben werden. Damit unterscheidet sich die neue Regelung von derjenigen bisherigen im DSG: Die Einsichtnahme in die eigenen Personendaten war nach DSG kostenlos für behördliches Handeln von geringem Umfang. Kostenlos waren die Einsichtgewährung in die eigenen Daten und kurze mündliche Auskünfte. Das heisst auf der andern Seite, dass nach DSG die schriftlich erteilte Auskunft und die «lange» mündliche Auskunft grundsätzlich kostenpflichtig waren. Das IDG verfolgt also einen neuen Ansatz, der bei der Gewährung von Zugang zu den eigenen Personendaten – unabhängig vom Aufwand – Kostenlosigkeit vorsieht. Diesem Ansatz liegt der Gedanke zugrunde, dass das Recht auf Zugang zu den eigenen Daten zum Kerngehalt des Grundrechts auf informationelle Selbstbestimmung gehört und nicht durch eine Gebührenpflicht ausgehöhlt werden darf.

Tipps Der Datenschutzbeauftragte rät aufgrund der Erfahrung aus mehreren konkreten Fällen, vor der Einsichtgewährung ein Aktenverzeichnis zu erstellen und dieses der einsichtnehmenden Person zur Unterschrift vorzulegen. Auf diese Weise kann später allenfalls dem Vorwurf begegnet werden, nicht alle Dokumente zur Einsicht vorgelegt (oder begründet nicht vorgelegt) zu haben.

—

1 § 11 KV.
2 § 11 Abs. 1 lit. j KV.
3 § 25 IDG.
4 Vgl. § 1 Abs. 1 lit. a IDG.
5 § 26 IDG.
6 Art. 13 BV und § 11 Abs. 1 lit. j KV.
7 § 19 DSG.
8 § 38 Abs. 2 OG.
9 Art. 29 Abs. 2 BV und § 12 Abs. 1 lit. b KV.
10 § 31 Abs. 2 IDG.
11 § 25 IDV.
12 § 25 Abs. 1 IDG.
13 § 31 Abs. 1 IDG.
14 § 20 Abs. 1 DSG.
15 § 29 Abs. 1 IDG.
16 Im Bundesrecht gibt es hingegen Art. 18 Abs. 1 BWIS (sog. «indirekte Auskunftsrecht»): «Der Datenschutz- und Öffentlichkeitsbeauftragte teilt der gesuchstellenden Person in einer stets gleichlautenden Antwort mit, dass in Bezug auf sie entweder keine Daten unrechtmässig bearbeitet würden oder dass er bei Vorhandensein allfälliger Fehler in der Datenbearbeitung eine Empfehlung zu deren Behebung an den NDB gerichtet habe» – was allerdings eher als direktes Nicht-Auskunftsrecht bezeichnet werden müsste.
17 Vgl. dazu auch Fall 7 (hinten Seite 32).
18 § 29 Abs. 4 IDG.
19 § 34 IDG.
20 § 34 Abs. 2 IDG.
21 § 31 Abs. 1 IDG.
22 § 33 IDG.
23 § 36 Abs. 2 IDG.

Fälle

Fall 1 Verlustscheinbewirtschaftung durch eine private Inkassofirma

Fall 2 Online-Zugriff auf Einwohnerdaten für einen Krankenversicherer?

Fall 3 Das flüchtige «Nach-Alkohol-riechen» im Polizeirapport

Fall 4 Eine «Generaleinwilligung für alle Fälle» bei der Sozialhilfe

Fall 5 Die elterlichen Einkommens- und Vermögensverhältnisse

Fall 6 Das «psychische Leiden» im Bericht des Vertrauensarztes

Fall 7 Vielsagend nicht sagen, was man nicht sagen darf

Fall 8 Die Schweigepflicht des Personals eines Vertragspartners eines Vertragspartners

Fall 1 Verlustscheinbewirtschaftung durch eine private Inkassofirma

Aus Effizienzgründen hat ein öffentliches Organ die Bewirtschaftung ihrer Verlustscheine einer privaten Inkassofirma überlassen. Ein betroffener Schuldner stösst sich an dieser Praxis und möchte wissen, ob die Weitergabe seiner Daten ohne sein Wissen und ohne seine Erlaubnis rechtens sei.

Öffentliche Organe des Kantons Basel-Stadt, wozu auch selbständige Anstalten des öffentlichen Rechts gehören, können das Bearbeiten von Informationen Dritten übertragen, wenn keine rechtliche Bestimmung oder vertragliche Vereinbarung entgegensteht und sichergestellt wird, dass die Informationen nur so bearbeitet werden, wie es das öffentliche Organ selbst tun dürfte[1]. Der Dritte – hier ein privates Inkassounternehmen, das auch Bonitäts- und Wirtschaftsauskünfte erteilt – soll im Auftrag des öffentlichen Organs und zur Erfüllung von dessen gesetzlicher Aufgabe Personendaten bearbeiten. Im Übrigen, so hält das IDG fest, bleibt das öffentliche Organ für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich[2].

Im konkreten Fall waren weder entgegenstehende rechtliche Bestimmungen (wie etwa ein besonderes Amtsgeheimnis) noch entgegenstehende vertragliche Vereinbarungen ersichtlich. Es galt deshalb zu prüfen, ob und wie das öffentliche Organ sicherstellt, dass die Informationen nur so bearbeitet werden, wie es selbst das auch tun dürfte, nämlich ausschliesslich zur Eintreibung der geschuldeten Gebühren. Mehr als das ist dem öffentlichen Organ und somit auch dem privaten Inkassounternehmen nicht erlaubt. Die Behörde hat mittels einer klaren vertraglichen Vereinbarung dafür zu sorgen, dass das private Inkassounternehmen sich an die datenschutzrechtlichen Vorgaben hält und die gelieferten Daten ausschliesslich zur Eintreibung der Forderungen verwendet.

Nach Prüfung der vorgelegten Unterlagen und Rücksprache mit dem zuständigen Rechtsdienst musste jedoch festgehalten werden, dass keine genügende Sicherung der obgenannten Verpflichtungen vorhanden war. Vielmehr fehlte es überhaupt an einem eigentlichen Vertrag zwischen den beiden Parteien.

