Datenschutzbeauftragter des Kantons Basel-Stadt

Bericht an den Grossen Rat

2015

Inhaltsübersicht

Einleitung

Themen

Der Datenschutzbeauftragte erstattet der Wahlbehörde jährlich Bericht über seine Tätigkeit, Feststellungen und Erfahrungen; der Bericht wird veröffentlicht (§ 50 IDG).

Fotokonzept: «Spuren»

Aus dem Alltag

Fälle

Anhang

Einleitung 2015: «Und – alles im Griff?»

Die Verfassung gibt den Behörden die Aufgabe, die Grundrechte der Bürgerinnen und Bürger zu achten, darunter auch das Grundrecht auf informationelle Selbstbestimmung. Mit einem Blick auf die Entwicklungen – technologische, gesellschaftliche und politische – stellt sich die Frage: Kommen die Behörden dieser Aufgabe nach? Inwiefern ist es überhaupt möglich, dieser Aufgabe nachzukommen? Was ist die Funktion des Datenschutzbeauftragten in dieser Sache? Und wie wichtig ist der Bevölkerung der Schutz ihrer Persönlichkeitsrechte?

Eine gute Frage

Alles im Griff? Da kommt an einem Anlass ein junger Grossrat auf mich zu und fragt interessiert: «Und – alles im Griff?» Das könnte man jetzt abtun als Smalltalk – was soll er denn sonst sagen? Mich hat die Frage aber nicht losgelassen. Es ist eigentlich eine sehr gute Frage!

Entwicklungen im Jahr 2015 Allein wenn wir uns vor Augen halten, was 2015 alles passiert ist und sich auf den Datenschutz – direkt oder indirekt auch auf die Verwaltung des Kantons – auswirkt oder auswirken wird: Haben wir dann alles im Griff? Informationssicherheit wird immer anspruchsvoller – kaum ist eine Lücke geschlossen, tauchen die nächsten zwei auf. Der Europäische Gerichtshof (EuGH) hat gegenüber Suchmaschinen ein Recht auf Vergessen anerkannt und etwas später das EU-Safe-Harbor-Abkommen mit den USA aufgehoben. Terroranschläge in Paris führen in der Öffentlichkeit reflexartig zur Forderung nach neuen Überwachungsmassnahmen. Und knapp vor Jahresende hat in der Europäischen Union der Trilog zwischen Parlament, Rat und Kommission mit einer Einigung bezüglich der EU-Datenschutzreform geendet – was durchaus direkte Auswirkungen auf Basel-Stadt haben wird: Der eine Erlass, die neue Datenschutzrichtlinie für die justizielle und polizeiliche Zusammenarbeit, ist schengenrelevant. Wenn also die Sicherheits- und Migrationsbehörden weiterhin vom Zugang zum Schengener Informationssystem (SIS) profitieren wollen, müssen Bund und Kantone ihre Datenschutzgesetzgebungen dem neuen Niveau anpassen. Dazu muss das baselstädtische Informations- und Datenschutzgesetz (IDG[1]) nicht total umgekrempelt werden – aber einige nicht unwesentliche Änderungen werden trotzdem erforderlich sein.

Verantwortung Alles im Griff? Als Datenschutzbeauftragter könnte man nun knapp antworten: «Nicht wir müssen es im Griff haben, sondern nur darauf hinarbeiten, dass die anderen es im Griff haben.» Die Verantwortung für den Umgang mit Informationen liegt – so regelt es das IDG – bei der Dateneignerin, beim öffentlichen Organ, das zur Erfüllung seiner gesetzlichen Aufgabe die Informationen bearbeitet. Nur – so verstehen wir unsere Aufgabe nicht. Sich derart banal aus der Verantwortung zu stehlen, wäre «die billige Tour».

Zuweisung der Verantwortung Klar liegt die Verantwortung nicht beim Datenschutzbeauftragten, wenn die Kantonspolizei einem Medienschaffenden eine bestimmte Information nicht zugänglich macht, weil ein öffentliches Geheimhaltungsinteresse gegenüber dem Zugangsinteresse der Öffentlichkeit überwiege. Klar liegt die Verantwortung nicht beim Datenschutzbeauftragten, wenn die Gebäudeversicherung Immobilien Basel-Stadt einen Onlinezugriff auf ihre Daten erlaubt. Und klar liegt die Verantwortung nicht beim Datenschutzbeauftragten, wenn ein Departement Personendaten durch ein ausländisches Unternehmen bearbeiten lässt, ohne dem Unternehmen die informations- und datenschutzrechtlichen Pflichten zu überbinden. Aber ebenso klar ist, dass der Datenschutzbeauftragte seine gesetzliche Aufgabe nicht erfüllt, wenn er dies einfach geschehen lässt.

Aufgaben des Datenschutzbeauftragten

Beratung Die Hauptaufgaben des Datenschutzbeauftragten sind Beratung und Kontrolle. Die Kantonspolizei kann ihn beiziehen für die Frage der Einschränkung des Informationszugangsrechts. Die Gebäudeversicherung muss ihm ihren Entscheid über die Einräumung eines Onlinezugriffs zur Vorabkontrolle unterbreiten. Und wenn er feststellt, dass Verträge über Auftragsdatenbearbeitungen ohne die gesetzlich erforderlichen Klauseln

abgeschlossen worden sind, kann er beim Departement vorstellig werden und zu erreichen versuchen, dass die Vereinbarung mit der Auftragnehmerin ergänzt wird. Da der Datenschutzbeauftragte aber nicht alles weiss, was in der Verwaltung läuft, ist er darauf angewiesen, dass sensibilisierte Mitarbeiterinnen und Mitarbeiter der Verwaltung merken, wenn sie ihn beiziehen sollten, damit sie die Rechte der betroffenen Personen nicht verletzen.

Kontrolle Der Datenschutzbeauftragte kontrolliert, ob der Umgang mit Informationen gesetzeskonform erfolgt. Aber auch solche Kontrollen können nie flächendeckend erfolgen, sondern bloss stichprobenweise. Auch hier ist es somit unerlässlich, dass aufmerksame Mitarbeiterinnen und Mitarbeiter der Verwaltung ihre Verantwortung wahrnehmen. Und wenn eine Datenschutz-Prüfung Defizite aufdeckt, geht es nicht um Schuldzuweisung, gegen die man sich verteidigen muss, sondern vielmehr um Anstösse zur Verbesserung – im Interesse des Schutzes der Grundrechte der betroffenen Personen.

Sensibilisierung Es ist unumgänglich, dass die Mitarbeiterinnen und Mitarbeiter der Verwaltung für die Aspekte Datenschutz und Öffentlichkeitsprinzip sensibilisiert sind. Daran arbeiten wir – und stellen dies in diesem Tätigkeitsbericht auch vor (Seiten 8 f.). Auf der anderen Seite stehen die Personen, über die staatliche Behörden Daten bearbeiten, die betroffenen Personen. Welche Erwartungen haben diese an die öffentlichen Organe? Wie wichtig ist ihnen der Schutz ihrer Persönlichkeitsrechte und der Zugang zu Informationen nach dem Öffentlichkeitsprinzip? Vier Fragen dazu konnten der Bevölkerung im Rahmen der Bevölkerungsbefragung 2015 unterbreitet werden. Wir stellen die entsprechenden Resultate vor, versuchen, sie zu interpretieren, und ziehen unsere Schlüsse daraus (Seiten 9 ff.).

Also alles im Griff? Es wäre vermessen, behaupten zu wollen, wir hätten «alles im Griff». Aber wir bemühen uns darum. Wir unterstützen die öffentlichen Organe in ihrem Bestreben, die Regeln des Datenschutzes und des Öffentlichkeitsprinzips einzuhalten. Wir unterstützen die Personen, deren Daten die öffentlichen Organe bearbeiten oder die um Zugang zu Informationen ersuchen, in der Wahrnehmung ihrer Rechte. Und oft vermitteln wir zwischen den staatlichen Stellen und den Privaten. Im Vorfeld der Rechtsetzung und der Umsetzung von Projekten treten wir quasi als «Fürsprecher» der Rechte der Betroffenen ein, die in dieser Phase ja nur selten mitwirken und ihre Rechte selber wahrnehmen können.

Zum Schluss

Dank Unsere Aufgabe könnten wir nicht erfolgreich erfüllen, wenn wir nicht von vielen Menschen und Institutionen unterstützt würden. Mein Dank gilt deshalb

— der Bevölkerung und den staatlichen Institutionen für das entgegengebrachte Vertrauen;
— allen, die sich mit Fragen zum Datenschutz und zum Informationszugang vertrauensvoll an uns wenden;
— allen Mitarbeiterinnen und Mitarbeitern der Verwaltung, der öffentlichrechtlichen Anstalten und der Gerichte, die mithelfen, datenschutzkonforme Lösungen zu finden und umzusetzen;
— den Kolleginnen und Kollegen der «Kleeblatt-Dienststellen» für die unkomplizierte Zusammenarbeit;
— den Präsidien und Mitgliedern des Grossen Rates, des Büros, der Datenschutz-Delegation des Büros und der Kommissionen für ihr Interesse an unserer Arbeit und ihre wertvolle Unterstützung;
— der Volontärin Katrin Gisler und dem Volontär Jonas Annasohn für ihre kritische Neugier und ihre aktive Mitarbeit und
— last but not least meinem Team – Markus Brönnimann, Katrin Gisler (befristet ab 1. November 2015), Katja Gysin (ab 1. Dezember 2015), Sandra Husi (bis 30. September 2015), Carmen Lindner (bis 30. November 2015), Daniela Waldmeier und Barbara Widmer –, das mit unverändert grossem Engagement, mit spannenden Diskussionen und konstruktiven Anregungen unsere Arbeit bereichert und vorangebracht hat. Nach rund 6 ¾ Jahren haben uns zwei Juristinnen aus dem «Startteam» verlassen, Sandra Husi-Stämpfli, meine Stellvertreterin, und Carmen Lindner. Ihnen beiden gebührt mein grosser Dank für ihren tollen und erfolgreichen Einsatz bei Aufbau der neuen Stelle! Beiden wünsche ich viel Erfolg und Befriedigung in ihrer weiteren beruflichen Laufbahn!

Beat Rudin, Datenschutzbeauftragter

1 Die in den Texten erwähnten Rechtsquellen und Materialien sind in einem Verzeichnis am Schluss des Berichts detailliert aufgeführt (Seite 50).

Themen

Thema 1 Für 84,4 % der Bevölkerung ist Datenschutz sehr wichtig

Thema 2 Die «schwierige» Dateneignerin

Thema 1

Für 84,4 % der Bevölkerung ist Datenschutz sehr wichtig

In der Bevölkerungsbefragung 2015 wurde gefragt, wie wichtig den Befragten der Schutz ihrer Persönlichkeitsrechte und das Öffentlichkeitsprinzip sind. Die Ansprüche der Bevölkerung sind diesbezüglich sehr hoch. Auf der anderen Seite zeigt sich in der Beratungstätigkeit des Datenschutzbeauftragten, dass Mitarbeitende der Verwaltung sich der Datenschutzrelevanz ihres Handelns nicht immer bewusst sind. Hier will die verstärkte Sensibilisierungstätigkeit des Datenschutzbeauftragten ansetzen.

Sensibilisierung?

Fragen Sensibilisierung spielt im Umfeld von Datenschutz und Öffentlichkeitsprinzip auf zwei Seiten eine Rolle:

— auf Seiten der Datenbearbeiterinnen und Datenbearbeiter: Ist ihnen bewusst, dass und welche Datenschutzregeln sie einzuhalten haben, wenn sie Daten über Bürgerinnen und Bürger bearbeiten? Ist ihnen bewusst, dass und welche Regel des Öffentlichkeitsprinzips sie zu beachten haben, wenn sie Informationen bearbeiten?

— auf Seiten der betroffenen Personen: Ist ihnen bewusst, dass sie Rechte haben, die sie gegenüber Datenbearbeiterinnen und Datenbearbeitern einfordern können? Wie wichtig sind ihnen Datenschutz und Öffentlichkeitsprinzip?

Teilweise mangelndes Bewusstsein Diese Fragen stellt sich der Datenschutzbeauftragte immer, wenn sich beispielsweise bei Beratungen zeigt, dass Mitarbeitende der Verwaltung sich gar nicht bewusst sind, dass bei ihren Tätigkeiten Datenschutzrecht gilt. Dementsprechend ist dann auch nicht garantiert, dass Datenbearbeitungen gesetzeskonform vorgenommen werden oder dass, wenn dies fraglich ist, der Datenschutzbeauftragte zur Unterstützung beigezogen wird.

Vorhaben Der Datenschutzbeauftragte hat sich deshalb 2015 vorgenommen, künftig stärker für die Sensibilisierung bei den Themen Datenschutz und Öffentlichkeitsprinzip aktiv zu werden. Auf der einen Seite sollte mit verschiedenen Sensibilisierungsaktivitäten das Sensorium der Mitarbeitenden der Verwaltung für Fragen des Datenschutzes und des Öffentlichkeitsprinzips gestärkt werden. Auf der anderen Seite nahm es ihn wunder, wie wichtig der Datenschutz für die Betroffenen, die Bürgerinnen und Bürger ist. Diesbezüglich ergab sich die Möglichkeit, in die Bevölkerungsbefragung 2015 Fragen zum Datenschutz und zum Öffentlichkeitsprinzip aufnehmen zu lassen.

Verwaltungsinterne Sensibilisierungsaktivitäten

«Personelle» Verstärkung Für die verwaltungsinterne Sensibilisierung konnte das Team des Datenschutzbeauftragten verstärkt werden – und das erst noch ohne Erhöhung des Headcounts. Der neue Mitarbeiter bekommt nämlich weder Lohn noch benötigt er einen Arbeitsplatz. Auch sozialversicherungstechnisch ist er anspruchslos …

Der neue Mitarbeiter bekommt weder Lohn noch benötigt er einen Arbeitsplatz. Auch sozialversicherungstechnisch ist er anspruchslos …

Datenschutz-Basilisk Der neue Mitarbeiter trat erstmals Ende Frühjahr 2015 auf – in «BS intern»[1], dem Personalmagazin für alle Mitarbeitenden und die Pensionierten der kantonalen Verwaltung. Der «Datenschutz-Basilisk» taucht plötzlich auf, wenn Mitarbeitende mit Fragen des Datenschutzes oder des Öffentlichkeitsprinzip konfrontiert sind – speziell wenn sie sich dessen gar nicht bewusst sind. In verständlicher und umgänglicher Art weist er auf mögliche Probleme und die geltenden Regeln hin. Er will damit die Leserinnen und Leser zu einem sorgsamen Umgang mit den eigenen und fremden Daten anhalten und ihnen die Bedeutung von Persönlichkeitsschutz und Transparenz bewusst machen (zu den im Jahr 2015 behandelten Themen vgl. hinten Seite 29). Und selbstverständlich hat der Datenschutz-Basilisk (abgekürzt: DSB) auch eine Website: <http://www.dsb.bs.ch>. Auf ihr können alle bisher erschienenen Beiträge abgerufen werden[2].

Schulungen und Referate Selbstredend wurden auch die bisher schon bestehenden Sensibilisierungsaktivitäten fortgesetzt. Zu den Schulungen, Referaten und Publikationen siehe hinten auf den Seiten 28 f.).

Die Bevölkerungsbefragung

Hintergrund Um mehr über die Bedeutung des Datenschutzes aus dem Blickwinkel der Betroffenen herauszufinden, hat sich der Datenschutzbeauftragte an das Statistische Amt gewandt. Eine separate Befragung der Bevölkerung zum Thema Datenschutz, wie sie beispielsweise der Datenschutzbeauftragte des Kantons Zürich hat durchführen lassen, stand ausser Betracht. Es bot sich aber die Gelegenheit, in der 2015 durch das Statistische Amt durchgeführten Bevölkerungsbefragung[3] Fragen zum Thema Datenschutz und Öffentlichkeitsprinzip zu platzieren.

Fragen an die Bevölkerung Die Integration in die Bevölkerungsbefragung des Statistischen Amtes führte zu einer Beschränkung der Anzahl Fragen. Mit Unterstützung durch die Spezialistinnen und Spezialisten des Statistischen Amtes wurden schliesslich vier Fragen[4] formuliert und in den Fragebogen aufgenommen:

— «Die öffentliche Verwaltung und private Unternehmen speichern Daten über Sie. Wie wichtig ist es Ihnen, dass Ihre persönlichen Daten von der öffentlichen Verwaltung und den privaten Unternehmen geschützt werden? Bitte geben Sie hier eine Note zwischen 1 = überhaupt nicht wichtig und 10 = sehr wichtig.»

— «Seit dem 1. Januar 2012 gilt im Kanton Basel-Stadt das Öffentlichkeitsprinzip: Das heisst, die Informationen der Verwaltung sind nicht mehr alle geheim, sondern in der Regel öffentlich zugänglich. Wie wichtig finden Sie das? Bitte geben Sie hier eine Note zwischen 1 = überhaupt nicht wichtig und 10 = sehr wichtig.»

— «Wie beurteilen Sie den Stellenwert, den der Datenschutz in der öffentlichen Diskussion hat? Wird er überbewertet, hat er den richtigen Stellenwert oder müsste er noch mehr thematisiert werden?»

— «Wissen Sie, dass Sie auf der Website des Datenschutzes des Kantons Basel-Stadt <www.dsb.bs.ch> umfassende Informationen zu Ihren Rechten finden?»

Zusammensetzung der Befragten Durch die Integration in die Bevölkerungsbefragung des Statistischen Amtes konnte eine grössere Anzahl Personen befragt werden, als dies bei einer gesonderten Befragung möglich gewesen wäre. Die Auswahl der Befragten erfolgte nach unterschiedlichen Kriterien. So sollten neben Personen mit Schweizer Bürgerrecht auch Ausländerinnen und Ausländer mit Bewilligung B und C befragt werden. Ebenso ist eine Altersdurchmischung von 18 bis über 69 Jahren angestrebt worden. Beteiligt haben sich schliesslich etwas über 1 500 Personen.

84,4 % der Befragten empfinden den Schutz der Personendaten, die von der öffentlichen Verwaltung und von privaten Unternehmen bearbeitet werden, als sehr wichtig und 91 % als eher oder sehr wichtig.

Die Ergebnisse[5]

Wichtigkeit des Persönlichkeitsschutzes Den Schutz der persönlichen Daten, die von der öffentlichen Verwaltung und von privaten Unternehmen bearbeitet werden, beurteilen die befragten Personen mit einem Mittelwert von 8,9 auf einer 10er-Skala; fasst man die Skalenwerte zusammen, dann empfinden 84,4% der Befragten den Schutz der Personendaten als sehr wichtig (Skalenwerte von 8 bis 10) und 91% als eher oder sehr wichtig (Skalenwerte 6-10)[6]. Frauen ist der Datenschutz etwas häufiger eher oder sehr wichtig (93%) als Männern (89%), Ausländerinnen und Ausländern (93%) häufiger als Schweizerinnen und Schweizern (90%). Anders als beim Geschlecht oder dem Bürgerrecht lassen sich bei den unterschiedlichen Haushalteinkommen kaum Unterschiede ausmachen. Nach Altersgruppen steigt die Beurteilung als eher oder sehr wichtig (Skalenwerte 6-10) von 93% (18-29-jährig, 30-39-jährig) leicht auf 95% (40-49-jährig) und sinkt dann wieder auf 93% (50-59-jährig, 60-69-jährig); bei den über 69-Jährigen fällt sie dann ab auf 87%. Interessant ist auch die Verteilung der Befragten, die den Datenschutz als überhaupt nicht wichtig ansehen (Skalenwert 1) oder keine Angaben machen: Am höchsten ist der Wert bei den über 69-Jährigen (8%); bei den anderen Altersgruppen liegt er bei 1% (18-29-Jährige) oder unter 1% (30-39-, 40-49- und 60-69-Jährige) und 3% (50-59-Jährige). >

Wichtigkeit des Öffentlichkeitsprinzips Verglichen mit der Wichtigkeit des Datenschutzes wird das seit 2012 geltende Öffentlichkeitsprinzip als weniger wichtig beurteilt; im Durchschnitt erreicht die Wichtigkeit einen Wert von 6,7 auf einer 10er-Skala[7]. Fasst man die Skalenwerte zusammen, dann empfinden 51% der Befragten das Öffentlichkeitsprinzip als sehr wichtig (Skalenwerte 8-10) und 69% als eher oder sehr wichtig (Skalenwerte 6-10)[8]. Das Öffentlichkeitsprinzip ist Männern etwas häufiger eher oder sehr wichtig (74%) als Frauen (64%), Schweizerinnen und Schweizern (69%) leicht häufiger als Ausländerinnen und Ausländern (67%). Auch bei der Frage nach der Wichtigkeit des Öffentlichkeitsprinzips unterscheiden sich die Werte bezüglich der unterschiedlichen Haushaltseinkommen kaum. Die Altersgruppe der 60-69-Jährigen weist mit 76% der höchsten Anteil an Bewertungen als eher oder sehr wichtig (Skalenwerte 6-10) auf; bei den anderen Altersgruppen bewegen sie sich zwischen 64% (über 69-Jährige) und 70% (30-39-Jährige). Vergleichsweise hoch ist bei dieser Frage die Anzahl derjenigen, die keine Angabe gemacht haben hinsichtlich der Wichtigkeit des Öffentlichkeitsprinzips (6%), wobei diesbezüglich insbesondere die weiblichen Befragten (8%), die Ausländerinnen und Ausländer (9%) sowie die über 69-Jährigen (9%) auffallen.

76% der Befragten finden, dass der Datenschutz so wie heute oder höher gewichtet werden sollte, während 16% ihn als überbewertet empfinden; 9% äussern keine Meinung zu dieser Frage.

Stellenwert des Datenschutzes Auf die Frage nach dem Stellenwert des Datenschutzes in der öffentlichen Diskussion gaben 42% der Befragten an, er sei genau richtig. 34% fanden, er müsste noch mehr thematisiert werden, während 16% ihn als überbewertet empfanden. Wie oben erwähnt bewerten die Ausländerinnen und Ausländer den Datenschutz als wichtiger als die Schweizerinnen und Schweizer. Dieser Unterschied zeigt sich auch bei der Beurteilung des Stellenwertes des Datenschutzes in der öffentlichen Diskussion: 44% der Ausländerinnen und Ausländer erachten ihn als unterbewertet, 35% als genau richtig und nur 8% als überbewertet. Die Schweizerinnen und Schweizer erachten ihn zu 33% als unterbewertet, zu 43% als genau richtig und zu 17% als überbewertet. Ins Auge sticht, dass 12% der Frauen (gegenüber 6% der Männer), 13% der Ausländerinnen und Ausländer (gegenüber 9% der Schweizerinnen und Schweizer) und 14% der über 69-Jährigen keine Angaben zu dieser Frage gemacht haben. Nach Altersgruppen fallen Unterschiede bei der Beurteilung als unterbewertet auf: 24% der über 69-Jährigen halten den Datenschutz in der öffentlichen Diskussion für unterbewertet, während diese Beurteilung bei den übrigen Altersgruppen zwischen 31% (18-29-Jährige) und 42% (40-49- und 50-59-Jährige) erreicht. Zusammengerechnet finden 76% der Befragten, dass Datenschutz so wie heute oder höher gewichtet werden sollte.

Kenntnis der Webseite Unabhängig des Geschlechts, der Nationalität, des Alters oder des Einkommens decken sich die Antworten hinsichtlich der Webseite des Datenschutzbeauftragten: Lediglich eine Minderheit (15%) weiss, dass sie sich auf <http://www.dsb.bs.ch> über ihre Rechte informieren kann. Überdurchschnittliche Ergebnisse hinsichtlich der Kenntnisse der Webseite zeigen sich bei Männern, bei 30-39- und 60-69-Jährigen sowie denjenigen mit einem Haushaltseinkommen unter 3000 Franken. Besonders gering ist das Wissen um die Webseite bei den weiblichen, den 18-29- sowie den über 69-jährigen Befragten.

