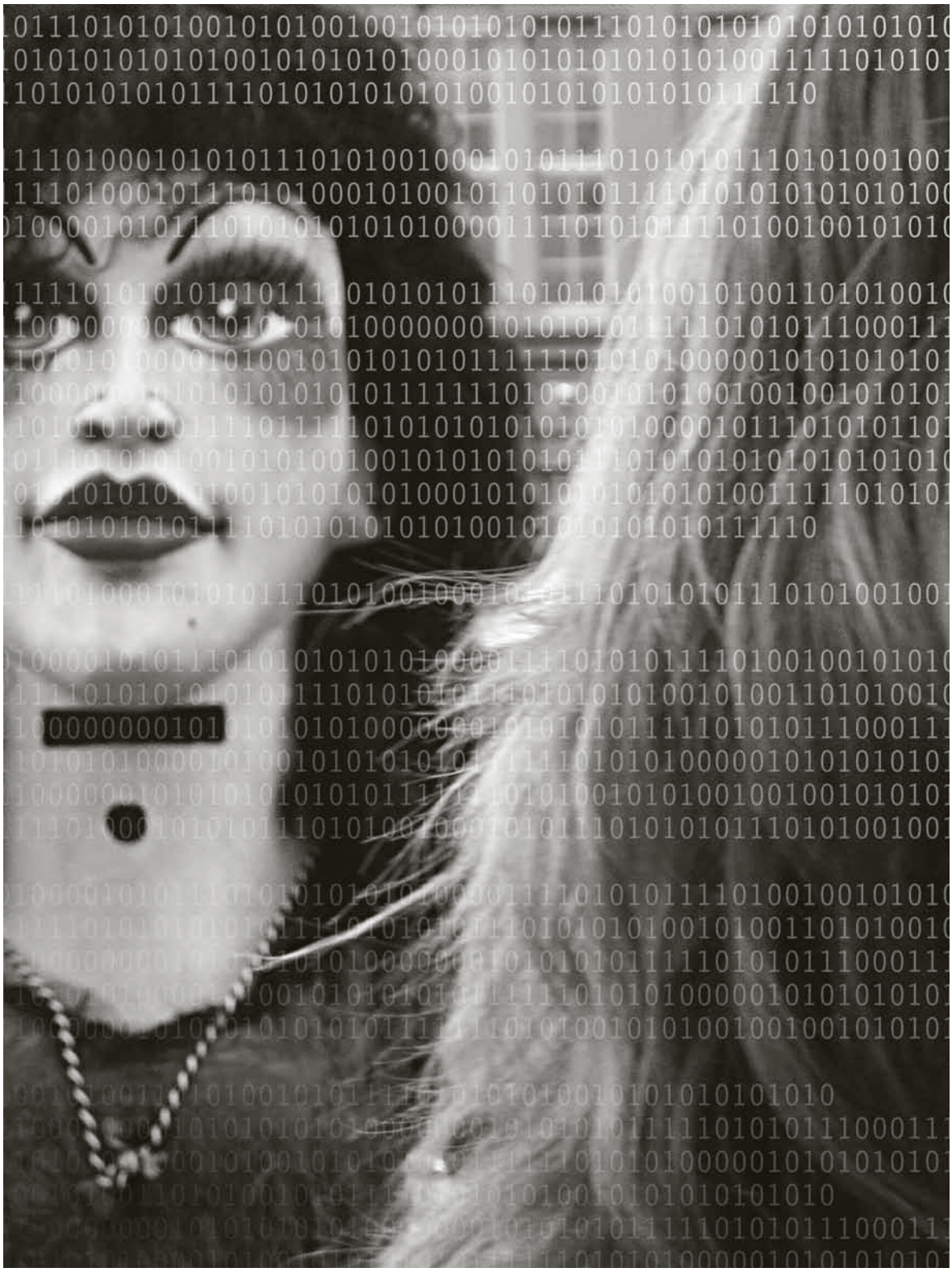
Datenschutzbeauftragter des Kantons Basel-Stadt

Bericht an den Grossen Rat



2012

Inhaltsübersicht

Einleitung

Themen

Der Datenschutzbeauftragte erstattet der Wahlbehörde periodisch Bericht über Umfang und Schwerpunkte der Tätigkeiten, über wichtige Feststellungen und Beurteilungen sowie über die Wirkung des Gesetzes; der Bericht wird veröffentlicht (§ 50 IDG).

Aus dem Alltag

Fälle

Anhang

Einleitung 2012 – Herausforderungen in einer digitalen Welt

Wir leben in einer schönen neuen digitalen Welt. Alles wird einfacher, bequemer. Doch um welchen Preis? Wir bezahlen zum Teil mit unserer Privatheit dafür. Diese Entwicklung betrifft nicht nur die Wirtschaft, sondern auch die staatlichen Behörden. Wie damit umgehen? Es braucht einen mehrdimensionalen Ansatz aus Selbstdatenschutz, Systemdatenschutz und klaren Regulierungen. Damit sind die staatlichen Organe von den rechtsetzenden Gremien bis zu den Rechtsanwendern in der Verantwortung.

Schöne neue digitale Welt!

Bequemer In welch schönem Zeitalter wir doch leben! Mit einem Fingerwischen holen wir uns die Information der ganzen Welt in die Stube. Oder in den Zug. Oder ins Büro. Rund um die Uhr, unabhängig von allen Öffnungszeiten. Ein Problem beim Textschreiben mit Word? Die Antwort ist irgendwo im Internet vorhanden. Eine Wette mit einem Bekannten? Sie finden den Beweis für Ihre Behauptung im Internet. Da gab's doch mal eine «Grease»-Parodie von Didi Hallervorden und Helga Feddersen? Die Suche in Youtube bringt das erhoffte Wiedersehen. Sie suchen ein Waschbrett? Gibt es bei einer Landwirtschaftlichen Genossenschaft in Deutschland. Und Musik kaufen Sie ja schon längstens nicht mehr im Musikgeschäft, sondern im iTunes-Store. Sie wissen nicht, wie Sie zur Burgfelderstrasse 101 gelangen? Ihr Smartphone weiss es. Es kennt auch die beste Verbindung mit dem Drämmli dorthin. Und warum die Fotos vom Smartphone mühsam auf den PC laden? Dropbox oder iCloud sorgen bequem dafür, dass Sie Ihre Fotos auf allen Ihren Devices immer dabei haben. Und dass Sie die Fotos Ihrer Freundin gezeigt haben, können Sie auch gleich allen Ihren Followers weitertwittern.

Auch in der Verwaltung Nicht nur Sie als Privatperson profitieren von den Errungenschaften der digitalen Welt. Cloud Computing verspricht auch Unternehmen und Verwaltungsstellen mehr für weniger Geld. Warum auch mehr ausgeben als nötig? Nicht nur Händler machen sich eBusiness zunutze, auch das Gesundheitswesen soll mit eHealth besser und effizienter werden. Warum am Schalter anstehen – mit eGovernment geht's auch bequem vom Fernsehsessel oder vom Sessellift aus.

Die Kehrseite Klar, Cloud Computing hat auch Schattenseiten. Wie sicher ist es, wenn die Daten irgendwo in der digitalen Weite des Internets beim Vertragspartner des Vertragspartners des Vertragspartners Ihres Providers liegen? Auch Sie hinterlassen beim digitalen Suchen oder Herunterladen Datenspuren. Die interessieren niemanden? Dann googeln Sie mal nach dem Stichwort «Big Data»! 33'600'000 Ergebnisse in 0.22 Sekunden! Big Data ist die Suche nach der Nadel, nicht bloss im Heuhaufen, sondern in allen Heuhaufen auf der ganzen Welt. Indem Sie Datenspuren hinterlassen, ermöglichen Sie den Big Data-Unternehmen, noch grössere Datenberge anzusammeln, die sie auswerten können. «Dank Big Data sehen wir Kundenbedürfnisse voraus», meint etwa Michael Wexler, Leiter Digital Insights bei Citigroup, in einem Interview mit dem gdi[1] und sieht in Big Data grosses Potenzial für den Finanzsektor. Nun werden wir also vorausberechnet! Auch wenn – wie das gdi festhält – der Datenschutz ein Thema bleibe ...

Die Begehrlichkeiten nehmen zu

Nur für den Finanzsektor? Was geht Big Data einen kantonalen Datenschutzbeauftragten an? Der Finanzsektor gehört – bitte schön – nicht zu seinem Aufsichtsbereich. Zu seinem Auftrag gehört aber die permanente Beobachtung der aktuellen nationalen und internationalen Situation im Bereich Datenschutz und Öffentlichkeitsprinzip und damit verbunden das Ergreifen bzw. Initiieren der notwendigen Massnahmen sowie die Information und Sensibilisierung der Öffentlichkeit, der politischen Organe und der öffentlichen Organe. Und mit ihren Datenbergen haben auch die staatlichen Organe viel vor. Nehmen Sie nur mal INDECT. INDECT ist das Akronym des EU-Forschungsprojektes «Intelligent information system supporting observation, searching and detection for security of citizens in urban environment» (zu deutsch: «Intelligentes Informationssystem zur Unterstützung von Überwachung, Suche und Erfassung für die Sicherheit von Bürgern in städtischer Umgebung»), eines von der Europäischen Union im Rahmen des 7. Forschungsrahmenprogramms finanzierten Vorhabens im Bereich der «Intelligenten Sicherheitssysteme». Es startete 2009 und soll fünf Jahre laufen. Nach Wikipedia ist

«Ziel des Projektes (…) nach offiziellen Angaben, durch die automatisierte Auswertung von Bildern aus der Videoüberwachung des öffentlichen Raums und deren Verknüpfung mit Informationen aus dem Internet und einer Vielzahl weiterer Datenquellen auf automatische Weise strafrechtlich relevante Bedrohungen und Taten zu erkennen. Erreicht werden soll dies vor allem durch die Bündelung und automatische, computergestützte Auswertung der Videodaten einer Vielzahl von Überwachungskameras in Echtzeit, um eine ‹präventive Polizeiarbeit› zu ermöglichen. Dazu soll unter anderem durch Computersoftware in den Videoüberwachungsbildern ‹abnormales Verhalten› im öffentlichen Raum erkannt werden. Dazu zählt nach Angaben von Kritikern – neben vielen anderen Kriterien – etwa ‹zu langes Sitzen› oder ‹auf dem Boden sitzen› in einem öffentlichen Verkehrsmittel oder in einem Flughafen, oder das Verlieren des eigenen Gepäcks. Auf Überwachungsbildern als ‹verdächtig› identifizierte Personen sollen durch computergestützte Gesichtserkennung automatisch identifiziert und von ferngesteuerten fliegenden Drohnen mit Überwachungskameras automatisch und selbständig verfolgt werden»[2].

Alles halb so wild? Damit kein Missverständnis aufkommt: Es liegt bei uns kein Drohnenüberwachungskonzept der Kantonspolizei Basel-Stadt (à la INDECT) zur Vorabkontrolle auf dem Tisch! Aber verschiedene Projekte sind in der Schweiz in Diskussion – etwa die automatische Nummernschilderkennung bei allen vorbeifahrenden Autos. Und Themen wie Cloud Computing – das Auslagern von Datenbearbeitungen in die Cloud – beschäftigen Bund und Kantone. Und damit sind wir längstens wieder im Zuständigkeitsbereich des Datenschutzbeauftragten angelangt.

Mehr Möglichkeiten – mehr Verantwortung

Mehrdimensionaler Ansatz Diese Entwicklungen verlangen unsere Aufmerksamkeit. Und sie lassen sich nicht einfach «abwickeln». Es braucht einen mehrdimensionalen Ansatz: Selbstdatenschutz, Systemdatenschutz und klare Regeln.

Selbstdatenschutz Wir alle müssen als Akteure in der schönen neuen Welt unseren Teil der Verantwortung übernehmen. Dazu braucht es einerseits Medienkompetenz, also die Fähigkeit, verantwortungsvoll mit den neuen Medien umzugehen, und andererseits das Bewusstsein für die Werte, die auf dem Spiel stehen.

Systemdatenschutz Datenschutz muss von Anfang an in der Technik mitberücksichtigt werden: «privacy inside»! Hinterher aus Datenschutzgründen Verbesserungen anbringen zu müssen ist regelmässig teurer, als die entsprechenden Vorkehrungen von Anfang an miteinzuplanen. Privatheitsfreundliche Technologien wie etwa Anonymisierung oder Pseudonymisierung müssen rechtzeitig eingebaut werden[3].

Regulierung Schliesslich braucht es auch klare Regeln. Im öffentlichrechtlichen Bereich ist es letztlich an der Politik zu entscheiden, in welche Richtung die Entwicklung im Kanton gehen soll – der Regierungsrat durch die operative Führung und die Rechtsetzung auf Verordnungsstufe, der Grosse Rat durch die Rechtsetzung auf Gesetzesstufe, durch die Budgethoheit und durch die Oberaufsicht.

Umsetzung im Kanton

Selbstdatenschutz Das geht zuallererst uns alle an, die wir uns in der digitalen Welt bewegen. Wir müssen abwägen, ob jede Bequemlichkeit den Verzicht auf unsere Privatheit rechtfertigt. Im privatrechtlichen Bereich läuft die Rechtfertigung weitgehend über unsere Einwilligung. Haben Sie die Allgemeinen Geschäftsbedingungen von Facebook[4] gelesen, bevor Sie einen Account eröffnet haben? Verwenden Sie eine privatheitsschonende Suchmaschine[5] oder eine, die alle Ihre Suchanfragen speichert? Und wollen Sie wirklich jeder App auf Ihrem Smartphone alle Zugriffsrechte («Permissions») einräumen, die sie verlangt?[6] Wie kann, ja soll der Kanton hier einwirken? Beschränkt ist es möglich im Rahmen der Schule: Sie kann den Schüler(inne)n stufengerecht Medienkompetenz vermitteln. Nur: Hat sie die Ressourcen und die Fachkompetenz dazu? Der Datenschutzbeauftragte kann ebenfalls in sehr begrenztem Ausmass Sensibilisierungsarbeit leisten, auch wenn seine Zuständigkeit sich primär auf die Verwaltungsstellen als Datenbearbeiterinnen richtet.

Systemdatenschutz Dieser Aspekt geht nicht nur IT-Entwickler etwas an, sondern auch die Stellen, die IT-Systeme beschaffen und einsetzen. Sie müssen dafür sorgen, dass die Lieferanten «privacy inside» anbieten und liefern. Deshalb ist es unerlässlich, dass im Projekthandbuch phasenentsprechend die Datenschutzanliegen ihren Niederschlag finden. Dem Datenschutzbeauftragten sind Vorhaben, insb. aus dem IT-Bereich, zur Vorabkontrolle vorzulegen[7]. Dadurch können die Datenschutzanliegen frühzeitig in den Projektprozess eingebracht werden. Mit der Schaffung der Stelle eines Informatikrevisors beim Datenschutzbeauftragten konnte die

Fachkompetenz entscheidend erhöht werden. Das nahmen die öffentlichen Organe des Kantons wahr, und seither werden mehr IT-Vorhaben zur Vorabkontrolle vorgelegt (oder vom Datenschutzbeauftragten zur Vorabkontrolle «geholt»). Allerdings ist das Bewusstsein, dass eine Pflicht zur Vorabkontrolle besteht, unterschiedlich ausgeprägt vorhanden. Am Spätherbstanlass «Mein Smartphone, ein Sicherheitsrisiko?» hat der Datenschutzbeauftragte die Gelegenheit benutzt, um auf diese Pflicht hinzuweisen.

Regulierung Eine Art Vorabkontrolle durch den Datenschutzbeauftragten ist auch hier vorgesehen: Er hat Stellung zu nehmen zu Erlassen, die für den Umgang mit Informationen oder den Datenschutz erheblich sind[8]. Wenn das Datenbearbeiten nicht bloss ein «Nebenschauplatz» ist, geschieht auch dieser Einbezug sinnvollerweise rechtzeitig, also nicht erst bei der letzten Vernehmlassung, wo am Grundkonzept kaum mehr etwas geändert werden kann. Letztlich entscheiden aber die rechtsetzenden Behörden in Bund, Kanton und Gemeinden, wie Daten bearbeitet werden sollen, wenn sie die Gesetze und Verordnungen verabschieden. Dabei sind die Persönlichkeitsschutzanliegen auch nicht die einzigen zu berücksichtigenden Aspekte. Wie die Anliegen im Gesamtkontext berücksichtigt werden, hat auch hier mit Wertungen zu tun. Ob eine Steuerstatistik grafisch dargestellt veröffentlicht werden soll, ob ein öffentliches Interesse daran besteht oder ob Sicherheitsinteressen entgegenstehen und vielleicht überwiegen, das können Grosser Rat und Regierungsrat steuern. Wenn der Entscheid für eine Veröffentlichung gefallen ist, dann hat das Statistische Amt dafür zu sorgen, dass die Persönlichkeitsrechte nicht verletzt werden[9], und hierfür kann es den Datenschutzbeauftragten beiziehen.

Wertungen Wie viel ist uns die Privatheit wert? Privatheit ist auf jeden Fall nicht nur Privatsache. Selbstbestimmung ist eine Funktionsvoraussetzung einer auf Freiheit und Verantwortung aufbauenden Gesellschaft. Das Gegenteil von informationeller Selbstbestimmung ist Fremdbestimmung, Manipulation. Wer (zu sehr) manipuliert ist, der kann nicht selbstverantwortlich handeln – und damit scheitert die Idee der auf Freiheit und Verantwortung aufbauenden Gesellschaft. Wer (zu sehr) manipuliert ist, kann nicht als mündige(r) Bürger(in) in der Demokratie verantwortungsvoll mitbestimmen; mit solchen Bürger(inne)n lässt sich kein (demokratischer) Staat machen. Und auch das System der auf Wettbewerb bauenden Marktwirtschaft kann nicht funktionieren, wenn die Konsument(inn)en zu sehr manipuliert sind. Deshalb muss dem Staat die informationelle Selbstbestimmung etwas wert sein. Allerdings hat es der (abstrakte) Wert «Privatheit» schwer, in (konkreten) Interessenabwägungen gegenüber handfesten Interessen im Einzelfall Oberhand zu gewinnen. Eine systematische Datenbekanntgabe hier, eine Videoüberwachung dort, die Erfassung von Daten am dritten Ort – sie lassen sich je im Einzelfall durchaus rechtfertigen. Doch wie viele Datenbekanntgaben, Videoüberwachungen und Datenerfassungen sind zu viel?

Glaubwürdigkeit Um die Frage nach dem Verhältnis zwischen (z.B.) Sicherheit und Freiheit kommt die kantonale Politik nicht herum – auch ausserhalb von Wahlkämpfen. Braucht es mehr Polizistinnen und Polizisten – oder könnte nicht mit mehr technischer Überwachung dasselbe erreicht werden? Das erfordert eine sachliche Diskussion in der Öffentlichkeit – Reflexion ist gefragt, nicht Reflex auf bestimmte Vorkommnisse. Und die Glaubwürdigkeit der Politik leidet, wenn – wie kürzlich im Bund – zuerst vor der Volksabstimmung über den biometrischen Pass hoch und heilig versprochen wird, die Polizei erhalte keinen Zugriff auf die Ausweisdatenbank, und dann, kaum sind die technischen Möglichkeiten geschaffen, diese Versprechen nicht mehr gelten sollen[10]. Präzis diese Glaubwürdigkeit ist hingegen gefragt, wenn beispielsweise – auch im Bund – der Einsatz von Staatstrojanern in engen gesetzlichen Grenzen erlaubt werden soll. Werden hier diese Grenzen auch gerade wieder aufgehoben, sobald die technischen Möglichkeiten geschaffen sind?

Anspruchsvoll Die Aufgabe von Politik und Verwaltung, das Abwägen zwischen den verschiedenen Interessen, denen der Staat gerecht werden muss, ist anspruchsvoll, aber letztlich auch spannend und dankbar. Das Team des Datenschutzbeauftragten engagiert sich gerne dabei.