Der Datenschutzbeauftragte empfahl daher dem öffentlichen Organ dringend, das Inkassounternehmen unter Androhung angemessener Sanktionen im Widerhandlungsfall ausdrücklich zu verpflichten, die bekannt gegebenen Verlustscheindaten ausschliesslich für die Eintreibung der bestimmten Forderungen zu verwenden. Insbesondere dürfen die Daten nicht in die Bonitätsdatenbank des Inkassounternehmens aufgenommen und für andere Inkassohandlungen oder Bonitätsauskünfte verwendet werden; das wäre mehr, als das öffentliche Organ selbst tun dürfte, und damit widerrechtlich. Bis zum Vorliegen einer entsprechenden Vereinbarung sollte auf die Übermittlung weiterer Daten verzichtet werden. Das öffentliche Organ erkannte, dass die aktuelle Praxis aus datenschutzrechtlicher Sicht nicht weiter aufrechterhalten werden konnte, stellte die Datenbekanntgabe an das Inkassounternehmen vorübergehend ein und begann mit der Ausarbeitung eines entsprechenden Vertrages.

Ist die vertragliche Sicherstellung der zweckgebundenen Nutzung der übermittelten Schuldner-Daten schliesslich erfolgt, bedarf es grundsätzlich keiner weiteren Voraussetzungen zur Auslagerung der Verlustscheinsbewirtschaftung mehr. Insbesondere ist die Einwilligung der von der ausgelagerten Datenbearbeitung betroffenen Personen nicht erforderlich, da das öffentliche Organ nur gesetzlich vorgesehene Datenbearbeitungen oder Datenbearbeitungen, die zur Erfüllung einer gesetzlichen Aufgabe nötig sind, übertragen darf. Der Gesetzgeber hat mit der Schaffung der entsprechenden Aufgabennorm bereits über die Zulässigkeit der Datenbearbeitung entschieden und der Einzelne damit kein Vetorecht mehr.

Ergebnis

Ein öffentliches Organ darf das Bearbeiten von Personendaten Dritten übertragen, wenn es insbesondere sicherstellt, dass die Daten nur so bearbeitet werden, wie es selbst das auch tun dürfte (§ 7 Abs. 1 lit. b IDG). Die sog. Verpflichtungserklärung sollte vertraglicher Natur sein und das private Unternehmen unter Androhung geeigneter Massnahmen zur Einhaltung der datenschutzrechtlichen Vorschriften verpflichten. Personen, deren Daten von der Auslagerung betroffen sind, müssen nicht darüber informiert werden, da das kantonale öffentliche Organ weiterhin für den datenschutzkonformen Umgang mit den Daten verantwortlich und somit ihr Ansprechpartner bleibt (§ 7 Abs. 2 IDG).

1 § 7 Abs. 1 IDG.
2 § 7 Abs. 2 IDG.

Fall 2 Online-Zugriff auf Einwohnerdaten für einen Krankenversicherer?

Ein Krankenversicherer möchte – wie in der Stadt Zürich – einen Online-Zugriff auf Daten der Einwohnerkontrolle, damit er bei Adressrecherchen nicht mehr in jedem Fall ein begründetes Auskunftsgesuch stellen muss. Ist das aus datenschutzrechtlicher Sicht zulässig?

Wer einer anderen Stelle oder Person einen Online-Zugriff auf «seine» Daten einräumt, gibt – datenschutzrechtlich betrachtet – Personendaten bekannt[1]. Das DSG bzw. das IDG verlangen für die Bekanntgabe von Personendaten eine gesetzliche Grundlage[2]. Weil die Dateneignerin beim Online-Zugriff nicht mehr kontrollieren kann, ob im konkreten Fall die Voraussetzung für die Datenbekanntgabe erfüllt sind, verlangte das DSG zusätzlich eine Autorisierung durch den Datenschutzbeauftragten[3]. Nach dem IDG und der IDV ist neu nur noch eine Vorabkontrolle durch den Datenschutzbeauftragten erforderlich[4].

Beim Online-Zugriffs-Gesuch des Krankenversicherers ist deshalb zuerst zu prüfen, ob sich auf Bundes- oder auf kantonaler Ebene eine Norm finden lässt, welche die Einwohnerkontrolle zu einer Datenbekanntgabe an die Versicherung verpflichtet oder ermächtigt. Als mögliche Norm kommt (für Leistungen der obligatorischen Krankenpflegeversicherung im KVG-Bereich) Art. 32 Abs. 1 lit. a ATSG in Frage. Danach geben (u.a.) die Verwaltungsbehörden der Kantone «den Organen der einzelnen Sozialversicherungen auf schriftliche und begründete Anfrage im Einzelfall kostenlos diejenigen Daten bekannt, die erforderlich sind für: a. die Festsetzung, Änderung oder Rückforderung von Leistungen; b. die Verhinderung ungerechtfertigter Bezüge; c. die Festsetzung und den Bezug der Beiträge; d. den Rückgriff auf haftpflichtige Dritte.»

Der Datenschutzbeauftragte kam zum Schluss, dass dieser Wortlaut nicht dahingehend ausgelegt werden kann, dass auch ein Online-Zugriff einer Versicherung gestattet wäre: Der Umstand, dass die Bestimmung für die Datenbekanntgabe explizit eine «schriftliche und begründete Anfrage im Einzelfall» voraussetzt, zeigt, dass Online-Zugriffe, bei denen die Dateneignerin logischerweise die Begründung im konkreten Einzelfall nicht überprüfen kann, vom Gesetzgeber nicht gewollt waren.

Auch auf kantonaler Ebene findet sich keine Norm, die einen Online-Zugriff gestattet. Demgegenüber hält das Gemeindegesetz des Kantons Zürich fest, dass die Gemeinde einem anderen öffentlichen Organ den Zugriff auf das Einwohner-Register erteilen kann, sofern eine rechtliche Bestimmung dies vorsieht[5]. Die entsprechende Bestimmung findet sich sodann in Art. 6 bis der Allgemeinen Datenschutzverordnung der Stadt Zürich, der Stadtrat hat schliesslich die «Vollzugsbestimmungen über die Onlinezugriffe auf Personendaten des Personenmeldeamtes der Stadt Zürich» beschlossen. Die Krankenkassen, welche einen Online-Zugriff auf das «eAdress-Portal» erhalten wollen, müssen vorgängig mit dem Personenmeldeamt der Stadt Zürich (der Einwohnerkontrollbehörde) einen schriftlichen Vertrag abschliessen.