Ins Auge springende Resultate

«Digital Natives» Die Beurteilung der sog. «Digital Natives»[9] könnte als Überraschung angesehen werden. Die Altersgruppe der 18-29-Jährigen ist grösstenteils mit Computer, Internet, Handy und allerlei digitaler Medien aufgewachsen. Ist darum zu erwarten, dass die Hemmschwelle zur Nutzung dieser Mittel und damit auch das Bewusstsein für den Datenschutz eher tief sind? Offensichtlich nicht. Drei Viertel aller befragten 18-29-Jährigen schätzen den Schutz ihrer Persönlichkeit als sehr wichtig ein, und lediglich 10% finden, dass der Datenschutz überbewertet wird.

Seniorinnen und Senioren Am anderen Ende der Altersgruppen stehen die über 69-jährigen Befragten. Sie sind «Digital Immigrants» (oder nicht einmal das). Sie sind erst im höheren Erwachsenenalter mit der digitalen Welt in Berührung gekommen, kennen mehrheitlich ihr Ausmass und die damit verbundenen Chancen und Risiken nicht vertieft. Halten sie deshalb Datenschutz für sehr wichtig – quasi aus Angst vor dem digitalen Unbekannten? Offensichtlich auch nicht. Im Vergleich zu den restlichen Befragten sehen

sie den Datenschutz stärker als überbewertet an und der Schutz der Privatsphäre ist ihnen eher nicht oder überhaupt nicht wichtig ist (oder sie äussern sich nicht dazu).

Ausländerinnen und Ausländer Die dritte Gruppe, welche aufgrund der Ergebnisse auffällt, sind die Befragten ohne Schweizer Bürgerrecht. Nicht einmal ein Prozent aller ausländischen Befragten finden den Schutz der persönlichen Daten nicht oder überhaupt nicht wichtig. Entsprechend kann ihnen der Stellenwert des Datenschutzes nicht hoch genug sein und er wird – im Vergleich zu den anderen Befragten – sehr viel mehr als «unterbewertet» eingestuft.

Ein Interpretationsversuch

Kontroverse Ergebnisse Während die «Digital Natives» den Stellenwert des Datenschutzes als angemessen ansehen und ihnen der Schutz der persönlichen Daten wichtig ist, gehen die Umfrageergebnisse der über 69-jährigen Befragten in eine andere Richtung. Sucht man nach einer Begründung für diese kontroversen Antworten, kann lediglich spekuliert werden.

Datenschutzbewusstsein durch Sensibilisierung Der Datenschutz ist in den Medien beinahe täglich präsent. Cloud Computing und «Big Data», Überwachung durch den Staat oder durch Private, die Sammelwut von Anbietern von Applikationen und Dienstleistungen sind nur ein paar wenige Stichworte, die dazu führen, dass Datenschutz regelmässig zum Thema in den Medien wird. «Digital Natives», die in den sozialen Medien unterwegs sind, werden immer wieder mit der Frage der Nutzung ihrer Daten konfrontiert. Durch diese Allgegenwart ist es verständlich und nachvollziehbar, dass eine Auseinandersetzung mit der Sicherheit der eigenen Daten stattfindet und dies zu einer Sensibilisierung mit der Thematik führt. Bei aller «Freizügigkeit» in Bezug auf ihre eigenen Daten – die «Digital Natives» scheinen sich ihrer Verletzlichkeit doch bewusst zu sein. Wie sich in Gesprächen mit Jungen auch zeigt: Sie ziehen durchaus auch Grenzen, wenn es darum geht, wie mit Personendaten umgegangen werden soll – dass es andere Grenzen sind als diejenigen, die Ältere ziehen würden, hat wohl auch mit dem unterschiedlichen Erfahrungshorizont zu tun.

Unwissen durch fehlende Praxis Das Gegenstück zu den «Digital Natives» bilden die befragten Seniorinnen und Senioren. In ihren Augen ist der Datenschutz eher überbewertet, und der Schutz der persönlichen Daten ist ihnen nicht in gleichem Ausmass wichtig wie den anderen Befragten. Grund dafür könnte – im Umkehrschluss zur vorherigen Argumentation – sein, dass sie sich mangels praktischer Relevanz einerseits weniger mit dem Datenschutz befassen wollen, andererseits aber auch nicht damit befassen müssen. Es ist verständlich, dass das Interesse geringer ist, wenn es um etwas geht, von dem man selber nicht direkt betroffen ist oder dies zumindest glaubt. Vor diesem Hintergrund sind die auffallenden Ergebnisse der über 69-jährigen Befragten nicht mehr so überraschend, wie dies auf den ersten Blick den Anschein machte.

Bei aller «Freizügigkeit» in Bezug auf ihre eigenen Daten – die «Digital Natives» scheinen sich ihrer Verletzlichkeit doch bewusst zu sein.

Und jetzt?

Der Beitrag des Datenschutzbeauftragten Wie kann der kantonale Datenschutzbeauftragte mit Sensibilisierung zu einem besseren Datenschutz beitragen? Sensibilisierung kann zwei Zielgruppen haben: die betroffenen Personen und die Datenbearbeiterinnen und Datenbearbeiter.

Sensibilisierung der Bevölkerung Die betroffenen Personen zeigen in der Bevölkerungsbefragung eine hohe Sensibilisierung: Datenschutz ist den Befragten wichtig bis sehr wichtig und erscheint den meisten von ihnen richtig bewertet oder gar unterbewertet. Was wohl verbessert werden könnte, ist das Bewusstsein für die Eigenverantwortung. Datenschutz kann nicht nur von den Datenbearbeiterinnen und Datenbearbeitern eingefordert werden – gerade im Verhältnis unter Privaten kann und muss auch jede Person für sich selber datenschutzbewusst handeln. Allerdings liegt genau dieser Bereich nicht im Zuständigkeitsbereich des kantonalen Datenschutzbeauftragten. Hier kann dieser nur insofern zur Verbesserung beitragen, indem er in der Öffentlichkeit das Thema Datenschutz (und auch die Selbstverantwortung der betroffenen Personen) weiterhin anspricht. Zu prüfen wird sein, wie er die Wahrnehmung der Website, auf welcher die betroffenen Personen über ihre Rechte informiert werden, verbessern kann. >

Sensibilisierung in der Verwaltung Wie die Bevölkerungsumfrage gezeigt hat, haben die betroffenen Personen sehr hohe Ansprüche an die Datenbearbeiterinnen und Datenbearbeiter. Sie erwarten, dass diese die Rechte der Betroffenen achten. Ausserdem haben sie eher das Gefühl, dass der Datenschutz unter- als überbewertet wird. Diesen Erwartungen gerecht zu werden, ist anspruchsvoll. Nach den Erfahrungen aus der Beratungs- und Kontrolltätigkeit des Datenschutzbeauftragten lässt sich schliessen, dass das Datenschutzbewusstsein innerhalb der Verwaltung recht unterschiedlich ist: Es gibt Bereiche und Dienststellen, die sich mit Datenschutzanliegen frühzeitig und regelmässig an den Datenschutzbeauftragten wenden – bei anderen ist das weniger der Fall. Wenn dann der Datenschutzbeauftragte z.B. aufgrund einer Anfrage einer betroffenen Person Kontakt aufnimmt, sind Mitarbeitende nicht selten überrascht, dass bei ihrem Handeln das Datenschutzrecht verbindliche Regeln aufstellt.

Wie die Bevölkerungsumfrage gezeigt hat, haben die betroffenen Personen sehr hohe Ansprüche an die Datenbearbeiterinnen und Datenbearbeiter.

Verstärkung der Sensibilisierungsbemühungen Der Datenschutzbeauftragte wird deshalb auch in Zukunft seine Sensibilisierungsbemühungen fortsetzen und verstärken – auch wenn bereits absehbar ist, dass der «Datenschutz-Basilisk» in «BS intern» nach sechs Kolumnen kein Gastrecht mehr geniessen wird. Es werden weitere Wege gesucht, um den «Datenschutz» noch stärker in die verwaltungsinternen Prozesse und Projekte zu bringen, so dass die berechtigten Ansprüche der Bevölkerung erfüllt werden können. Damit ist das Vertrauen der Bevölkerung in die Verwaltung auch in dieser Hinsicht gerechtfertigt.

1 Im Internet abrufbar unter <http://www.staatskanzlei.bs.ch/kommunikation/bs-intern.html>.
2 <http://www.dsb.bs.ch/ueber-uns/datenschutz-basilisk-startseite.html>.
3 <http://www.statistik.bs.ch/zahlen/befragungen/bevoelkerungsbefragung.html>.
4 <http://www.statistik.bs.ch/dms/statistik/befragungen/FB-BevBef-2015.pdf>, Fragen F30A-F30D, Seiten 20 f.
5 Für die detaillierten Ergebnisse vgl. den Ergebnisbericht (<http://www.statistik.bs.ch/dms/statistik/befragungen/Bericht-Bevoelkerung2015/Bev%C3%B6lkerung-2015.pdf>, Kurz-URL: <http://bit.ly/1MYyvx5>) (Seite 30) bzw. die Grundauswertung (<http://www.statistik.bs.ch/dms/statistik/befragungen/Grundauswertung-BevBef-2015/GA-BevBef-2015.pdf>, Kurz-URL: <http://bit.ly/1RQ2wDv>) (Seiten 105 ff.) auf der Website des Statistischen Amtes.
6 Ergebnisbericht (Fn. 5), Seite 30 und Tabelle 10-10 auf Seite 31.
7 Ergebnisbericht (Fn. 5), Seite 30 und Tabelle 10-10 auf Seite 31.
8 Grundauswertung (Fn. 5), Seite 106.
9 Personen, die mit der digitalen Welt aufgewachsen sind und diese nicht erst im Erwachsenenalter kennengelernt haben.

Thema 2

Die «schwierige» Dateneignerin

Das Informations- und Datenschutzgesetz weist der Dateneignerin – dem öffentlichen Organ, das zur Erfüllung seiner Aufgaben Informationen bearbeitet – eine zentrale Rolle zu. Doch die Praxis tut sich schwer mit der Bestimmung der Dateneignerin bzw. der Gesamtverantwortlichen und mit der passenden Zuordnung von Aufgaben, Kompetenzen und Verantwortlichkeiten (AKV). Ein Modell mit «organisatorischen Rollen» könnte helfen.

Ausgangslage

Dateneignerin Nach dem Informations- und Datenschutzgesetz trägt dasjenige öffentliche Organ die Verantwortung für den Umgang mit Informationen, das die Informationen zur Erfüllung seiner gesetzlichen Aufgaben bearbeitet[1]: die Dateneignerin. Das klingt einfach, klar und nach einer nachvollziehbaren, sinnvollen Vorgabe. Beim Versuch, das «öffentliche Organ» zu identifizieren, fällt aber bereits auf, dass es hier einen Interpretationsspielraum gibt. Insbesondere stellt sich die Frage, auf welcher *Hierarchiestufe* dieses «öffentliche Organ» anzusiedeln ist: Ist es der Gesamtregierungsrat als oberstes Gremium? Ein einzelnes Mitglied des Regierungsrates als Vorsteherin oder Vorsteher eines Departementes? Die Bereichsleiterin oder der Amts- oder Dienststellenleiter? Eine Abteilungsleiterin? Oder auch ein Sachbearbeiter? Und was gilt, wenn mehrere Organisationseinheiten gemeinsam einen Informationsbestand bearbeiten? Für diesen Fall schreibt das IDG, dass sie dann die Verantwortung untereinander regeln[2]. Davon ausgehend, dass eine geteilte Verantwortlichkeit in der Praxis meist problematisch ist, werden sich die Verantwortlichen darauf einigen müssen, dass es eine einzige Dateneignerin gibt, nach der sich alle anderen richten, oder dass es neben den Dateneignerinnen eine Gesamtverantwortliche gibt, die eine zentrale Funktion ausübt und die anderen Dateneignerinnen «koordiniert». Klar ist aber: Die Verantwortung muss vom *Fachbereich* getragen werden und kann nicht an einen Querschnittsbereich – z.B. an die IT (Zentrale Informatikdienste oder Departements-Informatik) oder an ein SAP-Kompetenzzentrum – delegiert werden.

Aufgaben, Kompetenzen, Verantwortlichkeiten Ein öffentliches Organ[3] kann seine Verantwortung nur wahrnehmen, wenn die «AKV» passen:

- *Aufgabe:* Welches Ergebnis soll erreicht werden?
- *Kompetenzen:* Welche Befugnisse und Ressourcen werden benötigt, um das Ergebnis zu erreichen (z.B. Weisungsbefugnisse, personelle und finanzielle Mittel)?
- *Verantwortung:* Welche Verantwortung ist mit der Erfüllung der Aufgabe verbunden (z.B. Ergebnisverantwortung, Budgetverantwortung)?

Nach dem Informations- und Datenschutzgesetz trägt die Dateneignerin die Verantwortung für den Umgang mit ihren Informationen.

Konstellationen

Zentral versus dezentral? Einen wesentlichen Einfluss auf die Zuordnung und die Ausgestaltung der AKV hat die Art der Systeme: Ob die Informationen in einem dezentralen oder in einem zentralen System bearbeitet werden, ist ein entscheidender Faktor. Die Diskussion, ob IT-Leistungen idealerweise zentral oder dezentral erbracht werden sollen, ist nahezu so alt, wie IT-Mittel für die Bearbeitung von Informationen eingesetzt werden, und oft auch von aktuellen Trends der IT-Branche beeinflusst. Beide Ansätze haben Vor- und Nachteile, Chancen und Risiken, die abgewogen werden müssen. Ideal ist es, im Einzelfall zu prüfen, welche Leistung in welcher Form, mit welchen Auswirkungen (auch bezüglich Informationssicherheit) und mit welchen berechtigten Ausnahmen erbracht respektive bezogen werden sollen. Unabhängig davon, ob Leistungen zentral oder dezentral erbracht werden, erscheint es unabdingbar, dass die Vorgaben,

>

die Aufteilung der AKV sowie die «gelebte Umsetzung» optimal auf die Art der Leistungserbringung ausgerichtet sind. Wenn beispielsweise Leistungen zentral erbracht und bezogen werden sollen, die oberste Leitung aber bei der Steuerung und Führung keine aktive Rolle einnimmt, werden höchstwahrscheinlich auf den unteren Führungsebenen systembedingte oder durch das System mindestens begünstigte Konflikte entstehen, die eskalieren können. Das kann zu Reibungsverlusten, zu Frust oder gar zu Blockaden zwischen Beteiligten führen.

Dezentral: Exklusiv genutzte Informationen Die einfachste Konstellation liegt dann vor, wenn eine Dienststelle eine Anwendung für sich selber betreibt, Daten also exklusiv für ihre Aufgabenerfüllung bearbeitet. Die Verantwortlichkeit kann entsprechend einfach ihr zugeordnet werden. Die Dienststellenleitung hat die Aufgabe, dafür zu sorgen, dass bei ihrem System alle informations- und datenschutzrechtlichen Vorgaben eingehalten werden; sie verfügt innerhalb ihres Zuständigkeitsbereichs über die notwendigen Befugnisse und Ressourcen, und sie muss sowohl das Ergebnis liefern als auch das Budget einhalten.

Eine für ein IT-System Gesamtverantwortliche kann nicht völlig frei entscheiden, welchen «Risikoappetit» sie hat und im welchem Umfang Massnahmen als angemessen gelten.

Zentral: Gemeinsam genutzte Daten oder geteilte Systeme Komplexer wird es, wenn mehrere Dateneignerinnen denselben Informationsbestand bearbeiten oder wenn sie sich für ihre Informationen ein System teilen. Dies ist bei *Datenpools* (z.B. beim kantonalen Datenmarkt oder beim Basler Informationssystem Sozialleistungen BISS) oder bei *IKT-Basisleistungen* (z.B. beim Datenablage-System FileBS und beim Mail-System MailBS) der Fall: Wer trägt jetzt wofür die Verantwortung? Wer sorgt dafür, dass «das Ganze» rechtmässig und sicher betrieben wird? Die einzelnen Dateneignerinnen sind nicht ohne weiteres in der Lage, die Gesamtverantwortung zu übernehmen, und müssen diese entsprechend anders regeln. In jedem Fall muss jemand – mit den notwendigen AKV – sicherstellen, dass nicht nur die einzelnen Teile «richtig» laufen, sondern dass das Gesamtsystem «richtig» läuft.

Ein möglicher Lösungsansatz

Unterscheidung «organisatorischer Rollen» An dieser eben erwähnten Typisierung könnte auch eine Lösung ansetzen: Bei gemeinsam genutzten Daten oder geteilten Systeme könnten Dateneignerinnen und Gesamtverantwortliche als «organisatorische Rollen» unterschieden werden. Einer Stelle muss die Gesamtverantwortung übertragen werden – den Dateneignerinnen verbleiben aber bestimmte Teile der Verantwortung. Wie die Abgrenzung zwischen diesen beiden Bereichen gezogen wird, wem welche Aufgabe zukommt, wer über welche Kompetenzen (Befugnisse und Ressourcen) verfügen kann und wer für welches Ergebnis verantwortlich ist, muss an die konkreten Gegebenheiten und Bedürfnisse angepasst werden. Hierbei wird es AKV geben, die zwingend bei einer der Rollen anzusiedeln sind, solche, die im Zusammenspiel zwischen den beiden Rollen wahrgenommen werden müssen, und wohl auch einige, die delegiert werden können. Der Datenschutzbeauftragte hat schon vor längerer Zeit angeregt, dass ein entsprechendes Modell ausgearbeitet wird, das sinnvollerweise auch festlegt, wie und in welchem Umfang Anpassungen erfolgen können.

Einbindung in die gesamtkantonale Organisation Zu beachten ist ausserdem, dass die Dateneignerin (oder Dateneignerinnen) und die Gesamtverantwortliche nicht im luftleeren Raum operieren, sondern in die «Gesamtorganisation» Kanton eingebunden sind. Eine für ein IT-System Gesamtverantwortliche kann nicht völlig frei entscheiden, wie sie die Risiken beurteilt, welchen «Risikoappetit» sie hat (also: welche Risiken sie als tragbar hinnimmt) und im welchem Umfang Massnahmen als angemessen gelten. Die baselstädtische Verwaltung hat sich entschieden, einen dreistufigen Ansatz zu implementieren (Grundschutzbedarf, erhöhter Schutzbedarf und hoher Schutzbedarf). Hierbei soll der Grundschutz (für die «gewöhnlichen», also nicht besonderen Personendaten) durch ein Set von Massnahmen gewährleistet werden, das flächendeckend umgesetzt werden muss. Hier braucht es Vorgaben, Steuerung und Controlling. Ausserdem werden die Dateneignerin und die Gesamtverantwortliche in der Regel nicht Fachkräfte in den Bereichen Datenschutz und Informationssicherheit sein. Darum sind sie auf Unterstützung angewiesen, z.B. durch die (Kantons- oder Departements-) Sicherheitsbeauftragten, durch juristische Fachstellen und die zuständigen IT-Organe. Auch die Zusammenarbeit mit diesen Stellen muss ausreichend klar geregelt sein. Es erscheint beispielsweise nicht sinnvoll,

dass jede Verantwortliche die Prozesse für die Informationssicherheit selbst «erfindet». Idealer erscheint es, dass ihre Organisationseinheit Vorgaben aus einem Kantons- oder zumindest Departements-ISMS (Information Security Management System) umsetzen und gegebenenfalls anpassen kann. Dies hat den Vorteil, dass die Verantwortliche unterstützt wird und die Prozesse nicht an der Organisationsgrenze der Verantwortlichen enden – gerade auch bei übergreifenden zentralen Systemen. Eine wesentliche Bedeutung kommt hierbei auch der «IT-Governance» zu, welche dieses Zusammenspiel und die zielgerichtete Steuerung über alle Fach- und Hierarchieebenen unterstützen soll.

Der Schutz von Informationen durch angemessene organisatorische und technische Massnahmen kann nur im Zusammenspiel zwischen Dateneignerin und Gesamtverantwortlicher wahrgenommen werden.

Aufgaben der Dateneignerin

Kernaufgaben Die folgenden Aufgaben müssen in jedem Fall von der Dateneignerin wahrgenommen werden:

— Sie muss den *Schutzbedarf analysieren*; nur sie kann den «Wert» der im System bearbeiteten Informationen bezüglich der Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit, Zurechenbarkeit und Nachvollziehbarkeit[4] beurteilen.

— Sie muss sicherstellen, dass die *gesetzlichen Vorgaben* (gesetzliche Grundlage, Verhältnismässigkeit, Richtigkeit, Zweckbindung, Erkennbarkeit) bei der Datenbearbeitung (und insbesondere auch bei der Datenbekanntgabe) eingehalten sind[5].

— Sie entscheidet aufgrund eines schriftlichen Gesuchs, ob ein anderes öffentliches Organ einen *Onlinezugriff* auf ihre Informationen eingeräumt erhält[6].

— Sie muss sicherstellen, dass die Informationen nach Ablauf der Aufbewahrungsfristen dem Staatsarchiv angeboten werden und in ihrer Organisationseinheit zuverlässig *vernichtet* werden[7].

— Sie muss sicherstellen, dass die Rechte der betroffenen Personen gewährleistet werden (Zugang zu den eigenen Personendaten, Berichtigung unrichtiger Personendaten, Unterlassung widerrechtlicher Bearbeitung usw.)[8].

— Sie muss sicherstellen, dass alle Verfahren, in denen Personendaten bearbeitet werden, in das entsprechende Verzeichnis aufgenommen werden[9].

Aufgaben der Gesamtverantwortlichen bei zentralen Systemen

Kernaufgaben Die folgenden Aufgaben müssen in jedem Fall von der Gesamtverantwortlichen wahrgenommen werden:

Koordination der Systemnutzung Die Gesamtverantwortliche muss die Nutzung des Systems koordinieren. Nötigenfalls muss sie Vorgaben oder Auflagen für die Nutzung erlassen. Wenn also z.B. ein zentrales System nur Grundschutz bietet, muss die Gesamtverantwortliche dies den systemnutzenden Dateneignerinnen kommunizieren; diese müssen dann dafür sorgen, dass in ihrem Verantwortungsbereich das System (ohne weitere Massnahmen) auch nur für Informationen genutzt wird, die keinen höheren als Grundschutzbedarf aufweisen – oder eben selber mit zusätzlichen Massnahmen für einen höheren Schutz sorgen. Damit die Dateneignerinnen den Umgang mit ihren Daten verifizieren können, muss die Gesamtverantwortliche gegebenenfalls Vorkehrungen treffen (z.B. Benutzerlisten der Zugriffsberechtigten auf die Daten der einzelnen Dateneignerinnen oder Protokollauszüge [Logs] zur Verfügung stellen usw.).

Die Gesamtverantwortliche ist die einzige, die das Gesamtrisikos des Systems (als «Summe» der Risiken der einzelnen Dateneignerinnen oder als eigene Gesamtbeurteilung) bestimmen kann.

Beurteilung des Gesamtsystems Die Gesamtverantwortliche ist die einzige, die das Gesamtsystem beurteilen kann. Sie muss entscheiden, wie hoch der «Wert», der Schutzbedarf des Gesamtsystems ist. Aufgrund der Kumulation der Informationen kann dieses einen höheren Schutzbedarf haben als die Informationen der einzelnen Dateneignerinnen. Mehrere «gewöhnliche» Personendaten aus verschiedenen Quellen können im zentralen System zu Persönlichkeitsprofilen[10] werden, was bezüglich des Schutzziels Vertraulichkeit zu einem erhöhten Schutzbedarf führt. Auch bezüglich des Gesamtrisikos des Systems ist die Gesamtverantwortliche die einzige, welche dieses (als «Summe» der Risiken der einzelnen Dateneignerinnen oder als eigene Gesamtbeurteilung) bestimmen kann. >

Aufgaben im Zusammenspiel Dateneignerin/ Gesamtverantwortliche

Kernaufgaben Die folgenden Aufgaben müssen im Zusammenspiel zwischen Dateneignerin und Gesamtverantwortlicher wahrgenommen werden.