Öffentlichkeitsprinzip

IDG in Kraft Das Berichtsjahr ist das erste Jahr unter der Geltung des neuen Informations- und Datenschutzgesetzes (IDG). Verständlicherweise ist eine Bewertung noch nicht möglich. Haben sich die neuen Regelungen bewährt? Hat die Verwaltung im Kanton Basel-Stadt den Paradigmenwechsel vom Geheimhaltungsprinzip mit Öffentlichkeitsvorbehalt zum Öffentlichkeitsprinzip mit Geheimhaltungsvorbehalt vollzogen?

Erste Erkenntnisse Trotzdem: Einiges lässt sich bereits feststellen, weil die ersten Zahlen vorliegen. Erstens wurde auch die baselstädtische Verwaltung von Kanton und Gemeinden nicht durch einen Ansturm von Zugangsgesuchen lahmgelegt; 48 mal wurde im ersten Jahr ein schriftliches Gesuch um Zugang zu Informationen, die bei

einem kantonalen öffentlichen Organ vorhanden sind, gestellt. Die Zahlen in der Statistik zeigen aber auch, dass die Verwaltung den Schritt zum (reaktiven) Öffentlichkeitsprinzip mitgetan hat: 77% der Gesuche wurden ganz oder teilweise gutgeheissen (über 10% waren beim Jahreswechsel noch nicht entschieden). Indem die nicht klassifizierten Regierungsratsbeschlüsse standardmässig publiziert werden, ist auch ein Schritt zum (pro-)aktiven Öffentlichkeitsprinzip gemacht. Der Datenschutzbeauftragte wird die Entwicklung im Auge behalten[11].

Tätigkeitsbericht

Einen Ausschnitt aus dem, was der Datenschutzbeauftragte im Jahr 2012 im Auge behalten hat, soll in diesem Tätigkeitsbericht dargestellt werden. Zwei *Themen* werden vertieft behandelt: IT-Governance (10 f.) und die unterschiedlichen Informationszugangsrechte (das verfahrensrechtliche Akteneinsichtsrecht, das datenschutzrechtliche Recht auf Zugang zu den eigenen Personendaten und das Recht auf Zugang zu Informationen nach dem Öffentlichkeitsprinzip, 12 ff.). Anschliessend folgt die Kurzdarstellung einer Auswahl von Themen *aus dem Alltag* des Datenschutzbeauftragten, aus der Beratungstätigkeit (18 ff.) und aus der Kontrolltätigkeit (28 f.), gefolgt von der Statistik (30 f.). Daran schliessen acht verschiedene *Fälle* an (34 ff.).

Zum Schluss

Danke! Unsere Aufgabe zum Schutz der Privatheit der Bürgerinnen und Bürger, über die öffentliche Organe Daten bearbeiten, könnten wir nicht erfolgreich erfüllen ohne die Unterstützung vieler Menschen und Institutionen. Mein Dank gilt deshalb

— der Bevölkerung und den staatlichen Institutionen für das entgegengebrachte Vertrauen;

— allen, die mit wachem Sinn und offenen Augen durch die Welt gehen, sich bewusst sind, dass verlorene Privatheit nicht im Laden um die Ecke oder im nächsten Online-Shop ersetzt werden kann, und deshalb mit Informationen über sich und über andere sorgsam umgehen;

— allen Privaten sowie Mitarbeiter(inne)n der Behörden von Kanton und Gemeinden, welche sich vertrauensvoll mit Datenschutzfragen an uns wenden und sich vielleicht wegen der Arbeitslast gedulden müssen, bis sie eine Antwort erhalten;

— allen Mitarbeiter(inne)n der Verwaltung, der öffentlichrechtlichen Anstalten und der Gerichte, die mithelfen, datenschutzkonforme Lösungen zu finden und umzusetzen;

— den Kolleg(inn)en der Ombudsstelle, der Finanzkontrolle und des Parlamentsdienstes für die unkomplizierte Zusammenarbeit;

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

— den Volontärinnen und dem Volontär – Nadine Battilana, Alexandra Büche und Angelo Imperiale – für ihre kritische Neugier und ihre aktive Mitarbeit

— und last but not least meinem Team – Markus Brönnimann, Sandra Husi-Stämpfli, Carmen Lindner, Daniela Waldmeier und Barbara Widmer, das mit unverändert grossem Engagement, mit bereichernden Diskussionen und konstruktiven Vorschlägen unsere Arbeit erleichtert und vorangebracht hat.

Beat Rudin, Datenschutzbeauftragter

1 Newsletter des Gottlieb Duttweiler-Instituts, <http://www.gdi.ch/de/Think-Tank/Trend-News/Detail-Page/Dank-Big-Data-sehen-wir-Kunden-beduerfnisse-voraus>.
2 <http://de.wikipedia.org/wiki/INDECT>.
3 § 14 IDG; «privacy by design» und «privacy by default» lauten Stichworte, welche die EU auch in ihrer neuen Datenschutzgesetzgebung verankern will, vgl. zu den EU-Revisionsbemühungen Sandra Husi-Stämpfli, EU: Zu neuen Ufern lockt ein Tag, digma 2012, 38 ff.
4 Bruno Baeriswyl, Kleingedrucktes unter der Lupe, Die Allgemeinen Geschäftsbedingungen von Sozialen Netzwerken versprechen keinen Datenschutz, digma 2010, 56 ff.
5 z.B. <http://www.ixquick.com/deu>.
6 Siehe «Sieben Goldene Regeln zur Smartphone-Sicherheit»: <http://www.dsb.bs.ch> über Veranstaltungen | Spätherbst-Anlass «Mein Smartphone, ein Sicherheitsrisiko?».
7 § 13 IDG.
8 § 44 lit. f IDG.
9 Vgl. Fall 6.
10 Vgl. Beat Rudin, Ein selten schönes Eigentor!, digma 2013, 44.
11 Vgl. hinten S. 30.

Themen

Thema 1 IT-Governance: Verantwortung und Informationssicherheit

Thema 2 Öffentlichkeitsprinzip – Zugang zu den eigenen Personendaten – Akteneinsichtsrecht

Thema 1

IT-Governance: Verantwortung und Informationssicherheit

Ohne Informations- und Kommunikationstechnologie kann der Staat heute seine Aufgaben nicht mehr erfüllen. Die Abhängigkeit von dieser Technologie bringt aber auch Risiken mit sich. Nach dem IDG trägt die Dateneignerin die Verantwortung für die Informationssicherheit. Mit der Zuordnung der Verantwortung alleine ist es jedoch noch lange nicht getan. Es braucht ein klares Commitment der obersten Führung dazu, verbindliche Regeln, geeignete Strukturen sowie bewusste und nachvollziehbare Entscheidungen.

Ausgangslage

Durchdringung Die Verwaltungen von Kanton und Gemeinden sind heute ohne Informations- und Kommunikationstechnologie (IKT) nicht mehr denkbar[1]. Dabei ist die IKT nicht einfach ein Werkzeug wie vielleicht früher die Schreibmaschine – man hätte die Verfügung auch von Hand schreiben können, wenn die Schreibmaschine ausgefallen wäre. Die Geschäftsprozesse der Verwaltung werden vielmehr von IKT regelrecht durchdrungen; viele staatliche Dienstleistungen können ohne die IKT gar nicht mehr erbracht werden.

Heterogenität Dabei ist sowohl die IKT-Landschaft als auch die Organisation und die Art der zu erbringenden Leistungen alles andere als homogen. Es herrscht ein «föderaler» Aufbau: Die Informatik wird je nach Aufgabenstellung von der Dienststelle selber, zentralisiert auf Departementsstufe oder gesamtkantonal betrieben. Gesamtkantonal zentralisierte Leistungen werden von den Zentralen Informatikdiensten (ZID) oder externen Dritten bezogen. Die Informatik trifft auf föderalistische und äusserst unterschiedliche Strukturen und Kulturen, auf sehr hierarchische wie etwa bei der Kantonspolizei oder auf eher partizipative wie bei den Schulen. Überlagert wird die Heterogenität durch die Tendenz, dass die IKT bedingt durch erhoffte Kostenoptimierung durch Skaleneffekte oder Verbesserung der Professionalität zunehmend zentralisiert und teilweise auch ausgelagert (Outsourcing) wird.

Schwierigkeit Diese Ausgangslage führt unweigerlich dazu, dass es schwierig bis unmöglich ist, die Risiken, die mit der IKT verbunden sind, in der Gesamtheit zu überblicken und im Griff zu halten. Es kann nicht gesagt werden, dass die Risiken aus dem Ruder laufen – aber auch nicht das Gegenteil. Eine Aussage zum Stand der Risiken ist schlicht nicht möglich, wenn beispielsweise ein Anwendungs- und ein Projektportfolio nur ansatzweise und nicht aktualisiert vorhanden sind.

Verantwortung nach IDG

Grundregel Das IDG legt die Verantwortlichkeit grundsätzlich fest: Verantwortlich für den Umgang mit den Informationen ist das öffentliche Organ, das zur Erfüllung seiner gesetzlichen Aufgabe Informationen (und insbesondere Personendaten) bearbeitet[2]. Die Verantwortung bleibt auch beim öffentlichen Organ, wenn es die Informationen bearbeiten lässt, also eine Leistung (beispielsweise IKT-Leistungen) von einem (verwaltungsinternen oder -externen) Dritten bezieht[3]. Zu dieser Verantwortung gehört auch die Informationssicherheit: Das öffentliche Organ hat die Informationen durch angemessene organisatorische und technische Massnahmen zu schützen[4].

Nicht beliebig Die heterogene Ausgangslage in Kombination mit dem benötigten Fachwissen im Bereich der Informationssicherheit macht klar, dass die Verantwortung nicht durch jedes öffentliche Organ (z.B. durch jede einzelne Dienststelle), das zur Erfüllung seiner Aufgabe IKT einsetzt und/oder IKT-Leistungen bezieht, nach eigenem Gutdünken wahrgenommen werden kann. Das öffentliche Organ kann auch nicht nach Belieben selber entscheiden, was angemessene technische oder organisatorische Massnahmen zum Schutz seiner Informationen sind und welche verbleibenden Risiken es übernehmen will.

Lösungsansatz

Grundsätzlich Vordringlich ist, dass im Bereich der Informationssicherheit die Aufgaben, Kompetenzen und Verantwortlichkeiten klar zugewiesen werden. Das beginnt bei der Dateneignerin (siehe sogleich) und geht über die verschiedenen Instanzen, im Kanton bis zum Regierungsrat als operativer Leitung. Wie die Erfahrung der letzten Jahre gezeigt hat, ist bei etlichen Daten nicht einmal geklärt, welches Organ Dateneignerin ist. Weiter ist der «Risikoappetit» zu bestimmen. Dazu wird ein durchgängiges Risikomanagement, wiederum bis hin zum Regierungsrat, nötig.

Verantwortung der Dateneignerin Die Dateneignerin – das öffentliche Organ, das die Informationen zur Aufgabenerfüllung bearbeitet oder bearbeiten lässt – muss vorerst den Schutzbedarf «ihrer» Informationen in Bezug auf die verschiedenen Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit, Zurechenbarkeit und Nachvollziehbarkeit)[5] beurteilen. Sodann muss sie dafür sorgen, dass die angemessenen organisatorischen und technischen Massnahmen zur Erreichung der Schutzziele getroffen werden. Das ist schon nicht einfach, wenn das Bearbeiten vollständig in ihrer Hand liegt (sie beispielsweise die Informatik selber betreibt), weil häufig das dazu notwendige spezifische Fachwissen nicht vorhanden ist. Auch kann es – aus einer Gesamtsicht – nicht allein bei der Dateneignerin liegen, die Angemessenheit der Massnahmen zu bestimmen. Geradezu unrealistisch wird es, wenn es allein an ihr liegen würde, sicherzustellen und durch Audits zu überprüfen, dass «ihre» Leistungserbringer (z.B. die Departementsinformatik, die ZID oder externe Provider wie die Swisscom) die notwendigen Massnahmen treffen.

Frameworks Mit diesem Problem steht der Kanton Basel-Stadt nicht allein da. Sowohl andere Gemeinwesen als auch die Privatwirtschaft sind damit konfrontiert. Aus diesem Grund gibt es auch internationale Regelwerke (Frameworks), welche (u.a.) notwendige Prozesse beschreiben[6], Massnahmen vorschlagen[7] oder Metriken zur Bestimmung der Zielerreichung anbieten[8]. Es braucht also nicht alles erfunden zu werden – und trotzdem reicht es nicht, sich an solchen Frameworks zu orientieren, um das Problem zu lösen. Frameworks sind keine Wunderheilmittel; jedes Framework hat sein «Spezialgebiet», ist in der Regel «generisch und/oder abstrakt» und muss immer auf die Gegebenheiten der Organisation angepasst werden. Notwendig sind also erstens ein klares Bekenntnis von oberster Ebene, zweitens angemessene organisatorische Strukturen, denen die Aufgaben, Kompetenzen und Verantwortlichkeiten zugeteilt werden und drittens bewusste und nachvollziehbare Entscheidungen.

Regelungen und Organisation Die Gesamtverantwortung liegt im Kanton beim Regierungsrat als operativer Leitung. Er hat die nötigen Regelungen[9] zu erlassen und die Organisation zu schaffen, die sicherstellt, dass er seine Verantwortung übernehmen kann. Zu regeln sind etwa die Aufgaben, Kompetenzen und Verantwortlichkeiten der verschiedenen Organe und Rollen in der Informatik, allenfalls auch die Standards und Frameworks, nach denen gearbeitet werden soll. Festzulegen und tatsächlich umzusetzen ist etwa, in welchen Prozessen und mit welchen Qualitätsansprüchen an die Prozesse beispielsweise die Strategie(weiter)entwicklung stattfindet. Organisatorisch braucht es etwa ein Organ, das Standards festlegt, also beispielsweise bestimmt, welche Massnahmen zwingend und in welcher Form umzusetzen sind, um den Grundschutz sicherzustellen usw. Schliesslich muss die Sorge um die Informationssicherheit in kantonale Risikomanagement-, Governance- bzw. IT-Governance-Vorkehren eingebettet sein.

Rolle des DSB Der Datenschutzbeauftragte wacht über die Einhaltung der Bestimmungen betreffend den Umgang mit Informationen[10]. Aus diesem Grund sehen wir es als unsere Aufgabe, auf die Dringlichkeit hinzuweisen, die Verantwortung für die Informationssicherheit nach § 8 IDG wahrzunehmen. Es gibt in diesem Bereich etliche Baustellen, auf denen die Arbeiten dringend voranzutreiben sind: insb. die Definition des Grundschutzes, die Regelung der Verantwortlichkeit, die Festlegung der Standards und Frameworks, aber auch das Identity and Access Management (IAM) mit einer stärkeren Authentisierung und die Speicherung und elektronische Übermittlung von besonderen Personendaten.

Dringlichkeit Das Inkrafttreten des IDG wurde vom Regierungsrat festgelegt, sobald die konkretisierenden Bestimmungen in der Informations- und Datenschutzverordnung (IDV) beschlossen waren. Es wurde damals darauf verzichtet, das Inkrafttreten des IDG auch von der Anpassung der Informatiksicherheitsverordnung (ISV) abhängig zu machen, weil diese nicht unter Zeitdruck, sondern eingebettet in die Regelung der IT-Governance erfolgen sollte. Damit war allerdings nicht gemeint, dass die Anpassung der ISV auf die lange Bank geschoben werden dürfe. Es ist dringend, die Risiken in Bezug auf die Abhängigkeit von der IKT aktiv anzugehen. Es ist ja nicht nötig, damit zu warten, bis – wie im Bundesnachrichtendienst – ein Mitarbeiter mit heiklen Informationen auf einer Festplatte hinausspaziert …

—

1 Vgl. dazu schon TB 2010, 19 ff.
2 § 6 IDG (Verantwortung).
3 § 7 Abs. 2 IDG (Bearbeiten im Auftrag).
4 § 8 IDG (Informationssicherheit).
5 § 8 Abs. 2 IDG.
6 Z.B. ISO 2700x (Normen der Internationale Organisation für Normung) und COBIT (Control Objectives for Information and Related Technology der Information Systems Audit and Control Association ISACA).
7 Z.B. ISO 2700x oder IT-Grundschutz-Kataloge des (deutschen) Bundesamtes für Sicherheit in der Informationstechnik (BSI).
8 Z.B. COBIT.
9 Vgl. dazu auch Barbara Widmer, Informationssicherheit in der Gesetzgebung, digma 2012, 124 ff.
10 § 44 lit. a IDG (Aufgaben).

Thema 2 Öffentlichkeitsprinzip – Zugang zu den eigenen Personendaten – Akteneinsichtsrecht

Es ist nicht einerlei, wenn sich jemand an ein öffentliches Organ wendet und Zugang zu Informationen verlangt. Das öffentliche Organ muss unterscheiden, ob es sich um ein auf das Öffentlichkeitsprinzip gestütztes Zugangsgesuch, um ein persönlichkeitsrechtlich begründetes Gesuch um Zugang zu den eigenen Personendaten oder um ein verfahrensrechtliches Akteneinsichtsgesuch handelt.

Problemstellung

Drei Zugangsrechte Schon unter dem früheren Datenschutzgesetz konnte jemand unter zwei Titeln Zugang zu Informationen verlangen: einerseits als (persönlichkeits- oder datenschutzrechtliches) Recht auf Auskunft und Einsicht und andererseits als (verfahrensrechtliches) Akteneinsichtsrecht nach dem Organisationsgesetz. Mit dem Inkrafttreten des Informations- und Datenschutzgesetzes kommt noch ein dritter Titel dazu: das Recht auf Zugang zu Informationen, die bei einem öffentlichen Organ vorhanden sind (Öffentlichkeitsprinzip). Das datenschutzrechtliche Recht auf Auskunft und Einsicht hat zudem eine Namensänderung erfahren: Es heisst neu Recht auf Zugang zu den eigenen Personendaten.

Nicht dasselbe Diese drei Zugangsrechte sind auseinanderzuhalten, weil sie sich in Bezug auf die Rechtsgrundlagen und den verfolgten Zweck, die berechtigten Personen, den Umfang und die Möglichkeiten zur Einschränkung sowie weitere Modalitäten (z.B. die Kostenpflicht) unterscheiden[1]. Das wurde beispielsweise zum Thema, als die Frage an den Datenschutzbeauftragten herangetragen wurde, ob eine betroffene Person tatsächlich zweimal innert wenigen Monaten kostenlos Zugang zu ihren eigenen Personendaten verlangen könne[2]. Erst nach diversen Nachfragen hat sich herausgestellt, dass es sich genau betrachtet gar nicht um Gesuche um Zugang zu den eigenen Personendaten gehandelt hat: Das erste Gesuch wurde in einem laufenden Verfahren um Zusprechung einer staatlichen Unterstützung und das zweite im folgenden Verfahren betreffend den Regressanspruch (die betroffene Person war inzwischen zu Vermögen gekommen) gestellt. Damit handelte es sich um zwei verfahrensrechtliche Akteneinsichtsgesuche – zwar der selben Partei, aber in zwei verschiedenen Verwaltungsverfahren.

Inwiefern? In der Folge sollen die drei Zugangsrechte mit ihren Unterschieden dargestellt werden, bevor das Verhältnis der drei zueinander genauer betrachtet wird.

Verfahrensrechtliches Akteneinsichtsrecht

Rechtsgrundlagen Das verfahrensrechtliche Akteneinsichtsrecht als Teilgehalt des Anspruchs auf rechtliches Gehör stützt sich auf Art. 29 Abs. 2 BV und § 12 lit. b KV; konkretisiert wird es gemeinhin in den Verwaltungsverfahrensgesetzen[3]. In unserem Kanton mit seiner höchst rudimentären Verwaltungsverfahrensregelung bestimmt § 38 Abs. 2 OG nur: «Das Verfahren, das dem Erlass einer Verfügung vorausgeht, hat in jedem Falle den grundlegenden rechtsstaatlichen Prinzipien für das Verwaltungsverfahren zu genügen, insbesondere die Grundsätze der Akteneinsicht und des rechtlichen Gehörs zu gewährleisten.»