Weil im Kanton Basel-Stadt das Online-Zugriffs-Gesuch schon an der mangelnden gesetzlichen Grundlage scheitert, erübrigte sich eine Beurteilung der Verhältnismässigkeit. Bereits eine summarische Betrachtung liess jedoch erhebliche Zweifel an der Erforderlichkeit eines Online-Zugriffs auf Daten aller Einwohner(innen) aufkommen.

Ergebnis

Die Bekanntgabe von Personendaten braucht eine gesetzliche Grundlage. Nach dem anwendbaren Bundesgesetz erhalten Organe der Sozialversicherungen von Verwaltungsbehörden auf schriftliche und begründete Anfrage im Einzelfall kostenlos bestimmte Daten. Damit lässt es keinen Spielraum für Online-Zugriffe, welche logischerweise von der Dateneignerin nicht im Einzelfall auf ihre Begründetheit geprüft werden können. Eine kantonale gesetzliche Grundlage für die Einräumung von Online-Zugriffen an Krankenversicherer existiert nicht. Deshalb müssen diese sich weiterhin im Einzelfall an die Einwohnerkontrolle wenden.

1 § 2 Abs. 3 DSG bzw. § 3 Abs. 5 IDG.
2 §§ 10 f. DSG bzw. § 21 IDG.
3 § 10 Abs. 2 DSG.
4 § 13 Abs. 1 IDG, konkretisiert § 2 Abs. 1 IDV, insb. lit. a.
5 § 38a Gemeindegesetz (des Kantons Zürich) vom 6. Juni 1926, LS 131.1.

Fall 3 Das flüchtige «Nach-Alkohol-riechen» im Polizeirapport

Die Polizei wird alarmiert, weil eine Frau – wie geraume Zeit vorher bereits einmal – auf den Balkon gesperrt ist. Nach ihren Angaben wurde sie von ihren sehr kleinen Kindern aus der Wohnung ausgesperrt. Die Polizist(inn)en halten im Polizeirapport fest, sie habe «nach Alkohol gerochen». Die betroffene Frau bestreitet dies und verlangt die Löschung der Textstelle. Zu Recht?

Eine von einer Datenbearbeitung betroffene Person kann vom verantwortlichen Organ verlangen, dass unrichtige Daten berichtigt werden[1]. Unrichtig sind Personendaten, wenn Umstände und Tatsachen bezogen auf die betroffene Person nicht sachgerecht wiedergegeben wurden. Dabei hat nicht die betroffene Person die behauptete Unrichtigkeit zu beweisen, sondern die datenbearbeitende Stelle die Richtigkeit der Informationen. Kann die Richtigkeit der Daten nicht bewiesen werden, so sind die Daten zu berichtigen oder – wenn eine Berichtigung nicht möglich ist – zu vernichten. Dieser Grundsatz gilt jedoch nicht für Daten, deren Richtigkeit bzw. Unrichtigkeit der Natur nach nicht (mehr) bewiesen werden kann. Das ist der Fall bei Wertungen menschlichen Verhaltens (sog. Werturteilen), aber auch bei Tatsachen, deren Richtigkeit ihrer Natur nach nicht mehr belegt werden kann. In diesen Fällen kann nur, aber immerhin die Aufnahme einer Gegendarstellung verlangt werden[2].

In einem Polizeirapport sind grundsätzlich Tatsachen festzuhalten, die von den diensthabenden Polizist(inn)en festgestellt wurden. Das «nach Alkohol riechen» ist eine Tatsache, die von den am Einsatzort anwesenden Polizist(inn)en festgestellt werden kann, aber «flüchtig» ist und naturgemäss bereits nach kurzer Zeit nicht mehr bewiesen werden kann. Ebenso wenig kann natürlich auch das Gegenteil, nämlich dass die betroffene Person nicht nach Alkohol gerochen habe, bewiesen werden. Allenfalls hätte die Feststellung der Polizist(inn)en zum Anlass genommen werden können, einen Alkoholtest bei der betreffenden Person durchzuführen (Atemtest oder Blutuntersuchung). Diese Überprüfungen werden jedoch nicht bei Hilfeleistungen vorgenommen, sondern eher dann, wenn Straftatbestände (etwa das Fahren in angetrunkenem Zustand) zur Debatte stehen.

Der (kantonale) Datenschutzbeauftragte kam zum Schluss, dass es sich in diesem Fall tatsächlich um Personendaten handelt, bei denen weder die Richtigkeit noch die Unrichtigkeit bewiesen werden kann, so dass die betroffene Person nur die Aufnahme einer Gegendarstellung verlangen kann. Das Verfahren dazu ist bei der Kantonspolizei in einer Dienstvorschrift konkret festgelegt: Danach informiert der/die (interne) Datenschutzbeauftragte der Kantonspolizei die antragstellende Person darüber, dass die Unrichtigkeit des Rapportes bestritten ist, bzw. darüber, dass die Korrektheit des Eintrags zum Zeitpunkt des Berichtigungsantrags nicht mehr nachgewiesen werden kann. Er/Sie bietet der betroffenen Person folgende Wahlmöglichkeit an:

— Sie kann verlangen, dass in einer Verfügung festgestellt wird, dass die Berichtigung des Rapportes abgelehnt wird, oder
— sie kann die Aufnahme eines Gegendarstellungsrapportes verlangen.

Im zweiten Fall wird dem ursprünglichen Polizeirapport ein Gegendarstellungsrapport angefügt. Dabei ist in der elektronischen Version des Dossiers sicherzustellen, dass das nachträglich erstellte Dokument so mit dem Originalrapport verknüpft wird, dass die Gegendarstellung auch wahrgenommen und nicht ihres Sinns entleert wird. Bei Papierakten ist die Gegendarstellung entweder an das Originaldokument anzuheften oder es muss mit einer Notiz auf dem ursprünglichen Dokument darauf verwiesen werden.

Ergebnis

In einem Polizeirapport können auch Tatsachen geschildert werden, die von den diensthabenden Polizist(inn)en festgestellt wurden, sich aber nach kurzer Zeit weder positiv noch negativ beweisen lassen. Die betroffene Person, welche die Richtigkeit solcher Rapportinhalte bestreitet, kann nur verlangen, dass eine Gegendarstellung aufgenommen wird. Durch geeignete Massnahmen muss die Kantonspolizei sicherstellen, dass bei einem Zugriff auf den ursprünglichen Rapport auch die Gegendarstellung zur Kenntnis genommen wird.