Angemessene Schutzmassnahmen Das IDG verlangt, dass das öffentliche Organ Informationen durch «angemessene organisatorische und technische Massnahmen»[11] schützt – eine absolut zentrale Vorgabe für die Wahrung des Datenschutzes insbesondere hinsichtlich einer ausreichenden Informationssicherheit. Diese Aufgabe *kann* nur im Zusammenspiel zwischen Dateneignerin und Gesamtverantwortlicher wahrgenommen werden, weil auch die Massnahmen zusammenspielen müssen. Wo Massnahmen für das Gesamtsystem greifen, braucht es keine spezifischen Massnahmen für die einzelnen Teile der Dateneignerinnen – wo ein Risiko nicht durch technische Massnahmen für das Gesamtsystem minimiert wird, braucht es vielleicht organisatorische Massnahmen der Dateneignerinnen. Beim Risikomanagement und, als Resultat daraus, bei der Bestimmung der angemessenen Massnahmen müssen Dateneignerin und Gesamtverantwortliche zusammenwirken – wie, das müssen sie untereinander aushandeln.

Beim Risikomanagement und bei der Bestimmung der angemessenen Massnahmen müssen Dateneignerin und Gesamtverantwortliche zusammenwirken – wie, das müssen sie miteinander aushandeln.

Vorabkontrolle Die Verantwortliche muss sicherstellen, dass die relevanten Projekte dem Datenschutzbeauftragten zur Vorabkontrolle vorgelegt werden – dazu müssen Dateneignerin und Gesamtverantwortlicher ihren Beitrag leisten, auch wenn schliesslich, je nach Absprache untereinander, eine der beiden das Projekt vorlegt[12].

Zusammenfassung

Feststellungen Im Rahmen seiner Beratungs- und Prüftätigkeit hat der Datenschutzbeauftragte festgestellt, dass es rund um die «Dateneignerin» grosse Unsicherheiten gibt. Die öffentlichen Organe tun sich schwer mit der Bestimmung der Dateneignerin bzw. der Gesamtverantwortlichen, mit der Zuordnung von AKV. Es besteht deshalb unzweifelhaft ein Bedarf, die gesetzlichen Vorgaben zu konkretisieren, damit sie operativ umgesetzt werden können.

Lösungsansatz Das hier skizzierte Modell der «organisatorischen Rollen» ist ein möglicher Lösungsansatz. Der Datenschutzbeauftragte will und kann aber diesbezüglich keine Vorgaben machen. Es liegt in der Verantwortung der Verwaltung, eine praktikable Lösung zu entwickeln. Das ist auch sinnvoll: Sie hat so einen Handlungsspielraum, um die konkrete Umsetzung an die Gegebenheiten (z.B. an die spezifische Aufgabe, an das Führungsverständnis, an den Risikoappetit oder auch an die Zentralisierungs-/Dezentralisierungsansprüche) anzupassen. Es erscheint aber sinnvoll, dass die erforderliche Konkretisierung insbesondere bezüglich AKV zentral erfolgt und dann bei Bedarf angepasst wird.

Unterstützungsangebot Der Datenschutzbeauftragte bietet für die Ausarbeitung seine Unterstützung an.

1 § 6 Abs. 1 IDG; vgl. zum Inhalt der Verantwortung PK-IDG/BS-Rudin, § 6 N 4 ff.
2 § 6 Abs. 2 IDG; vgl. dazu PK-IDG/BS-Rudin, § 6 N 32 ff.
3 Verantwortung übernehmen und tragen können natürlich nur Menschen – damit kommt die Verantwortung den Leitungsorganen des öffentlichen Organs zu (PK-IDG/BS-Rudin, § 6 N 3).
4 § 8 Abs. 2 IDG; vgl. dazu auch PK-IDG/BS-Baeriswyl, § 8 N 21 ff.
5 §§ 9-15 und 21-23 IDG.
6 §§ 9a ff. IDV.
7 § 16 IDG; . vgl. dazu auch PK-IDG/BS-Rudin, § 16 N 2 ff. und 13 ff.
8 §§ 26 und 27 IDG; vgl. dazu auch PK-IDG/BS-Rudin, § 26 N 1 ff. und PK-IDG/BS-Husi, § 27 N 4 ff.
9 § 24 IDG und § 16 IDV; vgl. dazu auch PK-IDG/BS-Husi, § 24 N 1 ff.
10 § 3 Abs. 4 lit. b IDG.
11 § 8 Abs. 1 IDG.
12 § 13 IDG und §§ 2-4 IDV; vgl. dazu PK-IDG/BS-Rudin, § 13 N 2 ff.

Informationssicherheit und Datenschutz müssen Chefsache sein!

Missbrauchs- und Sicherheitsvorfälle mit grossem Ausmass mehren sich und rücken – wie etwa der jüngst publik gewordene Einbruch ins Informationssystem der RUAG – immer mehr ins Licht der Öffentlichkeit. Informationssicherheit ist nicht «nice to have». Wie in allen Bereichen ist auch die behördliche Tätigkeit zunehmend von der IT abhängig. Die Einschätzung, dass Daten des Bundes für Einbrecher attraktiver seien als kantonale Daten, erhöht vielleicht die Wahrscheinlichkeit eines Angriffs auf jene – das Schadensausmass ist aber nicht weniger gravierend:

— Ein «Data Breach» kann die staatliche Aufgabenerfüllung gefährden, wenn etwa Informationen von Aufsichts- oder Strafverfolgungsbehörden gestohlen, verändert oder vernichtet werden.

— Ein Einbruch kann das Leben von Staatsangestellten gefährden, wenn die Identität von Personen offengelegt wird, die etwa in der verdeckten Fahndung oder im Staatsschutzbereich arbeiten, und

— er kann die Persönlichkeits- und andere Rechte der Personen verletzen, die ihre Daten öffentlichen Organen anvertraut haben oder deren Daten von diesen erhoben worden sind.

Ein «innen gut – aussen bös»-Konzept, das schwergewichtig auf Perimeterschutz setzt und «innen» die Informationen relativ ungeschützt lässt, wird den Anforderungen einer vernetzten Welt und den sich ändernden Bedrohungsszenarien zu wenig entgegensetzen können. Wer weiss, dass es keine absolute Einbruchsicherheit gibt, muss sich die Frage stellen, in welchen Systemen und durch wen er sensitive oder wichtige Daten bearbeiten lassen will. In fehlender Informationssicherheit liegt damit ein erhebliches Risiko für das Gesamtunternehmen. Kein Wunder, ist in vielen grösseren Unternehmen die Verantwortung für den zuverlässigen Einsatz der IT bei der obersten Leitung angesiedelt und rapportiert die für die Umsetzung – um damit auch für die Einhaltung der Informationssicherheit verantwortliche Stelle meistens direkt an die oberste Leitung. Um eine ausreichende Sicherheit zu erreichen, ist es unabhängig von der Organisation unabdingbar, dass die oberste Leitung die IT (inklusive die Informationssicherheit) auf ihrem Radarschirm hat und Verantwortung übernimmt («Management Committment»).

Das gilt es auch im staatlichen Bereich zu beachten. Klar – es gibt keine 100%ige Sicherheit. Nur: Wenn Informationen einmal «draussen» sind, kann niemand sie zurückholen. Ein materieller Schaden kann vielleicht entschädigt werden, also auf der «Geldseite» rückgängig gemacht werden – die Vereitelung der staatlichen Aufgabenerfüllung und die Verletzung der Persönlichkeitsrechte der betroffenen Bürgerinnen und Bürger aber nicht. Informationssicherheit und damit auch Datenschutz muss Chefsache sein!

Aus dem Alltag

Einblicke in die Beratungstätigkeit

Einblicke in die Kontrolltätigkeit

Besondere Berichtspunkte

Statistik

Aus dem Alltag

Einblicke in die Beratungstätigkeit

Der Datenschutzbeauftragte behandelt in seiner Beratung eine ausserordentlich breite Palette von Themen: von Auftragsdatenbearbeitungen und neuen Anmeldeformularen für Mietinteressentinnen und Mietinteressenten über Vorabkontrollen zu Onlinezugriffsgesuchen und Videoüberwachungen, Schulungen und Weiterbildungsreferate bis hin zur Zusammenarbeit mit anderen Datenschutzbehörden, um Synergien zu nutzen.

Auftragsdatenbearbeitung

Immer häufiger Immer wieder tauchte im Berichtsjahr das Thema der Auftragsdatenbearbeitung auf. Immer häufiger lagern öffentliche Organe das Bearbeiten von Personendaten an Dritte aus. Das ist zulässig, wenn keine rechtliche Bestimmung oder vertragliche Vereinbarung entgegensteht[1]. Ausserdem muss das auftraggebende öffentliche Organ sicherstellen, dass die Informationen nur so bearbeitet werden, wie es selber das tun dürfte[2]. Dabei stellen sich heikle Fragen – man denke nur an das Stichwort «Cloud Computing» und die damit verbundenen Versprechen.

Auftragsdatenbearbeitung Eine Auftragsdatenbearbeitung liegt vor, wenn ein öffentliches Organ im Rahmen der Erfüllung seiner gesetzlichen Aufgabe eine dritte Person (Auftragnehmerin) beauftragt, Informationen und insbesondere Personendaten zu bearbeiten. Diese Auftragnehmerin bearbeitet damit die Informationen für Zwecke des auftraggebenden öffentlichen Organs, nicht für ihre eigenen Zwecke. Dabei soll die Informationsbearbeitung Hauptzweck oder mindestens zentraler Bestandteil des Vertragsverhältnisses bilden. Das ist beispielsweise der Fall,

— wenn ein öffentliches Organ die Verlustscheinbewirtschaftung an ein privates Inkassounternehmen auslagert,

— wenn ein darauf spezialisiertes Unternehmen Bilddaten für eine Amtsstelle erheben soll,

— wenn ein privates Umfrageinstitut beauftragt wird, eine Kundenzufriedenheitsumfrage für eine Verwaltungsstelle vorzunehmen, oder

— wenn eine Amtsstelle Rechnungen, Bussenverfügungen o.ä. durch ein externes Unternehmen drucken und versenden lässt.

Abgrenzungen Abzugrenzen ist die Auftragsdatenbearbeitung einerseits von einer *Aufgabenübertragung*[3]. Eine solche liegt vor, wenn eine private Person oder Organisation eine gesetzliche Aufgabe zur Erfüllung übertragen erhält. Diese Person oder Organisation wird informations- und datenschutzrechtlich selber zu einem öffentlichen Organ, das dem IDG untersteht[4] und für dessen Mitarbeitende nach dem Staatsbeitragsgesetz die jeweils anwendbaren gesetzlichen Verschwiegenheitspflichten (den besondere Amtsgeheimnissen) gelten[5]. Andererseits ist die Auftragsdatenbearbeitung von einer *Datenbekanntgabe*[6] zu unterscheiden. Eine solche liegt dann vor, wenn ein öffentliches Organ gestützt auf eine gesetzliche Grundlage einer dritten Person oder Organisation Informationen bekannt gibt, damit diese sie zu eigenen Zwecken bearbeiten kann.

Es hat sich gezeigt, dass die Verträge, welche die Auftragnehmerinnen vorschlagen, die Pflichten, die ihnen vom auftraggebenden öffentlichen Organ überbunden werden müssen, nicht oder nicht hinreichend klar umschreiben.

Unterstützungsbedarf der Dienststellen Viele Amtsstellen benötigen Unterstützung für die Ausformulierung der vertraglichen Regelungen. Ausserdem hat sich gezeigt, dass die Verträge, welche die Auftragnehmerinnen vorschlagen, die Pflichten, die ihnen vom auftraggebenden öffentlichen Organ überbunden werden müssen, nicht oder nicht hinreichend klar umschreiben. Der Datenschutzbeauftragte hat deshalb den Entwurf eines Leitfadens erarbeitet. Er wird im Jahr 2016 bei einzelnen Departements-Rechtsdiensten in Vernehmlassung gegeben und anschliessend veröffentlicht.

Maschinenlesbare Stimm- und Wahlzettel

Erstmaliger Einsatz Anlässlich der Abstimmung vom 8. März 2015 wurden im Kanton Basel-Stadt erstmals maschinenlesbare Stimmzettel eingesetzt. Diese Stimmzettel sollen nicht mehr von Wahlhelferinnen und -helfern ausgezählt, sondern mittels Scannern eingelesen und ausgewertet werden.

Datenschutzkonform Der Datenschutzbeauftragte hat im Vorfeld der Abstimmung geprüft, ob die neuen Stimmzettel und das Auswertungsverfahren den datenschutz- und informationssicherheitsrechtlichen Vorgaben entsprechen. Er hat die geplante Verwendung aus folgenden Gründen als konform angesehen:

— Das Stimm- und Wahlgeheimnis wird auch mit den neuen Stimmzetteln gewahrt: Es ist nach der Trennung der Briefumschläge (d.h. der Stimmrechtsausweise) von den darin enthaltenen Zetteln nicht mehr möglich, einzelne Stimmabgaben bestimmten Personen zuzuordnen.

— Unklar ausgefüllte oder beschädigte Stimmzettel, die von den Scannern möglicherweise nicht eingelesen werden können, werden von Hand ausgesondert. Es wird dann im Vier-Augen-Prinzip überprüft, ob allenfalls trotz Verschmutzung oder nicht-vorschriftsgemässem Ankreuzen die Aussage der Wählerin bzw. des Wählers ausgelesen werden kann.

— Die Funktionsfähigkeit der Scanner wird vor dem Wahl- bzw. Abstimmungswochenende eingehend mit Test-Unterlagen geprüft.

— Weder die verwendeten Server noch die verwendeten Laptops sind ans Internet oder an ein externes Netzwerk angeschlossen. Dank dieser autonomen Netzwerkkonfiguration (in sich geschlossenes Netzwerk ohne Internetanschluss) mit zwei Laptop-Arbeitsplätzen ist ein externer Zugriff ausgeschlossen. Sämtliche Geräte sind in einem separaten, abgeschlossenen Raum mit eingeschränkter Zugangsberechtigung aufgestellt.

— Die ermittelten Resultate werden anhand von Stichproben plausibilisiert und dann nicht via Internet oder USB-Stick o. ä. übermittelt, sondern nach dem Vier-Augen-Prinzip kontrolliert auf Papier übertragen und weitergeleitet.

Anmeldeformular von Immobilien Basel-Stadt

Anmeldeformular Immobilien Basel-Stadt verfügt seit Februar 2015 über ein überarbeitetes Anmeldeformular für Mietinteressentinnen und -interessenten. Bei der Überarbeitung hat Immobilien Basel-Stadt eng mit dem Datenschutzbeauftragten zusammengearbeitet.

Das neue Anmeldeformular von Immobilien Basel-Stadt hält sich enger an die Vorgaben des EDÖB als etliche Formulare privater Liegenschaftsverwaltungen.

Neuerungen Das aktuelle Anmeldeformular weist insbesondere die folgenden Neuerungen auf:

— Neu findet ein zweistufiges Auswahlverfahren statt. In einem ersten Schritt verlangt Immobilien Basel-Stadt von den Mietinteressentinnen und -interessenten nur eine Selbstdeklaration über die Einkommenssituation; es werden noch keine Belege verlangt.

— Bei der Selbstdeklaration des Brutto-Jahreseinkommens werden weniger genaue Angaben verlangt, als es der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) in seinem Merkblatt tut. Die Angaben werden aber bis zur Grenze von 150 000 Franken erhoben, weil der Mietpreisindex seit der Festlegung der Limite von 100 000 Franken durch den EDÖB im Jahre 1994 um fast 30% gestiegen ist und weil Immobilien Basel-Stadt auch Wohnungen vermietet, die nur mit einem Einkommen von über 100 000 Franken tragbar sind.

— Einkommensnachweise (und Ausweiskopien) werden erst in einem zweiten Schritt von denjenigen Personen verlangt, die in die engste Wahl gekommen sind. Es erscheint dem Datenschutzbeauftragten nachvollziehbar und verhältnismässig, diesen zweiten Schritt parallel bei denjenigen (wenigen) Personen durchzuführen, die alle in die engste Wahl gekommen sind.

— Referenzen und Informationen zur bisherigen Wohnsituation sind neu freiwillig anzugeben.

Datenschutzkonform Der Datenschutzbeauftragte des Kantons Basel-Stadt erachtet das neue Anmeldeformular als mit den datenschutzrechtlichen Vorgaben vereinbar. Die Abweichungen vom Merkblatt des EDÖB sind aus Sicht des Datenschutzbeauftragten nachvollziehbar und bringen teilweise sogar Verbesserungen für die Mietinteressentinnen und Mietinteressenten mit sich. >

Jetzt besser als manche Konkurrenten Das neue Anmeldeformular von Immobilien Basel-Stadt hält sich enger an die Vorgaben des EDÖB als etliche Formulare privater Liegenschaftsverwaltungen. Der Datenschutzbeauftragte ist überzeugt, dass mit dem neuen Vorgehen ein gerechter Ausgleich zwischen den Interessen der Mietinteressentinnen und Mietinteressenten und den Bedürfnissen von Immobilien Basel-Stadt gefunden werden konnte.

Es ist nicht erforderlich, dass die Wohnadressen und Handynummern von Mitarbeiterinnen und Mitarbeitern eines Wohnheims für Besucherinnen und Besucher sichtbar ausgehängt werden.

Elterngespräche – zwingend mit der Tagesstrukturleitung?

Verhältnismässigkeit Eine Klassenlehrerin wandte sich an den Datenschutzbeauftragten mit der Frage, ob es nicht problematisch sei, dass die Leitung der Tagesstruktur an ihrer Primarschule zwingend bei allen halbjährlichen Standortgesprächen mit den Eltern und Schülern, welche Tagesstrukturangebote beanspruchen, dabei sein wolle, und es dabei auch nicht für erforderlich erachte, die Eltern vorgängig zu informieren. Nach diversen Abklärungen bei Fachpersonen kam der Datenschutzbeauftragte zum Schluss, dass es zur Aufgabenerfüllung sowohl der Klassenlehrpersonen wie auch des Tagesstrukturteams geeignet und erforderlich sein kann, dass die Standortgespräche gemeinsam durchgeführt werden. Dass die Tagesstrukturleitung *zwingend* bei diesen Gesprächen anwesend sein soll, erschien aus Sicht des Datenschutzbeauftragten nicht verhältnismässig: Schule und Tagesstruktur verfolgen unterschiedliche Ziele, die Kinder bewegen sich in unterschiedlichen Umfeldern, deren Vermischung unter Umständen sogar nachteilig sein kann. Es muss daher jeweils geprüft werden, ob ein gemeinsames Standortgespräch und der damit verbundene Informationsaustausch tatsächlich zur Aufgabenerfüllung sowohl der Schule wie auch der Tagesstruktur beitragen kann.

Transparenz Dabei auf eine vorgängige Information der Eltern und der Kinder, welche bei diesen Gesprächen auch zugegen sind, zu verzichten, dürfte das Vertrauensverhältnis, welches sich unter Umständen zwischen Kindern und Tagesstrukturbetreuung entwickelt hat, erheblich stören. Auch ist es ausgesprochen fraglich, ob es für die Aufgabenerfüllung und Anliegen der Schule bzw. der Tagesstruktur wirklich zielführend ist, wenn sich nicht sämtliche Parteien eines Gesprächs auf die Situation vorbereiten können, sondern «auf dem falschen Fuss erwischt» werden.

Kontaktdaten von Mitarbeitenden am Anschlagbrett

Kontaktaufnahme ausserhalb der Arbeitszeit Ein Mitarbeiter eines Wohnheims störte sich daran, dass seine privaten Kontaktdaten (Wohnadresse und Handynummer) ohne seine Einwilligung am für sämtliche Bewohnerinnen und Bewohner, Besucherinnen und Besucher und Mitarbeiterinnen und Mitarbeiter einsehbaren allgemeinen Anschlagbrett des Wohnheims veröffentlicht wurden. Diese Liste, so die Heimleitung, vereinfache die Kontaktaufnahme für alle Beteiligten auch ausserhalb der Dienstzeiten.

Nur für Kolleginnen und Kollegen Der Datenschutzbeauftragte kam zum Schluss, dass es zwar für die Arbeitskolleginnen und -kollegen des fraglichen Mitarbeiters durchaus erforderlich sein könnte, ihn rasch zu kontaktieren: In Notfall-Situationen oder im Falle von Personalmangel kann es für die Aufrechterhaltung des Betriebs eines Wohnheims wesentlich sein, dass Teammitglieder auch zuhause kontaktiert werden können. Für die Bewohnerinnen und Bewohner sowie für Besucherinnen und Besucher ist diese Information jedoch nicht erforderlich, diese können sich jederzeit an die Schichtleitung oder das Personal vor Ort wenden und müssen in aller Regel einzelne Mitarbeiterinnen und Mitarbeiter nicht privat kontaktieren können. Die Liste mit den Kontaktdaten wurde daraufhin vom allgemein zugänglichen Anschlagbrett entfernt und in den Räumlichkeiten des Betreuungsteams aufgelegt.

Fotos in der Eingangshalle einer Alterssiedlung

Recht am eigenen Bild Der Datenschutzbeauftragte wurde von der Leiterin einer staatlich subventionierten Alterssiedlung mit der Frage kontaktiert, ob im Eingangsbereich des Haupthauses eine Pinnwand mit Portraitaufnahmen von Bewohnerinnen und Bewohnern sowie mit Bildern von Festanlässen aufgehängt werden dürften bzw. was es dabei zu beachten gelte. Da das Aufhängen von Fotos im allgemein zugänglichen Bereich einer Alterssiedlung zur Erfüllung der allgemeinen Aufgaben der Altersbetreuung nicht erforderlich ist, sondern vielmehr dazu dienen soll, «einen freundlichen Eindruck» und das Gefühl der

«Heimeligkeit» zu vermitteln, bedarf es der Einwilligung der abgelichteten Personen – eine gesetzliche Grundlage, welche das Aufhängen der Bilder erlauben würde[7], besteht nicht. Sollten die fraglichen Personen nicht mehr in der Lage sein, sich ihren Willen nach vorgängiger Aufklärung zu bilden und zu äussern, so sind die Angehörigen zu kontaktieren.

Bilder von einem Anlass Sollen an Anlässen Fotos gemacht und diese später veröffentlicht werden, so ist im Vorfeld bzw. während des Anlasses auf diesen Umstand hinzuweisen. Abgelichtete Personen müssen in jedem Fall in die Veröffentlichung ihrer Bilder einwilligen – auch dann, wenn sie nicht einzeln portraitiert wurden, sondern auf einem Stimmungsbild erkennbar sind.

Anonymisierung und Spezialwissen

Seltene Krankheit Eine Frau war vor längerer Zeit in der Frauenklinik im Universitätsspital in Behandlung. Sie war an einer ausserordentlich seltenen Krankheit erkrankt, die erst nach geraumer Zeit diagnostiziert werden konnte. Das Ärzteteam hat den Fall einige Zeit später in einem medizinischen Fachjournal dargestellt. Die Publikation kann auch via Internet erworben werden.

Erkannt Die Patientin wurde vor kurzem von einer Bekannten auf die Publikation angesprochen: «Das bist doch du!». Sie hat sich an den Datenschutzbeauftragten gewandt, weil sie sich durch die (anonymisierte) Darstellung ihres Falles in einer medizinischen Fachzeitschrift in ihren Persönlichkeitsrechten verletzt fühlt.

Anonymisiert Aus datenschutzrechtlicher Sicht verletzt eine Publikation in anonymisierter Form die Persönlichkeitsrechte der betroffenen Person nicht, wenn die Anonymisierung tatsächlich so erfolgt, dass eine Person ohne spezifisches Zusatzwissen nicht mehr eruieren kann, um wen es sich im geschilderten Fall handelt. Im vorliegenden Fall sind die identifizierenden Merkmale fast vollständig entfernt. Es wird einzig das Alter der Patientin genannt; ausserdem kann aus der Schilderung geschlossen werden, dass die Patientin in der Frauenklinik im Universitätsspital Basel behandelt wurde, was zwar mit einer gewissen Wahrscheinlichkeit, aber ohne Gewissheit auf die Wohnregion schliessen lässt. Schliesslich erfährt man über die Krankheit, den Verlauf und Nebenerscheinungen einiges, etwa dass die Patientin ein posttraumatisches Syndrom mit reaktiver Depression entwickelt hat oder dass sie sich in ihrer Weiblichkeit nach wie vor beeinträchtigt fühlt.