Zweck Das Akteneinsichtsrecht dient primär der Verfahrensgerechtigkeit: Die betroffene Person erhält die Möglichkeit, die Sachgerechtigkeit von Entscheidung und Begründung zu prüfen und so wirksam und sachbezogen Stellung nehmen zu können, was die Chancen für eine richtige Wahrheits- und Rechtsfindung erhöht.

Berechtigte Personen Berechtigt zur Akteneinsicht sind grundsätzlich die *Parteien* im Verwaltungsverfahren, in dessen Akten die Einsicht verlangt wird.

Gegenstand Das Akteneinsichtsrecht umfasst alle Verfahrensakten, die dem öffentlichen Organ im fraglichen Verfahren als Grundlage für die Entscheidung dienen – also nicht nur solche, die Informationen über die gesuchstellende Partei selbst enthalten. Was nicht entscheidungsrelevant ist, ist nicht Gegenstand des verfahrensrechtlichen Akteneinsichtsrechts. Hier stellt sich dafür die Frage, was mit solchen Akten generell

zu geschehen hat[4]. Wir empfehlen, solche Aktenstücke nicht ins Dossier aufzunehmen, sondern der einreichenden Person zurückzusenden.

Einschränkungen Der Anspruch auf Einsicht in Verfahrensakten geht – analog zur Baselbieter Regelung[5] – nur soweit, als nicht überwiegende öffentliche oder private Interessen, insbesondere von Gegenparteien, ihre Geheimhaltung erfordern. Der Inhalt eines Aktenstückes, in welches die Einsicht verweigert wird, muss jedoch soweit bekannt gegeben werden, als dies ohne Verletzung der zu schützenden Interessen möglich ist[6]. Solange das Interesse einer noch nicht abgeschlossenen amtlichen Untersuchung es erfordert, kann die Akteneinsicht aufgeschoben werden[7].

Datenschutzrechtliches Recht auf Zugang zu den eigenen Personendaten

Rechtsgrundlagen Das datenschutzrechtliche (oder: persönlichkeitsrechtliche) Recht auf Zugang zu den eigenen Personendaten[8] stützt sich auf Art. 13 Abs. 1 BV und § 11 Abs. 1 lit. j KV, welche das Grundrecht auf informationelle Selbstbestimmung garantieren. In der Kantonsverfassung wird es sogar ausdrücklich als Teilgehalt des Grundrechts auf Datenschutz erwähnt («Recht auf Einsichtnahme»). Konkretisiert wird das Recht in § 26 IDG.

Zweck Das Recht auf Zugang zu den eigenen Personendaten dient dem Zweck, die Persönlichkeitsrechte der betroffenen Person zu schützen. Sie kann erfahren, ob und, falls ja, welche Daten über sie bearbeitet werden; dadurch wird sie auch erst in die Lage versetzt, ihre weiteren Rechte wahrzunehmen[9].

Berechtigte Personen Berechtigt zum Zugang zu den eigenen Personendaten ist jede Person, über die ein öffentliches Organ Personendaten bearbeitet, unabhängig davon, ob sie in ein Verwaltungsverfahren involviert ist oder war oder nicht.

Gegenstand Das Recht auf Zugang zu den eigenen Personendaten umfasst alle Personendaten, die vom angefragten öffentlichen Organ über die gesuchstellende Person bearbeitet werden, unabhängig davon, ob es Tatsachendarstellungen oder Werturteile sind.

Einschränkungen Das öffentliche Organ hat den Zugang zu Informationen im Einzelfall ganz oder teilweise zu verweigern oder aufzuschieben, wenn eine besondere gesetzliche Geheimhaltungspflicht oder ein überwiegendes öffentliches oder privates Interesse entgegensteht[10].

Das Recht auf Zugang zu den eigenen Personendaten dient dem Zweck, die Persönlichkeitsrechte der betroffenen Person zu schützen.

Eine Geheimhaltungsbestimmung, die den Zugang der gesuchstellenden Person zu ihren eigenen Personendaten untersagt, gibt es im kantonalen Recht nicht. Da grundsätzlich Informationen über andere Personen nicht unter dieses Zugangsrecht fallen, scheinen entgegenstehende private Interessen auf den ersten Blick irrelevant. Informationen können jedoch auch mehrere Personen betreffen: So sagt z.B. die Aussage einer Person über eine andere Person über beide Personen etwas aus: Einerseits natürlich über die durch die Aussage direkt betroffene Person, andererseits aber auch über die Informantin bzw. den Informanten: Wer hat informiert? Woran stört sich diese Person? Vielleicht auch: Warum hat sie informiert? Deshalb kann es trotzdem nötig sein, eine Interessenabwägung vorzunehmen. Eine ausdrückliche Regelung enthält das IDG zum Schutz vor einem sog. Aufklärungsschaden: Würde der Zugang zu den eigenen Personendaten im medizinischen oder psychiatrischen Bereich nach der Beurteilung des öffentlichen Organs die gesuchstellende betroffene Person zu stark belasten, kann er einer Person ihres Vertrauens gewährt werden; sofern die betroffene Person es ausdrücklich wünscht, ist ihr aber direkt und umfassend Zugang zu ihren Personendaten zu gewähren[11].

Modalitäten Für den Zugang zu den eigenen Personendaten dürfen in keinem Fall Kosten erhoben werden[12].

Zugang zu Informationen (Öffentlichkeitsprinzip)

Rechtsgrundlagen Das Recht auf Zugang zu Informationen, die bei einem öffentlichen Organ vorhanden sind, stützt sich auf § 75 Abs. 2 KV (Öffentlichkeitsprinzip in seiner reaktiven Ausformung). Konkretisiert wird es in § 25 IDG. Beim Öffentlichkeitsprinzip steht nicht das Zugangsinteresse einer bestimmten Person im Vordergrund, sondern jenes der Öffentlichkeit; das Zugangsrecht ist ein sog. «Jedermanns-Recht». >

Zweck Bezweckt wird mit dem Zugangsrecht nach dem Öffentlichkeitsprinzip, das Handeln der öffentlichen Organe transparent zu gestalten und damit die freie Meinungsbildung und die Wahrnehmung der demokratischen Rechte zu fördern[13].

Berechtigte Personen Der Anspruch auf Zugang zu Informationen, die bei einem öffentlichen Organ vorhanden sind, steht jeder Person zu[14], unabhängig davon, ob sie irgendeinen Bezug zur gewünschten Information hat oder nicht.

Gegenstand Das Recht auf Informationszugang umfasst alle Informationen, die bei einem öffentlichen Organ[15] vorhanden sind, ausgenommen Aufzeichnungen, die noch nicht fertig gestellt sind[16].

Einschränkungen Das öffentliche Organ hat den Zugang zu Informationen im Einzelfall ganz oder teilweise zu verweigern oder aufzuschieben, wenn eine besondere gesetzliche Geheimhaltungspflicht oder ein überwiegendes öffentliches oder privates Interesse entgegensteht[17]. Ausserdem legt das IDG fest, dass beim Zugang zu Informationen im Sinne des Öffentlichkeitsprinzips alle Personendaten zu anonymisieren sind[18]. Ziel ist die Transparenz des Verwaltungshandelns, nicht die gläserne Bürgerin oder der gläserne Bürger[19]!

Der Anspruch auf Zugang zu Informationen, die bei einem öffentlichen Organ vorhanden sind, steht jeder Person zu, unabhängig davon, ob sie einen Bezug zur Information hat oder nicht.

Modalitäten Das IDG sieht vor, dass für das Verfahren auf Zugang zu Informationen in der Regel keine Gebühren erhoben werden[20]. Eine angemessene Gebühr nach Aufwand kann erhoben werden bei aufwändigen Verfahren, wie bei komplizierten Verhältnissen oder bei umfangreichen Anonymisierungen von Informationen, und für die Anfertigung von Kopien oder sonstigen Datenträgern für die gesuchstellende Person[21]. Die IDV enthält den entsprechenden Gebührenkatalog[22].

Verhältnis zueinander

Öffentlichkeitsprinzip Wie stehen die drei Zugangsrechte zueinander? Einfach ist das Auseinanderhalten von Öffentlichkeitsprinzip einerseits und den anderen beiden Zugangsrechten andererseits. Bei jenem ist keinerlei Bindung zwischen den gewünschten Informationen und der gesuchstellenden Person vorausgesetzt, und es werden keine Personendaten herausgegeben. Bei diesen muss die gesuchstellende Person entweder Partei im fraglichen Verfahren oder betroffene Person sein, über welche das öffentliche Organ Personendaten bearbeitet. Das Recht auf Zugang nach Öffentlichkeitsprinzip kann deshalb jederzeit – unabhängig von einem Verfahren – und von jeder Person – unabhängig davon, ob die Informationen in irgendeinem Bezug zu ihr stehen – geltend gemacht werden, auch vor, nach oder parallel zu einem Gesuch nach einem der anderen beiden Zugangsrechte.

Akteneinsichtsrecht oder Datenschutz-Zugangsrecht? Schwieriger ist es, das verfahrensrechtliche Akteneinsichtsrecht und das Recht auf Zugang zu den eigenen Personendaten auseinanderzuhalten. Primär ist darauf abzustellen, in welchem Rahmen und mit welcher Begründung oder mit welchem Ziel ein Gesuch gestellt wird. In einem laufenden Verfahren steht wohl das Akteneinsichtsrecht im Vordergrund, ausserhalb eines solchen Verfahrens das datenschutzrechtliche Zugangsrecht. Spricht das Gesuch von Daten zur Person («alles, was über mich in den Akten steht»), dann ist ebenfalls eher der Zugang zu den eigenen Personendaten gemeint; spricht es von anderen Akten («die Stellungnahme des Einsprechers»), dann geht es um das Akteneinsichtsrecht. Gibt die gesuchstellende Person als Zweck die Sachgerechtigkeit der Entscheidung an, dann steht ein Akteneinsichtsgesuch im Vordergrund; falls es erkennbar um den Schutz der Persönlichkeitsrechte (und allenfalls um weitere Rechte der betroffenen Person) geht, dürfte es sich um das datenschutzrechtliche Zugangsrecht handeln.

Beides? Wenn eine Person in einem Verwaltungsverfahren Partei ist und über sie Daten bearbeitet werden, dann kann es durchaus sein, dass beide Rechtsansprüche in Frage kommen. Es kann auch sein, dass beide Ansprüche miteinander oder zeitlich nacheinander geltend gemacht werden. Das öffentliche Organ hat dann beide Gesuche zu beantworten. Es ist dabei durchaus möglich, dass zu Informationen, die beim einen Zugangsrecht nicht herausgegeben werden müssten (z.B. Daten über andere Personen beim datenschutzrechtlichen Recht auf Zugang zu

den eigenen Personendaten), nach dem anderen Zugangsrecht uneingeschränkt Einsicht gewährt werden muss (z.B. weil es Informationen über diese andere Person als Gegenpartei in entscheidrelevanten Akten eines Verwaltungsverfahrens sind). Die beiden Rechte schliessen sich nicht aus, sondern bestehen kumulativ nebeneinander.

Das verfahrensrechtliche Recht auf Akteneinsicht und das Recht auf Zugang zu den eigenen Personendaten schliessen einander nicht aus, sondern bestehen kumulativ nebeneinander.

Empfehlung Kann bei einem Gesuch nicht eindeutig entschieden werden, auf welches Zugangsrecht sich der oder die Gesuchsteller(in) stützt, so dass beide Ansprüche geprüft werden müssen, kann das öffentliche Organ dies in demselben Akt tun. Wir empfehlen in jedem Fall, die beiden Behandlungen klar zu gliedern, also methodisch korrekt jeweils die Anspruchsvoraussetzungen und die Einschränkungsmöglichkeiten zu prüfen und – falls verfügt werden muss – im Entscheiddispositiv separat aufzuführen.

Unterstützung Der Datenschutzbeauftragte unterstützt die öffentlichen Organe, wenn es darum geht, Zugangsgesuche richtig einzuordnen und korrekt zu behandeln.

—

1 Vgl. dazu (nicht spezifisch auf das baselstädtische Recht bezogen) Rainer J. Schweizer/Dean Kradolfer/Patrick Sutter, Das Verhältnis zwischen datenschutzrechtlichen Persönlichkeitsrechten, Verfahrensgerechtigkeit und Amtsöffentlichkeit zueinander, in: Bruno Baeriswyl/Beat Rudin (Hrsg.), Perspektive Datenschutz, Praxis und Entwicklungen in Recht und Technik, Zürich 2002, 235 ff.
2 Das baselstädtische Recht hat diesbezüglich keine Regelung, wie sie etwa der Bund kennt: Nach Art. 2 VDSG/Bund entfällt die Kostenlosigkeit des Zugangs zu den eigenen Personendaten, wenn der antragstellenden Person in den zwölf Monaten vor dem Gesuch die gewünschten Auskünfte bereits mitgeteilt wurden und kein schutzwürdiges Interesse an einer neuen Auskunftserteilung nachgewiesen werden kann.
3 Z.B. im Bund in Art. 26 ff. VwVG/Bund; im Kanton Basel-Landschaft in § 14 VwVG/BL und in den §§ 1 ff. Vo VwVG/BL.
4 Beispiel: Was passiert mit der Kopie der Scheidungsklage, die der Ex-Mann einer Ausländerin dem Migrationsamt zuschickt, die aber für den weiteren Entscheid über den Aufenthaltsstatus der Ausländerin irrelevant ist?
5 Art. 27 Abs. 1 VwVG/Bund.
6 § 14 Abs. 1 und 1 VwVG/BL.
7 So für den Bund Art. 27 Abs. 1 lit. c VwVG/Bund.
8 Vgl. dazu auch TB 2011, 21 ff.
9 § 27 IDG: Recht auf Berichtigung unrichtiger Personendaten, Recht auf Unterlassung des widerrechtlichen Bearbeitens von Personendaten, Recht auf Beseitigung der Folgen unrechtmässigen Bearbeitens von Personendaten und Recht auf schriftliche Feststellung der Widerrechtlichkeit des Bearbeitens von Personendaten.
10 § 29 Abs. 1 IDG.
11 § 29 Abs. 4 IDG.
12 § 36 Abs. 2 IDG.
13 § 1 Abs. 2 lit. a IDG.
14 § 25 Abs. 1 IDG.
15 Ausgenommen sind einzig Private, die zu eine öffentlichen Organ werden, weil und soweit ihnen von Kanton oder Gemeinden die Erfüllung öffentlicher Aufgaben übertragen ist (§ 25 Abs. 1 i.V.m. § 3 Abs. 1 IDG).
16 § 25 Abs. 1 IDG, konkretisiert in § 17 IDV.
17 § 29 Abs. 1 IDG.
18 § 30 IDG.
19 Ratschlag 08.0637.01, 3, 7, 49.
20 § 36 Abs. 1 IDG.
21 § 36 Abs. 2 lit a und b IDG.
22 § 28 IDV (Aufwändige Verfahren [§ 36 Abs. 2 lit. a IDG]) bzw. § 29 IDV (Reproduktion [§ 36 Abs. 2 lit. b IDG]).

Aus dem Alltag

Einblicke in die Beratungstätigkeit

Einblicke in die Kontrolltätigkeit

Statistische Auswertungen

Aus dem Alltag

Einblicke in die Beratungstätigkeit

Der Aufgabenstrauss des Datenschutzbeauftragten ist bunt und bringt täglich neue spannende Herausforderungen. 366 Geschäfte (+ 7%) wurden neu eröffnet. Auf den folgenden Seiten wird ein Ausschnitt aus der Beratungstätigkeit zu Datenschutz und Öffentlichkeitsprinzip gezeigt: von der Verwendung von Statistikdaten im Verwaltungsalltag über die Problematik von Vorgangslisten im Einbürgerungsverfahren bis zur Verwendung von öffentlich zugänglich gemachten Informationen.

Statistikdaten und Schulpflicht

Privatschulen müssen sowohl dem Statistischen Amt Angaben über ihre Schüler(innen) für die Bildungsstatistik des Bundes liefern als auch dem Erziehungsdepartement, damit dieses die Wahrnehmung des Schulobligatoriums prüfen und allenfalls durchsetzen kann. Der sehr weitreichende Datensatz, welcher dem Statistischen Amt abgeliefert werden muss, umfasst auch (aber nicht nur) jene Daten, welche vom Erziehungsdepartement benötigt werden. Der Einfachheit halber wollten die Privatschulen das Statistische Amt mit der Weiterleitung der für das Erziehungsdepartement wesentlichen Daten betrauen – so hätte nur noch ein Fragebogen ausgefüllt werden müssen. Allerdings hätte das Statistische Amt, welches in seinen Datenbearbeitungen rechtlich privilegiert[1] ist, damit gegen das «Rückflussverbot» verstossen: Daten, welche zu statistischen Zwecken erhoben und vom Statistischen Amt bearbeitet worden sind, dürfen nicht in den Verwaltungsablauf zurückfliessen. Der Datenschutzbeauftragte hat gemeinsam mit dem Erziehungsdepartement und dem Statistischen Amt folgende Lösung erarbeitet, um die Privatschulen gleichwohl entlasten zu können: Das Erziehungsdepartement und das Statistische Amt führen die Erhebung gleichzeitig und nicht mehr zeitlich versetzt durch. Das Statistische Amt erstellt eine Tabelle, deren Spalten unterschiedlicher Farbe sind. Die Privatschulen füllen zwar die ganze Tabelle (einmal) aus und senden auch die ganze Tabelle an das Statistische Amt, kopieren dann aber diejenigen Spalten, welche das Erziehungsdepartement benötigt und welche farblich entsprechend hervorgehoben sind, in eine neue Tabelle und lassen diese Daten dem Erziehungsdepartement zukommen.

Adressbekanntgabe für die Jungbürgerfeier

In Basel findet jedes Jahr eine Feier für jene Jugendlichen, welche volljährig geworden sind, statt. Mit der Jungbürgerfeier soll «der ‹politische Geburtstag› von den in Basel-Stadt lebenden, mündig gewordenen jungen Schweizer(inne)n in würdiger Umgebung und mit ‹zeitgemässem› Rahmenprogramm» begangen werden. An der Jungbürgerfeier werden auch Informationen über die mit der Mündigkeit erlangten Rechte und Pflichten der Bürger(innen) vermittelt, was grundsätzlich zum Aufgabenbereich der Staatskanzlei gehört. Darf die Staatskanzlei die mit der Erfüllung dieser Aufgabe verbundene Organisation der Jungbürgerfeier einem anderen öffentlichen Organ (beispielsweise den Basler Zünften) oder einer Privatperson übertragen und dazu u.a. Adressdaten der Jungbürger(innen) bekanntgeben? Wenn die Organisation von einem anderen öffentlichen Organ (mit-) übernommen werden soll und sichergestellt ist, dass die Informationen nur so bearbeitet werden, wie es dies die Staatskanzlei tun dürfte, muss die Antwort auf diese Frage, «ja» heissen[2]. Und auch die Übertragung an eine Privatperson ist grundsätzlich zulässig, wenn mittels einer Verpflichtungserklärung und der Festlegung von Sanktionen im Widerhandlungsfall sichergestellt wird, dass die fraglichen Daten ausschliesslich für die Organisation der Jungbürger(innen)feier genutzt und nicht beispielsweise zu Werbezwecken für andere Veranstaltungen des Organisationskomitees weiterverwendet werden. Ein Missverständnis, das zu unzutreffenden Vorwürfen an den Datenschutzbeauftragten geführt hat[3], konnte (anfangs 2013) im direkten Gespräche mit dem Vorsitzenden Meister beseitigt werden.