1 § 21 Abs. 1 DSG bzw. § 27 Abs. 1 lit. a IDG.
2 § 21 Abs. 3 DSG bzw. § 12 Abs. 3 IDV.

Fall 4 Eine «Generaleinwilligung für alle Fälle» bei der Sozialhilfe

Damit die Sozialhilfe die Bedürftigkeit einer gesuchstellenden Person abklären kann, braucht sie allenfalls Informationen von verschiedensten Ämtern, Stellen und Personen. Die Sozialhilfe stützt sich dabei sowohl auf gesetzliche Grundlagen wie auch auf eine Einwilligungserklärung der gesuchstellenden Personen – zu Recht?

Die Sozialhilfe muss bedürftige Personen beraten, ihre materielle Sicherheit gewährleisten sowie ihre Selbständigkeit erhalten und fördern[1]. Um die Bedürftigkeit einer Person abzuklären, muss die Sozialhilfe von verschiedenen anderen Stellen und Personen Informationen einholen können.

Dieses Vorgehen stellt datenschutzrechtlich gesehen seitens der Sozialhilfe ein Datenbearbeiten[2], für die angefragten Stellen und Personen ein Bekanntgeben von Personendaten dar[3]. Voraussetzung dafür ist jeweils das Vorliegen einer gesetzlichen Grundlage. Soweit es sich dabei um besondere Personendaten[4] handelt, muss diese Grundlage sogar ein Gesetz im formellen Sinne[5] sein, welches entweder die Datenbearbeitung explizit regelt (sog. unmittelbare gesetzliche Grundlage) oder eine Aufgabe nennt, zu deren Erfüllung die Datenbearbeitung erforderlich ist (sog. mittelbare gesetzliche Grundlage).

§ 2 Abs. 1 SHG stellt eine derartige mittelbare Grundlage für das Datenbearbeiten durch die Sozialhilfe dar. Zusätzlich dazu auferlegt das SHG bestimmten Personen und Stellen eine Auskunftspflicht[6]. Die Bekanntgabe derjenigen Informationen, die zur richtigen Handhabung des SHG erforderlich sind, durch diese Personen und Stellen, ist gesetzlich gerechtfertigt. Weitere gesetzliche Grundlagen bestehen für die Datenbekanntgabe durch die Sozialversicherungen[7].

Die Sozialhilfe möchte bei ihren Abklärungen jedoch zusätzlich auf Personen und Stellen zurückgreifen können, welche im SHG nicht erwähnt werden. Für deren Datenbekanntgeben gibt das SHG keine Rechtfertigung – es braucht deshalb eine Einwilligung der gesuchstellenden Person bzw. eine Entbindung von Berufsgeheimnissen wie beispielsweise dem ärztlichen. Bisher musste die gesuchstellende Person bei der Gesuchstellung folgende generelle Erklärung unterschreiben: «Ich erkläre meine Einwilligung zu Anfragen bei weiteren Behörden, Versicherungen und Banken, bei Institutionen zur Arbeitsintegration sowie bei Krankenkassen, behandelnden Ärztinnen und Ärzten und weiteren Personen (z.B. Vermieter) und Organisationen, soweit die Information zur richtigen Handhabung der Sozialhilfe notwendig ist. Ich entbinde die kontaktierten Stellen und Personen vom Berufs- und Amtsgeheimnis und ermächtige sie, der Sozialhilfe die erforderlichen Auskünfte zu erteilen.»

Nach Ansicht des Datenschutzbeauftragten ist eine derart weit gehende Generaleinwilligung, von deren Unterzeichnung die Anhandnahme eines Falles abhängt, zu unbestimmt und unverhältnismässig.

Eine Verbesserung könnte auf verschiedenen Wegen herbeigeführt werden, zum Beispiel:

— Indem der Gesetzgeber das SHG präziser fasst; allerdings müsste die Frage, inwieweit weitere Auskunftspflichten verfassungskonform sind, sorgfältig geprüft werden[8]; oder

— indem die Sozialhilfe im Einzelfall, wenn aufgrund von Anhaltspunkten klar ist, wo Nachforschungen notwendig sind, spezifischere Einwilligungen und Entbindungserklärungen verwendet. Falls die gesuchstellende Person in solchen Fällen die hinreichend bestimmt formulierte Einwilligung nicht gibt, ist zu prüfen, ob sie die gesetzliche Mitwirkungspflicht verletzt und allenfalls entsprechende Sanktionen verhängt werden müssen.

Ergebnis

Eine derart weit gehende Generaleinwilligung («… bei weiteren Behörden, Versicherungen und Banken, bei Institutionen zur Arbeitsintegration sowie bei Krankenkassen, behandelnden Ärztinnen und Ärzten und weiteren Personen … und Organisationen, … entbinde die kontaktierten Stellen und Personen vom Berufs- und Amtsgeheimnis und ermächtige sie, der Sozialhilfe die erforderlichen Auskünfte zu erteilen») von deren Unterzeichnung die Anhandnahme eines Falles abhängt, ist u. E. zu unbestimmt und unverhältnismässig. Die Sozialhilfe ist dabei, in Zusammenarbeit mit dem Datenschutzbeauftragten eine bessere Lösung zu finden.

1 § 2 Abs. 1 SHG.
2 §§ 5 und 6 DSG, § 9 IDG.
3 § 10 DSG, § 21 IDG bzw. entsprechende Regelungen des DSG-Bund oder anderer kantonaler DSG.
4 § 2 Abs. 2 DSG und § 3 Abs. 4 lit. a Ziff. 3 IDG.
5 § 6 lit. a und b DSG, § 9 Abs. 2 IDG.
6 § 28 Abs. 3 SHG: Personen, die mit den unterstützten Personen in Haushaltgemeinschaft leben oder ihnen gegenüber unterhalts- oder unterstützungspflichtig sind, Arbeitgeber der unterstützten Personen und der mit ihnen in Haushaltgemeinschaft lebenden Angehörigen sowie Verwaltungs- und Gerichtsbehörden des Kantons und seiner Gemeinden.
7 Art. 50a Abs. 1 1it. e AHVG; Art. 66a Abs. 2 IVG; Art. 26 ELG; Art. 97a Abs. 1 lit. f AVIG; Art. 84a Abs. 1 lit. h KVG; Art. 97 Abs. 1 lit. i UVG; Art. 86a Abs. 1 lit. a BVG.
8 Eine ähnliche Fragestellung aus dem Kanton Bern ist seit Dezember 2011 beim Bundesgericht hängig: Beschwerde in öffentlichrechtlichen Angelegenheiten: <http://www.avenirsocial.ch/cm_data/Beschwerde_SHG_anonym.19.12.11.pdf>.