Spezialwissen Mit diesen Informationen können «gewöhnliche» Leserinnen und Leser keinesfalls auf eine bestimmte Person schliessen. Möglich ist das hingegen mit spezifischem Zusatzwissen. Alle Personen, die im Spital in die Behandlung involviert waren, dürften den Fall der richtigen Person zuordnen können – sie unterstehen aber alle dem ärztlichen Berufsgeheimnis. Ausserdem dürften diejenigen Personen den Fall der Frau zuordnen können, die von ihr oder aus ihrem Umfeld die Information über die Krankheit erhalten hatten. Diese Personen kennen aber die Hauptinformation (ihre seltene Krankheit) bereits – unangenehm ist für die betroffene Frau dabei natürlich, dass die Dritten dank diesem Zusatzwissen zusätzliche und sehr heikle Informationen über den Krankheitsverlauf oder über Nebenerscheinungen erfahren.

Die Qualität einer Anonymisierung misst sich am allgemein verfügbaren Wissen, nicht am Spezialwissen bestimmter Personen.

Beurteilung aus Datenschutzsicht Aus datenschutzrechtlicher Sicht misst sich die Qualität der Anonymisierung aber – wie erwähnt – am allgemein verfügbaren Wissen, nicht am spezifischen Zusatzwissen bestimmter Personen. Andernfalls wäre, solange irgendjemand ein Zusatzwissen haben könnte, eine Anonymisierung schlicht unmöglich. Deshalb erscheint aus datenschutzrechtlicher Sicht die anonymisierte Publikation des Falles in einem Fachjournal zulässig.

Informationspflicht? Aus medizin(publikations)-ethischer Sicht lässt sich allenfalls die Frage stellen, ob die Patientin vorgängig hätte informiert (oder sogar um ihre Einwilligung zur Publikation gebeten?) werden müssen. Der Datenschutzbeauftragte hat sogar diese Frage einer Person aus dem Umfeld der Ethikkommission Nordwest- und Zentralschweiz unterbreitet, aber leider keine Antwort erhalten. Der Patientin und ihrem Rechtsvertreter konnte die datenschutzrechtliche Situation erklärt werden. >

Datenbekanntgabe an ausserkantonale Polizeibehörden

Regelmässige Anfragen Im Rahmen der polizeilichen Zusammenarbeit werden Mitarbeitende der Kantonspolizei immer wieder von Angehörigen anderer Polizeikorps um Personenauskünfte gebeten – teilweise auch retrospektiv: Welche Personen waren Ende Januar an einer bestimmten Adresse angemeldet? Rein technisch ist eine Auskunftserteilung möglich, da (bestimmte) Mitarbeitende der Kantonspolizei die Möglichkeit haben, über den kantonalen Datenmarkt auf Daten der Einwohnerkontrolle zu greifen. Ganz wohl war den Mitarbeitenden der Kantonspolizei bei diesen Auskünften nicht, weshalb das Einwohneramt, die Kantonspolizei und der Datenschutzbeauftragte die Problematik gemeinsam klärten.

Aktuell und vollständig? Obschon die Kantonspolizei grundsätzlich befugt wäre, Informationen aus dem Datenmarkt im Rahmen der interkantonalen Polizeizusammenarbeit (Amtshilfe) an andere Polizeibehörden bekannt zu geben, kann bei den polizeilichen Auskünften aus dem Datenmarkt nicht sichergestellt werden, dass die Informationen tatsächlich aktuell und vollständig sind, ob also allenfalls Zusatzangaben für die Kantonspolizei nicht ersichtlich, jedoch für die Bekanntgabe wesentlich sind. Entsprechend haben die Einwohnerdienste und die Kantonspolizei folgendes Vorgehen vereinbart: Die Kantonspolizei leitet während der Bürozeiten der Einwohnerdienste Adressanfragen weiter und beantwortet die Anfragen nicht selbst. Können Anfragen ausserhalb der Bürozeiten der Einwohnerdienste nicht erst am nächsten Arbeitstag beantwortet werden, insbesondere während der Nachtschicht, dann erteilen die Mitarbeitenden der Kantonspolizei die gewünschte Auskunft, jedoch mit dem Hinweis, dass die Angaben unter Umständen nicht vollständig bzw. nicht à jour sind.

Bekanntgabe von Kandidaturen für Volkswahlen

Sachverhalt Dem Datenschutzbeauftragten wurde zugetragen, das Wahlbüro würde noch nicht eingereichte Kandidaturen für Volkswahlen «ausplaudern». Die Abklärungen haben Folgendes ergeben: Eine Person hatte ihre Kandidatur für die Richterwahlen vom November 2015 gegenüber dem Leiter Wahlen und Abstimmungen angekündigt, sie aber knapp vor Ablauf der Anmeldefrist noch nicht rechtsgültig eingereicht. Der Wahlbüroleiter bemerkte in einem Gespräch gegenüber dem Sekretariat der Partei, welche die bis zu diesem Zeitpunkt einzige Kandidatur eingereicht hatte, beiläufig, sie müssten sich auf eine Kampfwahl einstellen. Die Rückfrage «Kandidiert Herr X?» wurde dann vom Leiter Wahlen und Abstimmungen nicht verneint. Andernfalls hätte er, da die Vermutung zutraf, gelogen. Ganz korrekt wäre die Antwort gewesen, das würde man ein paar Tage später sehen. Diese Antwort wäre aber wohl trotzdem als Bestätigung interpretiert worden.

Beurteilung Es kann sich bei Kandidaturen für eine Volkswahl wesensnotwendig nicht um ein echtes Geheimnis handeln. Im vorliegenden Fall war sie zwar noch nicht rechtskräftig eingereicht, sondern erst angekündigt. Trotzdem wussten im fraglichen Zeitpunkt schon eine Reihe von Personen davon – nämlich mindestens diejenigen, welche die Anmeldung der Kandidatur unterstützt haben. Üblicherweise dürften auch viele Personen innerhalb der Partei davon Kenntnis haben. Der Datenschutzbeauftragte hat der vorgesetzten Stelle empfohlen, das Vorgehen vor der Veröffentlichung von Kandidaturen mit den Mitarbeitenden anzuschauen und falls nötig zu regeln. Die Empfehlung stiess auf offene Ohren.

Die Kantonspolizei leitet Anfragen anderer Polizeikorps, wer zu einem bestimmten Zeitpunkt an einer bestimmten Adresse gemeldet war, an die Einwohnerdienste weiter.

Überprüfung der Grundkompetenzen

Grundkompetenzen Die EDK, die Schweizerische Konferenz der Erziehungsdirektoren, hat 2011 nationale Bildungsziele beschlossen. Sie legen die Grundkompetenzen fest, welche die Schülerinnen und Schüler in der Schulsprache, in den Fremdsprachen, in Mathematik und Naturwissenschaften erwerben sollen. Ab 2016 soll die Überprüfung der Grundkompetenzen (ÜGK) beginnen. Dazu werden in einer ersten Runde Schülerinnen und Schüler der 9. Klasse in Mathematik geprüft.

Kontextfragebogen Die Prüfung besteht nicht nur aus einer Mathematik-Prüfung, sondern umfasst auch einen sog. Kontextfragebogen. Darin sollen die Schülerinnen und Schüler u.a. sehr persönliche Fragen über sich und ihre Familie, über die Schule, über ihre Motivation, über die Mathematikhausaufgaben und

über ihre beruflichen Zukunftsperspektiven beantworten. In einem Kanton, der damit ein Pilotprojekt durchführen sollte, haben die Fragen (zum Teil zu Gesundheitsaspekten und strafbaren Handlungen) und das Setting der «Prüfung» mehr als nur für Irritationen gesorgt. Der Datenschutzbeauftragte hat sich gemeinsam mit den Datenschutzbeauftragten der Kantone Zürich, Zug, Bern und Aargau der datenschutzrechtlichen Fragen angenommen.

Änderungen und offene Fragen Die Delegation, die sich 2015 zweimal mit den Expertinnen und Experten der EDK getroffen hat, hat erreicht, dass auf gewisse sehr heikle Fragen verzichtet wird bzw. dass sie umformuliert werden. Trotzdem bestehen noch offene Fragen:

— Damit die Teilnahme der in einer Stichprobenziehung ausgewählten Schülerinnen und Schüler obligatorisch ist, müssen die notwendigen Rechtsgrundlagen vorhanden sein. Der Rechtsdienst der EDK macht geltend, dass es neben Art. 10 des HarmoS-Konkordats[9] weder auf kantonaler noch auf interkantonaler Ebene zusätzlicher Rechtsgrundlagen bedürfe. Das ist nicht unumstritten: Das Konkordat verpflichtet die Kantone zur Durchführung von Referenztests – ob das aber eine hinreichende Grundlage ist für die Pflicht der Schülerinnen und Schüler, den Kontextfragebogen auszufüllen, wird in jedem Kanton zu prüfen sein.

— Falls die Teilnahmepflicht durch die Rechtsgrundlagen abgedeckt ist, müssen die Schülerinnen und Schüler über ihr Recht, Fragen nicht zu beantworten, informiert sein – und das «Auslassen» einer Frage muss technisch möglich sein (der Fragebogen wird am PC ausgefüllt).

— Die Schülerinnen und Schüler wie auch ihre Eltern sind über die «Prüfung» vorgängig zu informieren. Dabei genügt es nicht, bloss zu sagen, es würden die Mathematik-Kenntnisse geprüft und «Informationen erfasst, die einen Einfluss auf den Lernerfolg haben können». Die Information muss so erfolgen, dass die Eltern, denen die Kinder nach dem Ausfüllen von konkret gestellten Fragen erzählen, nicht vor den Kopf gestossen sind. Dass der Fragebogen nicht vorgängig veröffentlichen wird, ist zwar unter dem Aspekt der Transparenz unschön, aber es ist nachvollziehbar, damit ein «Vorbereiten» verhindert werden kann.

— Eine blosse Information «Die Daten werden vertraulich behandelt» reicht nicht aus. Es ist adressatengerecht darüber zu informieren, was mit den Daten geschieht, solange die Schülerinnen und Schüler noch identifizierbar sind, wann die Daten pseudonymisiert oder anonymisiert werden, wem sie anschliessend zur Verfügung gestellt werden können, in welcher Form Forscherinnen und Forscher die Daten erhalten, wie lange die Daten derart bearbeitet werden dürfen usw.

Fortsetzung Der Datenschutzbeauftragte bleibt – gemeinsam mit den anderen involvierten Datenschutzbeauftragten – in Kontakt mit der EDK. Er wird ausserdem die Umsetzung im Kanton Basel-Stadt mitverfolgen und beratend zur Seite stehen.

Videoüberwachung

Vorabkontrollen Dem Datenschutzbeauftragten wurden im Jahr 2015 zehn Projekte (2014:10) für den Einsatz von Videoüberwachungsanlagen zur Vorabkontrolle vorgelegt. Dabei handelte es sich in lediglich einem Fall um eine gänzlich neue Anlage, die übrigen Anlagen sollten entweder ergänzt (z.B. diejenige des Kunstmuseums im Erweiterungsbau), umgestaltet oder in ihrem Betrieb verlängert werden.

Ende 2015 wurden durch kantonale und kommunale öffentliche Organe im Kanton Basel-Stadt knapp weniger als 800 Kameras betrieben.

Anzahl der Kameras Nach den Unterlagen des Datenschutzbeauftragten werden durch (kantonale und kommunale) öffentliche Organe im Kanton Basel-Stadt aktuell knapp weniger als 800[10] Kameras betrieben. Nicht mitgezählt sind:

— die Kameras in den Fahrzeugen und Depots der Basler Verkehrsbetriebe[11],

— die Kameras in den staatlichen Parkhäusern[12],

— die Kameras der Basler Kantonalbank[13] und

— die von der Polizei gestützt auf das Polizeigesetz[14] zur Beweissicherung eingesetzten Kameras.

Veröffentlichung der Reglemente Noch keinen Überblick hat der Datenschutzbeauftragte zurzeit über die Einhaltung der Pflicht, die Reglemente, welche die Bestimmungen im IDG für jede einzelne Videoüberwachungsanlage konkretisieren, zu veröffentlichen. Er wird die Einhaltung der Publikationspflicht im kommenden Jahr kontrollieren. >

Ausblick Mit dem Inkrafttreten des Informations- und Datenschutzgesetzes per 1. Januar 2012 trat auch die neue Regelung für die Videoüberwachung in Kraft. Damit hatte sich für den Betrieb von Videoüberwachungsanlagen einiges geändert: Erstens findet sich die gesetzliche Grundlage für den Betrieb der Videoüberwachungsanlagen seither in § 17 IDG, womit es keiner gesetzlichen Grundlage in einem Spezialgesetz mehr bedarf. Zweitens ist seither der Betrieb der Anlage nicht mehr vom Datenschutzbeauftragten zu bewilligen: Das Reglement muss von der Departementsleitung, dem Gemeinderat, dem Appellationsgericht oder der Direktion selbständiger Anstalten und Körperschaften erlassen werden[15]. Dafür ist seither drittens das Reglement, bevor es erlassen oder verlängert werden kann, dem Datenschutzbeauftragten zur Vorabkontrolle vorzulegen[16]. Die Reglemente dürfen nur befristet erlassen werden – das Gesetz legt vier Jahre als Maximalfrist fest[17].

Soll eine Videoüberwachung verlängert werden, ist das Vorhaben samt Vorfallsliste und Evaluationsbericht dem Datenschutzbeauftragten zur Vorabkontrolle vorzulegen.

Verlängerung Deshalb laufen die nach der neuen Regelung erlassenen Reglemente ab dem Jahr 2016 aus. Vor einer allfälligen Verlängerung ist die Wirksamkeit der Videoüberwachung zu evaluieren[18]. Die erlassende Stelle (Departementsleitung, Direktion selbständiger Anstalten usw.) darf eine Verlängerung des Reglements ins Auge fassen, wenn die Wirksamkeit der Anlage belegt ist. Dazu ist in der Regel die Auswertung der Vorfallsliste (samt den anlässlich der Vorfälle ergriffenen Massnahmen) erforderlich. Nötigenfalls sind Anpassungen vorzunehmen: Wirkungslose Videoüberwachungsanlagen sind abzubauen, allenfalls müssen Kameras umplatziert werden oder Lücken im Dispositiv durch neue Kameras geschlossen oder die Betriebsbedingungen geändert werden. Wenn die zum Reglementserlass zuständige Stelle zum Schluss kommt, dass die Videoüberwachung (gegebenenfalls mit Anpassungen) weiterbetrieben werden soll, dann hat sie das Vorhaben samt Vorfallsliste und Evaluationsbericht dem Datenschutzbeauftragten wiederum zur Vorabkontrolle vorzulegen[19].

Vorabkontrollen zu Onlinezugriffs-Gesuchen

Verantwortung der Dateneignerinnen Wenn ein öffentliches Organ einen Onlinezugriff auf Daten eines anderen öffentlichen Organs erhalten will, muss es ein Gesuch an die Dateneignerin stellen. Diese Gesuche sind dem Datenschutzbeauftragten zur Vorabkontrolle zu unterbreiten. Mit dem letzten Tätigkeitsbericht[20] hat der Datenschutzbeauftragte darauf hingewiesen, dass er vermutet, dass etliche dieser Onlinezugriffs-Bewilligungen abgelaufen sind. Die Dateneignerinnen sind dafür verantwortlich, dass nur von ihr bewilligte Zugriffe möglich sind. Sie müssen deshalb die Bezügerinnen ihrer Daten anhalten, ein neues oder ein Verlängerungsgesuch zu stellen, ansonsten ist der Onlinezugriff aufzuheben. Vor allem die Gebäudeversicherung Basel-Stadt hat 2015 systematisch alle Bezügerinnen ihrer Daten aufgefordert, ein solches Gesuch zu stellen; andernfalls würde der Zugriff unterbunden. Diese Aktion hat dazu geführt, dass mehrere Zugriffe, die zur Aufgabenerfüllung von Datenbezügerinnen nicht mehr erforderlich waren, aufgehoben werden konnten.

Stand Gesamthaft konnten im Jahr 2015 17 Vorabkontrollen zu Onlinezugriffs-Gesuchen abgeschlossen werden. Eine ansehnliche Zahl davon konnten behandelt werden, weil verwaltungsseitig endlich eine Dateneignerin für die dreizehnstellige AHV-Nummer (AHVN13) bestimmt worden war. Sieben Gesuche waren am Jahresende noch hängig.

Elektronischer Workflow Die Zentralen Informatikdienste (ZID) sind aktuell daran, die Voraussetzungen zu schaffen, damit die Onlinezugriffs-Gesuche künftig in einem elektronischen Workflow abgewickelt werden können. Anfangs 2017 sollte das Projekt umgesetzt sein. Damit dürfte es für die Dateneignerinnen einfacher werden, ihre Verantwortung wahrzunehmen. Dann sollte es auch ausgeschlossen sein, dass – wie im Berichtsjahr – festgestellt werden muss, dass ein privates Unternehmen immer noch einen Onlinezugriff auf diverse Verwaltungsdaten besass, obwohl seit seiner Privatisierung vor etlichen Jahren die gesetzlichen Voraussetzungen nicht mehr gegeben waren.

Vernehmlassungen

Vorlagepflicht Der Datenschutzbeauftragte hat Stellung zu Erlassen zu nehmen, die für den Umgang mit Informationen oder den Datenschutz erheblich sind[21]. Damit er dies tun kann, ist es erforderlich, dass ihm von den verantwortlichen Stellen die Erlassentwürfe vorgelegt werden[22]. Die Vorlagen sind ihm spätestens im Rahmen der verwaltungsinternen Vernehmlassung vorzulegen. Stehen der Umgang mit

Informationen oder das Bearbeiten von Personendaten im Mittelpunkt der Vorlage, ist zu empfehlen, bereits früher eine Stellungnahme zum Entwurf einzuholen[23]. Das geschah im Berichtsjahr beispielsweise beim Entwurf zum Tagesbetreuungsgesetz, bei welchem datenschutzspezifische Fragen bereits vor der Vernehmlassung geklärt werden konnten.

Vorgelegt Im Jahr 2015 wurden dem Datenschutzbeauftragten 15 (2014: 15) Erlasse zur Vernehmlassung vorgelegt. Die Spannweite reichte von Bundesvernehmlassungen zu geplanten Revisionen des Gesetzes über genetische Untersuchungen am Menschen (GUMG), des Schuldbetreibungs- und Konkursgesetzes (SchKG) und des Strafgesetzbuches (StGB) über Bundesvernehmlassungen zu neuen Gesetzen wie dem Bundesgesetz über die Aufarbeitung der fürsorgerischen Zwangsmassnahmen und Fremdplatzierungen vor 1981 (AFZFG) bis hin zu kantonalen Vernehmlassungen, etwa zum Publikationsgesetz, zur geplanten Totalrevision des Aufenthaltsgesetzes oder zum Jodtabletten-Verteilkonzept. Nicht mitgezählt sind hier die Vernehmlassungen zu den Schengen- und Dublin-Weiterentwicklungen[24], zu denen teilweise auch Stellung zu nehmen ist. Besondere Erwähnung sollen im Folgenden nur die Vernehmlassungen zum Bundesgesetz über die Aufarbeitung der fürsorgerischen Zwangsmassnahmen und Fremdplatzierungen vor 1981 (AFZFG) und zur Totalrevision des kantonalen Gesetzes über das Aufenthaltswesen (Aufenthaltsgesetz) finden.

Damit der Datenschutzbeauftragte Stellung zu Erlassen nehmen kann, ist es erforderlich, dass ihm von den verantwortlichen Stellen die Erlassentwürfe vorgelegt werden.

Mitwirkung Noch stärker ist der Einbezug, wenn der Datenschutzbeauftragte bereits bei der Ausarbeitung eines Erlassentwurfs mitwirken kann. Das war im Berichtsjahr etwa der Fall beim Entwurf zu einem Kundenportalgesetz, beim Entwurf zu einer Revision des Informations- und Datenschutzgesetzes und bei der Verordnung zum eHealth-Pilotversuch.

Aufarbeitung der fürsorgerischen Zwangsmassnahmen und Fremdplatzierungen

Nicht vorgelegt Obschon der Datenschutzbeauftragte bei dieser wichtigen Thematik vom zuständigen Departement nicht zur Stellungnahme zuhanden der kantonalen Vernehmlassung eingeladen wurde, konnte fristgerecht eine Beurteilung der Vorlage abgegeben werden. Zudem konnte die Stellungnahme des Datenschutzbeauftragten via privatim, die Vereinigung der Schweizerischen Datenschutzbeauftragten, anderen Datenschutzbehörden zur Verfügung gestellt werden.

Stellungnahme Der Datenschutzbeauftragte hat verschiedene aus datenschutzrechtlicher Sicht positive Regelungen des Entwurfs zum AFZFG begrüsst und eine Klärung angemahnt:

— Art. 10 des Entwurfs zum AFZFG erklärt die kantonalen Informations-, Datenschutz- und Archivgesetze auch für jene Institutionen für anwendbar, welche mit fürsorgerischen Zwangsmassnahmen oder Fremdplatzierungen befasst waren, jedoch nicht unter die in ihrem Sitzkanton geltenden Informations-, Datenschutz- und Archivgesetze fallen würden. Diese Klärung ist zu begrüssen, da auch heute die Feststellung des anwendbaren Datenschutzrechts in der Praxis oftmals Schwierigkeiten bereitet, wenn private Institutionen öffentliche Aufgaben wahrnehmen und dabei der Umfang der Aufgabenübertragung nicht zweifelsfrei geklärt werden kann. Das gilt erst recht für die durch das Gesetz geregelten Fälle, die 35 Jahre und mehr zurückliegen, als es noch gar keine (Informations- und) Datenschutzgesetze und auch nicht durchgehend Archivgesetze gab.

— Indem Art. 10 des Entwurfs zum AFZFG die kantonalen Informations- und Datenschutzgesetze für alle im jeweiligen Kanton gelegenen Institutionen, die mit fürsorgerischen Zwangsmassnahmen oder Fremdplatzierungen befasst waren, für anwendbar erklärt, wird auch die Aufsichtszuständigkeit geklärt: Die Beratung und Kontrolle des Datenbearbeitens durch die fraglichen Institutionen obliegt damit den kantonalen Datenschutzbeauftragten.

— Art. 11 des Entwurfs zum AFZFG sieht für Betroffene oder deren Angehörige einen «einfachen und kostenlosen Zugang zu den sie betreffenden Akten» vor. Allfällige Einschränkungsgründe, wie beispielsweise überwiegende öffentliche oder private Interessen[25], nennt Art. 11 des Entwurfs zum AFZFG nicht. Es stellte sich die Frage, ob der Zugang zu den Informationen für die Betroffenen und, nach ihrem Tod, ihre Angehörigen mit der detaillierten Regelung in Art. 11 des Entwurfs zum AFZFG abschliessend geregelt werden soll. Der Datenschutzbeauftragte empfahl >

daher, in der kantonalen Stellungnahme vom Bund zu fordern, im Gesetzestext klar zu regeln, ob der Zugang nach dem anwendbaren kantonalen Informations-, Datenschutz- oder Archivrecht aufgrund überwiegender öffentlicher oder privater Interessen ganz oder teilweise eingeschränkt werden kann oder nicht.

Totalrevision kantonales Gesetz über das Aufenthaltswesen

Vorgelegt Das Justiz- und Sicherheitsdepartement hat im Berichtsjahr eine Vorlage zur Totalrevision des Aufenthaltsgesetzes und den Entwurf zu einem Gesetz über Niederlassung und Aufenthalt (fortan: NAG) in die Vernehmlassung geschickt.