Dilemma bei der Datenbekanntgabe und beim Online-Zugriff

Die Bewährungshilfe bezieht zur Erfüllung ihrer Aufgabe[4] vom Betreibungsamt die Auszüge aus dem Betreibungsregister der von ihr betreuten Personen (ca. 600 bis 800 Fälle pro Jahr). Bezieht sie diese Informationen wie bisher einzeln, dann entsteht ein Problem: Das Betreibungsamt erfährt etwas, was es ausser für den Entscheid über die Datenbekanntgabe nicht braucht – es braucht für seine Aufgabenerfüllung nicht zu wissen, ob jemand von der Bewährungshilfe betreut wird, der im Betreibungsregister eingetragen ist (oder auch nicht). Ein Online-Zugriff der Bewährungshilfe auf die Datenbank des Betreibungsamtes könnte diese Situation entschärfen: So erfährt das Betreibungsamt nicht, über wen die Bewährungshilfe Daten bezieht[5]. So gut diese Lösung aussieht – auch sie schafft ein Problem: Die Mitarbeiter(innen) der Bewährungshilfe können so nicht nur auf die Betreibungsregisterdaten ihrer Klient(inn)en zugreifen, sondern auch auf die Daten der zig'tausend anderen im Betreibungsregister eingetragenen Personen. Das ist unzulässig und die Einräumung des Online-Zugriffs unverhältnismässig.

Das Betreibungsamt braucht für seine Aufgabenerfüllung nicht zu wissen, ob jemand von der Bewährungshilfe betreut wird.

Soll jetzt der Online-Zugriff verweigert werden? Dann stecken wir wieder im ersten Problem. Ein Dilemma: Entweder erfährt die datenbesitzende Behörde zu viel oder die datenempfangende Behörde hat Zugriff auf Daten von zu vielen Personen. Eine Lösung könnte theoretisch darin bestehen, dass der Zugriff nur aus einem Geschäftsfall des datenempfangenden Organs heraus überhaupt möglich ist und dass der Zugriff auf Daten anderer Personen technisch verunmöglicht wird. Das dürfte bei vielen Anwendungen unmöglich oder mindestens sehr schwer zu implementieren sein. Eine andere Lösung besteht darin, dass alle Zugriffe der Bewährungshilfe geloggt werden und die Leitung der Bewährungshilfe regelmässig Stichprobenkontrollen durchführt, bei denen geprüft wird, ob die Mitarbeiter(innen) nur berechtigterweise auf Betreibungsregisterdaten zugegriffen haben. Der Datenschutzbeauftragte unterstützt die laufenden Bemühungen, eine Standardlösung zu entwickeln, damit die Log-Daten für solche Stichprobenkontrollen verwendet werden können, ohne dass die Persönlichkeitsrechte der Mitarbeiter(innen) verletzt werden.

Die «Zusicherungsfalle»

Nach § 29 IDG hat ein öffentliches Organ die Bekanntgabe von oder den Zugang zu Informationen im Einzelfall ganz oder teilweise zu verweigern oder aufzuschieben, wenn eine besondere gesetzliche Geheimhaltungspflicht oder ein überwiegendes öffentliches oder privates Interesse entgegensteht. Ein privates Interesse kann vorliegen, wenn die Bekanntgabe von oder der Zugang zu Informationen verlangt wird, die dem öffentlichen Organ von Dritten freiwillig mitgeteilt worden sind und deren Geheimhaltung es zugesichert hat[6]. Kann die Mitarbeiterin auf einer Amtsstelle nun grosszügig Geheimhaltung zusichern, um – beispielweise in einem Sorgerechtsstreit – an spannende Information über die involvierten Personen zu kommen? Die IDG-Bestimmung kann eine Falle sein, worauf schon im Ratschlag aufmerksam gemacht wurde: Private wären, so heisst es zur Begründung, kaum mehr bereit, den Behörden freiwillig Informationen zu liefern, wenn diese Informationen trotz Zusicherung der Geheimhaltung jedermann bekannt gegeben werden könnten; allerdings bleibe die grundsätzliche Frage auch weiterhin unbeantwortet, inwiefern ein öffentliches Organ überhaupt verbindlich Geheimhaltung zusagen kann. Nehmen wir an, dass die betroffene Person ein Gesuch um Zugang zu den eigenen Personendaten stellt, sich mit der Einschwärzung nicht abspeisen lässt und im Rekursfall schliesslich vom Gericht Recht bekommt. Die Mitarbeiterin steckt dann in einer ungemütlichen Situation: Soll sie die Zusicherungszusage brechen oder soll sie die gerichtliche Entscheidung missachten? Ohnehin ist zu berücksichtigen, dass die Regelung von § 29 Abs. 3 lit. c IDG formell nur bei den Zugangsrechten nach dem IDG (Zugang zu den eigenen Personendaten, Zugang zu Informationen nach dem Öffentlichkeitsprinzip) und der Bekanntgabe von Personendaten zur Aufgabenerfüllung gilt, nicht aber beim verfahrensrechtlichen Akteneinsichtsrecht[7].

Online-Zugriff auf Handelsregisterbelege

Das Handelsregister Basel-Stadt bietet die Möglichkeit, Belege zu einzelnen Einträgen in digitaler Form zu bestellen. Auf diesen Belegen sind regelmässig Personendaten enthalten – ist dies allenfalls problematisch? Das Handelsregister, welches die Einträge im Hauptregister, die Anmeldungen und die entsprechenden Belege umfasst, ist öffentlich[8]. >

Die Kantone sind verpflichtet, die Einträge im Hauptregister für Einzelabfragen im Internet unentgeltlich zur Verfügung zu stellen[9]. Sodann sind die Handelsregisterämter ermächtigt, in Papierform vorliegende Handelsregisterbelege zwecks Aufbewahrung elektronisch einzulesen und zu beglaubigen und die Originale auf Papier anschliessend zu vernichten. Weiter dürfen die Handelsregisterämter elektronische Kopien von Anmeldungen, Belegen oder sonstigen Dokumenten wie auch von eigenhändigen Unterschriften erstellen[10]. Eine Beschränkung des Einsichtsrechts auf nur in Papierform eingereichte Originale der Handelsregisterbelege bzw. eine Regelung, dass Kopien ebenfalls nur in Papierform an das Publikum abgegeben werden dürfen, ist weder in Art. 927 ff. OR noch in der Handelsregisterverordnung vorgesehen und dürfte auch nicht im Sinne der leichten Zugänglichkeit sein. Das Handelsregisteramt verfügt somit über die erforderlichen gesetzlichen Grundlagen zur Bekanntgabe der Handelsregisterbelege auch im Internet.

Die Kantone sind verpflichtet, die Einträge im Hauptregister für Einzelabfragen im Internet kostenlos zur Verfügung zu stellen.

Dies löst aber das Problem nicht, dass viele dem Handelsregister eingereichte Unterlagen Informationen über Personen offen legen, die eigentlich gar nichts im Handelsregister zu suchen hätten: So können sich beispielsweise im Protokoll einer Sitzung des Verwaltungsrates oder des Stiftungsrates neben den handelsregisterrelevanten Informationen (z.B. die Erteilung einer Vertretungsvollmacht) auch Angaben zu einem personalrechtlichen Streit oder zu einer fallspezifischen Frage der Personalvorsorge finden. Wenn die Protokolle *tel quel*, d.h. ohne vorgängiges Einschwärzen der entsprechenden Stellen, eingereicht werden, so erscheinen die Personendaten ebenfalls im Internet. Für diese Problematik gibt es derzeit keine rechtliche Lösung – die Handelsregisterämter sind nicht verpflichtet, die ihnen eingereichten Dokumente auf nicht-handelsregisterrelevante Informationen hin zu prüfen; gleichzeitig scheint aber auch kein rechtlicher Spielraum zu bestehen, die eingereichten und im Internet publizierten Dokumente nachträglich einzuschwärzen und in überarbeiteter Form noch einmal im Internet zu veröffentlichen. Der Datenschutzbeauftragte hat angeregt, dass dieses Thema auf Bundesebene zwischen dem Eidgenössischen Handelsregisteramt und dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten angegangen wird.

Vorgangslisten im Einbürgerungsverfahren

Seit rund zwei Jahren beschäftigt sich der Datenschutzbeauftragte mit der Frage, ob und allenfalls unter welchen Voraussetzungen die Staatsanwaltschaft den Einbürgerungsorganen der Bürgergemeinden Vorgangslisten einbürgerungswilliger Personen oder Auszüge daraus bekannt geben darf[11]. Es ist nachvollziehbar, dass die kommunalen Einbürgerungsbehörden – im rechtlich zulässigen Rahmen – Informationen für die Beurteilung der Integration benötigen. Ebenso einleuchtend ist die Forderung der Staatsanwaltschaft, des verantwortlichen öffentlichen Organs, dass eine Lösung möglichst einfach umsetzbar sein muss. Nach langen erfolglosen Versuchen rückte im Herbst 2012 eine rechtstaatlich vertretbare und für alle Beteiligten umsetzbare Lösung in Reichweite. Sie musste aber in Anbetracht der im Entwurf zum Bundesgesetz über das Strafregister-Informationssystem VOSTRA[12] bestätigten Regelung, dass die kommunalen Einbürgerungsbehörden nur den Privatauszug aus dem Strafregister und keine über die darin enthaltenen Informationen hinausgehenden Angaben zur einbürgerungswilligen Person erhalten sollen, wieder fallen gelassen werden. Falls die Bundesregelung bezüglich des VOSTRA-Auszuges abschliessend sein sollte, dürfte eine Aushändigung der Vorgangslisten eine Umgehung der restriktiven Bundesregelung darstellen und deshalb unzulässig sein. Falls die Bundesregelung bezüglich des VOSTRA-Auszuges nicht abschliessend wäre, sondern kantonalen Regelungsspielraum belässt, wäre es am Kanton, entsprechendes Recht zu setzen.

Falls die Bundesregelung bezüglich des VOSTRA-Auszuges abschliessend sein sollte, dürfte eine Aushändigung der Vorgangslisten unzulässig sein.

Dabei müsste klar entschieden werden, ob von den kantonalen Einbürgerungsorganen der (künftig so genannte) VOSTRA-Behördenauszug «2plus» an die kommunalen Einbürgerungsorgane weitergegeben werden darf und ob und allenfalls unter welchen Voraussetzungen die Staatsanwaltschaft verpflichtet ist, den Einbürgerungsorganen auf kantonaler und/oder kommunaler Ebene die Vorgangslisten bezüglich

einbürgerungswilliger Personen auszuhändigen. Aufgrund des Inhalts der Vorgangslisten (besondere Personendaten, zum Teil noch nicht erhärtete oder – bei Nichtanhandnahme, Einstellungen oder Freisprüchen unter Umständen gar widerlegte – Angaben) und der Zweckänderung geht der Datenschutzbeauftragte davon aus, dass der zweite Entscheid bezüglich der Vorgangslisten auf Gesetzesstufe und nicht bloss auf Verordnungsstufe getroffen werden müsste. In diesem Sinne empfahl der Datenschutzbeauftragte der Departementsleitung des JSD, diese Fragen im Lichte der Bundesgesetzgebung zu prüfen und gegebenenfalls einen entsprechenden Rechtsetzungsprozess einzuleiten.

Überwachung der Nutzung der Internet- und E-Mail-Dienste

Im Bereich der Internet- und E-Mailnutzung ist es dem Arbeitgeber Basel-Stadt ein Anliegen, dass die korrekte Verwendung der vom Kanton zur Verfügung gestellten Internet- und E-Mail-Dienste garantiert, die Daten- und Anwendungssicherheit gewährleistet und die Einhaltung u.a. des Datenschutzes sichergestellt wird. Zur Erreichung dieses Zwecks sieht die Weisung vom 22. Oktober 2003 für die Benutzung von Informatikmitteln in der Verwaltung des Kantons Basel-Stadt vor, dass bei Verdacht auf Missbrauch Einsicht in die Aufzeichnungsprotokolle der Internetnutzung genommen werden kann. Aus rechtsstaatlicher Sicht vermag eine solch unbestimmte Formulierung in einer Weisung den Eingriff ins Grundrecht auf informationelle Selbstbestimmung der betroffenen Personen jedoch nicht zu rechtfertigen[13]. Der Datenschutzbeauftragte hat deshalb gemeinsam mit Vertretern des Zentralen Personaldienstes (ZPD), der Fachstelle Informatik und Organisation (FIO) und der Zentralen Informatikdienste (ZID) am Entwurf einer Verordnung zur Überwachung der Nutzung von Internet- und E-Mail-Diensten (IÜV) mitgearbeitet. Die Verordnung regelt, was als missbräuchliche Nutzung der Internet- und E-Mail-Dienste zu verstehen ist und wie das Verfahren zur Überwachung der Internet- und E-Mail-Nutzung aussieht. Die Verordnung wurde im Berichtsjahr in die Vernehmlassung geschickt. Fraglich ist u.a. noch, ob sich die auf Verlangen des Personaldienstes aufgenommene retrospektive Auswertung des E-Mail-Verkehrs zur Verfolgung von Cybermobbing auf eine genügende gesetzliche Grundlage stützen kann; der Datenschutzbeauftragte meint nein.

Datenschutzrechtliche Aufsicht über die Listenspitäler

Seit dem 1. Januar 2012 ist die neue Spitalfinanzierung[14] in Kraft. Die Kantone haben eine Planung für eine bedarfsgerechte Spitalversorgung aufzustellen und gestützt darauf eine Spitalliste zu erstellen, auf der die Leistungsaufträge der Spitäler («Listenspitäler») aufzuführen sind[15]. An die stationären Leistungen der Listenspitäler im Bereich der obligatorischen Krankenpflege (OKP) bezahlt der Kanton einen Anteil von mindestens 55 Prozent[16]. Damit entfallen bezüglich der Finanzierung der Spitäler die bisherigen Unterschiede zwischen den öffentlichrechtlichen Spitälern (Kantons-, Bezirks- und Stadtspitäler) und den Privatspitälern.

Sämtliche Listenspitäler nehmen im Rahmen ihrer Leistungsaufträge öffentliche Aufgaben des Kantons wahr und unterstehen insoweit dem kantonalen IDG und der kantonalen Datenschutzaufsicht.

Die Geltung der (Informations- und) Datenschutzgesetze und damit die Zuweisung der Aufsichtstätigkeit knüpft an die datenbearbeitende Person an: Für das Datenbearbeiten durch Private und Bundesorgane gilt das Bundesdatenschutzgesetz, die Aufsicht über jene Datenbearbeiter obliegt dem EDÖB. Für kantonale und kommunale öffentliche Organe des Kantons Basel-Stadt gilt hingegen das kantonale Informations- und Datenschutzgesetz, die Aufsicht fällt in den Zuständigkeitsbereich des kantonalen Datenschutzbeauftragten. Als öffentliche Organe im Sinne des IDG gelten jedoch auch Private, denen von Kanton oder Gemeinden eine öffentliche Aufgabe übertragen wird[17]. Es stellt sich somit die Frage, ob und inwieweit die Listenspitäler nach der KVG-Revision öffentliche Aufgaben erfüllen und, damit zusammenhängend, wem die datenschutzrechtliche Aufsicht zukommt. Im Rahmen eines Rechtsgutachtens, welches von privatim, der Vereinigung der schweizerischen Datenschutzbeauftragten, in Auftrag gegeben wurde, hat Prof. Dr. Bernhard Rütsche (Universität Luzern) diese Frage untersucht[18]. Dabei ist er zum Schluss gekommen, dass sämtliche Listenspitäler, unabhängig ihrer Rechtsform, im Rahmen ihrer kantonalrechtlichen Leistungsaufträge öffentliche Aufgaben wahrnehmen. Es handelt sich dabei um sog. kantonale Versorgungsaufgaben. Dies hat zur Folge, dass dem kantonalen Datenschutzbeauftragten im Rahmen der Leistungsaufträge die Aufsicht über sämtliche Listenspitäler zukommt. Unbeeinflusst davon bleiben die Anwendbarkeit des Bundesdatenschutzgesetzes und die >

Zuständigkeit des EDÖB ausserhalb der Leistungsaufträge, also beispielsweise bei medizinischen Behandlungen, welche durch Privatspitäler erbracht, aber nicht von der OKP übernommen werden.

Bedrohungsmanagement

Was tun, wenn Kund(inn)en der öffentlichen Verwaltung mit Gewalt – entweder gegen sich selbst oder gegen die Angestellten der jeweiligen Stelle – drohen? Die Angestellten der kantonalen Verwaltung haben die Möglichkeit, sich an die Psycho-Sozialen Dienste der Kantonspolizei (PSD) zu wenden. Dieses interdisziplinäre Team aus Psycholog(inn)en, Sozialarbeiter(inne)n und Pflegefachpersonen übernimmt oftmals die Funktion eines Auffangbeckens für jene sozialen Aufgaben, die sich keiner anderen Polizeiabteilung zuordnen lassen, und fungiert als wesentliche Schnittstelle zu anderen Institutionen und Organen. Die PSD stützen ihre Tätigkeit weitestgehend auf das Polizeigesetz[19] bzw. auf Art. 285 StGB («Gewalt und Drohung gegen Behörden und Beamte»).

Für ein kantonales Bedrohungsmanagement genügt der sehr allgemein gehaltene polizeiliche Auftrag zur Aufrechterhaltung der öffentlichen Sicherheit und Ordnung nicht.

Die Durchführung einer fundierten Gefährdungseinschätzung erfordert beispielsweise das Bearbeiten von Angaben über den Gesundheitszustand einer Person, über allfällige Unterstützungsleistungen durch Sozialhilfe oder andere Institutionen, über religiöse Überzeugungen oder über bereits ergangene Strafurteile – dies alles sind besondere Personendaten im Sinne von § 3 Abs. 4 IDG. Das IDG verlangt dafür das Vorliegen entweder einer *ausdrücklichen* gesetzlichen Verpflichtung oder Ermächtigung oder aber, dass das Bearbeiten bzw. die Bekanntgabe zur Erfüllung einer in einem Gesetz *klar umschriebenen* Aufgabe *zwingend notwendig* ist[20]. Diesen Anforderungen vermag der sehr allgemein gehaltene polizeiliche Auftrag zur Aufrechterhaltung der öffentlichen Sicherheit und Ordnung nicht zu genügen, und auch die Konstruktion einer mittelbaren gesetzlichen Grundlage über Art. 285 StGB bringt nicht die für das Bearbeiten von besonderen Personendaten geforderte inhaltliche Bestimmtheit. Wie bereits anlässlich der Spezialkontrolle im Jahr 2011 festgestellt, ist es unabdingbar, dass die Tätigkeit der PSD der Kantonspolizei mit dem entsprechenden gesetzlichen Rahmen versehen wird.

Der Datenschutzbeauftragte wird sich beratend in die Diskussion eines aus rechtsstaatlicher Sicht vertretbaren rechtlichen Rahmens für ein kantonales Bedrohungsmanagement, welches beispielsweise auch Drohungen gegenüber Sozialhilfemitarbeiterinnen oder gegenüber Mitarbeitern des Finanzdepartements aufgreift, einbringen.

Videoüberwachung

Mit dem Inkrafttreten des IDG hat sich für den Betrieb von Videoüberwachungsanlagen einiges geändert: Erstens findet sich die gesetzliche Grundlage für den Betrieb der Videoüberwachungsanlagen nun in § 17 IDG, womit es keiner gesetzlichen Grundlage in einem Spezialgesetz mehr bedarf. Zweitens wird der Betrieb der Anlage nicht mehr vom Datenschutzbeauftragten bewilligt: Das Reglement muss von der Departementsleitung, dem Gemeinderat, dem Appellationsgericht oder der Direktion selbständiger Anstalten und Körperschaften erlassen werden[21]. Dafür ist drittens das Reglement, bevor es erlassen oder verlängert werden kann, dem Datenschutzbeauftragten zur Vorabkontrolle vorzulegen[22]. Im Jahr 2012 liefen die noch unter der Ägide des DSG ausgesprochenen Bewilligungen für den Betrieb von 15 Videoüberwachungsanlagen öffentlicher Organe des Kantons Basel-Stadt aus. Für diese Anlagen bestanden aber noch keine Dokumente, welche eine vertiefte Evaluation im Rahmen der Vorabkontrolle erlaubt hätten – das DSG sah eine solche Evaluation nicht vor. Der Datenschutzbeauftragte führte daher eine Vorabkontrolle «light» durch. Dabei hatten die Betreiber(innen) Auskunft über den Einsatz der Kameras zu geben und soweit als möglich deren Erforderlichkeit zu belegen. Gestützt auf die Reglemente für den Betrieb der Kameras, die Berichte über die Geeignetheit und Erforderlichkeit der Anlagen und teilweise auch basierend auf Vor-Ort-Besichtigungen beurteilte der Datenschutzbeauftragte die 15 Anlagen und stellte den Betreiber(inne)n schliesslich seine Prüfungsresultate der Vorabkontrolle zu. Die nächste Evaluation dieser Kameras wird anfangs 2016 erfolgen, wenn die Verlängerung der auf vier Jahre befristeten Reglemente ansteht.