Fall 5 Die elterlichen Einkommens- und Vermögensverhältnisse

Die Abteilung Prämienverbilligungen und Mietzinsbeiträge des Amtes für Sozialbeiträge teilt einem unter 25-jährigen Mann, welcher um eine Krankenkassen-Prämienverbilligung ersucht hatte, in der ablehnenden Verfügung auch die detaillierten Einkommens- und Vermögensverhältnisse seiner Eltern mit. Darf es das?

Werden einer Person, welche um eine Prämienverbilligung ersucht hat, in der ablehnenden Verfügung die Einkommens- und Vermögensverhältnisse (der Eltern) bekannt gegeben, so stellt dies eine Datenbekanntgabe im Sinne von § 21 IDG dar. Voraussetzung für eine Bekanntgabe ist danach entweder das Vorliegen einer unmittelbaren gesetzlichen Grundlage, d.h. einer Norm, welche die Bekanntgabe explizit vorsieht, oder einer sogenannten mittelbaren gesetzlichen Grundlage, also einer Bestimmung, welche eine Aufgabe nennt, zu deren Erfüllung die Bekanntgabe erforderlich ist.

Das für die Beurteilung und Berechnung von Prämienverbilligungen zuständige Organ ist nach dem Harmonisierungsgesetz Sozialleistungen (SoHaG) zur Datenbearbeitung befugt[1]. Um den Anspruch auf Prämienverbilligung prüfen zu können, muss die Abteilung für Prämienverbilligung und Mietzinsbeiträge Einsicht in das massgebliche Einkommen der wirtschaftlichen Haushaltseinheit nehmen können. Zur wirtschaftlichen Haushaltseinheit zählen nebst dem oder der Antragsteller(in) selbst auch dessen Ehegattin bzw. deren Ehegatte, registrierte(r) Partner(in), im gemeinsamen Haushalt lebende Konkubinatspartner(innen) mit gemeinsamen Kindern oder Konkubinatspartner(innen) nach fünfjähriger Lebensgemeinschaft, sowie minderjährige und volljährige Kinder bis 25 Jahre in Erstausbildung. Befindet sich die antragstellende Person selbst noch in Erstausbildung und ist jünger als 25 Jahre, so bestimmt sich deren Haushaltseinheit gemäss der Haushaltseinheit der Eltern[2]. Damit ist für die Berechnung das Einkommen und Vermögen der Eltern gemäss der aktuellsten Steuerveranlagung massgebend[3].

Infolge dieser rechtlichen Konstellation hat sich bei der Abteilung für Prämienverbilligung und Mietzinsbeiträge die Praxis etabliert, Gesuche von unter 25-Jährigen in Erstausbildung nur dann zu bearbeiten, wenn sie gemeinsam mit den Eltern gestellt worden sind. Als gemeinsame Gesuchsteller werden Eltern und Kind sodann als *ein* Verfügungsadressat behandelt. Die Verfügung über Gewährung oder Ablehnung des Gesuches wird damit auch beiden eröffnet.

Aufgrund des verfassungsrechtlichen Anspruchs auf rechtliches Gehör[4] beinhaltet die Verfügung nebst dem Entscheid immer auch eine Begründung, wie es zum Entscheid kam. Die Begründung muss dabei so formuliert sein, dass der oder die Verfügungsadressat(in) entscheiden kann, ob er oder sie die Verfügung anfechten will. Ausserdem muss die Begründung die für den Entscheid relevanten Punkte, hier die zugrundeliegende Berechnung des massgeblichen Einkommens, nennen, damit der oder die Verfügungsadressat(in) in einem allfälligen Rekurs darauf eingehen und sie gegebenenfalls widerlegen kann.

Im vorgelegten Fall kam die Abteilung für Prämienverbilligung und Mietzinsbeiträge zum Schluss, dass das massgebliche Einkommen der Familie zu gross sei, um einen Beitrag an die Krankenkassenprämien zu übernehmen. Dem antragstellenden Sohn wurde die diesbezügliche Verfügung – wie rechtlich vorgeschrieben – mitsamt der der Entscheidung zugrundeliegenden Begründung (inklusive der aktuellen Steuerveranlagung der Eltern) eröffnet. Dieses Vorgehen ist aus datenschutzrechtlicher Sicht zulässig, da für die Bekanntgabe die erforderlichen gesetzlichen Grundlagen bestehen.

Ergebnis

Das von der Abteilung Prämienverbilligung und Mietzinsbeiträge gewählte Vorgehen, Gesuche von jungen Erwachsenen unter 25 Jahren in Erstausbildung nur zu bearbeiten, wenn sie gemeinsam mit den Eltern gestellt werden, erachten wir als durchaus zulässig. Die daraus resultierende Konsequenz, dass dadurch beide Parteien als ein Verfügungsadressat angesehen werden, womit sowohl den Eltern als auch dem Kind die der Verfügung zugrundeliegende Berechnung inklusive der aktuellen Steuerveranlagung als Teil dieser Berechnung eröffnet wird, ist aus datenschutzrechtlicher Sicht nicht zu beanstanden.

1 § 20 SoHaG.
2 § 5 Abs. 3 SoHaG.
3 § 13 SoHaV.
4 § 12 lit. b KV.

Fall 6 Das «psychische Leiden» im Bericht des Vertrauensarztes

Dem Personaldienst eines Departements wird vom Vertrauensärztlichen Dienst mitgeteilt, dass ein Mitarbeiter aufgrund eines «psychischen Leidens» zu 100% arbeitsunfähig sei. Der Mitarbeiter hat zuvor eine Entbindungserklärung unterzeichnet, welche den Vertrauensärztlichen Dienst ermächtigt, Auskunft über das betroffene Organsystem oder die betroffene Körperregion zu erteilen, nicht aber Diagnose oder Befunde mitzuteilen.