Stellungnahme Der Datenschutzbeauftragte hat die Vorlage grundsätzlich begrüsst. Mit dem NAG wird eine modernisierte Rechtsgrundlage geschaffen für die mit dem Bearbeiten von Personendaten erfolgenden Eingriffe in das Grundrecht der informationellen Selbstbestimmung der betroffenen Personen. Der Datenschutzbeauftragte hat zu einigen Formulierungen Klärungen vorgeschlagen. Ausserdem hat er empfohlen,

— die Erhebung von Daten durch die Einwohnerkontrolle für andere Organe präziser zu regeln,

— die Bekanntgabe von Daten zur Erstellung von offiziellen Schriften der Gemeinden noch einmal zu prüfen,

— bei der Einführung von Adressanfragen per Internet zu konkretisieren, wie die angesprochene Missbrauchsverhinderung realisiert werden soll, und

— die vorgeschlagene Regelung des Zugriffs auf Personendaten im Abrufverfahren grundlegend zu überarbeiten.

Schengen- und Dublin-Weiterentwicklungen

Dynamische Rechtsentwicklung Im Jahr 2015 wurden acht (2014: 12) Schengen- und Dublin-Weiterentwicklungen mitgeteilt, die kantonsintern vom Datenschutzbeauftragten geprüft werden konnten. Die Weiterentwicklungen warfen unseres Erachtens keine datenschutzrechtlichen Fragestellungen auf; sie betrafen in der Regel bloss Detailfragen.

Medienanfragen

Breites Interesse Das Medieninteresse an Datenschutzfragen hat im Berichtsjahr etwas abgenommen: 14 (2014: 20) mal wurde der Datenschutzbeauftragte von Zeitungen, Radio- und Fernsehstationen um Stellungnahmen zu unterschiedlichsten Themen gebeten: Die Verwendung von maschinenlesbaren Stimm- und Wahlzetteln, die «geleakten» Betreibungsregisterauszüge, der Einsatz von Kameras durch die Swiss Football League um das St. Jakobs-Stadium herum, die WMS-Schülerinnen und Schüler, die an die Antworten für die Abschlussprüfungen gelangten, das «Safe Harbor-Urteil» des Europäischen Gerichtshofes – das Interesse der Medien und der Öffentlichkeit an datenschutz- und informationsrechtlichen Themen war im Jahr 2015 wieder erfreulich breit.

Schulungen, Referate und Publikationen

Reges Interesse Auch in diesem Jahr blieb das Interesse an bereichsspezifischen datenschutz- und öffentlichkeitsrechtlichen Schulungen sowie an Referaten gross: Der Datenschutzbeauftragte hat im Berichtsjahr sieben (2014: 6) Schulungen für öffentliche Organe durchgeführt; hinzu kommen noch fast doppelt so viele Referate und Weiterbildungsbeiträge, die ebenfalls der Sensibilisierung dienen.

Das Interesse der Medien und der Öffentlichkeit an datenschutz- und informationsrechtlichen Themen war im Jahr 2015 wieder erfreulich breit.

Schulungen Der Datenschutzbeauftragte hat die folgenden sieben Schulungen für öffentliche Organe durchgeführt:

— zweimal das Seminar «Datenschutz und Öffentlichkeitsprinzip: kurz erklärt» im Rahmen des kantonalen Weiterbildungsangebotes;

— zwei Schulungen für Mitarbeiterinnen und Mitarbeiter von Einwohnerdiensten im Rahmen des Weiterbildungsangebotes des Verbandes der Schweizerischen Einwohnerdienste (VSED);

— eine Schulung zu Datenschutz im Umfeld der Schwarzarbeitsbekämpfung für die Mitglieder der Arbeitsgruppe «Bekämpfung der Schwarzarbeit»;

— eine Schulung zu Videoüberwachung für die Mitarbeiterinnen und Mitarbeiter der Gartenbäder und

— das Modul «Datenschutz, Amtsgeheimnis und Archivierung», das Teil des Lehrplans der KV-Lehre in der öffentlichen Verwaltung bildet.

Referate und Weiterbildungsbeiträge Ausserdem haben der Datenschutzbeauftragte bzw. seine Mitarbeitenden mehrere Referate gehalten und Weiterbildungsbeiträge erbracht, so unter anderem:

— ein Referat zur (General-)Einwilligung in der klinischen Forschung, insbesondere zur schweizerischen Regelung im Vergleich zum rechtlichen Umfeld in Europa, anlässlich des SCTO[26]-Forums «Klinische Forschung»;

— ein Referat zum «Recht am eigenen Bild» anlässlich der Kommunikationskonferenz des Präsidialdepartements;

— ein Referat zu «Open Government Data und Datenschutz» an der öffentliche Tagung anlässlich des Frühjahrsplenums von privatim, der Vereinigung der schweizerischen Datenschutzbeauftragten;

— ein Referat zu «Datenschutz an Schulen» für die Mitglieder des Elternrats der Schulen Theodor;

— ein Workshop zu «Persönlichkeitsrechte versus Aufbewahrung und Archivierung von Daten: eine Auslegeordnung» anlässlich des achten Datenschutztages an der Universität Freiburg;

— ein Referat zu aktuellen Fragen zu Datenschutz, Informationszugang und Informationssicherheit an der Informationsveranstaltung des Amtes für Wirtschaft und Arbeit;

— ein Gespräch zu «Bits and Bites – Wie gläsern wollen wir sein?» in der Ausstellung Poetics and Politics im Haus der elektronischen Künste (HeK);

— eine Einführung in die Datenschutzgrundlagen für die Sicherheitsbeauftragten der Departemente und

— ein Referat zum «Balanceakt zwischen Sozialen Medien und Datenschutz» anlässlich des 50-Jahr-Jubiläums der Schweizerischen Arbeitsgemeinschaft für Klinische Krebsforschung (SAKK).

Datenschutz-Basilisk Mit der Kolumne in «BS intern» hat der Datenschutz die folgenden Themen angesprochen:

— *Die tollen Ferienfotos auf dem Smartphone:* Das Smartphone wie ein offenes Buch? Ein gut gewähltes Passwort schützt unsere Daten auf mobilen Geräten. Aber was ist ein gutes Passwort? Wie viele verschiedene Passwörter braucht man? Der Datenschutz-Basilisk gibt praktische Tipps.

— *Das Öffentlichkeitsprinzip – eine Hexerei?* Wie steht das Amtsgeheimnis zum Öffentlichkeitsprinzip? Welche Interessen gilt es zu berücksichtigen und wer entscheidet, was herausgegeben wird? Alles halb so wild, beruhigt der Datenschutz-Basilisk.

— *Digitaler Schutzschild für Mails:* Viele Amtsstellen müssen heikle Informationen verschicken. Ohne zusätzliche Schutzmassnahmen ist eine E-Mail ungefähr so sicher wie eine offen verschickte Postkarte – oder wie es die Informatik-Konferenz in einer Weisung festhält: «E-Mail gleich Postkarte»[27]. Wer auch heikle Daten versenden muss, möge dieses Bedürfnis anmelden.

Ohne zusätzliche Schutzmassnahmen ist eine E-Mail ungefähr so sicher wie eine offen versandte Postkarte.

Publikationen Auch in diesem Jahr haben der Datenschutzbeauftragte und seine Mitarbeitenden verschiedentlich zu Themen des Datenschutzes und des Öffentlichkeitsprinzips publiziert. Der Datenschutzbeauftragte ist u.a. Mitherausgeber und Redaktor von «digma»[28], der Zeitschrift für Datenrecht und Informationssicherheit aus dem Haus Schulthess Juristische Medien AG, und der «digma-Schriften zum Datenrecht» aus dem gleichen Verlag. In dieser Funktion verfasst er regelmässig Einführungsartikel[29] sowie den «schlusstakt»[30]. Barbara Widmer publiziert regelmässig in der Rubrik «Der Blick nach Europa und darüber hinaus»[31]. Sandra Husi-Stämpfli hat bis zu ihrem Austritt vierteljährlich die News aus den Datenschutzbehörden und drei weitere Artikel (einmal gemeinsam mit Katrin Gisler)[32] veröffentlicht. Ausserdem sind von Sandra Husi-Stämpfli und dem Datenschutzbeauftragten in Stämpflis Handkommentar Datenschutzgesetz Kommentierungen zu sieben DSG-Artikeln[33] erschienen – vom Datenschutzbeauftragten ausserdem in Stämpflis Handkommentar Humanforschungsgesetz zu fünf HFG-Artikeln[34]. Beachtenswert ist schliesslich auch die Dissertation von Daniela Waldmeier zu «Informationelle Selbstbestimmung – ein Grundrecht im Wandel?»[35].

Veranstaltungen

Europäischer Datenschutztag Wie gewohnt hat der Datenschutzbeauftragte aus Anlass des Europäischen Datenschutztages zu einem Apéro eingeladen. Der Anlass bietet Gelegenheit, mit den Grossrätinnen und Grossräten aus dem Grossratsbüro, der Geschäftsprüfungs- und der Justiz-, Sicherheits- und Sportkommission, mit den Präsidien der anderen >

Grossratskommissionen, mit den Leiterinnen und Leitern und den Ansprechpersonen aus den Dienststellen, mit denen der Datenschutzbeauftragte regelmässig zu tun hat, ungezwungen ins Gespräch zu kommen.

Symposium on Privacy and Security 2015 fand die 20. Ausgabe des Symposium on Privacy and Security in Zürich statt. Die Datenschutzbeauftragten der Kantone Zürich und Basel-Stadt, denen seit Jahren die Programmgestaltung obliegt, erhielten die Möglichkeit, Gäste zur Teilnahme am Jubiläums-Symposium einzuladen. 17 Jubiläumsgäste aus Basel haben den Festakt im Auditorium Maximum der ETH Zürich mit ihrer Teilnahme beehrt, allen voran die Grossratspräsidentin und drei weitere Mitglieder des Grossen Rates sowie Präsidien von Gerichten und Dienststellenleiterinnen und -leiter aus der Verwaltung und der «grossratsaffilierten» Stellen.

Zusammenarbeit

Gesetzlicher Auftrag Der Datenschutzbeauftragte arbeitet zur Erfüllung seiner Aufgaben mit den Organen der anderen Kantone, des Bundes und des Auslandes, welche die gleichen Aufgaben erfüllen, zusammen[36]. Dank dieser Zusammenarbeit lassen sich Synergien nutzen.

Kantonsübergreifend Auch im Jahr 2015 stellte die kantonsübergreifende Zusammenarbeit ein wesentliches Element der Tätigkeit des Datenschutzbeauftragten dar. So arbeiteten der Datenschutzbeauftragte und seine Mitarbeiterinnen und Mitarbeiter nicht nur aktiv im privatim-Büro, sondern auch in den privatim-Arbeitsgruppen «Gesundheit» (Daniela Waldmeier), «Schule» (bis zur Auflösung der Arbeitsgruppe: Sandra Husi-Stämpfli) und «ICT» (Markus Brönnimann) mit. Barbara Widmer war aktiv beteiligt am Aufbau von «TerrAudit». In diesem Verein können sich die Grundbuchämter und Datenschutzbeauftragten der Kantone, die sich an «Terravis» beteiligen, zusammenschliessen, um eine interkantonal koordinierte wirksame Aufsicht über die Plattform «Terravis» sicherzustellen. «Terravis» ist ein elektronisches Grundbuch-Informationssystem (eGRIS), über welches die angeschlossenen kantonalen Grundbuchämter Grundbuchinformationen mit Berechtigten austauschen. Basel-Stadt ist (noch) nicht an «Terravis» beteiligt – das Vorhandensein einer wirksamen Aufsicht wäre aber auf jeden Fall Voraussetzung für einen allfälligen Beitritt. Schliesslich ist der Datenschutzbeauftragte (zusammen mit Daniela Waldmeier als Stellvertreterin) Mitglied der Ethikkommission der Pädagogischen Hochschule der FHNW.

National Im Bereich von eHealth vertrat Barbara Widmer die kantonalen Datenschutzbeauftragten in den Arbeitsgruppen «Standards & Architektur» und «Aufbau & Vernetzung» von eHealth Suisse. Der Datenschutzbeauftragte wurde von der nationalrätlichen Kommission für soziale Sicherheit und Gesundheit (SGK-N) als Vertreter der kantonalen Datenschutzbeauftragten zu einem Hearing zum Krebsregistrierungsgesetz eingeladen.

Dank der Zusammenarbeit mit den Organen der anderen Kantone, des Bundes und des Auslandes, welche die gleichen Aufgaben erfüllen, lassen sich Synergien nutzen.

International Weiterhin intensiv beschäftigt hat den Datenschutzbeauftragten auch die Revision des Datenschutzrechts auf EU-Ebene[37]. Die Interessen der Kantone in der Datenschutz-Arbeitsgruppe der Konferenz der Kantonsregierungen und in der Schengen Coordination Group (SCG), welche die Joint Supervisory Authority of Schengen (JSA) abgelöst hat, wurden im Jahr 2015 ebenfalls vom Datenschutzbeauftragten des Kantons Basel-Stadt vertreten (Sandra Husi-Stämpfli bis zu ihrem Austritt). Damit war sichergestellt, dass die laufenden Entwicklungen im Bereich des Datenschutzes in der EU konzentriert und zeitnah beurteilt werden können. Schliesslich erlangte der Datenschutzbeauftragte auch die Akkreditierung bei der Internationalen Konferenz der Datenschutzbeauftragten und konnte damit an der 2015 in Amsterdam stattfindenden Konferenz teilnehmen. Dabei erhielt er aus erster Hand Informationen über die bevorstehende Datenschutzreform der EU und über die Bemühungen zur Regelung des Datenaustausches mit den USA, nachdem der Europäische Gerichtshof (EuGH) das Safe-Harbor-Abkommen aufgehoben hat.

Aber auch kantonsintern Auf kantonaler Ebene brachte der Datenschutzbeauftragte sein Fachwissen auch im Berichtsjahr in der Basler Expertengruppe «Datenschutz im Gesundheitswesen» ein, in der er sich regelmässig mit Vertreterinnen und Vertretern des Universitätsspitals, der Schweizerischen Akademie der Medizinischen Wissenschaften (SAMW), von Novartis und Roche und einem auf diesem Gebiet stark engagierten Advokaturbüro über aktuelle Datenschutzfragen im Gesundheitsbereich austauscht. Ausserdem wirken seine Mitarbeiterinnen und Mitarbeiter in etlichen verwaltungsinternen Arbeitsgruppen und Steuerungs-Gremien mit, oftmals bloss in beratender Funktion, um die Unabhängigkeit nicht zu gefährden.

1 § 7 Abs. 1 lit. a IDG; vgl. dazu PK-IDG/BS-Rudin, § 7 N 19 ff.
2 § 7 Abs. 1 lit. b IDG; vgl. dazu PK-IDG/BS-Rudin, § 7 N 32 ff.
3 Zur Abgrenzung von der Aufgabenübertragung vgl. PK-IDG/BS-Rudin, § 7 N 11.
4 § 3 Abs. 1 lit. c IDG, vgl. dazu PK-IDG/BS-Rudin, § 3 N 10 ff.
5 § 4 Abs. 3 des Staatsbeitragsgesetzes.
6 Zur Abgrenzung von der Aufgabenübertragung vgl. PK-IDG/BS-Rudin, § 7 N 12 ff.
7 Erfordernis der gesetzlichen Grundlage für die Bekanntgabe von Personendaten, § 21 Abs. 1 lit. a IDG.
8 Art. 10 HarmoS-Konkordat (Bildungsmonitoring): «In Anwendung von Art. 4 des Konkordats über die Schulkoordination vom 29. Oktober 1970 beteiligen sich die Vereinbarungskantone zusammen mit dem Bund an einem systematischen und kontinuierlichen, wissenschaftlich gestützten Monitoring über das gesamte schweizerische Bildungssystem. Die Entwicklungen und Leistungen der obligatorischen Schule werden regelmässig im Rahmen dieses Bildungsmonitorings evaluiert. Ein Teil davon ist die Überprüfung der Erreichung der nationalen Bildungsstandards namentlich durch Referenztests im Sinne von Art. 8 Absatz 4.»
9 Weder auf kantonaler noch auf interkantonaler Ebene
10 Noch nicht enthalten sind in dieser Zahl die neuen Kameras im Erweiterungsbau des Kunstmuseums; zu ihnen hat der Datenschutzbeauftragte bereits Stellung genommen, sie werden jedoch erst im Frühjahr 2016 in Betrieb genommen.
11 Für das Datenbearbeiten durch konzessionierte Transportunternehmen gilt nach Art. 54 des Bundesgesetzes vom 20. März 2009 über die Personenbeförderung (Personenbeförderungsgesetz, PBG) das Bundesdatenschutzgesetz; für die Aufsicht ist der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte zuständig. Vgl. dazu TB 2010, 10 f. und PK-IDG/BS-Rudin, § 2 N 37 ff.
12 Das Datenbearbeiten der Betreiberin Immobilien Basel-Stadt im Bereich der Bewirtschaftung des Finanzvermögens fällt nach § 2 Abs. 2 lit. a IDG nicht im Geltungsbereich des IDG; vgl. dazu PK-IDG/BS-Rudin, § 2 N 13 f.
13 Die Basler Kantonalbank ist zwar eine Anstalt des kantonalen öffentlichen Rechts (§ 1 Abs. 1 und 2 des Kantonalbankgesetzes), fällt aber aufgrund seiner Teilnahme am wirtschaftlichen Wettbewerb aus dem Geltungsbereich des IDG; vgl. dazu PK-IDG/BS-Rudin, § 2 N 13 f.
14 § 58 PolG (Bild- und Tonaufnahmen zur Beweissicherung); vgl. dazu PK-IDG/BS-Husi, § 17 N 11.
15 § 18 Abs. 2 IDG; vgl. dazu PK-IDG/BS-Husi, § 18 N 26 ff.
16 § 18 Abs. 4 IDG; vgl. dazu PK-IDG/BS-Husi, § 18 N 34 ff.
17 § 18 Abs. 3 Satz 1 IDG; vgl. dazu PK-IDG/BS-Husi, § 18 N 32.
18 § 18 Abs. 3 Satz 2 IDG; vgl. dazu PK-IDG/BS-Husi, § 18 N 33.
19 § 18 Abs. 4 IDG; vgl. dazu PK-IDG/BS-Husi, § 18 N 43 ff.
20 TB 2014, 12 ff.
21 § 44 lit. f IDG.
22 PK-IDG/BS-Schilling 2014, § 44 N 29 ff.
23 PK-IDG/BS-Schilling 2014, § 44 N 32.
24 Vgl. dazu hinten Seite 28.
25 Vgl. dazu § 29 IDG.
26 Die Swiss Clinical Trial Organisation (SCTO) mit Sitz in Basel ist die die zentrale Kooperationsplattform für die patientenorientierte, klinische Forschung in der Schweiz – eine gemeinschaftliche Initiative des Schweizerischen Nationalfonds (SNF) und der Schweizerischen Akademie der Medizinischen Wissenschaften (SAMW).
27 Informatik-Konferenz Basel-Stadt, Weisung vom 22. Oktober 2003 für die Benutzung von Informatikmitteln in der Verwaltung des Kantons Basel-Stadt (mit Änderungen vom 15. September 2004 und 7. März 2013), Ziff. 8.
28 2015 mit den Schwerpunktthemen «Klinikinformationssysteme» (2015.1), «20. Symposium on Privacy and Security» (2015.2), «Datenlecks» (2015.3) und «Staatsschutz und Aufsicht» (2015.4).
29 Beat Rudin, Datenschutz und IT-Sicherheit im Spital (digma 2015, 4 f.); Bruno Baeriswyl/Ueli Maurer/Beat Rudin, 20 Jahre Symposium on Privacy and Security (digma 2015, 33 f.); Beat Rudin, Staatsschutz zwischen Freiheit und Sicherheit (digma 2015, 128 f.); ausserdem Ders, Klassifikation – eine Etikette «für alles»? (digma 2015, 100 ff.).
30 Beat Rudin, Die Botschaft les' ich wohl, allein ... (digma 2015, 32); Ders., Ehrenwert vielleicht – aber auch korrekt? (digma 2015, 76); Ders., Mehr Gewicht für den Datenschutz!, (digma 2015, 124); Ders., Datenschutz stärken – in der Verfassung! (digma 2015, 172).
31 Barbara Widmer, Wenn der Zweck die Mittel heiligen soll (digma 2015, 30 f.); Dies., Demokratische Wahlen – wer wählt wen? (digma 2015, 72 f.); Dies., Bargeld lacht – auch wenn das Ende droht (digma 2015, 122 f.); Dies., mHealth – Health for me – or others? (digma 2015, 170 f.)
32 Sandra Husi, Widerrechtliche Daten ins Archiv? (digma 2015, 24 ff.); Dies., Sorgenkind wird Vorbild: Statistikgesetz BS (digma 2015, 112 ff.); Dies./Katrin Gisler, «Und cheese!»: Fotos auf Schulhomepages (digma 2015, 156 ff.).
33 Beat Rudin, Art. 2, 3 und 8, Sandra Husi-Stämpfli, Art. 9, 10 und 17a sowie ausserdem Entstehungsgeschichte, in: Bruno Baeriswyl/Kurt Pärli (Hrsg.), Stämpflis Handkommentar Datenschutzgesetz, Bern 2015.
34 Beat Rudin, Art. 3 lit. e bis i, 32, 33, 34 und 35 sowie zu den Ziff. 1 bis 3 des Anhangs, in: Bernhard Rütsche (Hrsg.), Stämpflis Handkommentar Humanforschungsgesetz, Bern 2015.
35 Stefanie-Daniela Waldmeier, Informationelle Selbstbestimmung – ein Grundrecht im Wandel?, Dissertation Zürich 2015.
36 § 48 IDG.
37 TB 2012, 26 f.

Aus dem Alltag

Einblicke in die Kontrolltätigkeit

Der Datenschutzbeauftragte kontrolliert nach einem autonom aufzustellenden Prüfprogramm die Anwendung der Bestimmungen über den Umgang mit Informationen. Im Jahr 2015 konnten vier Datenschutz-Prüfungen abgeschlossen werden, zwei sind noch am Laufen. Ausserdem arbeitet der Datenschutzbeauftragte mit dem Staatsschutzkontrollorgan zusammen.

Übersicht

Abgeschlossen Der Datenschutzbeauftragte hat im Berichtsjahr vier Prüfungen (2014: 5) abschliessen können:

— eine Datenschutz-Prüfung zu «Konsul»,

— eine Datenschutz-Prüfung beim Bereich der Gesundheitsdienste im Gesundheitsdepartement,

— eine Querschnitts-Prüfung zu Datenlöschung und -vernichtung und

— eine «SIS-Kontrolle» bei der Kantonspolizei.

Begonnen Zwei weitere Datenschutz-Prüfungen konnten im Berichtsjahr begonnen werden – sie werden aber erst im Folgejahr abgeschlossen werden können:

— eine Datenschutz-Prüfung zu Datenbanken bei der Kantonspolizei und

— eine Datenschutz-Prüfung im Universitätsspital Basel.

Abgeschlossen: Datenschutz-Prüfung zu «Konsul»

Prüfgebiet Der Datenschutzbeauftragte hat die Anwendung «Konsul», die in mehreren Bereichen der Verwaltung für die Geschäftsverwaltung eingesetzt wird, geprüft.

Feststellungen Innerhalb des vom Datenschutzbeauftragten definierten Prüfungsumfangs wurde unter anderem folgender Handlungsbedarf ausgemacht:

— Die Zuständigkeiten im Zusammenspiel mit den verschiedenen Gremien sind unzureichend definiert.

— Die Passworte sowohl für User als auch für Administratorinnen und Administratoren sind unzureichend und somit zu unsicher, was ja bei einer generellen Passwortqualitäts-Prüfung im Jahr 2014 schon festgestellt wurde[1].

— Es existiert keine Risikoanalyse als Grundlage für angemessene Massnahmen zum Schutz der bearbeiteten Informationen.

— Die Berechtigungsverwaltung ist unzureichend ausgestaltet.

— Die Möglichkeiten für die Auswertung der aktuellen Berechtigungen der Benutzerinnen und Benutzer sind mangelhaft.

Empfehlungen Der Datenschutzbeauftragte hat gegenüber der Staatskanzlei als der Gesamtverantwortlichen für die Geschäftsverwaltung «Konsul» verschiedene Empfehlungen ausgesprochen. Die Frist für die Rückmeldung zu den Empfehlungen läuft erst im Frühjahr 2016 ab.