«Rückwirkung» des Öffentlichkeitsprinzips

Im Zusammenhang mit einem Gesuch um Einsicht in den Bericht zur Subventionspraxis der offenen Kinder- und Jugendarbeit von 2002 hat sich die Frage gestellt, ob das Öffentlichkeitsprinzip auch für Dokumente gelte, welche vor dem Inkrafttreten des IDG erstellt wurden. Die Antwort gibt das IDG selbst: Nach § 25 Abs. 1 IDG unterstehen sämtliche bei einem öffentlichen Organ vorhandenen und fertig gestellten Informationen dem Öffentlichkeitsprinzip, wobei es keine zeitliche Begrenzung gibt. Die Unterlagen müssten, sofern keine Einschränkungsgründe im Sinne von § 29 IDG vorliegen, herausgegeben werden. Anders gestaltet sich die Regelung des Bundes. Art. 23 BGÖ hält fest, dass das Öffentlichkeitsprinzip nur für jene Dokumente gelte, die nach dem Inkrafttreten des BGÖ erstellt worden sind.

Wenn einer Person gestützt auf das Öffentlichkeitsprinzip Zugang zu Informationen gewährt wird, so müssen stehen diese Informationen auch allen anderen Personen zu («access to one, access to all»).

Verwendung von öffentlich zugänglich gemachten Informationen

Im Jahr 2012 wurde der Datenschutzbeauftragte mehrmals mit der Frage konfrontiert, ob die Informationen, die einer Person gestützt auf das Öffentlichkeitsprinzip[23] zugänglich gemacht worden sind, von dieser einem breiten Publikum zur Verfügung gestellt werden dürfen, ob also die empfangende Person solche Informationen *tel quel* – beispielsweise im Internet – veröffentlichen darf[24]. Grundsätzlich ja. Ein Gebot, in irgendeiner bestimmten Weise mit der zugänglich gemachten Information umzugehen, oder ein Verbot, in irgendeiner bestimmten Weise mit der zugänglich gemachten Information umzugehen, stellt eine Einschränkung des Zugangsrechts dar und ist nur zulässig unter den Voraussetzungen des § 29 IDG (besondere gesetzliche Geheimhaltungsbestimmung, überwiegendes öffentliches oder privates Geheimhaltungsinteresse). Allerdings ist zu prüfen, ob unter diesen Voraussetzungen die fragliche Information überhaupt herausgegeben werden darf oder ob die Zugangsgewährung zu ihr (oder zu den «gefährlichen» Teilen) aus diesen Gründen nicht *überhaupt* zu verweigern ist. Das Recht auf Zugang zu Informationen nach dem Öffentlichkeitsprinzip ist – anders als das verfahrensrechtliche Akteneinsichtsrecht und das Recht auf Zugang zu den eigenen Personendaten[25] – ein «Jedermannsrecht». Wenn einer Person also gestützt auf das Öffentlichkeitsprinzip Zugang zu Informationen gewährt wird, so stehen diese Informationen auch allen anderen Personen zu («access to one, access to all»[26]). So gesehen könnte auch das öffentliche Organ, das Zugang gewährt hat, die Informationen selber gleich im Internet aufschalten – ein Vorschlag, der aus Verwaltungskreisen auch schon vorgebracht, aber nicht umgesetzt wurde.

Bekanntgabe von Kontoauszügen

Ein Einwohner der Gemeinde Bettingen verlangt vom Gemeinderat Zugang zu Auszügen des kommunalen Personalaufwandkontos. Personendaten, wozu auch der Lohn einer bestimmten Person gehört, müssen nach § 30 Abs. 1 IDG anonymisiert werden, wenn nicht der Zugang zu diesen Daten schon wegen überwiegender privater Interessen (§ 29 Abs. 3 IDG) einzuschränken ist. Da die Gemeinde nur über wenige Angestellte verfügt, wäre unter Umständen trotz Anonymisierung der Daten offenkundig, welche Person wie viel verdient. Mit einer solchen «Anonymisierung» kann der Personenbezug nicht wirksam entfernt werden, so dass die Informationen als nicht anonymisiert gelten müssen. Nach § 30 Abs. 2 IDG richtet sich der Zugang zu nicht anonymisierten Personendaten nach den Bestimmungen für die Bekanntgabe. Dementsprechend brauchte der Gemeinderat eine gesetzliche Grundlage (i.S.v. § 21 IDG), welche ihm die Bekanntgabe der Einkommen der Gemeindeangestellten erlauben würde. Über eine derartige Rechtsgrundlage verfügte der Gemeinderat jedoch nicht, womit der Zugang zu diesen Daten verweigert werden musste. >

Vernehmlassungen

Dem Datenschutzbeauftragten wurden 15[27] Entwürfe für Verordnungen oder Gesetze zur Vernehmlassung vorgelegt. Das Spektrum reichte hierbei von Änderungen des Ausschaffungsrechts über die Anpassung des Staatsvertrags über das Universitäts-Kinderspital beider Basel bis hin zu Anpassungen des kantonalen Grundbuchrechts. Im Folgenden sollen fünf Vernehmlassungen näher vorgestellt werden:

Solange nicht eine Grundsatzdiskussion über die Vor- und Nachteile einer Verwendung der AHVN13 zu Administrativzwecken geführt worden ist, sollte von der Verwendung der AHVN13 abgesehen werden.

Statistikgesetz

Der Datenschutzbeauftragte hatte dem Statistischen Amt bei der Ausarbeitung des Gesetzesentwurfs beratend zur Seite gestanden: Das lang erwartete kantonale Statistikgesetz wurde schliesslich im Juli 2012 in die Vernehmlassung geschickt. In seiner Vernehmlassungsantwort unterstrich der Datenschutzbeauftragte erneut, dass die Schaffung einer formellgesetzlichen Grundlage für die Tätigkeit des Statistischen Amtes aus rechtstaatlichen Überlegungen unverzichtbar sei. In diesem Zusammenhang wies er aber auch darauf hin, dass es zwar nachvollziehbar sei, dass die breit gefächerte Tätigkeit des Statistischen Amtes nicht umfassend und bestimmt in einem Gesetz im formellen Sinne verankert werden könne. Die in einer ersten Ausarbeitungs-Phase geplante Konkretisierung lediglich in einem vom Regierungsrat verabschiedeten Mehrjahresprogramm vermochte wiederum aus rechtsstaatlicher Sicht nicht zu genügen. Die nun im Entwurf vorgeschlagene Lösung, wonach der Regierungsrat in einer Verordnung die hauptsächlichen Tätigkeitsgebiete der öffentlichen Statistik festhält sowie die dazu erforderlichen Befragungen umschreibt, wurde daher vom Datenschutzbeauftragten begrüsst.

Beurkundung des Personenstands und Grundbuchrecht

Der Bundesgesetzgeber lud zur Vernehmlassung über eine einheitliche Erfassung natürlicher Personen im Personenstandsregister sowie über eine Anpassung der Modalitäten zur Erfassung von Personendaten im Grundbuch ein. Der Datenschutzbeauftragte begrüsste zwar die geplante einheitliche Erfassung natürlicher Personen im Personenstandsregister, drückte aber seine Besorgnis dahingehend aus, dass eine kontinuierliche Verknüpfung und Ausweitung des Personenstandsregisters geplant sei – sollten diese Pläne tatsächlich umgesetzt werden, so bedürfte es dazu zwingend einer formellgesetzlichen Grundlage, welche die Verknüpfungen und die damit verbundenen Zugriffsrechte usw. hinreichend bestimmt regelt. Die anvisierte Verwendung der Sozialversicherungsnummer (AHVN13) als Personenidentifikator im Grundbuch erachtete der Datenschutzbeauftragte als problematisch: Solange nicht eine grundlegende Diskussion über die Vor- und Nachteile einer Verwendung der AHVN13 zu Administrativzwecken geführt und allenfalls ein Grundsatzentscheid für die Verwendung mit klaren Voraussetzungen und strikten Rahmenbedingungen auf Gesetzesstufe gefällt worden ist, sollte von der Verwendung der AHVN13 abgesehen werden.

Strafregistergesetz

Die Vorlage zur Ablösung der Verordnung über das Strafregister (VOSTRA-Verordnung) durch ein Strafregistergesetz[28] konnte in verschiedenen Punkten begrüsst werden: Mit der expliziten Regelung, dass VOSTRA ausschliesslich zur Erfüllung gesetzlich vorgesehener Aufgaben genutzt werden darf und die Weitergabe von VOSTRA-Daten in einem Gesetz im formellen Sinne vorgesehen sein muss, wurde dem Legalitätsprinzip Rechnung getragen. Ebenso wurde mit der Etablierung unterschiedlicher Behördenauszüge und verschiedener Zugangsmöglichkeiten (Online-Zugriff bzw. Papier-Auszug auf Gesuch hin) ein Gegengewicht zur geplanten Ausweitung des Kreises der Zugangsberechtigen geschaffen und das Verhältnismässigkeitsprinzip gewahrt. Ebenso begrüsst werden konnte die Neuerung, wonach sich das Auskunftsrecht der betroffenen Personen neu auch auf die Hilfsdatenbank erstrecken soll. Wie auch in der Vernehmlassung zur Beurkundung des Personenstands und dem neuen Grundbuchrecht machte der Datenschutzbeauftragte auf die Problematik der Verwendung der AHVN13 zu Administrativzwecken aufmerksam.

UKBB-Staatsvertrag

Die beiden Basel begannen mit der Revision des Vertrags vom 16. Februar 1988 zwischen den Kantonen Basel-Stadt und Basel-Landschaft über das Universitäts-Kinderspital beider Basel[29]. Im Rahmen der Vernehmlassung empfahlen sowohl der Datenschutzbeauftragte des Kantons Basel-Stadt wie auch die Aufsichtsstelle Datenschutz des Kantons Basel-Landschaft, den Vertragsentwurf um einen § 23a mit dem Wortlaut *«Für den Umgang mit Informationen gilt das Informations- und Datenschutzrecht des Sitzkantons»* zu ergänzen. Damit ist interkantonal unmissverständlich geklärt, welches Datenschutzrecht auf Datenbearbeitungen im UKBB-Kontext zur Anwendung gelangt. Grundsätzlich ist das baselstädtische IDG anwendbar und der Basler Datenschutzbeauftragte zur Aufsicht zuständig. Weil das UKBB aber auch Patient(inn)en aus dem Kanton Basel-Landschaft behandelt und damit eine öffentliche Aufgabe des Kantons Basel-Landschaft erfüllt, wäre es – ohne eine ausdrücklich anders lautende Regelung – nach dem Informations- und Datenschutzgesetz des Kantons Basel-Landschaft ein öffentliches Organ nach IDG/BL. Das würde dazu führen, dass in diesem Fall das IDG/BL zu Anwendung gelangte und die Aufsichtsstelle Datenschutz des Kantons Basel-Landschaft für die Aufsicht zuständig wäre. Um diese Verkomplizierung zu verhindern, ist eine Regelung wie die vorgeschlagene vorzusehen.

Schengen- Weiterentwicklungen

Das Jahr 2012 führte zu 13[30] Weiterentwicklungen des Schengen-Besitzstandes, welche die Schweiz umsetzen muss. Der Datenschutzbeauftragte wurde durch den Rechtsdienst des JSD regelmässig über diese Weiterentwicklungen informiert und hat jeweils Stellung genommen; aus datenschutzrechtlicher Sicht brachte keine der neuen Regelungen Handlungsbedarf auf kantonaler Ebene mit sich.

Tagung zu Öffentlichkeitsprinzip und Open Government Data

Am 1. Januar 2012 trat das IDG in Kraft. Es vereint im selben Erlass sowohl die Regelungen zum Datenschutz als auch zur Umsetzung des Öffentlichkeitsprinzips. Die Einführung des Öffentlichkeitsprinzips ist aber noch nicht das Ende einer langjährigen Entwicklung hin zu mehr Transparenz und Rechtssicherheit. Mit dem Konzept von Open Government Data (OGD) soll der Umgang mit Daten, die von staatlichen Stellen generiert werden, noch weiter vereinfacht werden. Bestehende nicht-personenbezogene Daten sollen so zur Verfügung gestellt werden, dass sie von interessierten Kreisen ausgewertet, weitergenutzt und angereichert werden können. Insbesondere im angelsächsischen Raum, in Schweden und in Deutschland veröffentlichen zahlreiche Verwaltungen ihre Informationen nach den Grundsätzen von OGD und tragen damit zu einer transparenten und schlanken Verwaltung bei. Gemeinsam mit der Staatskanzlei (federführend: Peter Haber(†)) hat der Datenschutzbeauftragte am Freitag, 20. Januar 2012, eine Tagung zu «Öffentliche Informationen und offene Daten» durchgeführt.

Open Government Data-Projekte sind darauf zu prüfen, ob nicht durch die Verknüpfbarkeit der veröffentlichten Persönlichkeitsrechte verletzt werden.

Im historischen Basler Grossratssaal haben Experten aus dem In- und Ausland den aktuellen Stand von Öffentlichkeitsprinzip sowie OGD diskutiert und mögliche Handlungsmöglichkeiten für die Zukunft aufgezeigt[31]. Mit über 100 Teilnehmer(inne)n aus Politik, Verwaltung und Privatwirtschaft war die Tagung ausserordentlich erfolgreich. Für die weitere Entwicklung ist aus Datenschutzsicht darauf zu achten, dass mit der Zunahme der Datenmenge auch die Gefahr der ReIdentifizierung von betroffenen Personen wächst[32]. Deshalb sind Open Government Data-Projekte sorgfältig darauf zu prüfen, ob nicht mit der Veröffentlichung von Daten aufgrund der Verknüpfbarkeit Persönlichkeitsrechte verletzt werden – denn auch hier gilt: Die transparente Verwaltung ist das Ziel, nicht der «gläserne Bürger»! >

Schulungen und Referate

Dass Öffentlichkeitsprinzip und Datenschutzrecht unterschiedlichste Personengruppen interessieren und tangieren, zeigt das breite Spektrum an Schulungen und Referaten, welche vom Datenschutzbeauftragten und seinem Team im Jahr 2012 angeboten wurden. Ein Auszug: Die Einführung «Das IDG kurz erklärt» fand viermal statt und richtete sich an Kaderangehörige aller Stufen der Verwaltung. Beim Bau- und Verkehrsdepartement (BVD) wurde eine IDG Schulung durchgeführt, im Rahmen derer BVD- spezifische Fragestellungen diskutiert wurden; eine derartige Schulung fand auch beim Erziehungsdepartement statt. Weitere Schulungen wurden beim Amt für Wirtschaft und Arbeit, beim der Abteilung Sucht im Gesundheitsdepartement und bei der Steuerverwaltung durchgeführt. Den Mitgliedern der European Law Students Association (ELSA) wurde wiederum ganz allgemein aus der Tätigkeit des Datenschutzbeauftragten berichtet. Anlässlich einer Schulung an der Pädagogischen Hochschule der FHNW zum Thema Datenschutz und Bildungsforschung wurde die Problematik der Befragungen von Schüler(inne)n intensiv diskutiert, und am Lehrerbildungstag der Allgemeinen Gewerbeschule wurde im Rahmen eines Referats auf die datenschutzrechtlichen Fragestellungen des Schulalltags aufmerksam gemacht. Der Gemeinderat und die Gemeindeverwaltung der Gemeinde Bettingen wiederum erhielten eine Einführung in das neue Öffentlichkeitsprinzip und konnten dabei Fragestellungen aus dem Verwaltungsalltag thematisieren. Und schliesslich wurde an der Konferenz der kantonalen BVG- und Stiftungsaufsichtsbehörden eine Vielzahl kniffliger Sachverhalte zum Thema Öffentlichkeitsprinzip und Datenschutz diskutiert.

Zusammenarbeit

Der Datenschutzbeauftragte arbeitet zur Erfüllung seiner Aufgaben mit den Organen der anderen Kantone, des Bundes und des Auslandes, welche die gleichen Aufgaben erfüllen, zusammen (§ 48 IDG). Die Zusammenarbeit mit anderen Organen stellt noch immer ein wesentliches Element der Tätigkeit des Datenschutzbeauftragten dar. So engagierte sich der Datenschutzbeauftragte nicht nur im Büro von privatim, der Vereinigung der schweizerischen Datenschutzbeauftragten, und in den privatim-Arbeitsgruppen Gesundheit, Schule und ICT intensiv, sondern behandelte interkantonale Projekte auch mit den tangierten Kantonen gemeinsam – so beispielsweise die Ausarbeitung von Richtlinien für die Leistungstests im Bildungsraum Nordwestschweiz (AG, BL, BS und SO) oder die Klärung der Frage des auf kantonsübergreifend organisierte Institutionen (wie beispielsweise die FHNW, die Christoph Merian Stiftung, die Rheinhäfen usw.) anwendbaren Datenschutzrechts.

Der Datenschutzbeauftragte arbeitet zur Erfüllung seiner Aufgaben mit den Organen der anderen Kantone, des Bundes und des Auslandes zusammen.

Mit dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) fand eine Zusammenarbeit in einzelnen Geschäften statt. Die seit 2009 bestehende Koordinationsgruppe der schweizerischen Datenschutzbeauftragten tagte zweimal unter seinem Vorsitz; eine in allen Kantonen durchgeführte und mit dem Bund koordinierte Kontrolle des Schengener Informationssystems (SIS) fand nicht statt. Aber auch über die Landesgrenzen hinaus fand im Berichtsjahr zum ersten Mal ein intensiver Austausch statt: Anlässlich eines Besuchs in Mainz konnten sich die Datenschutzbeauftragten der Kantone Basel-Stadt und Zürich über das wegweisende Konzept «Medienkompetenz macht Schule» des Datenschutzbeauftragten des Bundeslandes Rheinland-Pfalz informieren. Schüler(inne)n soll der (selbst)verantwortungsbewusste und kritische Umgang mit neuen Medien vermittelt werden. Das rheinland-pfälzische Projekt vermittelt im Rahmen von zwei- bis vierstündigen interaktiven Workshops Grundinformationen und klärt altersgerecht über Risiken auf. Die ausgetauschten Erfahrungen werden in die weitere Tätigkeit des Datenschutzbeauftragten im Bereich der Medienkompetenz einfliessen. Und zu guter Letzt ging natürlich auch die Reform des europäischen Datenschutzrechts

nicht an den kantonalen Datenschutzbehörden vorbei. Anlässlich der Konferenz der europäischen Datenschutzbeauftragten im Mai in Luxemburg, an welcher auch der Datenschutzbeauftragte des Kantons Basel-Stadt teilgenommen hatte, wurden die Reformen intensiv diskutiert. Zudem werden die Entwürfe innerhalb der Datenschutz-Arbeitsgruppe der Konferenz der Kantonsregierungen ausführlich behandelt – für den baselstädtischen Datenschutzbeauftragten nimmt Dr. Sandra Husi-Stämpfli an diesen Besprechungen teil. Frau Husi-Stämpfli vertritt auch die Interessen der Kantone in der Joint Supervisory Authority of Schengen (JSA) in Brüssel, womit die laufenden Entwicklungen im Bereich des Datenschutzes in der EU konzentriert und zeitnah beurteilt werden können.