Nach dem Personalgesetz dürfen Arbeitgeber(inne)n ihre Mitarbeitenden zur Untersuchung beim Vertrauensärztlichen Dienst (VAD) anmelden[1]. Was darf nun als Resultat aus dieser Untersuchung an den Personaldienst zurückfliessen? Die Mitteilung der Untersuchungsergebnisse (mithin Angaben über die Gesundheit) durch den VAD an den Personaldienst stellt datenschutzrechtlich eine Bekanntgabe von besonderen Personendaten[2] dar. Solche Daten darf das öffentliche Organ bekannt geben, wenn a) ein Gesetz dazu ausdrücklich verpflichtet oder ermächtigt (sog. unmittelbare gesetzliche Grundlage) oder b) dies zur Erfüllung einer in einem Gesetz klar umschriebenen Aufgabe zwingend notwendig ist (sog. mittelbare gesetzliche Grundlage) oder c) im Einzelfall die betroffene Person ausdrücklich zugestimmt hat oder, falls sie dazu nicht in der Lage ist, die Bekanntgabe in ihrem Interesse liegt und ihre Zustimmung in guten Treuen vorausgesetzt werden darf[3].

Das Personalgesetz sagt nicht, welche Informationen vom VAD zurückfliessen dürfen, und stellt damit bestenfalls eine mittelbare gesetzliche Grundlage dar, welche lediglich die Mitteilung erlaubt, dass sich die Feststellungen des VAD mit jenen des ursprünglichen ärztlichen Zeugnisses decken oder dass der VAD bezüglich Tatsache, Dauer oder Grad der Arbeitsunfähigkeit zu einem abweichenden Ergebnis gekommen ist[4]. Mehr Angaben braucht die vorgesetzte Stelle i.d.R. auch nicht, um ihre Aufgaben erfüllen und die notwendigen Entscheide bezüglich der erkrankten oder verunfallten Person treffen zu können[5]. Keinesfalls erfasst ist die Bekanntgabe von Diagnose oder Befunden, da dies sehr schwerwiegend in die Persönlichkeitsrechte der betroffenen Personen eingreift.

Auskünfte über den genannten Bereich hinaus bedürfen der Einwilligung der betroffenen Person[6], welche vorgängig aufzuklären ist (informed consent). Im konkreten Zusammenhang ist dies gleichzeitig eine Entbindung vom ärztlichen Berufsgeheimnis. Die Einwilligung gilt nur, wenn sie freiwillig erfolgt ist, was in Arbeitsverhältnissen aufgrund der faktischen Machtverhältnisse grundsätzlich als schwer zu erfüllen angesehen wird. Willigt die betroffene Person nicht in die Bekanntgabe der Informationen an ihre vorgesetzte Stelle ein, so ist dies zu respektieren und vom VAD dem Personaldienst so mitzuteilen.

Im konkreten Fall war eine Einwilligung in Bezug auf Mitteilungen über das betroffene Organsystem oder die betroffene Körperregion eingeholt worden. Die Mitteilung einer Diagnose oder eines Befundes war dabei explizit ausgenommen. Dass der vorgesetzten Stelle nun mitgeteilt worden war, die betroffene Person sei aufgrund eines «psychischen Leidens» zu 100% arbeitsunfähig, wurde damit begründet, dass die «Psyche» quasi als Organ betrachtet werden könne und der Passus «psychisches Leiden» keineswegs einer Diagnose oder einem Befund entspreche.

Die Argumentation des VAD vermag nicht zu überzeugen: Obgleich der Hinweis, jemand habe ein «psychisches Leiden» aus medizinisch-fachlicher Sicht keine Diagnose ist, wird diese Aussage in der Laiensphäre durchaus als (grobe) Diagnose interpretiert. Damit ist diese Information jedoch weder von der gesetzlichen Grundlage des § 21 PG noch von der eingeholten Einwilligung der betroffenen Person erfasst. Die Mitteilung des VAD an die zuständige Personalstelle, ein(e) Mitarbeitende habe ein «psychisches Leiden», erscheint somit als unzulässige Datenbekanntgabe.

Ergebnis

Die Bekanntgabe besonderer Personendaten, wie sie bei Abklärungen des Vertrauensärztlichen Dienstes anfallen, bedarf entweder einer formellgesetzlichen (mittelbaren oder unmittelbaren) Grundlage oder aber der Einwilligung der betroffenen Person. Damit diese rechtsgültig einwilligen kann, muss der mögliche Inhalt der Mitteilung am den oder die Arbeitgeber(in) klar umschrieben sein: Auch Angaben, die aus medizinisch-fachlicher Sicht weder Diagnose noch Befund sind, können besondere Personendaten enthalten bzw. Laien zu persönlichkeitsverletzenden (Fehl-)Schlüssen veranlassen. Der VAD hat diesen Fall zum Anlass genommen, seine Einwilligungserklärung gemeinsam mit dem Datenschutzbeauftragten zu überarbeiten.

1 § 21 PG.
2 § 2 Abs. 2 DSG bzw. § 3 Abs. 4 lit. a Ziff. 2 IDG.
3 § 10 Abs. 1 i.V.m. § 6 DSG bzw. § 21 Abs. 2 IDG.
4 Siehe dazu Roland Müller, Arztzeugnisse in arbeitsrechtlichen Streitigkeiten, AJP 2010, 171.
5 Art. 328 b OR.
6 § 21 Abs. 2 lit. c IDG.

Fall 7 Vielsagend nicht sagen was man nicht sagen darf

Eine Person verlangt Zugang zu den eigenen Personendaten. Das mit dem Gesuch konfrontierte öffentliche Organ steckt in einem Dilemma: Wenn nämlich öffentliche oder private Interessen einer Auskunft entgegen stehen, kann die Behörde nicht einfach «nichts» sagen oder gar lügen – aber überhaupt etwas mitzuteilen wäre unter Umständen auch schon zuviel. Was tun?

Der Zugang zu den eigenen Personendaten[1] gilt nicht absolut. Der Zugang ist ganz oder teilweise zu verweigern oder aufzuschieben, wenn eine besondere gesetzliche Geheimhaltungspflicht oder ein überwiegendes öffentliches oder privates Interesse entgegensteht[2]. Eine besondere gesetzliche Geheimhaltungspflicht, die den Zugang zu den Daten über die eigene Person a priori verbietet, gibt es im kantonalen Recht nicht[3]. Nicht selten können aber öffentliche oder private Interessen dem Zugang zu den eigenen Personendaten entgegenstehen. Als öffentliche Interessen kommen etwa die Sicherheit des Staates oder die öffentliche Sicherheit, die Wahrung der Beziehungen zu anderen Kantonen, dem Bund oder dem Ausland oder aber die Möglichkeit der zielkonformen Durchführung konkreter behördlicher, insbesondere polizeilicher Massnahmen in Frage.