Abgeschlossen: Datenschutz-Prüfung beim Bereich Gesundheitsdienste

Prüfgebiet Eine weitere Datenschutz-Prüfung führte der Datenschutzbeauftragte im Bereich Gesundheitsdienste des Gesundheitsdepartements durch.

Durchführung der Prüfung Nach einem zähflüssigen Start hat der Datenschutzbeauftragte zur Durchführung der Prüfung ein externes Prüfunternehmen beigezogen. Die Prüfung wurde inhaltlich im Berichtsjahr abgeschlossen. Einzig die formelle Schlussbesprechung konnte aus terminlichen Gründen bis Ende des Berichtsjahres noch nicht durchgeführt werden.

Wesentliche Feststellungen Innerhalb des vom Datenschutzbeauftragten definierten Prüfumfangs wurde unter anderem folgender Handlungsbedarf festgestellt:

— Die Aufgaben- und Rollenverteilung bezüglich des Datenschutzes und der Informationssicherheit sind zu wenig klar definiert.

— Grundlagen für eine angemessene Informationssicherheit wie beispielsweise ein Risikomanagement, ein ISMS[2] oder ISDS-Konzept[3] sind nicht formell dokumentiert.

— Die Verwaltung der Benutzerinnen und Benutzer weist Schwachstellen auf.

— Der Schutzbedarf («Wert» der bearbeiteten Informationen) als Grundlage für einen angemessenen Schutz ist nicht in jedem Fall festgehalten.

— Die Passwortqualität in einzelnen Systemen ist unzureichend und somit zu unsicher.

Empfehlungen Der geprüfte Bereich wurde aufgrund einer Reorganisation innerhalb der Gesundheitsdepartements neu strukturiert. Der Datenschutzbeauftragte hat gegenüber den Leiterinnen und Leitern der betroffenen Stellen und gegenüber dem Generalsekretariat verschiedene Empfehlungen ausgesprochen. Die Frist für die Rückmeldung zu den Empfehlungen läuft erst im Frühjahr 2016 ab.

Abgeschlossen: Querschnitts-Prüfung zu Datenlöschung und -vernichtung

Feststellungen Der Datenschutzbeauftragte hat innerhalb der Kantonsverwaltung eine Querschnittsprüfung zum Thema Datenlöschung und -vernichtung (unter der Berücksichtigung der Vorgaben zur Archivierung) durchgeführt. Dabei hat er anhand der von den Dienststellen zurückgemeldeten Informationen unter anderem festgestellt, dass

— die konzeptionellen Grundlagen bezüglich den Aufbewahrungsfristen weitgehend fehlen und

— in der Folge die Daten in der Mehrzahl der Systeme nicht gelöscht werden.

Empfehlungen Das Informations- und Datenschutzgesetz legt unmissverständlich fest, dass «nicht mehr benötigte Personendaten, die von der gemäss Archivgesetz zuständigen Stelle als nicht archivwürdig beurteilt werden, (...) vom öffentlichen Organ zu vernichten»[4] sind. Entsprechend empfiehlt der Datenschutzbeauftragte, die konzeptionellen Grundlagen zu erarbeiten und diese, wenn immer möglich, mittels automatisierter Verfahren in den IT-Systemen umzusetzen. Um eine höhere Effizienz und Effektivität zu erzielen, gilt es zu prüfen, ob kantonale Umsetzungsvorgaben oder Hilfestellungen für die Dateneignerinnen zur Verfügung gestellt werden sollen. Angesichts der Deutlichkeit des Widerspruchs zwischen gesetzlicher Vorgabe und Feststellung gilt es auch zu prüfen, ob den Verantwortlichen grundsätzlich Hilfestellungen bezüglich der Aufgaben, Kompetenzen und Verantwortlichkeiten (AKV)[5], die sie als Dateneignerin wahrnehmen müssten, zur Verfügung gestellt werden sollen. Auch stellt der Datenschutzbeauftragte fest, dass einige Datenpools nicht gemeldet wurden, und schliesst daraus, dass die Gesamtverantwortung für diese möglicherweise noch unzureichend geregelt ist. Diese Pendenz sollte aber bis spätestens 16. Februar 2016 erledigt sein, da bis zu diesem Zeitpunkt die Rechtsgrundlagen für Datenpools geschaffen werden müssen[6].

Umsetzung Der Gesamtregierungsrat will den Empfehlungen des Datenschutzbeauftragten Folge leisten.

Abgeschlossen: SIS-Kontrolle bei der Kantonspolizei

Prüfgebiet Der Datenschutzbeauftragte hat im Jahr 2015 eine Kontrolle der Nutzung des Schengener Informationssystems (SIS) bei der Kantonspolizei durchgeführt. Dabei wurden zum einen konkrete Abfragen des SIS durch die Mitarbeiterinnen und Mitarbeiter überprüft. Zum anderen wurde allgemein untersucht, ob die bestehenden Zugriffsberechtigungen tatsächlich zur Aufgabenerfüllung der jeweiligen Abteilungen bzw. Personen benötigt werden und ob entsprechende Berechtigungskonzepte bestehen.

Bei einer Querschnittsprüfung wurde festgestellt, dass die Daten in der Mehrzahl der Systeme nicht wie vom Informations- und Datenschutzgesetz festgelegt gelöscht werden.

Feststellungen Im Rahmen der Stichprobenkontrollen konnte festgestellt werden, dass den meisten Mitarbeiterinnen und Mitarbeitern bewusst ist, dass mit jeder von ihnen getätigten RIPOL- , FABER- oder ZEMIS-Abfrage automatisch auch ein Abgleich mit dem SIS erfolgt. Der Nutzen, welchen diese automatischen Abfragen für die Aufgabenerfüllung mit sich bringen, scheint jedoch nach Einschätzung der befragten Personen eher gering: Treffer werden, wenn überhaupt, lediglich beim Abgleich der Hotelmeldescheine mit dem RIPOL/SIS erzielt, im übrigen Dienstalltag wurde von den befragten Personen bislang keine Treffer verzeichnet. Weiter konnte festgehalten werden, dass das Datenschutzbewusstsein der Mitarbeiterinnen und Mitarbeiter sehr gross ist. In organisatorischer Hinsicht bestehen hingegen Defizite bezüglich der Berechtigungskonzepte: Die Zugriffsberechtigungen erscheinen zu wenig skaliert. >

Empfehlungen Der Datenschutzbeauftragte empfahl vor diesem Hintergrund einmal mehr, die Verknüpfung des SIS mit den nationalen Informationssystemen auf Bundesebene zu prüfen. Inzwischen hat sich herausgestellt, dass die Berechtigungen bei den Bundessystemen stärker differenziert werden können als bisher angenommen. Der Datenschutzbeauftragte hat deshalb der Kantonspolizei empfohlen, die Frage der Zugriffsberechtigungen auf Bundessysteme genauer zu prüfen. Ausserdem wurde empfohlen, interne Schulungen regelmässig zu wiederholen und brush ups» anzubieten.

Die Schengen-Koordinationsgruppe der schweizerischen Datenschutzbeauftragten hat auch 2015 keine koordinierte Kontrolle durchgeführt.

Wiederum keine koordinierte Kontrolle Die Schengen-Koordinationsgruppe der schweizerischen Datenschutzbeauftragten hat auch im Jahr 2015 keine koordinierte Kontrolle durchgeführt[7].

Kontrolltätigkeit im Bereich des Staatsschutzes

Koordination Das Staatsschutzkontrollorgan und der Datenschutzbeauftragte trafen sich wie üblich zu einer koordinierenden Sitzung. Dabei wurden Fragen zu Berührungspunkten zwischen der Fachgruppe 9 und anderen öffentlichen Organen des Kantons Basel-Stadt behandelt. Der Datenschutzbeauftragte wird im Rahmen seiner Datenschutz-Prüfungen auch Schnittstellen zur Fachgruppe 9 unter die Lupe nehmen.

1 Vgl. zur allgemeinen Prüfung der Passwortqualität auch bereits TB 2014, 29.
2 Information Security Management System.
3 Informationssicherheits- und Datenschutzkonzept.
4 § 16 IDG; vgl. dazu PK-IDG/BS-Rudin, § 16 N 13 ff.
5 Allgemein zu den AKV der Dateneignerin vgl. vorne TB 2015, 13 ff.
6 § 1b Abs. 2 IDV, eingefügt durch RRB vom 11. Februar 2014 (wirksam seit 16. Februar 2014). Ziff. II. des RRB enthält folgende Übergangsbestimmung: «Im Zeitpunkt des Wirksamwerdens dieser Änderung bestehende Datenpools (§ 1a) sind innerhalb von zwei Jahren an die Vorgabe dieses Rechtserlasses anzupassen.»
7 Siehe für die vergangenen Jahre ebenfalls TB 2011, 14, TB 2012, 26, TB 2013, 28, und TB 2014, 29.

Besondere Berichtspunkte

Pilotversuche, Informationszugangsgesuche und Geschäftslast

Der Datenschutzbeauftragte hat den Auftrag, zu bestimmten Punkten jährlich zu berichten – sei es aus dem Verordnungsrecht, sei es durch einen Auftrag des Grossen Rates. Diese besonderen Berichtspunkte sollen hier zusammengefasst werden.

Pilotversuche mit besonderen Personendaten

IDG-Ergänzung Ende 2013 wurde das Informations- und Datenschutzgesetz um den § 9a (Bearbeiten von besonderen Personendaten im Rahmen von Pilotversuchen) ergänzt[1]. Mit § 9a IDG soll ermöglicht werden, dass unter engen Voraussetzungen und zeitlich befristet im Rahmen von Pilotversuchen besondere Personendaten bearbeitet werden dürfen, ohne dass die nach § 9 Abs. 2 IDG erforderliche formellgesetzliche Grundlage besteht. Ohne eine solche Regelung müsste der Gesetzgeber bemüht werden, eine Regelung in einem Gesetz im formellen Sinn zu schaffen, von der man gerade noch nicht weiss, wie sie aussehen soll. Damit würde die Gefahr gross, dass eine äusserst vage Formulierung gewählt würde: Es würde dann genau die Steuerungskraft, welche die Regelung – gerade auch in datenschutzrechtlicher Sicht – entwickeln soll, verloren gehen.

Voraussetzungen Pilotversuche können nach § 9a IDG nun für die Dauer von maximal fünf Jahren[2] statt auf einer formellgesetzlichen Grundlage auf Basis einer regierungsrätlichen Verordnung durchgeführt werden. Die Voraussetzungen werden im IDG umschrieben. Der neue Paragraf darf nicht dazu dienen, etwas einzuführen, von dem man schon weiss, wie es aussehen soll, wofür man aber die gesetzliche Grundlage zu schaffen verschlafen hat. Vorausgesetzt wird:

— dass die *Aufgaben*, die diese Bearbeitung erforderlich machen, *in einem Gesetz* geregelt sind (also beispielsweise bei einem Pilotversuch mit einem elektronischen Patientendossier: die Pflicht, die Gesundheitsversorgung sicherzustellen),

— dass ausreichende *Massnahmen zur Verhinderung von Persönlichkeitsverletzungen* getroffen werden (insbesondere in Bezug auf organisatorische und technische Massnahmen, z.B. im Bereich der Informationssicherheit) und

— dass die praktische Umsetzung einer Datenbearbeitung *zwingend* eine *Testphase* vor dem Wirksamwerden des Gesetzes erfordert[3].

— Ausserdem muss vorher im Rahmen einer *Vorabkontrolle* die Beurteilung der oder des Datenschutzbeauftragten eingeholt werden[4].

Testphase zwingend erforderlich Die praktische Umsetzung einer Datenbearbeitung kann eine Testphase dann zwingend erfordern, wenn:

— die Erfüllung einer Aufgabe technische Neuerungen erfordert, deren Auswirkungen zunächst evaluiert werden müssen,

— die Erfüllung einer Aufgabe bedeutende organisatorische oder technische Massnahmen erfordert, deren Wirksamkeit zunächst geprüft werden muss, insbesondere bei der Zusammenarbeit mit öffentlichen Organen des Bundes und anderer Kantone und Privaten, oder

— sie die Übermittlung von besonderen Personendaten an Dritte mittels eines Abrufverfahrens erfordert.

Regelung durch Verordnung Nach § 9a IDG kann der Regierungsrat unter den erwähnten Voraussetzungen das Bearbeiten von besonderen Personendaten im Rahmen eines Pilotversuchs bewilligen. Dabei muss er die Modalitäten der Datenbearbeitung in einer Verordnung regeln[5]. Die Verordnungsregelung muss zweierlei enthalten:

— einerseits alle Regeln, die das Gesetz, welches die Verordnung zeitlich befristet ersetzen darf, zu enthalten hätte, und

— andererseits auch die Bestimmungen, die zur Konkretisierung der Gesetzesbestimmung auf Verordnungsstufe zu erlassen wären und die logischerweise auch noch nicht bestehen[6]. >

Evaluation Zweck der Durchführung von Pilotversuchen ist es, fehlende Erkenntnisse zu gewinnen. Mit den gewonnenen Informationen soll dann entscheiden werden, ob überhaupt und wenn ja, *wie* die «richtige» formellgesetzliche Grundlage geschaffen werden soll. Der JSSK war es ausserordentlich wichtig, dass alle Pilotversuche korrekt im Hinblick auf den Zweck, zu dem sie durchgeführt werden, ausgewertet werden. Sie hat deshalb in den § 9a IDG zusätzlich den Abs. 4 eingefügt: Jedes Pilotprojekt ist zu evaluieren. Das setzt voraus, dass bereits bei der Planung des Pilotversuches diese Evaluation mitgeplant wird. Es ist nachvollziehbar, dass nicht jeder auszuwertende Aspekt bereits zum vornherein genauestens festgelegt werden kann – auch im Laufe des Pilotversuches können neue für die definitive Fortführung entscheidende Aspekte auftauchen oder Aspekte, deren Auswertung geplant ist, an Wesentlichkeit verlieren. Änderungen müssen deshalb möglich sein. Trotzdem muss bereits im Zeitpunkt der Beurteilung durch den Datenschutzbeauftragten ein Evaluationskonzept vorliegen.Schliesslich liegt der Zweck eines Pilotversuchs genau darin: dass die Grundlagen für den Entscheid über die Weiterführung der Datenbearbeitung gewonnen werden.

Der Zweck eines Pilotversuchs liegt darin, die Grundlagen für den Entscheid über die Weiterführung einer Datenbearbeitung zu gewinnen.

Überprüfung durch den Datenschutzbeauftragten Die JSSK hat bei der Behandlung der IDG-Ergänzung grossen Wert darauf gelegt, dass die Umsetzung des § 9a IDG eng begleitet wird. Insbesondere soll – neben der vorgängigen Beurteilung im Rahmen einer Vorabkontrolle – auch nachträglich kontrolliert werden: Der Datenschutzbeauftragte soll überprüfen, ob Pilotversuche nach Ablauf der fünfjährigen Versuchsphase, falls die notwendige formellgesetzliche Grundlage nicht geschaffen wurde, auch tatsächlich definitiv eingestellt worden sind[7].

Laufende Pilotversuche Genau genommen lief im Jahr 2015 kein solcher Pilotversuch.

Vorbereitungen für Pilotversuche Im Laufe des Berichtsjahres wurde aber ein Pilotversuch so vorbereitet, dass er am 1. Januar 2016 beginnen konnte («erweiterte Gefährderansprache»); bei einem zweiten wurden die Vorbereitungen fortgesetzt (eHealth-Modellversuch «eHealth am Rhy»).

Der Regierungsrat hat 2015 die Verordnung für den Pilotversuch «Erweitere Gefährderansprache» erlassen, so dass der Pilotversuch am 1. Januar 2016 beginnen kann.

Pilotversuch «Erweiterte Gefährderansprache» Auf Antrag des Justiz- und Sicherheitsdepartements hat der Regierungsrat am 25. August 2015 die Verordnung über die Meldung von gefährdenden Personen im Rahmen eines Pilotversuchs («erweiterte Gefährderansprache») (PVV-Erweitere Gefährderansprache) erlassen; sie wurde per 1. Januar 2016 wirksam. Der Pilotversuch soll aufzeigen, ob durch die Meldung von gefährdenden Personen gemäss § 37a PolG, die aber nicht weggewiesen und mit einem Rückkehrverbot belegt werden, bei der zuständigen Beratungsstelle dazu führt, dass mehr gefährdende Personen von der Beratungsstelle angesprochen werden können. Zudem soll untersucht werden, ob die gefährdenden Personen nach der Erstansprache auf freiwilliger Basis an geeigneten Massnahmen zur Vermeidung von physischer Gewalt teilnehmen. Weitere Ziele sind die Evaluation der Tauglichkeit der Voraussetzungen zur Meldung von Personen gemäss § 2 der Verordnung und die Überprüfung der Tauglichkeit und Notwendigkeit der übermittelten Informationen an die zuständige Beratungsstelle[8].

Beurteilung Der Datenschutzbeauftragte wurde von den Verantwortlichen des Justiz- und Sicherheitsdepartements für die Erarbeitung der Verordnung, für das begleitende Datenschutzkonzept und für die Ausarbeitung des Evaluationskonzepts aktiv einbezogen. Die Vorgaben des IDG wurden eingehalten. Der Datenschutzbeauftragte wird im Jahr 2016 auch die Evaluation begleiten. Der Pilotversuch ist auf ein Jahr befristet[9]. Von der gesetzlichen Regelung her könnte er auch noch verlängert werden; andernfalls müsste die erweitere Gefährderansprache – selbst wenn die Evaluation sie als erfolgreich zeigt – unterbrochen werden, bis die für den «Normalbetrieb» notwendige formellgesetzliche Grundlage geschaffen ist.

eHealth-Modellversuche 2015 hat der Bundesgesetzgeber das ePatientendossier-Gesetz (EPDG) verabschiedet. Die Referendumsfrist lief ungenutzt ab. Es wird damit gerechnet, dass das Gesetz samt den Ausführungsregelungen 2017 in Kraft gesetzt wird. Zwischen März und Juni 2016 findet die Anhörung zum Ausführungsrecht statt. Im Hinblick auf die Umsetzung des Bundesrechts sind kantonale eHealth-Modellversuche wichtig: Mit ihnen soll getestet werden, wie das elektronische Patientendossier funktionieren kann. Allerdings sind die Rechtsgrundlagen des Bundes noch nicht in Kraft. Das heisst, dass für kantonale Pilotversuche kantonale Rechtsgrundlagen geschaffen werden müssen und ausschliesslich der Kanton die Verantwortung für die Durchführung übernehmen muss.

Pilotversuch «eHealth am Rhy» Seit längerem wird an den Grundlagen für einen solchen Pilotversuch gearbeitet[10]. Im letzten Jahr ging es damit auch zügig vorwärts. In mehreren intensiven Besprechungen mit dem eHealth-Verantwortlichen und dem Rechtsdienst des Gesundheitsdepartements konnte der Datenschutzbeauftragte Stellung zum Entwurf der Pilotversuchsverordnung nehmen. Mit der Verordnung muss ja einerseits die noch nicht existierende (Bundes-)Gesetzesgrundlage ersetzt werden – gleichzeitig muss allerdings auch das Ausführungsrecht auf Verordnungsstufe «simuliert» werden: So sollen die vom Koordinationsgremium eHealth Suisse ausgearbeiteten Standards für verbindlich erklärt werden. Kurz: kein triviales Projekt. Der Regierungsrat sollte die Pilotversuchsverordnung im Frühling 2016 verabschieden können.

Informationszugangsgesuche nach dem Öffentlichkeitsprinzip

Berichtspflicht Nach § 31 Abs. 2 IDV stellt die Staatskanzlei die Statistik über die bei der kantonalen Verwaltung schriftlich eingereichten Informationszugangsgesuche nach dem Öffentlichkeitsprinzip der oder dem Datenschutzbeauftragten zur Berichterstattung nach § 50 IDG zu. Daraus kann abgeleitet werden, dass im Tätigkeitsbericht über die Umsetzung des Öffentlichkeitsprinzips zu berichten ist.

Statistik Die Zahlen finden sich – über die gesamte kantonalen Verwaltung zusammengefasst – im Statistikteil dieses Tätigkeitsberichts (Seite 40). Aufgeschlüsselt nach Departementen veröffentlicht der Regierungsrat sie in seinem Verwaltungsbericht[11].

Erfasste Gesuche Wichtig für die Interpretation der Daten ist zu wissen,

— dass nur die Gesuche bei der *kantonalen Verwaltung* erfasst sind – nicht diejenigen der autonomen Anstalten des öffentlichen Rechts und der Gemeinden, und

— dass nur *schriftlich* eingereichte Gesuche erfasst werden, nicht aber mündliche Gesuche.

Auf tiefem Niveau stabil Die Zahl der schriftlich bei der kantonalen Verwaltung eingereichten Gesuche (19; 2014: 18) ist gegenüber dem Vorjahr stabil – auf tiefem Niveau: Gegenüber dem ersten Jahr, in welchem das Öffentlichkeitsprinzip galt, beträgt der Rückgang über 60%. Die geringe Anzahl ist schwierig zu interpretieren. Es war auch in anderen Kantonen festzustellen, dass nach einer ersten «Welle» von Gesuchen die Zahlen zurückgingen. Es kann aber aufgrund der dünnen Faktenlage weiterhin nicht gesagt werden,

— ob nach ersten Gerichtsfällen die Grenzen des Öffentlichkeitsprinzips klarer geworden sind,

— ob die öffentlichen Organ pro-aktiv mehr Informationen von sich aus zur Verfügung stehen, so dass weniger Gesuche um Informationszugang nötig sind,

— ob vermehrt Gesuche nicht mehr schriftlich gestellt werden müssen, weil die öffentlichen Organe auch auf mündliche Nachfragen rasch reagieren, oder

— ob generell das Interesse an behördlichen Informationen zurückging.

Für den eHealth-Modellversuch müssen kantonale Rechtsgrundlagen geschaffen werden, und der Kanton muss die Verantwortung für die Durchführung übernehmen.

Erledigung Im Berichtsjahr wurden 45% der Gesuche ganz oder teilweise gutgeheissen (2014: 39%). 35% der Gesuche (2014: 50%) wurden ganz abgewiesen. Über 20% der Gesuche (2014: 11%) waren Ende des Berichtsjahres noch nicht rechtskräftig entschieden. Die Abweisungsquote von über einem Drittel (im ersten Jahr, in welchem das Öffentlichkeitsprinzip galt, wurde nur jedes achte Gesuch ganz abgewiesen) ist ohne weitere Abklärungen schwierig zu interpretieren: >

— Ist die Bereitschaft der öffentlichen Organe, sich in die Karten blicken zu lassen, gering?

— Waren die Gesuche «schlecht», indem sie Zugang etwa zu Informationen verlangen, die klarerweise unter die Einschränkungen von § 29 IDG – z.B. gesetzliche Geheimhaltungsbestimmungen – fallen?

— Handelt es sich um eine natürliche Schwankung?

Der Datenschutzbeauftragte behält die weitere Entwicklung im Auge und fördert die wirksame Umsetzung des Öffentlichkeitsprinzips.

Entwicklung weiterhin beobachten Der Datenschutzbeauftragte behält die weitere Entwicklung im Auge und fördert die wirksame Umsetzung des Öffentlichkeitsprinzips. Er hat im Berichtsjahr unter anderem an einer Schulung des Vereins «oeffentlichkeitsgesetz.ch» für Medienschaffende mitgewirkt und dabei auf die Möglichkeiten und Grenzen des Zugangs zu Informationen nach dem baselstädtischen Informations- und Datenschutzgesetz hingewiesen. Ausserdem unterstützt er weiterhin die Anpassungsbemühungen bezüglich § 30 IDG[12]. Die vergleichsweise strenge Regelung soll derjenigen des Bundes angenähert werden: Dort dürfen ausnahmsweise Personendaten in nicht anonymisierter Form zugänglich gemacht werden, wenn daran ein überwiegendes öffentliches Interesse besteht[13].

Statistik zu den Geschäften des Datenschutzbeauftragten

Statistik Die Statistik zu den Geschäften des Datenschutzbeauftragten im Jahr 2015 (mit Vorjahresvergleich) findet sich auf den Seiten 40 f.