—

1 Siehe dazu § 22 Abs. 4 IDG.
2 § 7 Abs. 1 lit. b IDG.
3 Basler Banner Nr. 43, November 2012, Editorial.
4 Art. 93-96 StGB.
5 Die technischen Zugriffsdaten fallen zwar an, werden aber korrekterweise vom Betreibungsamt nicht bearbeitet.
6 § 29 Abs. 3 IDG.
7 Vgl. zur Unterscheidung zwischen dem verfahrensrechtlichen Akteneinsichtsrecht, dem Recht auf Zugang zu den eigenen Personendaten und dem Recht auf Zugang zu Informationen nach dem Öffentlichkeitsprinzip vorne 12 ff.
8 Art. 930 OR i.V.m. Art. 10 HRegV.
9 Art. 12 Abs. 2 HRegV.
10 Art. 12a Abs. 2 HRegV.
11 So schon TB 2010, 27.
12 Strafregistergesetz, StReG. Die Vernehmlassungsunterlagen finden sich unter <http://www.bj.admin.ch/content/bj/de/home/themen/sicherheit/gesetzgebung/strafregister.html>.
13 Vgl. Tätigkeitsbericht 2010, 14 ff., insb. 16.
14 Bundesgesetz über die Krankenversicherung (KVG) (Spitalfinanzierung), Änderung vom 21. Dezember 2007, AS 2008 2049 ff., <http://www.admin.ch/ch/d/as/2008/2049.pdf>.
15 Art. 39 Abs. 1 lit. d und e KVG.
16 Art. 49a Abs. 2 KVG.
17 § 3 Abs. 1 lit. c IDG.
18 Bernhard Rütsche, Datenschutzrechtliche Aufsicht über die Spitäler – Surveillance de la protection des données dans les hôpitaux, digma-Schriften Band 6, Zürich/Basel/Genf 2012.
19 Insbesondere § 2 PolG.
20 § 9 Abs. 2 bzw. § 21 Abs. 2 IDG.
21 § 18 Abs. 2 IDG.
22 § 18 Abs. 4 IDG.
23 § 25 IDG.
24 Das geschah z.B. mit der zugänglich gemachten Nichtanhandnahme-Verfügung der Staatsanwaltschaft in einem Fall, in welchem eine Mitarbeiterin des BVD durch eine Wochenzeitung implizit der Bestechlichkeit verdächtigt wurde.
25 Vgl. vorne 12 ff., insb. 13 f.
26 Ratschlag 08.0637.01, 42.
27 Im Vorjahr: 8. Die Schengen-Weiterentwicklungen sind separat gezählt.
28 Vgl. Fn 12.
29 UKBB-Staatsvertrag, SG 331.300.
30 Im Vorjahr: 10.
31 Vgl. dazu auch die Beiträge von Peter Haber, André Golliez, Andreas Neméth, Johann Mittheisz und Beat Rudin in digma 2012.2.
32 Vgl. dazu Beat Rudin, Datenschutzpendenzen bei OGD, digma 2012, 62 ff.; und Bruno Baeriswyl, «Big Data» ohne Datenschutz-Leitplanken, digma 2013, 14 ff.

Aus dem Alltag

Einblicke in die Kontrolltätigkeit

Der Datenschutzbeauftragte – so sieht es § 44 lit. a IDG vor – kontrolliert nach einem autonom aufzustellenden Prüfprogramm die Anwendung der Bestimmungen über den Umgang mit Informationen. Im Jahr 2012 wurden zwei Datenschutz-Audits abgeschlossen und ein weiterer begonnen. In Koordination mit dem Staatsschutzkontrollorgan wurde der Informationsfluss zwischen FG9 und Migrationsamt kontrolliert. Ausserdem wurde eine Schengen-Kontrolle begonnen und ein Follow-up durchgeführt.

Datenschutz-Audit beim Arbeitsintegrationszentrum (AIZ)

Der Datenschutzbeauftragte hat beim Arbeitsintegrationszentrum, einer Abteilung des Amtes für Wirtschaft und Arbeit (AWA), ein Datenschutz-Audit durchgeführt. Er stellte fest, dass für einen angemessenen Schutz der Informationen teilweise die konzeptionellen Grundlagen fehlen. Dieses Resultat deckt sich auch mit den Feststellungen aus den Datenschutz-Audits aus dem Jahr 2011.

Datenschutz-Audit beim Amt für Umwelt und Energie

Aufgrund der Erfahrungen vergangener Audits und einer Neu-Beurteilung der Gesamtsituation hat sich der Datenschutzbeauftragte dazu entschlossen, sein Vorgehen bei den Datenschutz-Audits anzupassen. Beim Amt für Umwelt und Energie (AUE) wurde das Audit auf die spezifischen Gegebenheiten und Risiken des Amtes statt an einem Standardprüfprogramm ausgerichtet. Auch im AUE fehlen teilweise konzeptionelle Grundlagen. Zudem stand die Einbindung der Informatik in die Gesamtorganisation – insbesondere das Zusammenspiel mit der Departementsinformatik – im Fokus der Prüfung.

Datenschutz-Audit bei der Sozialhilfe

Der Datenschutzbeauftragte hat bei der Sozialhilfe Basel-Stadt ein Datenschutz-Audit begonnen. Der Fokus lag auf den konzeptionellen Grundlagen und dem Einsatz der in der Sozialhilfe eingesetzten Fachanwendung Tutoris. Bei der Sozialhilfe wird das Thema Datenschutz aktiv bearbeitet und sie ist sich der Problematik in ihrem Bereich bewusst. Der Einsatz der Fachanwendung Tutoris erfüllt aber zum Zeitpunkt des Audits nicht alle Anforderungen aus dem IDG. Das Audit wird im ersten Halbjahr 2013 abgeschlossen.

Kontrolle der Staatsschutztätigkeit

Das Migrationsamt ist eine der Amtsstellen, die nach Art. 13 BWIS zu Auskünften an den Nachrichtendienst des Bundes (NDB) oder an die Kantone zuhanden des NDB verpflichtet sind. Nach Art. 13 Abs. 3 BWIS hat das Migrationsamt unaufgefordert dem NDB Meldung zu erstatten, wenn es konkrete Gefährdungen der inneren oder der äusseren Sicherheit feststellt; weitere Meldungen hat es aufgrund der allgemeinen Informationsaufträge (Art. 11 BWIS) oder aufgrund von Aufträgen im Einzelfall zu erstatten. In Koordination mit dem Staatsschutzkontrollorgan[1] hat der Datenschutzbeauftragte den Informationsaustausch zwischen dem Migrationsamt und der Fachgruppe 9 (FG 9, das kantonale Staatsschutzorgan) untersucht. Der Verdacht, dass unkontrolliert Meldungen vom Migrationsamt an die FG 9 gehen, konnte durch eine Untersuchung durch den Leiter des Migrationsamtes nicht erhärtet werden. Die Suche gestaltete sich sehr aufwändig, weil in der Geschäftskontrolle die Informationen, die an die FG 9 gingen, nicht einfach zu eruieren waren. Künftig werden Anfragen der FG 9 und die Meldung an die FG 9 in der Geschäftskontrolle des Migrationsamtes so erfasst, dass eine Auswertung jederzeit und ohne aufwändiges Durchforsten der Dokumente möglich sein wird. Ausserdem wurden die

Mitarbeiter(innen) des Migrationsamtes erneut darauf hingewiesen, dass Anfragen der FG 9 und allfällige Meldungen des Migrationsamtes an die FG 9 ausschliesslich über die Abteilungs- oder Amtsleitung des Migrationsamtes abgewickelt werden.

Schengen-Kontrolle

Nachdem im Jahr 2010/2011 die Datenbearbeitungen der Staatsanwaltschaft und der Kantonspolizei im Schengen-Kontext kontrolliert wurden, startete im Herbst 2012 die Kontrolle bei der Jugendanwaltschaft und beim Migrationsamt. Das Kick-off-Meeting fand am 19. Dezember 2012 statt. Es soll geprüft werden, ob die für die Datenbearbeitungen erforderlichen rechtlichen Grundlagen vorhanden sind und eingehalten werden. Ist nachvollziehbar, wer Zugriff auf das Schengener Informationssystem (SIS) nehmen kann? Unter welchen Voraussetzungen erfolgt die Abfrage des SIS? Besteht ein Kontrollverfahren, um zu prüfen, ob die Abfragen tatsächlich zur Aufgabenerfüllung – und nicht etwa, um die neue Kollegin zu «überprüfen» – erfolgt sind? Die Resultate der Kontrolle werden im zweiten Quartal 2013 vorliegen.

Der Datenschutzbeauftragte hat in Koordination mit dem Staatsschutzkontrollorgan den Informationsaustausch zwischen dem Migrationsamt und der Fachgruppe 9 untersucht.

Im selben Zeitrahmen wird auch das Follow-Up zur im Jahr 2010/2011 durchgeführten Kontrolle vorgenommen: Es wird nachgeprüft, ob die damals noch fehlenden internen Listen der SIS-Nutzer(innen) und der entsprechenden Zugriffsberechtigten erstellt und aktuell (gehalten) sind, und ob für die Nutzung des «scharfen SIS» zu Schulungszwecken klare Vorgaben gemacht wurden (das Schulungs-Tool ist wenig praxistauglich, eine Verbesserung des Lehrmittels obliegt jedoch fedpol).

Follow-up beim Sozialdienst der Kantonspolizei

Im Jahr 2011 wurde beim Sozialdienst der Kantonspolizei eine Spezialkontrolle durchgeführt. Dabei wurde festgestellt, dass der Sozialdienst zwar die Funktion eines Auffangbeckens für jene sozialen Aufgaben, die sich keiner anderen Polizeiabteilung zuordnen lassen, übernimmt. Die bestehenden Rechtsgrundlagen genügen aber aufgrund ihrer Unbestimmtheit aus datenschutzrechtlicher Sicht nicht oder höchstens bedingt für die vom Sozialdienst vorgenommene Bearbeitung der teilweise sensitiven Personendaten. Mittlerweile wurden aus dem Sozialdienst die «Psycho-Sozialen Dienste der Kantonspolizei» (PSD). Damit wurde eine gross angelegte Um- bzw. Neustrukturierung vollzogen. Die PSD haben damit begonnen, die einzelnen Datenflüsse festzuhalten und, wo möglich, entsprechende Rechtsgrundlagen zuzuordnen. Ablaufschemata und Zuständigkeiten wurden ausgearbeitet und Aufbewahrungsfristen den Aufgabenbereichen entsprechend festgelegt. Der Datenschutzbeauftragte wurde bei diesen Prozessen jeweils zur Beratung beigezogen.

—

1 Vgl. zur Koordination der Staatsschutzaufsicht TB 2011, 13 f.

Aus dem Alltag

Statistische Auswertungen 2012 (mit Vorjahresvergleichen)

A Geschäfte

	2012		2011		2010		2009	
	Anzahl	%	Anzahl	%	Anzahl	%	Anzahl	%
Anzahl eröffnete Geschäfte	366		341		323		230	
prozentuale Veränderung gegenüber Vorjahr		7		6		40		*

* Vorjahr erst ab 1. Mai 2009 erfasst

B Indikatoren gemäss Budget

	2012		2011	
	Anzahl	%	Anzahl	%
Anteil komplexer Beratungen				
prozentualer Anteil an allen Beratungen		9		7
Innert 14 Tagen abgeschlossene nicht-komplexe Beratungen				
prozentualer Anteil an allen nicht-komplexen Beratungen		61		50
Durchgeführte Audits				
Anzahl durchgeführte Audits	2		2	
Durchgeführte Schulungen für öffentliche Organe				
Anzahl durchgeführte Schulungen	11		12	

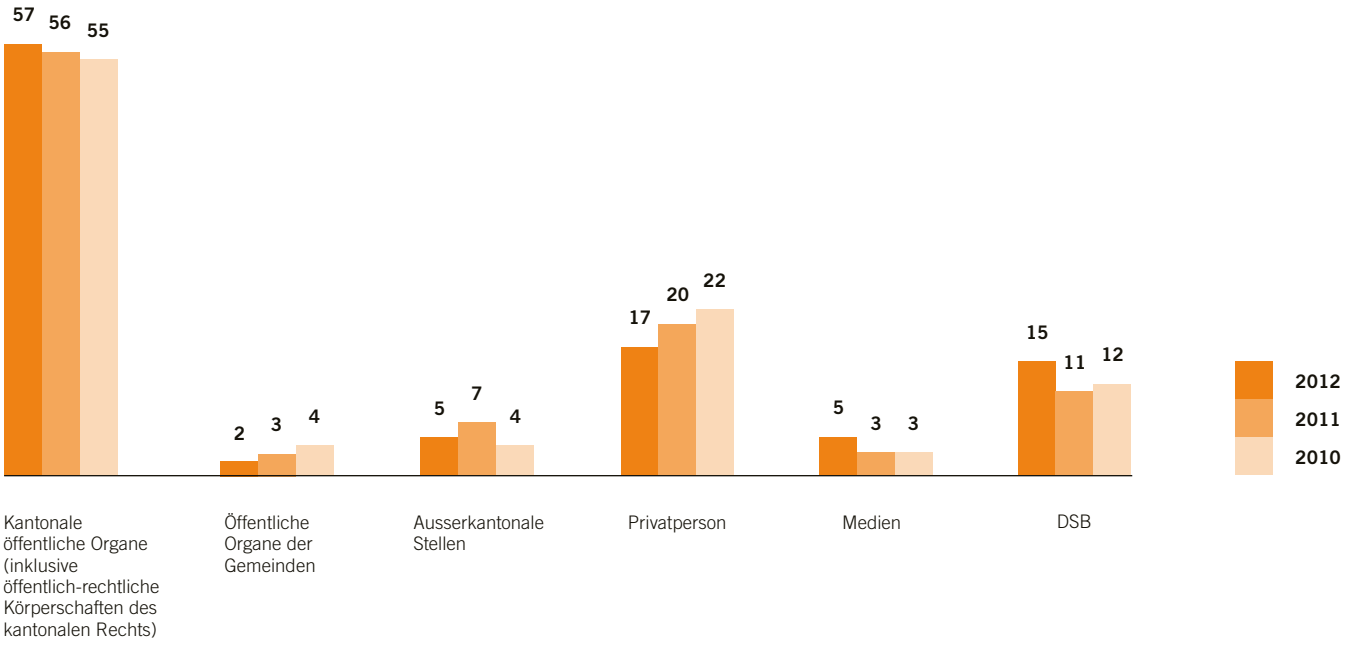
Indikatoren erfasst ab 2011

C Öffentlichkeitsprinzip

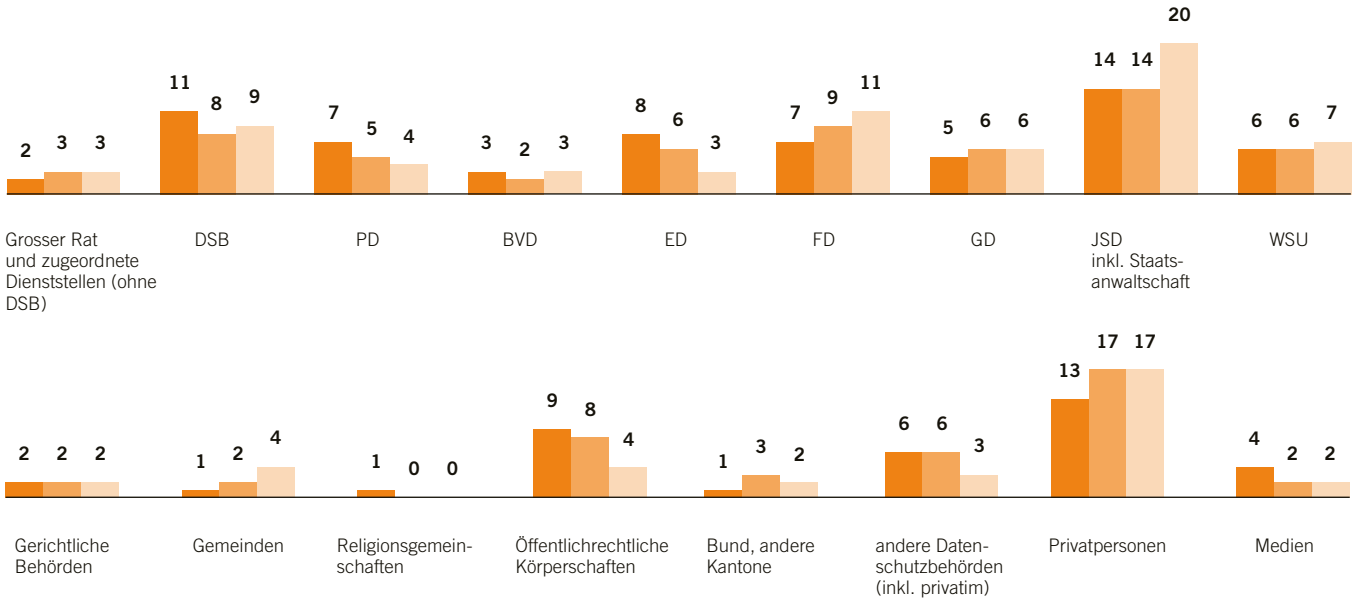
	2012	
	Anzahl	%
In der kantonalen Verwaltung eingereichte Gesuche nach § 25 IDG		
Anzahl eingereichte Gesuche	48	
Behandlung der Gesuche nach § 25 IDG		
Anzahl gutgeheissener Gesuche	29	60
Anzahl teilweise gutgeheissener Gesuche	8	17
Anzahl ganz abgewiesener Gesuche	6	13
Anzahl noch nicht rechtskräftig entschiedener Gesuche	5	10

Öffentlichkeitsprinzip ab 2012
Zahlen erfasst durch die Staatskanzlei aufgrund der Meldungen der Departemente (§ 31 IDV).

D Initianten: Veranlasser der Geschäfte (A) in %



E In die Geschäfte (A) involvierte Stellen in %



Fälle

Fall 1 Gefährdungsmeldung und Berufsgeheimnis

Eine Person mit Lehrbefugnis ist zur Behandlung per FFE (fürsorgerischer Freiheitsentzug, seit 1.1.2013: fürsorgerische Unterbringung nach Art. 426 ff. ZGB) in den Universitären Psychiatrischen Kliniken (UPK) eingewiesen und soll nun als «Springer(in)» unterrichten können. Was können die Betreuenden unternehmen, wenn sie daran zweifeln, dass das gut gehen kann?

Eine Person (A.) wurde vorerst per FFE (fürsorgerischer Freiheitsentzug[1]) zur Begutachtung, drei Monate später zur Behandlung in die Universitären Psychiatrischen Kliniken (UPK) eingewiesen. Sie leidet unter einer Psychose (aus dem Formenkreis der Schizophrenie) mit Auftreten von Zwängen, ist unauffällig, solange sie die Medikamente regelmässig nimmt, was aber nicht immer der Fall ist.

A. besitzt die Lehrbefugnis. Im Rahmen der Behandlung hat sie die Frage gestellt, ob sie sich auf Lehrer(innen)stellen bewerben solle, was von den Betreuenden im Sinne der Perspektiven-Schaffung bejaht wurde. Sie hat – ohne Vorstellungsgespräch – in einer Primarschule kurzfristig eine Anstellung erhalten als Lehrperson («Springer(in)»). Die Betreuenden haben Bedenken; es könne vielleicht gut gehen – was aber, wenn eine Psychose ausgelöst wird? Damit stellt sich die Frage: Darf die UPK die Schulbehörden informieren, damit diese die notwendige Risikoeinschätzung vornehmen und allenfalls Massnahmen zur Risikoverminderung (von Nichteinsatz bis zu begleitetem oder beaufsichtigtem Einsatz usw.) treffen können? Dafür gibt es – wenn nicht schon ein Gesetz bei einer Meldepflicht oder einem Melderecht vom Berufs- oder besonderen Amtsgeheimnis entbindet[2] – zwei Wege:

Erster Weg: Die Betreuenden in der UPK versuchen im Gespräch, A. entweder dazu zu bewegen, die Schulbehörden von sich aus zu informieren oder die Betreuenden vom Berufsgeheimnis zu entbinden[3]. Sie können ihr Bemühen auch begründen: Wenn sich – selbst bei erfolgreichen ersten Einsätzen – dereinst einmal herausstellt, dass A. ihre gesundheitlichen Probleme, die u.U. ihre Eignung in Frage stellen, verheimlicht hat, gefährdet dies unweigerlich die langfristige Anstellung. Im Sinne der Transparenz sollen die Betreuenden A. darauf hinweisen, dass sie sich, wenn A. nicht einwilligt, vom Berufsgeheimnis entbinden lassen müssen, weil sie nicht verantworten können, dass A. diesen Einsatz leistet, ohne dass die Anstellungsbehörde die konkreten Umstände kennt.