Falls der Zugang zu Daten zum Schutz der zielkonformen Durchführung konkreter behördlicher, insbesondere polizeilicher Massnahmen verweigert werden darf (oder muss), stellt sich die Frage, wie dies der gesuchstellenden Person mitgeteilt werden kann, ohne dass aus der Mitteilung auf die Information, die geheim gehalten werden darf (oder muss), geschlossen werden kann?

Nehmen wir an, eine Person wüsste gerne, ob gegen sie ein polizeiliches Vorermittlungsverfahren läuft, und verlangt Zugang zu den eigenen Personendaten. Und schon steckt das angefragte öffentliche Organ im Dilemma:

— Wenn kein solches Verfahren im Gange ist: Ja wäre unrichtig. Nein wäre die korrekte Antwort. Einen Grund für eine Einschränkung der Auskunft gibt es – wenn nur diese Konstellation betrachtet wird – nicht.

— Wenn ein solches Verfahren im Gange ist: Ja wird die Polizei nicht sagen wollen, wenn sie das Verfahren nicht gefährden will. Nein darf sie nicht sagen, weil das eine Lüge wäre. Korrekt wäre die Aussage, man gebe wegen eines überwiegenden öffentlichen Interesses nicht Auskunft.

Die gesuchstellende Person, die nicht weiss, ob ein Verfahren gegen sie läuft, kann deshalb aus der «Nicht-Antwort» auf die gewünschte, aber verweigerte Antwort schliessen.

Wie kann die Polizei Auskunft erteilen, ohne zu sagen, was sie (zulässigerweise) nicht sagen darf oder muss? Vielleicht kann sie das Verfahren «aussitzen»: Wenn innert der 30tägigen Frist für die Zugangsgewährung[4] die Massnahme zielkonform umgesetzt werden kann, entfällt anschliessend das Geheimhaltungsinteresse. Aber sonst?

Eine Lösungsmöglichkeit besteht in der Verwendung von Alternativ-Begründungen. Denkbar wäre beispielsweise: «Es sind entweder keine Ihre Person betreffenden Daten bei uns vorhanden oder wir können Ihnen zu diesen aus Gründen überwiegender öffentlicher oder privater Interessen ganz oder teilweise oder vorläufig keinen Zugang gewähren». Das öffentliche Organ lässt damit die kritische Frage offen, ob es nun schlicht keine entsprechenden Daten bearbeitet oder ob eben doch gewisse Gründe gegen einen Zugang sprechen könnten. Möchte sich die betroffene Person gegen die (vermeintliche) Verweigerung wehren, so kann sie die Verfügung anfechten. Korrekterweise muss das öffentliche Organ nach dem Wegfall des Einschränkungsgrundes die zutreffende Auskunft erteilen.

Ergebnis

Stellt eine Person ein Gesuch um Zugang zu ihren eigenen Personendaten, können Gründe gegen einen (vollumfänglichen) Zugang sprechen. Eine (teilweise) Verweigerung bzw. ein Aufschub des Zugangs ist zu begründen. Allerdings kann gerade die Begründung dazu führen, dass mehr gesagt wird, als gesagt werden darf – etwa wenn öffentliche oder private Interessen gegen einen Zugang sprechen und ebendiese Interessen in der Begründung genannt werden. Die öffentlichen Organe sollten in diesen Fällen eine Formulierung wählen, welche es offen lässt, ob kein Zugang mangels Personendaten oder aufgrund von entgegenstehenden Interessen gewährt werden konnte. Nach Wegfall des Einschränkungsgrundes ist aber die korrekte Auskunft zu erteilen.

1 § 19 DSG bzw. § 26 IDG; vgl. dazu auch Thema 3 (vorne Seiten 23 ff.).
2 § 20 DSG bzw. § 29 IDG.
3 Auch im Bundesrecht gibt es soweit ersichtlich nur eine solche Bestimmung: Art. 18 BWIS für den Staatsschutzbereich.
4 § 35 IDG.

Fall 8 Die Schweigepflicht des Personals eines Vertragspartners eines Vertragspartners

Ein öffentliches Organ mit sehr heiklen Daten ist in einer Liegenschaft eingemietet. Ein Teil der Liegenschaftswartung erfolgt aufgrund eines Vertrages mit der Liegenschaftseigentümerin durch eine Drittfirma. Wie kann das öffentliche Organ sicherstellen, dass alle Mitarbeiter(innen) der Wartungsfirma, die mit den sensitiven Daten in Berührung kommen können, verschwiegen sind?

Das öffentliche Organ ist verantwortlich für den Umgang mit Personendaten[1], auch wenn es die Daten nicht selber bearbeitet, sondern durch Dritte bearbeiten lässt[2]. Ein «Bearbeiten» liegt nicht nur vor, wenn jemand mit diesen Daten etwas Konkretes tun, sie verwenden, ändern oder mit anderen zusammenführen muss; es reicht, dass sie jemandem zugänglich sind[3]. Mit einer Clean Desk Policy liesse sich das umsetzen: Wenn das Reinigungspersonal kommt, liegt kein Dossier mehr auf dem Pult, steckt kein Fax mehr im Faxgerät und steht kein Ordner in einem unabgeschlossenen Schrank. Das ist faktisch nicht überall möglich. Ausserdem kann das Reinigungspersonal auch ein Gespräch mitkriegen und daraus Personendaten erfahren. Also muss das öffentliche Organ auch dafür sorgen, dass das Reinigungspersonal einer Schweigepflicht untersteht.

Das ist einfach, wenn das öffentliche Organ die Reinigung mit eigenem Personal besorgen lässt. Dieses untersteht wie alle anderen Angestellten des Kantons dem Personalgesetz und damit der dort verankerten Pflicht zur Verschwiegenheit[4]. Um dieser Pflicht Nachdruck zu verleihen, lassen verschiedene Amtsstellen ihre Mitarbeiter(innen) zusätzlich periodisch eine ausdrückliche Verschwiegenheitserklärung unterzeichnen.