Recht stabile Geschäftszahl Im Berichtsjahr sind 411 Geschäfte neu eröffnet worden (2014: 400); die Zahl ist geringfügig höher als im Vorjahr (11 Geschäfte, 3%).

Komplexere Fälle Der Anteil komplexer (und damit ressourcenintensiver) Geschäfte an allen Beratungen hat sich bei rund einem Achtel eingependelt (13%; 2014: 15%; 2013: 11%). Gegenüber dem Vorjahr entspricht dies einer Abnahme um 2 Prozentpunkte. Darunter fallen insbesondere grössere Vorabkontrollen.

Rasche Erledigung Von den nicht-komplexen Beratungsgeschäften konnten 61% (2014: 58%) innert 14 Tagen seit Eingang abgeschlossen werden.

Audits Die Zahl der im Berichtsjahr abgeschlossenen Audits beträgt auf 4 (2014: 5). Weitere Details dazu finden sich auf den Seiten 32 ff.

Schulungen Im Berichtsjahr wurden 7 Schulungen für öffentliche Organe durchgeführt (2014: 6). Hinzu kommen noch fast doppelt so viele Referate und Weiterbildungsbeiträge, die dem gleichen Zweck dienen.

Initianten Die Stellen bzw. Personen, welche die Geschäfte veranlasst haben, verteilen sich im Berichtsjahr nur geringfügig anders als in den Vorjahren. Fast zwei Drittel aller Geschäfte wurden durch eine Anfrage kantonaler öffentlicher Organe initiiert. Details dazu finden sich auf Seite 41.

Involvierte Stellen Bei den in die Geschäfte involvierten Stellen sind die Zahlen stabil. Es gab einzig eine Verschiebung vom Justiz- und Sicherheitsdepartement (-5 Prozentpunkte; 2014: +8) hin zum Departement für Wirtschaft, Soziales und Umwelt (+4 Prozentpunkte). Auch diese Schwankung bewegt sich aber im Rahmen der üblichen jährlichen Verschiebungen.

1 Ratschlag 13.0739.01; Bericht 13.0739.02; Beschluss Nr. 13/46/10G des Grossen Rates vom 13. November 2013.
2 § 9a Abs. 3 IDG.
3 § 9a Abs. 1 lit. a-c IDG. Vgl. dazu generell auch PK-IDG/BS-Husi, § 9a N 1 ff., insb. N 6 ff.
4 § 9a Abs. 1 IDG (Einleitungssatz): zur Vorabkontrolle: § 13 IDG, §§ 2-4 IDV; PK-IDG-Rudin, § 13 N 1 ff.
5 § 9a Abs. 5 IDG.
6 PK-IDG/BS-Husi, § 9a N 23.
7 Bericht 13.0739.02, 5 f.
8 § 2 PVV-Erweiterte Gefährderansprache.
9 § 8 PVV-Erweiterte Gefährderansprache.
10 Vgl. z.B. TB 2014, 33, sowie das Geschäft 13.0737 des Grossen Rates (Ausgabenbericht betreffend eine Investition als einmalige Einkaufssumme im Rahmen einer Private-Public-Partnership (PPP) und Betriebsbeiträge für den eHealth-Modellversuch Basel-Stadt).
11 Jahresbericht 2015 (des Regierungsrates), Öffentlichkeitsprinzip, S. 159
12 Vgl. TB 2014, 34, und PK-IDG/BS-Rudin, § 30 N 21 ff.
13 Art. 9 BGÖ i.V.m. Art. 19 Abs. 1bis DSG.

Aus dem Alltag

Statistische Auswertungen 2015 (mit Vorjahresvergleichen)

A Geschäfte

	2015		2014		2013		2012	
	Anzahl	%	Anzahl	%	Anzahl	%	Anzahl	%
Anzahl eröffnete Geschäfte	411		400		403		366	
prozentuale Veränderung gegenüber Vorjahr		3		-1		10		7

B Indikatoren gemäss Budget

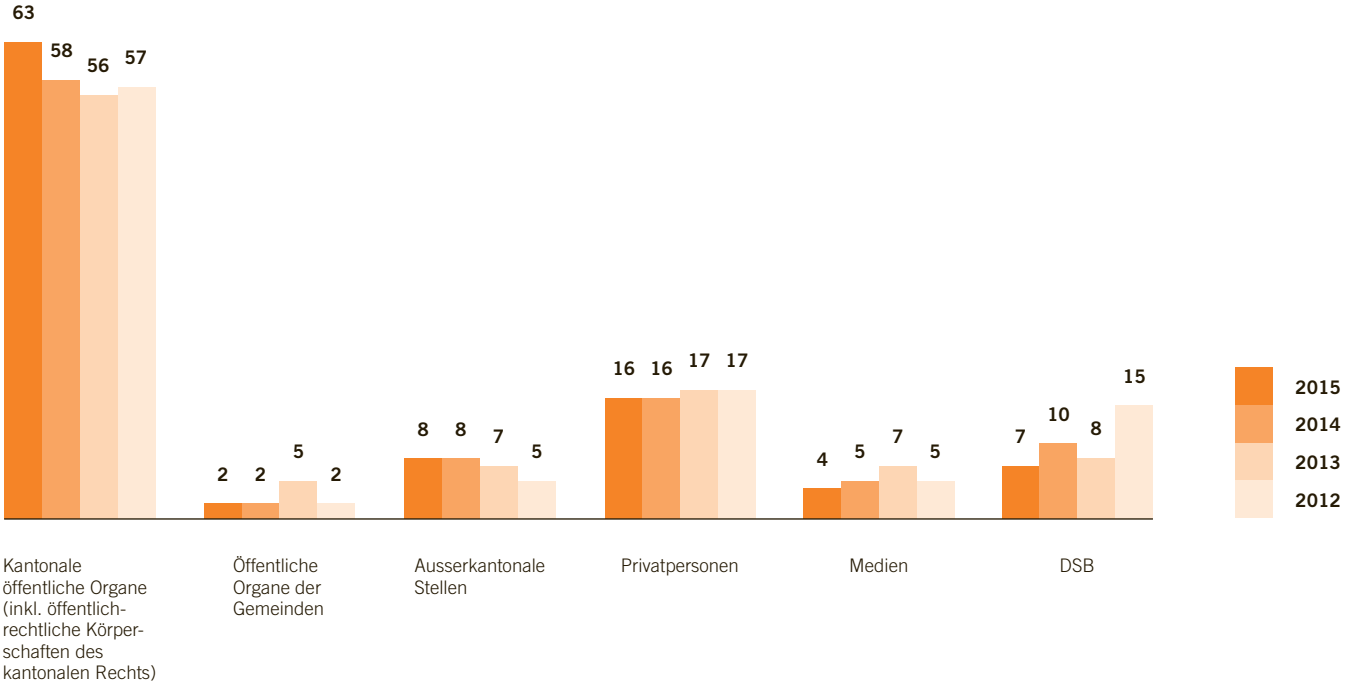
	2015		2014		2013		2012	
	Anzahl	%	Anzahl	%	Anzahl	%	Anzahl	%
Anteil komplexer Beratungen								
prozentualer Anteil an allen Beratungen		13		15		11		9
Innert 14 Tagen abgeschlossene nicht-komplexe Beratungen								
prozentualer Anteil an allen nicht-komplexen Beratungen		61		58		54		50
Durchgeführte Audits								
Anzahl durchgeführte Audits	4		5		4		2	
Durchgeführte Schulungen für öffentliche Organe								
Anzahl durchgeführte Schulungen	7		6		7		11	

C Öffentlichkeitsprinzip

	2015		2014		2013		2012	
	Anzahl	%	Anzahl	%	Anzahl	%	Anzahl	%
Eingereichte Gesuche nach § 25 IDG								
Anzahl eingereichte Gesuche	19		18		30		48	
prozentuale Veränderung gegenüber Vorjahr		6		-40		-38		100
Behandlung der Gesuche nach § 25 IDG								
Anzahl gutgeheissener Gesuche		35		28		37		60
Anzahl teilweise gutgeheissener Gesuche		10		11		17		17
Anzahl ganz abgewiesener Gesuche		35		50		37		13
Anzahl noch nicht rechtskräftig entschiedener Gesuche		20		11		10		10

Öffentlichkeitsprinzip ab 2012.
Zahlen erfasst durch die Staatskanzlei aufgrund der Meldungen der Departemente (§ 31 IDV).
Zahlen aufgeschlüsselt nach Departementen: Jahresbericht 2015 (des Regierungsrates), Öffentlichkeitsprinzip, S. 159.

D Initianten: Veranlasser der Geschäfte (A) in %



E In die Geschäfte (A) involvierte Stellen in %

Fälle

Fall 1 Aktenbeizug im Strafverfahren: Gilt das IDG – oder nicht?

Das Informations- und Datenschutzgesetz findet keine Anwendung «in hängigen Verfahren der Strafgerichtsbarkeit». Was gilt nun für öffentliche Organe (oder auch für Privatpersonen), die von der Staatsanwaltschaft im Rahmen eines hängigen Strafverfahrens, bei dem sie aber weder Partei noch andere Verfahrensbeteiligte im Sinne der Strafprozessordnung sind, aufgefordert werden, Unterlagen herauszugeben?

Die Staatsanwaltschaft führt eine strafrechtliche Untersuchung durch. Der beschuldigten Person wird beispielsweise Sozialversicherungsbetrug vorgeworfen. In diesem Zusammenhang fordert die Staatsanwaltschaft ein öffentliches Organ und ein privates Unternehmen auf, bestimmte Unterlagen einzureichen. Beim öffentlichen Organ werden etwa Akten aus dem Sozialversicherungsverfahren eingeholt, in welchem die beschuldigte Person Sozialversicherungsleistungen beansprucht hat. Beim privaten Unternehmen geht es um Sachverhalte, die möglicherweise im Widerspruch stehen zu den Angaben, welche die beschuldigte Person gegenüber dem öffentlichen Organ gemacht hat.

Das Informations- und Datenschutzgesetz findet keine Anwendung in hängigen Verfahren der Strafgerichtsbarkeit[1]. Für das Datenbearbeiten der Staatsanwaltschaft gilt deshalb in einem hängigen Strafverfahren nicht das IDG, sondern die Strafprozessordnung. Wie steht es aber mit der Herausgabe der Unterlagen durch das öffentliche Organ und das Privatunternehmen?

Das öffentliche Organ und das Privatunternehmen sind nicht «im hängigen Strafverfahren». Sie sind – in den hier behandelten Fällen – weder Parteien noch andere Verfahrensbeteiligte. Für die Frage, ob sie nun nach der Aufforderung durch die Staatsanwaltschaft Personendaten bekannt geben dürfen oder müssen, gilt das Datenschutzrecht, das allgemein für ihr Datenbearbeiten gilt: also das Bundesdatenschutzgesetz[2] für das Datenbearbeiten des privaten Unternehmens bzw. das IDG für dasjenige des öffentlichen Organs.

Erschwert das die Strafuntersuchung? Nein. Das (Informations- und) Datenschutzgesetz enthält ja als sog. «formelles Datenschutzrecht»[3] nur die *Grundsätze für das Datenbearbeiten:*

— Das Datenbearbeiten durch das private Unternehmen verletzt die Persönlichkeit der betroffenen Person, also hier der beschuldigten Person, und ist damit – weil die Persönlichkeit ein absolutes Rechtsgut darstellt – a priori widerrechtlich[4]. Die Widerrechtlichkeit kann aber durch einen Rechtfertigungsgrund beseitigt werden – nämlich durch die Einwilligung der betroffenen Person, durch ein überwiegendes öffentliches oder privates Interesse oder durch Gesetz[5].

— Ein öffentliches Organ darf (u.a.) Personendaten bekannt geben, wenn eine gesetzliche Bestimmung zur Bekanntgabe verpflichtet oder ermächtigt[6].

In beiden Fällen kann also ein *Gesetz* die Datenbekanntgabe rechtfertigen. Im vorliegenden Kontext ist für beide dieses die Datenbekanntgabe rechtfertigende Gesetz – im Sinne des sog. «materiellen Datenschutzrechts», das *bereichsspezifisch* die *konkreten Datenbearbeitungsregeln* enthält[7] – die Strafprozessordnung. Sie regelt den Beizug von Akten[8] und die Beschlagnahme von Gegenständen, die als Beweismittel gebraucht werden[9]. Damit sind öffentliche Organe berechtigt bzw. verpflichtet, Personendaten bekannt zu geben, bzw. wird die Widerrechtlichkeit des Datenbearbeitens von Privatpersonen beseitigt.

Ergebnis

Für das Bearbeiten von Personendaten gilt für öffentliche Organe des Kantons Basel-Stadt das Informations- und Datenschutzgesetz, für Privatpersonen das Bundesdatenschutzgesetz (sog. «formelles Datenschutzrecht»). Das gilt auch dann, wenn sie von der Staatsanwaltschaft aufgefordert werden, Unterlagen herauszugeben, welche die Staatsanwaltschaft im Rahmen eines Strafverfahrens benötigt. Die Strafprozessordnung ermächtigt oder verpflichtet sie hingegen als sog. «materielles Datenschutzrecht» zur Datenbekanntgabe.

1 § 2 Abs. 2 lit. b IDG; vgl. dazu PK-IDG/BS-Rudin, § 2 N 18 ff.
2 Art. 2 Abs. 1 DSG/Bund.
3 Vgl. zur Unterscheidung zwischen dem sog. «formellen Datenschutzrecht» und dem sog. «materiellen Datenschutzrecht» PK-IDG/BS-Rudin, Grundlagen N 43 ff.; Beat Rudin/Sandra Husi, Art. 37 DSG N 1 ff., in: Urs Maurer-Lambrou/Gabor-Paul Blechta (Hrsg.), Basler Kommentar Datenschutzgesetz Öffentlichkeitsgesetz, Basel 2014.
4 Art. 12 Abs. 1 DSG/Bund.
5 Art. 13 Abs. 1 DSG/Bund.
6 § 21 Abs. 1 lit. a IDG; vgl. dazu PK-IDG/BS-Rudin, § 21 N 3 ff.
7 Im Sinne des sog. «materiellen Datenschutzrechts»; vgl. dazu Fn. 3.
8 Art. 194 StPO.
9 Art. 263 ff. StPO.

Fall 2 Zugang zu Nichtanhandnahme-verfügungen der Staatsanwaltschaft

Im Zusammenhang mit der «Honoraraffäre» hat die Staatsanwaltschaft das entsprechende Gebaren aller Mitglieder des Regierungsrates untersucht. In sechs Fällen hat sie Nichtanhandnahmeverfügungen erlassen. Ein Journalist verlangt nun gestützt auf das Öffentlichkeitsprinzip Zugang zu diesen sechs Verfügungen. Darf die Staatsanwaltschaft sie herausgeben, obwohl die nach IDG zwingend verlangte Anonymisierung nicht möglich ist?

Das Informations- und Datenschutzgesetz findet (u.a.) keine Anwendung in hängigen Verfahren der Strafrechtspflege[1]. Mit einer *Nichtanhandnahmeverfügung*[2] oder mit einer *Einstellungsverfügung*[3] entscheidet die Staatsanwaltschaft, gar keine Untersuchung zu eröffnen bzw. ein eröffnetes Verfahren zu beenden, ohne den Fall vor Gericht zu bringen. Mit der formell rechtskräftigen Erledigung eines Strafverfahrens durch Urteil oder einen anderen verfahrenserledigenden Entscheid (wie eben Einstellungsverfügung oder Nichtanhandnahmeverfügung) endet die Rechtshängigkeit und das IDG kommt wieder – wie vor Beginn der Rechtshängigkeit – zur Anwendung.

Nach dem IDG kann jede Person voraussetzungslos Zugang zu den bei einem öffentlichen Organ vorhandenen Informationen verlangen[4]. Dieser Zugang zu Informationen wird jedoch nicht einschränkungslos gewährt: Ein öffentliches Organ hat 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[5]. Auf jeden Fall aber sind Personendaten zwingend zu anonymisieren[6]. Falls eine Anonymisierung nicht möglich ist, weil z.B. bekannt ist, um welche Person es sich handelt[7] oder handeln muss[8], dann richtet sich der Zugang nach den Bestimmungen für die Bekanntgabe von Personendaten. Ohne gesetzliche Bekanntgabeermächtigung oder -verpflichtung[9] bzw. ohne Einwilligung der betroffenen Person[10] ist somit eine Bekanntgabe unzulässig. Damit müsste also das Gesuch des Journalisten abgewiesen werden.

«Müsste», denn die Anonymisierungspflicht des IDG wird «übersteuert» durch das Prinzip der Justizöffentlichkeit aus der Bundesverfassung: «Gerichtsverhandlung und Urteilsverkündung sind öffentlich. Das Gesetz kann Ausnahmen vorsehen»[11]. Mittlerweile ist von der Lehre[12] und Rechtsprechung[13] anerkannt, dass sich der Grundsatz der Justizöffentlichkeit nicht nur auf die eigentlichen Gerichtsverfahren und die damit verbundenen Urteile (inkl. Strafbefehle) bezieht, sondern auf sämtliche Sach- und Prozessentscheide[14] der Staatsanwaltschaft bezieht, mit denen ein Strafverfahren mit Bezug auf die betreffende Instanz abgeschlossen wird. In den Anwendungsfällen von Art. 30 Abs. 3 BV bleibt deshalb kein Raum für eine kantonalrechtliche Einschränkung. Das bedeutet, dass die absolute Anonymisierungspflicht nach IDG bei einem Zugangsgesuch, das sich auf Strafurteile, Strafbefehle, Einstellungs- oder Nichtanhandnahmeverfügungen in Strafsachen bezieht, nicht zur Anwendung kommt. Die Staatsanwaltschaft kann also zu den Nichtanhandnahmeverfügungen Zugang gewähren.

Ergebnis

Bei Zugangsgesuchen, die sich auf Strafurteile, Strafbefehle, Einstellungs- oder Nichtanhandnahmeverfügungen in Strafsachen beziehen, kommt die absolute Anonymisierungspflicht nach IDG nicht zum Zug. Bei solchen Gesuchen ist aber zu prüfen, ob Einschränkungen zum Schutz überwiegender privater oder öffentlicher Interessen vorgenommen werden müssen. Bei öffentlichen Interessen darf das nicht vorschnell angenommen werden, damit das Ziel des Prinzips der Justizöffentlichkeit nicht vereitelt wird. Private Interessen beispielsweise von Drittpersonen können aber durchaus schützenswert sein und gegenüber dem Zugangsinteresse der Öffentlichkeit überwiegen; solchen Interessen ist etwa durch Abdeckungen oder Einschwärzungen Rechnung zu tragen.

1 § 2 Abs. 2 lit. b IDG; vgl. dazu PK-IDG/BS-Rudin, § 2 N 18 ff.
2 Art. 310 StPO; vgl. dazu BSK-StPO-Omlin, Art. 310 Rz. 1 ff., insb. N 9 ff.
3 Art. 319 ff. StPO; vgl. dazu BSK-StPO-Grädel/Heiniger, Art. 319 N 1 ff. (und die nachfolgenden Artikelkommentierungen).
4 § 25 IDG; vgl. dazu PK-IDG/BS-Rudin, § 25 N 7 ff.
5 § 29 Abs. 1 IDG; vgl. dazu PK-IDG/BS-Rudin, 29 N 1 ff., insb. N 11 ff.
6 § 30 Abs. 1 IDG; vgl. dazu PK-IDG/BS-Rudin, § 30 N 4 ff.
7 Weil z.B. die Gesuchstellerin Zugang zu einer Verfügung zu einer bestimmten Person oder in einem bestimmten Fall verlangt, sie also auch nach einer «Anonymisierung» genau weiss, wer die betroffene Person ist.
8 Wenn z.B. bei mehreren Verfügungen aufgrund von Kontextinformationen die Zuordnung zu bekannten Personen möglich ist (etwa bei parallelen Verfahren gegen sechs Mitglieder einer Exekutivbehörde) und diese Kontextinformationen nicht eingeschwärzt werden kann, weil sonst kein Informationsgehalt mehr vorhanden ist.
9 Im Sinne von §§ 20 ff. IDG.
10 § 21 Abs. 1 und 2 IDG, jeweils lit. c.
11 Art. 30 Abs. 3 BV.
12 Matthias Michlig, Öffentlichkeitskommunikation der Strafbehörden unter dem Aspekt der Amtsgeheimnisverletzung (Art. 320 StGB), Zürich 2013, § 1 lit. d; Jascha Schneider-Marfels, Einsichtnahme in behördliche Dokumente, Strafakten und Strafurteile, Medialex 2014, S. 121, 124 f.; SGK-BV³-Steinmann, Art. 30 N 64 f.; BSK-BV-Reich, Art. 30 N 52 (m.w.H.).
13 Vgl. dazu z.B. BGE 134 I 286 (Verein gegen Tierfabriken VgT, Nichtanhandnahme- und Einstellungsverfügungen), E 6.4; BGE 137 I 16 (Nef, Einstellungsverfügung), E 2.4.; BGer-Urteil 1B_68/2012 vom 03.07.2012 (FIFA, Einstellungsverfügung), E 4.3.
14 Das Prinzip der Justizöffentlichkeit gewährt aber keinen Zugang zu den Verfahrensakten – diese unterstehen dem Amtsgeheimnis nach StPO Art. 73 StPO. Vgl. dazu BSK-StPO-Saxer/Thurnheer, Art. 73 N 5 und Art. 60 N 36.

Fall 3 Endlich Rente – geht das das Betreibungsamt etwas an?

Grosses Staunen bei S, der bisher berufstätig war und dessen Lohn gepfändet war: Nachdem er aus medizinischen Gründen frühpensioniert wurde, erhält er vom Betreibungsamt ein Schreiben, worin dieses darauf hinweist, dass er neu eine Rente erhalte und dass die Pfändung dieser Rente direkt mit seiner Pensionskasse abgewickelt werde. Ist da alles korrekt gelaufen?

Das Betreibungsamt wickelt die Lohnpfändungen[1] direkt mit dem Arbeitgeber der Arbeitnehmerin bzw. des Arbeitnehmers ab. Der dafür erforderliche Informationsaustausch stützt sich auf Art. 93 Abs. 3 SchKG – eine unmittelbare gesetzliche Grundlage im Sinne des IDG[2].

Das Betreibungsamt könnte die Lohnpfändungen nicht durchführen, wenn es nicht über Angaben zu den Einkommensverhältnissen der fraglichen Person verfügte. Um sicher zu gehen, dass auch die richtigen bzw. vollständigen Daten angegeben werden, dürfen diese Daten direkt beim Arbeitgeber erhoben werden. Dabei soll nicht nur verhindert werden, dass die betroffene Person bewusst falsche Daten angibt und sich der Pfändung zu entziehen bzw. die Pfändungssituation zu erleichtern sucht. Der direkte Informationsaustausch zwischen Betreibungsamt und Arbeitgeber kann durchaus auch im Interesse der betroffenen Person sein, nämlich dann, wenn aufgrund von Anpassungen der Sozialabzüge oder der Lohnhöhe auch die Pfändungsquote zugunsten der betroffenen Person angepasst werden soll. Das Betreibungsamt Basel-Stadt ersucht daher die jeweiligen Arbeitgeber, pfändungsrelevante Veränderungen im Arbeitsverhältnis von sich aus zu melden.

Scheidet ein Mitarbeiter oder eine Mitarbeiterin aus dem Berufsleben aus und erhält, aus welchen Gründen auch immer, künftig eine Rente, so stellt dies eine wesentliche Veränderung in der Einkommenssituation der betroffenen Person dar. Für das Betreibungsamt bedeutet dies, dass künftig nicht mehr die vom Arbeitgeber ausgerichteten Gehaltszahlungen, sondern die von der Rentenanstalt geleisteten Zahlungen gepfändet werden müssen. Damit sich die Neu-Rentnerin bzw. der Neu-Rentner der Pfändung nicht entziehen kann, ist es daher erforderlich, dass der ehemalige Arbeitgeber das Betreibungsamt nicht nur über das Ende der Lohnzahlungen, sondern auch über den Umstand, dass und von wem neu eine Rente ausgerichtet wird, informiert. Dass das Betreibungsamt diese Informationen erhebt, ist für die Aufgabenerfüllung des Betreibungsamts geeignet und erforderlich und damit aus datenschutzrechtlicher Sicht zulässig. Nicht wissen muss das Betreibungsamt hingegen den Grund für die Rente – ob es sich dabei also um eine Frühpensionierung, eine gesundheitsbedingte Pensionierung oder um eine reguläre Pensionierung handelt, ist für die Aufgabenerfüllung, d.h. die Durchführung der Rentenpfändung, nicht relevant.