Zweiter Weg: Die Betreuenden der UPK lassen sich durch das Gesundheitsdepartement vom Berufsgeheimnis entbinden und informieren die zuständigen Schulbehörden. Voraussetzung dafür ist, dass die UPK es nicht verantworten kann, dass A. diesen Einsatz leistet, ohne dass die Anstellungsbehörde die konkreten Umstände kennt und mindestens durch geeignete Massnahmen das Risiko mindern kann. Offen bleibt die Frage, ob sich die UPK vom Berufsgeheimnis entbinden lassen darf oder muss – m.a.W. ob ihre Schutzpflicht gegenüber A. und möglicherweise auch gegenüber allfällig durch A. Gefährdeten zu einer Melde*pflicht* führt oder nur zu einem Melderecht, das gegenüber allfällig entgegenstehenden Interessen an einer erfolgreichen Behandlung von A. abgewogen werden muss. Je nach der Schwere der Gefährdung ist u.E. von einer Melde*pflicht* auszugehen.

Ergebnis

Wenn eine Schutzpflicht und ein Berufsgeheimnis (oder Amtsgeheimnis) kollidieren, kann sich eine Behörde durch die betroffene Person oder durch zuständige (oder vorgesetzte) Behörde vom Geheimnis entbinden lassen.

1 Seit 1.1.2013: fürsorgerische Unterbringung nach Art. 426 ff. ZGB.

2 Zum Beispiel Art. 15d Abs. 3 SVG, wonach Ärzte in Bezug auf Meldungen, dass eine Person wegen einer körperlichen oder psychischen Krankheit, wegen eines Gebrechens oder wegen einer Sucht Motorfahrzeuge nicht sicher führen kann, vom Berufsgeheimnis entbunden sind.

3 Der konkrete Fall konnte auf diese Weise gelöst werden, weil A. von sich aus auf die Stelle verzichtet hat. Es hat sich im Übrigen bei der Schule, welche A. ohne Vorstellungsgespräch anstellen wollte, nicht um eine Basler Schule gehandelt. Der Datenschutzbeauftragte hat in der Folge die entsprechenden Aufsichtsbehörden involviert.

Fall 2 Herausgabe der Krankengeschichte – eine Entscheidung mit Folgen

Immer wieder kommt es vor, dass Patient(inn)en nach erfolgter Behandlung in einem Spital die Krankengeschichte im Original herausverlangen. Bisher wurde verbreitet die Meinung vertreten, einer Herausgabe stehe nichts entgegen, wenn die Patient(inn)en vorgängig eine Haftungsverzichtserklärung unterzeichnet haben. Trifft das zu?

Nach dem Gesundheitsgesetz sind Fachpersonen im Gesundheitswesen verpflichtet, über jede Patientin und jeden Patienten eine Dokumentation anzulegen[1]. Im Kern enthält diese Dokumentation Angaben über die diagnostischen Abklärungen und Untersuchungen, über die therapeutischen und pflegerischen Massnahmen sowie über den Inhalt und den Ablauf der Aufklärung über die zuvor erwähnten Punkte. Damit erfüllt die Dokumentation primär zwei Funktionen: Zum einen dient sie der behandelnden Medizinalperson (dies umfasst meistens auch noch die Pflegefachpersonen und Physiotherapeut(inn)en o.ä.) als materialisiertes Gedächtnis, zum anderen kommt ihr Beweisfunktion in einem allfälligen Haftungsprozess zu.

In der Praxis kamen Spitäler dem Wunsch nach der Herausgabe der Originalkrankengeschichte[2] zum Teil nach, wenn die Patient(inn)en vorgängig einen Haftungsverzicht erklärt hatten. Aus rechtlicher Sicht ist es allerdings fraglich, ob ein Anspruch auf Herausgabe der Originalkrankengeschichte besteht und ob eine Haftungsverzichtserklärung vor Gericht überhaupt standhalten würde.

Die erste Frage ist schnell beantwortet. Das kantonale Gesundheitsgesetz sieht *keinen* Herausgabeanspruch vor. Die Patient(inn)en haben hingegen das Recht, jederzeit Kopien ihrer Krankengeschichte zu erhalten[3]. Dass die Patient(inn)en jedoch keinen Herausgabeanspruch haben, bedeutet jedoch noch nicht, dass das Spital ihnen die Krankengeschichte nicht aushändigen *darf*. Es ist also noch die zweite Frage zu beantworten, ob eine in solchen Situationen häufig verlangte Haftungsverzichtserklärung überhaupt vor Gericht standhalten würde.

Soweit Ärztinnen und Ärzte in einem öffentlichen Spital tätig sind, kommt im Falle eines Schadens in aller Regel das kantonale Haftungsgesetz zur Anwendung[4]. Dieses äussert sich jedoch nicht zur Zulässigkeit eines Haftungsverzichts, womit für die Beantwortung der noch offenen Frage auf die Bestimmungen des Privatrechts geschielt werden muss. Im Rechtsverhältnis zwischen Privaten gilt es als unzulässig, im Voraus Vereinbarungen abzuschliessen, mit denen die Haftung für grobe Fahrlässigkeit oder gar Verschulden ausgeschlossen werden soll. Nach richterlichem Ermessen kann sogar der Verzicht auf die Haftung für leichte Fahrlässigkeit als nichtig erklärt werden, wenn die Verantwortlichkeit aus dem Betrieb eines obrigkeitlich konzessionierten Gewerbes erfolgt[5], was bei der Ausübung des Arztberufs nach vorherrschender Rechtsauffassung[6] der Fall ist. Gleiches gilt für den Betrieb eines Spitals. Darüber hinaus wird die Auffassung vertreten, die Haftung für Körperschäden könne generell weder ausgeschlossen noch beschränkt werden, da es sich bei der körperlichen Unversehrtheit um ein derart zentrales Rechtsgut handle, dass jegliche Freizeichnung als sittenwidrig und damit als nichtig zu beurteilen sei[7]. Wenn also schon im Bereich der Privatautonomie von der Unzulässigkeit einer Haftungsverzichtserklärung für Körperschäden ausgegangen werden muss, so erscheint es als äusserst stossend, einem öffentlichen Organ ein derartiges Verhalten zuzugestehen.

Ergebnis

Die Patienten besitzen keinen Rechtsanspruch auf Herausgabe ihrer Originalkrankengeschichte, wohl aber ein Recht auf Kopien. Den Spitälern ist auch abzuraten, die Originalkrankengeschichte auszuhändigen, wenn die Patienten vorgängig einen Haftungsverzicht erklärt haben, weil es äusserst ungewiss ist, ob ein solcher Haftungsverzicht vor Gericht anerkannt würde. Ein Spital, das die Originalkrankengeschichte im Vertrauen auf die Gültigkeit einer Haftungsverzichtserklärung herausgegeben hat, läuft Gefahr, in einem Haftungsprozess mangels Beweismittel ohne adäquate Verteidigungsmöglichkeit dazustehen.

1 § 29 GesG.
2 Dem würde in der digitalen Welt die Löschung der Daten aus dem (Klinik-)Informationssystem entsprechen.
3 § 29 Abs. 3 GesG.
4 Ratschlag 10.0228.01, 78.
5 Art. 100 Abs. 2 OR.
6 Walter Fellmann, Die Haftung des Arztes in der Schweiz, in: Franz Wenzel (Hrsg.), Handbuch des Fachanwalts Medizinrecht, 2. Aufl., Köln 2009, 1668.
7 Vgl. Art. 20 OR.

Fall 3 Einwilligung oder gesetzliche Grundlage: Die eine Seite der Datenbekanntgabe

Viele öffentliche Stellen erbitten sich das Einverständnis derjenigen Person, über welche Personendaten an andere Stellen weitergegeben werden. Willigt die betroffene Person nicht ein, dann greifen die öffentlichen Stellen auf eine gesetzliche Grundlage zurück, welche die Datenbekanntgabe erlaubt. Ein zulässiges Vorgehen? Und wie verhält es sich, wenn die angefragte Drittperson oder Stelle einem Berufs- oder einem besonderen Amtsgeheimnis unterstellt ist?

Um eine Leistung erbringen zu können, ist eine öffentliche Stelle oftmals darauf angewiesen, von einer anderen Stelle oder anderen Personen Informationen über eine(n) Bürger(in) einzuholen: Damit die Volkszahnklinik ihrem Auftrag der sozialen Zahnpflege[1] nachkommen kann, muss sie beispielsweise wissen, ob Herr Müller allenfalls Ansprüche auf Unterstützungsleistungen hat (was bei der Rechnungsstellung zu berücksichtigen wäre). Damit die Sozialhilfe allfällige Rückforderungsansprüche geltend machen kann, muss sie in Erfahrung bringen können, ob Frau Meier geerbt hat[2].

Datenschutzrechtlich stellt das Nachfragen durch das öffentliche Organ, das die Daten erhalten will, ein *Bearbeiten* von Personendaten dar – konkret ein Erheben von Personendaten. Das ist zulässig unter den Voraussetzungen von § 9 IDG (gesetzliche Grundlage, Verhältnismässigkeit). Gleichzeitig werden mit der Anfrage aber auch Daten bekannt gegeben: dass Herr Müller bei der Volkszahnklinik in Behandlung ist oder dass Frau Meier sich – in welcher Rolle auch immer – in einem Abklärungsverfahren bei der Sozialhilfe befindet. Für das Nachfragen bei anderen Stellen oder Personen müssen deshalb die Bekanntgabevoraussetzungen des § 21 IDG (gesetzliche Grundlage oder Einwilligung, Verhältnismässigkeit) erfüllt sein. Die Rechtfertigung durch eine *Einwilligung* hat der Gesetzgeber bewusst als «Notlösung» konzipiert: Das Legalitätsprinzip würde untergraben, wenn ein öffentliches Organ, sollte es ihm an einer vom Gesetzgeber geschaffenen und damit demokratisch legitimierten Grundlage für sein Handeln fehlen, jedes Mal auf die Einwilligung der betroffenen Person zurückgreift – daher die gewollte Einschränkung auf den «Einzelfall».

Zwei Kontrollfragen helfen in diesen Fällen:

— Soll mit der Einwilligung dem öffentlichen Organ erlaubt werden, dass es *mehr* Daten oder *andere* Daten einholt, als es zur Aufgabenerfüllung benötigt? Nein, wird die Antwort auf diese Frage regelmässig lauten. Also – das zeigt diese Antwort – besitzt das öffentliche Organ die nach IDG notwendige gesetzliche Grundlage (mindestens in Form der mittelbaren gesetzlichen Grundlage[3]) und *braucht* deshalb gar keine Einwilligung. Bei einem Ja – es sollen mehr oder andere Daten eingeholt werden dürfen, als zur Erfüllung der gesetzlichen Aufgabe erforderlich ist – würde wohl das Verhältnismässigkeitsprinzip verletzt.

— Was geschieht, wenn sich ein(e) Klient(in) weigert, diese Vollmacht oder Ermächtigung zu erteilen? Oft bekommt der Datenschutzbeauftragte auf diese Frage die Antwort: Dann hole man die Daten trotzdem ein, weil dafür ja die gesetzliche Grundlage bestehe – ohne die Daten könne das öffentliche Organ seine gesetzliche Aufgabe nicht erfüllen …

Die betroffene Person, der vorgegaukelt wird, sie könne einwilligen oder nicht, muss sich ziemlich verschaukelt vorkommen, wenn sie feststellt, dass auch bei einem Nein die Datenbekanntgabe erfolgt. Oft wird auf Formularen aus falsch verstandener «Kundenfreundlichkeit» eine (Schein-)Einwilligung vorgesehen. Richtig wäre, schlicht für Transparenz zu sorgen. Also nicht «Ich willige ein, dass …», sondern «Ich nehme zur Kenntnis, dass …».

Ergebnis

Wenn eine (unmittelbare oder mittelbare) gesetzliche Grundlage für eine Datenbearbeitung (insb. für das Einholen von Informationen bei einer anderen Stelle oder Person) besteht, ist Transparenz zu schaffen und nicht eine (Schein-)Einwilligung vorzugaukeln.

1 § 11 GesG.
2 § 2 i.V.m. § 17 SHG.
3 § 9 Abs. 1 lit. b bzw. § 9 Abs. 9 lit. b IDG.

Fall 4 Entbindung: Die andere Seite der Datenbekanntgabe

Ein öffentliches Organ darf zur Erfüllung seiner gesetzlichen Aufgabe von einer anderen Stelle oder Person Personendaten über eine Klientin oder einen Klienten erheben. Damit ist aber noch nicht sichergestellt, dass das angefragte öffentliche Organ oder die angefragte Person auch Auskunft erteilen darf (oder muss).

Nehmen wir an, dass ein öffentliches Organ, damit es seine gesetzliche Aufgabe erfüllen kann, über eine Klientin oder einen Klienten Daten benötigt, die bei einem anderen öffentliche Organ oder bei einer privaten Person oder einem privaten Unternehmen vorliegen. Dieses Nachfragen hat zwei Seiten:

— Darf das öffentliche Organ überhaupt *fragen*? Diese eine Seite wird im Fall 3 behandelt.

— Darf oder *muss* das angefragte öffentliche Organ, die angefragten Privatperson oder das angefragte private Unternehmen *antworten*? Auf dieser anderen Seite stellt sich die Frage nach der Zulässigkeit separat nochmals.

Ein *öffentliches Organ* darf Personendaten bekannt geben, wenn a) eine gesetzliche Bestimmung dazu verpflichtet oder ermächtigt, oder b) dies zur Erfüllung einer gesetzlichen Aufgabe erforderlich ist 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[1]. Ausserdem hat das angefragte öffentliche Organ nach § 29 IDG zu prüfen, ob die Bekanntgabe von Informationen im konkreten Fall allenfalls ganz oder teilweise zu verweigern oder aufzuschieben ist, weil eine besondere gesetzliche Geheimhaltungspflicht oder ein überwiegendes öffentliches oder privates Interesse entgegensteht.

Für eine angefragte *private Person* – eine natürliche oder juristische Person – ist die Frage nach Art. 12 f. DSG/Bund zu beantworten: Eine Datenbekanntgabe kann durch die Einwilligung der betroffenen Person, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt sein.

Dabei kann es also durchaus vorkommen, dass einer Datenbekanntgabe ein Berufsgeheimnis (medizinisches Berufsgeheimnis, Anwaltsgeheimnis, Beichtgeheimnis usw.), ein besonderes Amtsgeheimnis oder ein überwiegendes öffentliches oder privates Interesse entgegensteht. In diesem Fall darf oder muss die angefragte Stelle oder Person die Bekanntgabe ganz oder teilweise einschränken.

Hier kann eine Entbindung durch die betroffene Person Klarheit schaffen. Wenn die Patientin ihre Ärztin vom Berufsgeheimnis oder ein Klient ein angefragtes öffentliches Organ vom besonderen Amtsgeheimnis entbindet, steht einer Auskunftserteilung nichts mehr im Wege. Wenn ein angefragtes öffentliches Organ eine Interessenabwägung im Sinne von § 29 IDG vornimmt, wird das private Interesse der betroffenen Person nicht mehr entgegenstehen oder nicht überwiegen, wenn diese Person selber in die Bekanntgabe einwilligt. Eine solche Entbindung soll möglichst konkret ausformuliert sein, so dass die betroffene Person abschätzen kann, in welchen Informationsaustausch sie ihre Einwilligung gibt.

Ergebnis

Eine Entbindung durch die betroffene Person führt dazu, dass ein angefragtes öffentliches Organ oder eine angefragte Privatperson Auskunft geben darf und nicht wegen eines Berufsgeheimnisses, wegen eines besonderen Amtsgeheimnisses oder wegen überwiegender entgegenstehender privater Interessen die Bekanntgabe einschränken muss. Eine solche Entbindungserklärung muss klar und möglichst konkret ausformuliert sein.

1 § 21 Abs. 1 IDG für «gewöhnliche» Personendaten; für die Bekanntgabe von besonderen Personendaten stellt § 21 Abs. 2 IDG qualifizierte Voraussetzungen auf. Für Bundesorgane oder öffentliche Organe anderer Kantone gelten die i.d.R. vergleichbaren Bestimmungen des DSG/Bund bzw. der entsprechenden kantonalen (Informations- und) Datenschutzgesetze.

Fall 5 Die Begründung der Einschränkung des Informationszugangs im Rekursverfahren

Ein öffentliches Organ schränkt den Zugang zu Informationen teilweise ein, worauf die Gesuchstellerin dagegen Rekurs einreicht. Wie kann das öffentliche Organ im Rekursverfahren seine Verfügung begründen, ohne gerade offenzulegen, was es geheim halten will?

Ein öffentliches Organ besitzt Informationen, die es zur Erfüllung seiner Aufgaben bearbeitet. Gestützt auf das Öffentlichkeitsprinzip[1] stellt eine Bürgerin das Gesuch um Zugang zu diesen Informationen.

Das öffentliche Organ prüft das Gesuch. Es kommt zum Schluss, dass die Informationen dem Recht auf Zugang unterstehen – es sind auch keine nicht fertig gestellten Aufzeichnungen. Das Recht auf Zugang steht der Bürgerin voraussetzungslos zu; sie muss sich weder über ihre Identität ausweisen noch ein besonderes Interesse geltend machen. Allerdings muss das öffentliche Organ prüfen, ob es den Zugang zu den Informationen im konkreten Fall ganz oder teilweise verweigern oder aufschieben muss, weil eine besondere gesetzliche Geheimhaltungsbestimmung oder ein überwiegendes öffentliches oder privates Interesse entgegensteht[2]. Im Rahmen dieser Prüfung kommt es zum Schluss, dass es bestimmte Teile der Information nicht zugänglich machen darf, weil andernfalls die öffentliche Sicherheit gefährdet ist oder die Privatsphäre von Drittpersonen verletzt wird[3]. Es teilt deshalb der Gesuchstellerin mit, dass es in Betracht ziehe, das Gesuch aufgrund eines überwiegenden öffentlichen Interesses teilweise abzuweisen[4]. Die Gesuchstellerin verlangt daraufhin den Erlass einer anfechtbaren Verfügung[5]. Das öffentliche Organ stellt nun die Frage, wie es in der Verfügung und erst recht in einem allfälligen Verfahren vor der Rekursinstanz die Abdeckung begründen kann, ohne gerade offenzulegen, was es geheim halten will.

Die Einschränkung muss in der Verfügung mindestens summarisch begründet werden. Das öffentliche Organ muss seinen Entscheid in einer Weise erläutern, die es der Gesuchstellerin erlaubt, diesen zumindest in den Grundzügen zu verstehen. Das heisst erstens, dass die Einschränkung sichtbar sein muss – es darf nicht einfach Text gelöscht werden, sondern es muss erkennbar sein, dass an dieser Stelle Text unzugänglich gemacht wird (z.B. durch eine schwarze Abdeckung). Zweitens muss summarisch angegeben sein, weshalb die Abdeckung erfolgt (z.B. bei einem Prüfbericht, in welchem Lücken in der IT-Sicherheit aufgedeckt wurden, durch die Erläuterung, dass die Offenlegung des eingeschwärzten Absatzes Angriffe auf das IT-System ermöglichen oder vereinfachen und damit die öffentliche Sicherheit gefährden würde).