Wenn das öffentliche Organ ein Reinigungsunternehmen beizieht, dann unterstehen dessen Angestellte nicht dem Personalgesetz. In den Vertrag mit dem Reinigungsunternehmen ist deshalb eine Klausel aufzunehmen, in welcher sich das Unternehmen verpflichtet,

— nur Mitarbeiter(inne)n einzusetzen, die eine vorformulierte (oder mindestens ebenso weit reichende) Verschwiegenheitserklärung unterzeichnet haben, und

— auf Verlangen dem öffentlichen Organ die unterzeichneten Erklärungen aller eingesetzten Mitarbeiter(innen) vorzulegen.

Die Verpflichtungen können ausserdem durch die Androhung einer Konventionalstrafe im Widerhandlungsfall verstärkt werden.

Etwas schwieriger wird es, wenn – wie im eingangs geschilderten Fall – gar nicht das öffentliche Organ, sondern die Vermieterin eine Drittfirma bezieht. In diesem Fall besteht zwischen dem öffentlichen Organ und der Reinigungsfirma kein Vertragsverhältnis. Aus dem Mietvertrag wird das öffentliche Organ wahrscheinlich nur eine Duldungspflicht haben: Es muss den von der Vermieterin beauftragten Personen Zutritt gewähren zu den Orten, an denen diese ihren Wartungs- oder Reinigungsauftrag zu erfüllen haben. Es wäre möglich, aber bei regelmässig arbeitendem Reinigungspersonal wohl untauglich, solche Personen durch Verwaltungsmitarbeiter(innen) begleiten zu lassen, um dafür zu sorgen, dass sie keine Daten sehen, die sie nicht sehen sollten.

Also muss in den (Miet- oder einem separaten) Vertrag mit der Vermieterin eine Klausel aufgenommen werden, in welcher sich die Vermieterin verpflichtet, allfällig beigezogenen Drittfirmen die Verpflichtung zu überbinden,

— nur Mitarbeiter(inne)n einzusetzen, die eine vorformulierte (oder mindestens ebenso weit reichende) Verschwiegenheitserklärung unterzeichnet haben, und

— auf Verlangen dem öffentlichen Organ die unterzeichneten Erklärungen aller eingesetzten Mitarbeiter(innen) vorzulegen.

Ergebnis

Das öffentliche Organ – letztlich die Leitung des öffentlichen Organs – ist verantwortlich für den Schutz von Informationen, insbesondere von Personendaten. Deshalb muss dem eingesetzten Personal eine Schweigepflicht auferlegt werden. Wenn ein Vertragspartner – oder gar der Vertragspartner eines Vertragspartners – das Personal einsetzt, dann ist die Verpflichtung, eine solche Pflicht aufzuerlegen, der Vertragskette entlang zu überbinden.

1 § 6 IDG.
2 § 7 Abs. 2 IDG.
3 § 3 Abs. 5 und 6 IDG.
4 § 19 PG.

Anhang

Verzeichnis der zitierten Gesetze und Materialen

Basel-Stadt

Bericht 08.0637.02 Bericht 08.0637.02 der Justiz-, Sicherheits- und Sportkommission vom 14. April 2010 zum Ratschlag 08.0637.01 betreffend Gesetz über die Information und den Datenschutz (Informations- und Datenschutzgesetz).

DSG Gesetz vom 18. März 1992 über den Schutz von Personendaten (Datenschutzgesetz, DSG), SG 153.260 (wirksam bis 31. Dezember 2011).

IDG Gesetz vom 9. Juni 2010 über die Information und den Datenschutz (Informations- und Datenschutzgesetz, IDG), SG 153.260 (wirksam ab 1. Januar 2012).

IDV Verordnung vom 5. August 2011 über die Information und den Datenschutz (Informations- und Datenschutzverordnung, IDV), SG 153.270 (wirksam ab 1. Januar 2012).

KGeoIG Geoinformationsgesetz (KGeoIG) vom 16. November 2011 (noch nicht in Kraft, Referendumsvorlage: Kantonsblatt 2011, 1834 ff.).

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

OG Gesetz vom 22. April 1976 betreffend die Organisation des Regierungsrates und der Verwaltung des Kantons Basel-Stadt (Organisationsgesetz, OG), SG 153.100.

PG Personalgesetz vom 17. November 1999, SG 162.100

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

SHG Sozialhilfegesetz vom 29. Juni 2000 (SHG), SG 890.100.

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

SoHaV Verordnung vom 25. November 2008 über die Harmonisierung und Koordination von bedarfsabhängigen Sozialleistungen (SoHaV), SG 890.710

Bund, international

AHVG Bundesgesetz vom 20. Dezember 1946 über die Alters- und Hinterlassenenversicherung (AHVG), SR 831.10.

ATSG Bundesgesetz vom 6. Oktober 2000 über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG), SR 830.1.

AVIG Bundesgesetz vom 25. Juni 1982 über die obligatorische Arbeitslosenversicherung und die Insolvenzentschädigung (Arbeitslosenversicherungsgesetz, AVIG), SR 837.0.

BV Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999, SR 101.

BVG Bundesgesetz vom 25. Juni 1982 über die berufliche Alters-, Hinterlassenen- und Invalidenvorsorge (BVG), SR 831.40.

BWIS Bundesgesetz vom 21. März 1997 über Massnahmen zur Wahrung der inneren Sicherheit, SR 120.

DSG-Bund Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG), SR 235.1.

ELG Bundesgesetz vom 6. Oktober 2006 über Ergänzungsleistungen zur Alters-, Hinterlassenen- und Invalidenversicherung (ELG), SR 831.30.

ISchV Verordnung vom 4. Juli 2007 über den Schutz von Informationen des Bundes (Informationsschutzverordnung, ISchV), SR 510.411.

IVG Bundesgesetz vom 19. Juni 1959 über die Invalidenversicherung (IVG), SR 831.20.

KVG Bundesgesetz vom 18. März 1994 über die Krankenversicherung (KVG), SR 832.10.

OR Bundesgesetz vom 30. März 1911 betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht), SR 220.

StPO Schweizerische Strafprozessordnung vom 5. Oktober 2007 (Strafprozessordnung, StPO), SR 312.0.

UVG Bundesgesetz vom 20. März 1981 über die Unfallversicherung (UVG), SR 832.20.

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
Markus Brönnimann
lic. iur. Carmen Lindner
Dr. iur. Sandra Husi-Stämpfli
Daniela Waldmeier, MLaw
lic. iur. Barbara Widmer, LL.M., CIA

Bericht an den Grossen Rat
Tätigkeitsbericht des
Datenschutzbeauftragten 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