Ergebnis

Ein öffentliches Organ darf Personendaten bearbeiten, wenn diese zur Aufgabenerfüllung geeignet und erforderlich sind. Damit eine Lohnpfändung im Sinne von Art. 93 SchKG durchgeführt werden kann, muss das Betreibungsamt auch wissen, von wem das Gehalt ausbezahlt wird. Verändern sich diese Verhältnisse, so ist das Betreibungsamt darüber zu informieren. Nicht verhältnismässig, d.h. für die Aufgabenerfüllung nicht geeignet und erforderlich, ist es hingegen, das Betreibungsamt auch über die detaillierten Gründe für eine Veränderung (Grund für die Rente usw.) zu informieren.

1 Nach Art. 93 i.V.m. Art. 92 des Bundesgesetzes vom 11. April 1889 über Schuldbetreibung und Konkurs (SchKG), SR 281.1.

2 Im Sinne von § 9 Abs. 1 lit. a IDG (für das Erheben der Daten) bzw. im Sinne von § 21 Abs. 1 lit. a IDG (für das Bekanntgeben der Daten vom Betreibungsamt an den Arbeitgeber); vgl. dazu PK-IDG/BS-Rudin, § 9 N 25 ff., insb. N 27, und § 21 N 3 ff., insb. N 5.

Fall 4 Zu viel Information für die Expertin

Bezieht L, ein Bezüger von Sozialleistungen, diese Leistungen zu Recht? Um darüber Klarheit zu erhalten, veranlasst das zuständige öffentliche Organ eine Untersuchung durch eine Fachperson. Welche Informationen darf das öffentliche Organ der Fachperson zur Aufgabenerfüllung weitergeben? Ist es gerechtfertigt, sie darüber zu informieren, dass der Verdacht, dass Leistungen zu Unrecht bezogen werden, das Resultat aus einer Überwachung durch eine andere Behörde war?

Dass bestimmte Amtsstellen, die Sozialleistungen zusprechen, zum Zwecke notwendiger Abklärungen[1] Fachpersonen beiziehen können, welche ärztliche oder fachspezifische Untersuchungen vornehmen, steht ausser Zweifel. Notwendig ist auch, dass die entsprechenden Expertinnen und Experten Informationen erhalten. Fraglich ist allerdings, wie viele Informationen über L bzw. über den Anlass für den Untersuchungsauftrag ihnen vorgängig mitgeteilt werden müssen und wie detailliert diese Informationen sein dürfen.

Wie kommt das öffentliche Organ zum Verdacht, der es eine Untersuchung anordnen lässt? Vielleicht sind es Hinweise von Nachbarn. Vielleicht hat ein anderes öffentliches Organ (z.B. eine polizeiliche Behörde) zur Erfüllung seiner gesetzlichen Aufgabe L überwachen lassen und ist dabei beiläufig auf Anhaltspunkte für den Verdacht gestossen, L beziehe Sozialleistungen zu Unrecht, und hat dies dem für diese Sozialleistungen zuständigen Amt mitgeteilt. Darf das Amt die Quelle des Verdachts der mit der Untersuchung beauftragten Fachperson mitteilen? L hat nichts gegen die Untersuchung, stört sich aber an der Mitteilung der Verdachtsquelle (im konkreten Fall eine behördlich angeordnete Überwachung).

Die Bekanntgabe von Daten an die Auftragnehmerin oder den Auftragnehmer ist rechtmässig. Aber ist sie auch verhältnismässig? Es dürfen nur diejenigen Informationen weitergegeben werden, die für die Erfüllung der Aufgabe, also hier der Untersuchung durch die Expertin bzw. den Experten, geeignet und erforderlich sowie der betroffenen Person zumutbar sind. Die Weitergabe allgemeiner sowie persönlicher Informationen über L ist zweifellos *geeignet*, die Fachperson so zu informieren, damit diese ihre Aufgabe erfüllen kann. *Erforderlich* sind diejenigen Angaben, ohne welche die Fachperson ihre Aufgabe nicht fachgerecht erfüllen kann. Das trifft sicher zu für Angaben zur betreffenden Person wie Personalien, Angabe zu früheren Abklärungen, zu den heute zu beantwortenden Fragen – diese Angaben benötigt die Expertin oder der Experte, um den Fokus der Untersuchung richtig zu legen. Auch die Feststellungen, welche die Zweifel an der Rechtmässigkeit des Leistungsbezugs aufkommen lassen, gehören dazu. Aber die Tatsache, dass diese Feststellungen aus einer Überwachung (in völlig anderem Aufgabenzusammenhang) stammen, ist hier zur Zweckerreichung nicht erforderlich. Im Gegenteil: Sie kann unrichtige Vermutungen auslösen und die Persönlichkeitsrechte der betroffenen Person verletzen – erst recht, wenn beispielsweise die Überwachung sie von einem Verdacht gerade befreit hat!

Ergebnis

Die Weitergabe von Informationen zur Erfüllung einer bestimmten Aufgabe muss rechts- sowie verhältnismässig sein. Jedes öffentliche Organ, das eine Fachperson für eine Untersuchung beizieht, muss sicherstellen, dass diejenigen, aber auch *nur* diejenigen Informationen weitergegeben werden, welche die Fachperson benötigt, um die Untersuchung fachgerecht ausführen zu können. Dazu gehört der Grund für die Untersuchung, also die abzuklärenden Verdachtsmomente, aber in aller Regel nicht die Quelle des Verdachts.

1 Art. 43 ATSG.

Fall 5 Der nicht-anonymisierte Zahlungsauftrag

Das Strafgericht zieht in einem Strafverfahren gegen B wegen des Verdachts auf Sozialversicherungsbetrug Akten des zuständigen Amtes bei, unter anderem Kopien von Zahlungsaufträgen. Das Amt liefert die verlangten Kopien, auf denen aber nicht allein Angaben zu B, sondern auch zu den anderen Personen verzeichnet sind, die gleichzeitig eine Auszahlung erhalten haben. Ist das korrekt?

In einem Strafverfahren wegen des Verdachts auf Sozialversicherungsbetrug verlangt das Strafgericht von einem öffentlichen Organ Kopien der Abrechnungen der Auszahlungen von drei Monaten; ausserdem schreibt es: «Bitte Kopien der Zahlungsaufträge ebenfalls einreichen.» Das öffentliche Organ liefert neben den Abrechnungen u.a. auch Kopien der Begleitlisten zu den Datenträgern «DTA Überweisung (Bank)», auf denen auch weitere Auszahlungsempfänger verzeichnet sind. Das Strafgericht leitet sämtliche Unterlagen unverändert an den Staatsanwalt und den Verteidiger des Angeklagten weiter; dieser schickt sie dem Angeklagten.

Auf die Datenlieferung des öffentlichen Organs an das Strafgericht ist das Informations- und Datenschutzgesetz anwendbar[1]. Eine Bekanntgabe[2] von (im konkreten Fall besonderen) Personendaten ist (u.a.) zulässig, wenn ein Gesetz dazu ausdrücklich verpflichtet oder ermächtigt (sog. unmittelbare gesetzliche Grundlage)[3]. Die relevante *gesetzliche Grundlage* findet sich in der Strafprozessordnung[4]: Dem Recht des Gerichts, die Aushändigung der Akten zu verlangen, steht die gesetzliche Pflicht der Verwaltungsbehörde gegenüber, die verlangten Akten auszuhändigen, soweit keine überwiegenden öffentlichen oder privaten Geheimhaltungsinteressen entgegenstehen. Damit ist in der StPO die vom IDG verlangte (formell-)gesetzliche Grundlage für die Datenbekanntgabe durch das öffentliche Organ gegeben.

Eine Datenbekanntgabe muss auch *verhältnismässig* sein[5]. In casu benötigt das Strafgericht zur Erfüllung seiner gesetzlichen Aufgabe Angaben zu den Bezügen des Angeklagten. Irgendwelche Angaben zu andern Sozialleistungsbezügerinnen oder -bezügern sind nicht erforderlich. Deshalb ist die Bekanntgabe von mehr Personendaten als jenen über die Taggeldbezüge der beschuldigten Person *unverhältnismässig* und damit unzulässig. Soweit verlangte Dokumente nicht ausschliesslich Angaben zu dieser Person enthalten, sind die Angaben zu anderen Personen so zu *anonymisieren*, dass das empfangende Strafgericht und die beteiligten Parteien, denen das Gericht die Unterlagen zustellen muss, nicht mehr eruieren können, wer die anderen Personen sind[6]. Dies ist im vorliegenden Fall nicht geschehen. Das Amt ist davon ausgegangen, dass es die verlangten Zahlungsaufträge als mögliche Beweise nicht verändern dürfe.

Die Bekanntgabe von Informationen über den Sozialleistungsbezug der angeklagten Person ist rechtmässig und verhältnismässig, die Aushändigung von Angaben über andere Personen (bzw. die Nichtanonymisierung solcher Angaben) hingegen nicht und damit unzulässig. Das Amt hat die Empfehlung des Datenschutzbeauftragten, solche Informationen künftig nicht zu liefern oder zu anonymisieren, angenommen. Dem Strafgericht gegenüber kann der Datenschutzbeauftragte keine förmliche Empfehlung zum Datenbearbeiten in hängigen Strafverfahren aussprechen. Er hat es aber gebeten, künftig Informationen, die an die Staatsanwaltschaft und/oder Parteivertreter weitergegeben werden sollen und deren Weitergabe Persönlichkeitsrechte von Unbeteiligten verletzen könnte, entweder vor der Zustellung zu anonymisieren oder der Stelle, von der sie stammen, zur Anonymisierung zurückzugeben.

Ergebnis

Ein öffentliches Organ darf dem Strafgericht nur Angaben zu der Person bekannt geben, zu der das Strafgericht Angaben verlangt. Informationen zu anderen Personen sind vorgängig zu anonymisieren.

1 Vgl. dazu Fall 1: TB 2015, 44.
2 Zu den einzelnen Prüfschritten bei einer Datenbekanntgabe vgl. die «Checkliste Datenbekanntgabe» des Datenschutzbeauftragten des Kantons Basel-Stadt, abrufbar unter <http://www.dsb.bs.ch/dms/dsb/download/Checkliste_Bekanntgabe_v1.0_20150611.pdf>(Kurz-URL: <http://bit.ly/21lXvGx>).
3 § 21 Abs. 2 lit. a IDG; vgl. dazu PK-IDG/BS-Rudin, § 21 N 34 ff.
4 Art. 194 StPO.
5 § 9 Abs. 3 IDG; vgl. dazu PK-IDG/BS-Rudin, § 9 N 51 ff.
6 Vgl. dazu Merkblatt «Anonymisierung in Word- und PDF-Dokumenten» des Datenschutzbeauftragten des Kantons Basel-Stadt, abrufbar unter <http://www.dsb.bs.ch/dms/dsb/download/DSB-BS_Merkblatt_Anonymisierung_technisch-/DSB-BS_Merkblatt_Anonymisierung_%28technisch%29.pdf> (Kurz-URL: <http://bit.ly/21lXFxO>).

Fall 6 Einscannen statt archivieren?

Immer wieder wollen öffentliche Organe vom Datenschutzbeauftragten wissen, ob Dokumente eingescannt werden und die Originale danach vernichtet werden dürfen. Schliesslich entstehen durch ein Papierarchiv über Jahre erhebliche Kosten, während ein digitales Archiv heute kaum mehr viel kostet. Kosten entstehen aber vielleicht später ...

Dokumente einscannen ist günstiger, als sie in Papierform zu archivieren. Immer wieder wollen öffentliche Organe deshalb wissen, ob dem Einscannen aus datenschutzrechtlicher Sicht etwas entgegensteht. Der Datenschutzbeauftragte hat die Frage in der Regel verneint. Er hat aber auch auf drei Punkte hingewiesen:

— Die Informationssicherheit für die digitale Ablage muss gewährleistet sein: Die Daten müssen insbesondere gegen unberechtigten Zugriff und unbefugte Bearbeitung gesichert sein[1].

— In welcher Form Unterlagen dem Archiv abzuliefern sind[2], ist direkt mit dem zuständigen Archiv (für die kantonale Verwaltung: mit dem Staatsarchiv) zu klären.

— Die Frage, inwieweit der Echtheitsbeweis mit eingescannten Dokumenten erbracht werden kann, ist höchstgerichtlich noch nicht entschieden.

Mittlerweile ist die Frage vom Bundesgericht in einem Fall zur beruflichen Alters , Hinterlassenen und Invalidenvorsorge entschieden worden[3]: Auch wenn ein öffentliches Organ rechtlich befugt ist, seine Akten elektronisch aufzubewahren, ändert das nichts daran, dass es die Beweislast für die Echtheit der Unterschrift trägt und sich im Falle der Vernichtung der Originalunterschrift nach dem Einscannen dem Risiko aussetzt, dass ihm der Echtheitsbeweis misslingt. Wenn die Echtheit eine Urkunde bestritten wird, kann unter Umständen ein Schriftgutachten eingeholt werden. Allerdings kann ein solches Gutachten nur anhand des Originals erstellt werden. Ist das Original nicht mehr vorhanden, weil die Geschäftsunterlagen nur noch digitalisiert aufbewahrt werden, dann ist der Beweis nicht möglich. Falls das öffentliche Organ die Beweislast trifft, dann trägt es auch die Rechtsfolgen, wenn der Beweis eben nicht gelingt.

Auch eine Amtsstelle kann in die Lage kommen, die Echtheit eines Dokumentes beweisen zu müssen – etwa wenn sie geltend macht:

— sie hätte Geld aufgrund einer Vollmacht an eine andere als die berechtigte Person ausbezahlt,

— sie hätte aufgrund einer Vollmacht einer anderen als der betroffenen Person Zugang zu den eigenen Personendaten gewährt[4] oder

— sie hätte aufgrund einer Einwilligungserklärung (informed consent) Proben und genetische Daten einer Patientin für die Forschung weiterverwendet[5].

In solchen Fällen trägt die Amtsstelle das Risiko, den Beweis nicht mehr erbringen zu können, wenn die Echtheit des Dokuments oder der Unterschrift bestritten wird.

Ein Privatunternehmen kann das Risiko abwägen: Was kostet mehr – über Jahre ein Papierarchiv betreiben oder ab und zu etwas bezahlen müssen, weil ein Beweis nicht erbracht werden kann? Eine Amtsstellen darf das nicht: Sie darf nicht die (Grund-)Rechte von Bürgerinnen und Bürgern verletzen, weil es billiger ist, als sie nicht zu verletzen.

Ein öffentliches Organ wird wohl in Zukunft eine Triage vornehmen müssen: Urkunden, mit denen möglicherweise ein Beweis erbracht werden muss, müssen (auch) in Papierform aufbewahrt werden. Andere Dokumente können hingegen nach dem Einscannen vernichtet werden – immer unter dem Vorbehalt, dass die archivrechtliche Frage mit dem zuständigen Archiv geklärt ist.

Ergebnis

Wer eingescannte Urkunden digital archiviert, die Originale aber vernichtet, muss die Rechtsfolgen tragen, wenn ein Beweis nicht erbracht werden kann, weil ohne Original kein Echtheitsgutachten erstellt werden kann. Öffentliche Organe werden in Zukunft Dokumente nach dem Einscannen nur vernichten dürfen, wenn mit ihnen kein Beweis erbracht werden muss und die Frage der Ablieferungspflicht mit dem zuständigen Archiv geklärt ist.

1 § 8 IDG.
2 Vgl. § 16 IDG; dazu PK-IDG/BS-Rudin, § 16 N 2 ff.
3 Schweizerisches Bundesgericht, II. sozialrechtliche Abteilung, Urteil 9C_632/2014 vom 31. August 2015 (<http://www.bger.ch/index/juridiction/jurisdiction-inherit-template/jurisdiction-recht/jurisdiction-recht-urteile2000.htm>, via Suche nach ‹9C_632/2014›).
4 § 26 IDG i.V.m. § 31 Abs. 2 IDG.
5 Art. 32 HFG.

Anhang Verzeichnis der zitierten Gesetze, Materialien und Literatur

Rechtsgrundlagen des Kantons Basel-Stadt

HarmoS-Konkordat Interkantonale Vereinbarung vom 14. Juni 2007 über die Harmonisierung der obligatorischen Schule (HarmoS), SG 419.600.
IDG Gesetz vom 9. Juni 2010 über die Information und den Datenschutz (Informations- und Datenschutzgesetz, IDG), SG 153.260.
IDV Verordnung vom 5. August 2011 über die Information und den Datenschutz (Informations- und Datenschutzverordnung, IDV), SG 153.270.
Kantonalbankgesetz Gesetz vom 30. Juni 1994 über die Basler Kantonalbank, SG 915.200.
PolG Gesetz vom 13. November 1996 betreffend die Kantonspolizei des Kantons Basel-Stadt (Polizeigesetz, PolG), SG 510.100.
PVV-Erweiterte Gefährderansprache Verordnung vom 25. August 2015 über die Meldung von gefährdenden Personen im Rahmen eines Pilotversuchs («erweiterte Gefährderansprache»), SG 510.420.
Staatsbeitragsgesetz Staatsbeitragsgesetz vom 11. Dezember 2013, SG 610.500.

Bundesrecht

ATSG Bundesgesetz vom 6. Oktober 2000 über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG), SR 830.1.
BGÖ Bundesgesetz vom 17. Dezember 2004 über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz, BGÖ), SR 152.3.
BV Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999, SR 101.
DSG Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG), SR 235.1.
EPDG Bundesgesetz vom 19. Juni 2015 über das elektronische Patientendossier (EPDG) (noch nicht in Kraft, Referendumsvorlage: BBl 2015 4865).
HFG Bundesgesetz vom 30. September 2011 über die Forschung am Menschen (Humanforschungsgesetz, HFG), SR 810.30.
SchKG Bundesgesetz vom 11. April 1889 über Schuldbetreibung und Konkurs (SchKG), SR 281.1.
StGB Schweizerisches Strafgesetzbuch vom 21. Dezember 1937, SR 311.0.
StPO Schweizerische Strafprozessordnung vom 5. Oktober 2007 (Strafprozessordnung, StPO), SR 312.0.

Materialien

Bericht 13.0739.02 Bericht 13.0739.02 der Justiz-, Sicherheits- und Sportkommission vom 16. Oktober 2013 zum Ratschlag betreffend Änderung des Gesetzes über die Information und den Datenschutz (IDG) zwecks Schaffung einer gesetzlichen Grundlage für die Bearbeitung von besonderen Personendaten im Rahmen von Pilotversuchen.
Ergebnisbericht Bevölkerungsbefragung 2015 Statistisches Amt des Kantons Basel-Stadt (Hrsg.), Ergebnisbericht Bevölkerungsbefragung, Basel 2016, <http://www.statistik.bs.ch/dms/statistik/befragungen/Bericht-Bevoelkerung2015/Bev%C3%B6lkerung-2015.pdf> (Kurz-URL: <http://bit.ly/1MYyvx5>).
Grundauswertung Bevölkerungsbefragung 2015 Statistisches Amt des Kantons Basel-Stadt (Hrsg.), Grundauswertung Bevölkerungsbefragung, Basel 2016, <http://www.statistik.bs.ch/dms/statistik/befragungen/Grundauswertung-BevBef-2015/GA-BevBef-2015.pdf> (Kurz-URL: <http://bit.ly/1RQ2wDv>).
Ratschlag 13.0739.01 Ratschlag 13.0739.01 des Regierungsrates vom 21. Mai 2013 betreffend Änderung des Gesetzes über die Information und den Datenschutz (IDG) zwecks Schaffung einer gesetzlichen Grundlage für die Bearbeitung von besonderen Personendaten im Rahmen von Pilotversuchen.
TB 2014 Tätigkeitsbericht des Datenschutzbeauftragten des Kantons Basel-Stadt, 2014, abrufbar unter <http://www.dsb.bs.ch/dms/dsb/download/publikationen/taetigkeitsberichte/2014_taetigkeitsbericht.pdf>.
TB 2013 Tätigkeitsbericht des Datenschutzbeauftragten des Kantons Basel-Stadt, 2013, abrufbar unter <http://www.dsb.bs.ch/dms/dsb/download/publikationen/taetigkeitsberichte/2013_taetigkeitsbericht/2013_Taetigkeitsbericht.pdf>.
TB 2012 Tätigkeitsbericht des Datenschutzbeauftragten des Kantons Basel-Stadt, 2012, abrufbar unter <http://www.dsb.bs.ch/dms/dsb/download/publikationen/taetigkeitsberichte/2012_taetigkeitsbericht/2012_Taetigkeitsbericht.pdf>.
TB 2011 Tätigkeitsbericht des Datenschutzbeauftragten des Kantons Basel-Stadt, 2011, abrufbar unter <http://www.dsb.bs.ch/dms/dsb/download/publikationen/taetigkeitsberichte/2011_taetigkeitsbericht.pdf>.
TB 2010 Tätigkeitsbericht des Datenschutzbeauftragten des Kantons Basel-Stadt, 2010, abrufbar unter <http://www.dsb.bs.ch/dms/dsb/download/publikationen/taetigkeitsberichte/2010_taetigkeitsbericht/2010_Taetigkeitsbericht.pdf>.

Literatur

BSK-BV Bernhard Waldmann/Eva Maria Belser/Astrid Epiney (Hrsg.), Basler Kommentar Bundesverfassung, Basel 2015 (zitiert: BSK-BV-Autor(in)), Art. Xx N yy.
BSK-StPO Marcel Alexander Niggli/Marianne Heer/Hans Wiprächtiger (Hrsg.), Basler Kommentar Schweizerische Strafprozessordnung/Jugendstrafprozessordnung, 2. Aufl., Basel 2014 (zitiert: BSK-StPO-Autor(in)), Art. Xx N yy.
PK-IDG/BS Beat Rudin/Bruno Baeriswyl (Hrsg.), Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Basel-Stadt, Zürich/Basel/Genf 2014 (zitiert: PK-IDG/BS-Autor(in) § xx N yy).
SGK-BV^3 Bernhard Ehrenzeller et al. (Hrsg.), St. Galler Kommentar zur Schweizerischen Bundesverfassung, 3. Auflage, Zürich/St. Gallen 2014 (zitiert: SGK-BV^3-Autor[in], Art. xx N yy.).

Abkürzungen

FABER Automatisiertes Fahrberechtigungsregister
FHNW Fachhochschule Nordwestschweiz
ISDS-Konzept Informationssicherheits- und Datenschutzkonzept
ISMS Information Security Management System
RIPOL Automatisiertes Polizeifahndungssystem
RRB Regierungsratsbeschluss
SCTO Swiss Clinical Trial Organisation
SIS Schengener Informationssystem
ZEMIS Zentrales Migrationsinformationssystem

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, Prof. Dr. iur., Advokat

Team
Markus Brönnimann, CISA
Katja Gysin, Fürsprecherin
(ab 1.12.2015)
Sandra Husi-Stämpfli, Dr. iur., LL.M.
(bis 30.9.2015)
Carmen Lindner, lic. iur.
(bis 30.11.2015)
Daniela Waldmeier, Dr. iur.
Barbara Widmer, Dr. iur., LL.M., CIA
Katrin Gisler, MLaw
(ab 1.11.2015 befristet)

Volontärin/Volontär:
Katrin Gisler, MLaw
(1.1.2015 - 30.6.2015)
Jonas Annasohn, MLaw
(1.7.2015 - 31.12.2015)

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

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

Gestaltung
Andrea Gruber,
Gruber Gestaltung, Basel

Druck
Gremper AG