Im Rekursverfahren ist v.a. die Rekursinstanz gefordert. Sie muss von der verfügenden Instanz (neben der eingeschwärzten Version) auch die «offene» Version erhalten sowie die ausführliche Begründung der Einschränkung, gleichzeitig aber dafür sorgen, dass die Rekurrentin die Information, um die gestritten wird, nicht erhält (auch nicht aus der ausführlichen Rekursantwort des öffentlichen Organs!), bevor nicht *rechtskräftig* darüber entschieden ist, dass sie sie bekommen darf – auch wenn der Rekurs gutgeheissen werden sollte, steht einer allenfalls betroffenen Drittperson, zu deren Privatsphären-Schutz bestimmte Informationen abgedeckt wurden, der weitere Rechtsweg noch offen! Das ist aber für die Rekursinstanzen nichts grundlegend Neues: Sie mussten schon bisher bei der Einschränkung des Rechts auf Zugang zu den eigenen Personendaten[6] z.B. darüber entscheiden, ob der Name eines Informanten herausgegeben oder geheim gehalten werden muss. Und auch hier galt: Information, die draussen ist, kann – anders als beispielsweise Geld – nicht zurückgerufen werden.

Ergebnis

Ein öffentliches Organ, das den Zugang zu einer Information, die bei ihm vorhanden ist, einschränken will, muss die Einschränkung erkennbar vornehmen und mindestens summarisch so begründen, dass die gesuchstellende Person die Einschränkung verstehen kann. Gegenüber der Rekursinstanz sind die eingeschwärzten Informationen offenzulegen und die Einschränkung ist ausführlich zu begründen. Die Rekursinstanz muss ihrerseits dafür sorgen, dass die obsiegende Partei die Information erst bekommt, wenn der Entscheid zu ihren Gunsten rechtskräftig ist.

1 § 75 Abs. 2 KV; § 25 IDG.
2 § 75 Abs. 3 KV; § 29 IDG.
3 § 29 Abs. 2 lit. a bzw. § 29 Abs. 1 lit. a IDG.
4 § 33 Abs. 2 IDG.
5 § 33 Abs. 4 IDG.
6 § 26 IDG, früher § 20 DSG.

Fall 6 Publikation von Statistik-Daten im digitalen Basler Stadtplan (GeoViewer)

Das Statistische Amt veröffentlicht in Zusammenarbeit mit dem Grundbuch- und Vermessungsamt kleinräumige statistische Daten im Internet-Stadtplan GeoViewer. Die Publikation umfasst Bevölkerungsdaten zu Alter, Herkunft, Einkommen, Vermögen, Sozialhilfe und Sesshaftigkeit sowie Daten zu Kleinwohnungen und zum Leerwohnungsbestand. Eine unzulässige Bekanntgabe von Personendaten?

Der Grosse Rat regte Ende der 1990er Jahre an, die Steuerstatistik zu publizieren. Wenn eine Statistik keine Personendaten enthält, braucht es für die Publikation keine gesetzliche Grundlage im Sinne von § 21 IDG. Aus Datenschutzsicht geht es also darum, dafür zu sorgen, dass in einer Statistik keine Personendaten mehr enthalten sind, das heisst, dass die veröffentlichten Daten keine Informationen mehr sind, «die sich auf eine bestimmte oder bestimmbare natürliche oder juristische Person beziehen»[1]. In der Praxis gilt die Faustregel, dass Durchschnittswerte, die sich auf mehr als 20 Personen beziehen, keinen Personenbezug mehr aufweisen[2].

Das Statistische Amt sorgt – nach Rücksprache mit dem Datenschutzbeauftragten – mit folgenden Massnahmen dafür, dass bei der raumbezogenen Publikation von Einkommens- und Vermögensverhältnissen im GeoViewer[3] keine Rückschlüsse auf einzelne Personen möglich werden:

— Es werden bestimmte *Daten* (Reineinkommen, Reinvermögen) nur als Durchschnittwert-*Kategorien*[4] *pro Wohnblock* angezeigt. Ein Wohnblock ist in aller Regel nicht etwa eine einzelne grosse Liegenschaft, sondern ein «Geviert», das von Strassen umgeben ist. Wenn in einem solchen Wohnblock *weniger als 30 Steuerveranlagungen* vorliegen, wird überhaupt kein Wert ausgewiesen.[5]

— Es werden *Anteile* (Quotienten: Altersquotient, Ausländeranteil, Jugendquotient, Sesshaftigkeit) in *Kategorien*[6] *pro Wohnblockseiten* angezeigt – also räumlich präziser als die erwähnten bestimmten Daten, aber eben nur als Quotienten. Ausserdem beruht bei Wohnblockseiten die Berechnung von Quotienten auf den Angaben zu *mindestens 4 Personen*, andernfalls wird kein Wert ausgewiesen[7].

— Ebenfalls nur pro *Wohnblock* wird der Sozialhilfequotient in *Kategorien*[8] angezeigt. Hier wird in Wohnblöcken mit *weniger* als *30 Personen kein Wert* ausgewiesen[9].

Werden diese Massnahmen umgesetzt, dann wird dem Öffentlichkeitsprinzip und dem Datenschutz Genüge getan, weil zwar staatliche Daten veröffentlicht werden, aber eben so, dass die Persönlichkeitsrechte der betroffenen Personen nicht verletzt werden. Ob aus anderen Gründen auf eine Publikation verzichtet werden soll, haben die politischen Organe (Regierungsrat und Grosser Rat) zu entscheiden. Dabei ist umfassend abzuwägen: Wird in «reichen» Gebieten mehr eingebrochen als in «ärmeren»? Oder sind Einfamilienhausquartiere unattraktiver, weil eine unbekannte Person mehr auffällt als in einer anonymen Grossüberbauung – oder weil es mehr Alarmanlagen hat? Und sagt ein Eintrag im GeoViewer überhaupt mehr, als man nicht ohnehin wahrnehmen kann, wenn man durch ein Quartier fährt, Google Street View benützt oder auch nur ein Luftbild ansieht?

Ergebnis

Die Publikation von Statistik-Daten im digitalen Stadtplan des Kantons Basel-Stadt ist aus datenschutzrechtlicher Warte zulässig, wenn dadurch keine Rückschlüsse auf einzelne Personen möglich werden. Indem nur Durchschnittswerte eines Gevierts à mindestens 30 Steuerveranlagungen, bestimmte Anteile pro Wohnblockseite nur bei mindestens vier Personen pro Anteil und der Sozialhilfequotient pro Geviert nur bei ebenfalls mindestens 30 Personen ausgewiesen werden, dürften keine Persönlichkeitsrechte verletzt werden. Ob aus anderen Gründen auf die Publikation verzichtet werden soll, ist politisch zu entscheiden.

1 § 3 Abs. 3 IDG.
2 50 Personen bei besonderen Personendaten (bei «sensitiven» Personendaten i.S.v. § 3 Abs. 4 lit. a Ziff. 1 IDG). Klar ist, dass bei sehr homogenen Verhältnissen der «Personenbezugswert» von Durchschnittsdaten höher ist als bei sehr homogenen Verhältnissen.
3 http://www.stadtplan.bs.ch/geoviewer/
4 ≤ 40'000, 40'000-49'999, 50'000-59'999, 60'000-69'999, ≥ 70'000 CHF.
5 Anzeige: «Aus Datenschutzgründen nicht ausgewiesen».
6 z.B. ≤ 10.0%, 10.0-19.9%, 20.0-29.9%, 30.0-59.9%, ≥ 60%.
7 Anzeige: «Aus Datenschutzgründen nicht ausgewiesen».
8 ≤ 2.0%, 2.0-3.9%, 4.0-5.9%, 6.0-7.9%, ≥ 8.0%.
9 Anzeige: «Aus Datenschutzgründen nicht ausgewiesen».

Fall 7 Videoüberwachung: Wenn die Kameras nun schon mal da sind …

Gewisse Schalterbereiche von öffentlichen Organen werden mit Videokameras überwacht, damit potentiell gewalttätige Personen von ihren Taten abgehalten und Zwischenfälle aufgeklärt werden können. Wenn die Kameras nun mal schon da sind: Dürften die Aufzeichnungen auch in allfälligen arbeitsrechtlichen Streitigkeiten genutzt werden?

Eine Dienststelle lässt nach verschiedenen Vorfällen mit gewalttätigen Kund(inn)en den Schalterbereich und einen Teil der Mitarbeiter(innen)büros gestützt auf § 17 IDG mit Videokameras überwachen. Diese Kameras dienen dem Schutz der Mitarbeiter(innen) bzw. der Aufklärung allfälliger Übergriffe auf Mitarbeiter(innen), was auch im Reglement zum Betrieb der Kameras (§ 18 Abs. 1 IDG) so festgehalten ist.

Wenn nun die Videoüberwachung schon mal eingerichtet ist, kommt die Frage auf, ob diese Aufzeichnungen auch genutzt werden dürften, wenn beispielsweise der Verdacht laut würde, dass einzelne Mitarbeiter(innen) ihre Arbeitszeit nicht zur Erfüllung ihrer Aufgaben nutzen, sondern ausgedehnte Pausen, Besuche in anderen Büros oder sogar Nickerchen machen. Wäre es zulässig, die Bilder stichprobenweise und bei begründetem Verdacht auf die mangelnde Arbeitsleistung der Mitarbeitenden auszuwerten? In einem Disziplinarverfahren wären die Aufzeichnungen ein ideales Beweismittel …

Das IDG lässt keinen Spielraum für einen anderen als den in § 17 umschriebenen Einsatz der Kameras. Der Wortlaut ist abschliessend gefasst. Würden die Bilder, welche zum Schutz von Personen und Sachen vor strafbaren Handlungen bzw. zur Verfolgung solcher Taten angefertigt wurden, in einem Disziplinarverfahren wegen mangelndem Arbeitseinsatz oder übermässigem «Pausenmachen» genutzt, so stellte dies eine Zweckänderung dar. Unter dem Titel «Zweckbindung» legt das IDG fest, dass Personendaten nur zu dem Zweck bearbeitet werden dürfen, zu dem sie erhoben worden sind, «soweit nicht eine gesetzliche Grundlage ausdrücklich eine weitere Verwendung vorsieht oder die betroffene Person im Einzelfall einwilligt»[1].

Soll Videoüberwachung eingesetzt werden, um kontrollieren zu können, ob die Mitarbeitenden arbeiten, dann müsste dafür zuerst eine separate gesetzliche Grundlage geschaffen werden. Dabei müsste vor allem die Verhältnismässigkeit kritisch geprüft werden. Ausserdem enthält die Arbeitsverordnung[2], die auch für die öffentlichen Arbeitgeber gilt, ein Überwachungsverbot bezüglich des Verhaltens der Angestellten. Sind Überwachungs- oder Kontrollsysteme aus andern Gründen erforderlich (wie beispielsweise zur Vermeidung von Straftaten), sind sie so zu gestalten und anzuordnen, dass die (psychische) Gesundheit der Arbeitnehmer(innen) dadurch nicht beeinträchtigt wird. Statt eines Systems, das immer aufzeichnet, wäre mit einem System, das nur aufzeichnet, wenn und solange beispielsweise eine Kasse oder ein Betäubungsmittelschrank geöffnet ist, der Verhältnismässigkeit eher Rechnung getragen.

Ergebnis

Das IDG erlaubt den Einsatz von Videokameras ausschliesslich zum Schutz von Personen und Sachen vor strafbaren Handlungen beziehungsweise zur Verfolgung solcher strafbarer Handlungen. Die Überwachung des Arbeitsplatzes im Sinne einer Mitarbeiter(innen) überwachung für den Fall arbeitsrechtlicher Streitigkeiten ist davon nicht erfasst und daher ohne separate gesetzliche Grundlage unzulässig.

1 § 12 IDG
2 Art. 26 ArGV 3.

Fall 8 E-Mail-Disclaimer: Kein «Outsourcing der Verantwortung»

Bekommen Sie auch E-Mails mit einem Disclaimer, mit dem Ihnen verboten wird, die Informationen der Nachricht zu verwenden oder weiterzugeben, falls Sie nicht der rechtmässige Empfänger sind? Manchmal wird gar gedroht, es sei strafbar oder Sie würden haften, wenn Sie gegen diese Aufforderung verstossen. Sind solche Disclaimer sinnvoll?

Mit einem Disclaimer am Ende von E-Mails versuchen sich Absender(innen) eines E-Mails vor dem Schaden zu schützen, der entstehen kann, weil sie ein E-Mail an eine falsche Adresse schicken. Und nun sollen Sie als Empfänger(in) es richten. Bemerkenswerterweise stehen die Disclaimer erst am Schluss des Mail-Textes – wer Mails nicht von hinten zu lesen beginnt, hat also den Inhalt, der nicht für ihn bestimmt ist, bereits gelesen, wenn er auf die Aufforderung stösst.

Die Verantwortlichkeit für das Datenbearbeiten – in diesem Fall: das Bekanntgeben per E-Mail – ist im IDG klar geregelt: «Die Verantwortung für den Umgang mit Informationen trägt dasjenige öffentliche Organ, das die Informationen zur Erfüllung seiner gesetzlichen Aufgaben bearbeitet»[1] oder durch Dritte bearbeiten lässt[2]. Wer ein E-Mail verschickt, ist und bleibt also verantwortlich dafür, dass das Informations- und Datenschutzgesetz eingehalten wird. Gerade weil Daten, die an Dritte (nicht nur an Private, sondern auch an andere öffentliche Organe) bekannt gegeben werden, faktisch den Einflussbereich des bekanntgebenden öffentlichen Organs verlassen, formuliert das IDG Voraussetzungen für die Datenbekanntgabe[3]. Das öffentliche Organ, das diese Voraussetzungen nicht einhält, also etwa Personendaten an Unberechtigte weitergibt, kann sich der Verantwortung für seine unrechtmässige Datenbekanntgabe durch einen Disclaimer nicht entziehen – gleich wie bei der durch die Zustellung an Unberechtigte allenfalls begangenen Amtgeheimnisverletzung: Diese wird durch die Bekanntgabe des Geheimnisses begangen und nicht aufgehoben durch die Aufforderung an den Empfänger, das Mitgeteilte gleich wieder zu vergessen, falls es ihm unberechtigterweise mitgeteilt worden sei.

Immerhin aber könnte mit der Bitte an unberechtigte Empfänger möglicherweise – aber ohne rechtliche Wirkung – auf ein immerhin schadenminderndes Verhalten hingewirkt werden, nach dem Motto: Nützt es nichts, so schadet es (wenigstens) nicht. Das ist aber kritisch zu hinterfragen: Erstens wirkt das, was jemand nicht wissen sollte, häufig umso interessanter. Und zweitens: Schadet es wirklich nicht? Erfahrungsgemäss kann die Einführung von Sicherheitsmassnahmen dazu führen, dass deswegen unsicherer gehandelt wird («ich kann schneller in die Kurve fahren, denn mein Auto besitzt ja ein ABS»), so dass der durch die Sicherheitsmassnahmen angepeilte Sicherheitsgewinn aufgrund des sorgloseren Umgangs gleich wieder reduziert oder sogar vereitelt wird.

Wenn ein E-Mail-Disclaimer zu weniger Sorgfalt beim Versenden von E-Mails führt («ich muss mich nicht mehr so genau vergewissern, ob der Empfänger der richtige ist, denn ich hänge ja einen Disclaimer an»), dann würde das Risiko von Persönlichkeitsrechts- und Amtsgeheimnisverletzungen im Resultat eher vergrössert. Wird diese Gefahr als gering eingeschätzt, könnte ein Disclaimer allenfalls Sinn machen. Aber sicher nicht in Form einer Drohung mit Strafe und Haftung, sondern als Bitte, das Mail unverzüglich zu löschen und den Absender zu informieren.

Ergebnis

Ein Disclaimer befreit nicht von der datenschutzrechtlichen Verantwortung des Datenbearbeiters für das korrekte Datenbearbeiten. Er kann also die Haftung für eine Verletzung der Persönlichkeitsrechte oder des Amtsgeheimnisses in keinem Fall beseitigen. Mit einem Disclaimer kann höchstens – wenn auch rechtlich nicht verbindlich – auf ein schadenminderndes Verhalten durch den unberechtigten Empfänger hingewirkt werden.

1 § 6 Abs. 1 IDG.
2 § 7 Abs. 2 IDG.
3 §§ 21 ff. IDG.

Anhang

Verzeichnis der zitierten Gesetze und Materialien

Rechtsgrundlagen des Kantons Basel-Stadt

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

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

IDV Verordnung vom 9. August 2011 über die Information und den Datenschutz (Informations- und Datenschutzverordnung, IDV), SG 153.270.

Gesundheitsgesetz Gesundheitsgesetz vom 21. September 2011, SG 300.100.

KV Verfassung des Kantons Basel-Stadt vom 23. März 2005 (KV), 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.

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

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

UKBB-Vertrag Vertrag vom 16. Februar 1998 zwischen den Kantonen Basel-Stadt und Basel-Landschaft über das Universitäts-Kinderspital beider Basel (Kinderspitalvertrag), SG 331.300.

VBG Gesetz vom 12. April 1944 über die Vormundschaftsbehörde und den behördlichen Jugendschutz, SG 212.400 (wirksam bis 31. Dezember 2012).

Weisung Weisung vom 22. Oktober 2003 für die Benutzung von Informatikmitteln in der Verwaltung des Kantons Basel-Stadt.

Rechtsgrundlagen des Kantons Basel-Landschaft

IDG/BL Gesetz vom 10. Februar 2011 über die Information und den Datenschutz (IDG BL), SGS 162.

VwVG/BL Verwaltungsverfahrensgesetz Basel-Landschaft vom 13. Juni 1988 (VwVG BL), SGS 175.

Vo VwVG/BL Verordnung vom 30. November 2004 zum Verwaltungsverfahrensgesetz Basel-Landschaft (Vo VwVG BL), SGS 175.11.

Bundesrecht

ArGV 3 Verordnung 3 vom 18. August 1993 zum Arbeitsgesetz (Gesundheitsvorsorge, ArGV 3, SR 822.113).

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

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

HRegV Handelsregisterverordnung vom 17. Oktober 2007 (HRegV), SR 221.411.

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

IVV Verordnung vom 17. Januar 1961 über die Invalidenversicherung (IVV), SR 832.201.

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.

StGB Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (StGB), SR 311.0.

SVG Strassenverkehrsgesetz vom 19. Dezember 1958 (SVG), SR 741.01.

VDSG/Bund Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (VDSG), SR 235.11.

VOSTRA-Verordnung Verordnung vom 29. September 2006 über das Strafregister (VOSTRA-Verordnung), SR 331.

VwVG/Bund Bundesgesetz vom 20. Dezember 1968 über das Verwaltungsverfahren (Verwaltungsverfahrensgesetz, VwVG), SR 172.021.

ZPO Schweizerische Zivilprozessordnung vom 19. Dezember 2008 (Zivilprozessordnung, ZPO), SR 272.

Materialien

GRB 10/36/09G Grossratsbeschluss vom 8. September 2010 betreffend das Gesuch der Christengemeinschaft um Kantonale Anerkennung gem. § 133 der baselstädtischen Kantonsverfassung.

GRB 12/02/11G Grossratsbeschluss vom 11. Januar 2012 betreffend das Gesuch der Neuapostolischen Kirche Schweiz, Bezirk Basel um Anerkennung als Kirche nach § 133 der Verfassung des Kantons Basel-Stadt.

GRB 12/42/11G Grossratsbeschluss vom 17. Oktober 2012 betreffend das Gesuch der Kulturvereinigung der Aleviten und Bektaschi und des Alevitischen Kulturzentrums Regio Basel um kantonale Anerkennung gemäss § 133 der baselstädtischen Kantonsverfassung.

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

Ratschlag 10.0228.01 Ratschlag 10.0228.01 vom 30. August 2010 betreffend Gesetz über die öffentlichen Spitäler des Kantons Basel-Stadt (ÖSpG).

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
Beat Rudin, Dr. iur., Advokat

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

Volontär(in):
Alexandra Büche, MLaw
(1. 10. 2011 - 31. 3. 2012)
Angelo Imperiale, MLaw
(1. 4. - 30. 9. 2012)
Nadine Battilana, MLaw
(1. 10. 2012 - 30. 6. 2013)

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

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

Gestaltung
Andrea Gruber,
Visuelle Gestaltung, Basel

Druck
Gremper AG