Datenschutzbeauftragter des Kantons Basel-Stadt

Bericht an den Grossen Rat

2014

Inhaltsübersicht

Einleitung

Themen

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

Aus dem Alltag

Fälle

Anhang

Einleitung 2014 – Gesetzgeber und Verantwortung

Die Verfassung gibt dem Gesetz eine Schlüsselrolle in der Gestaltung staatlichen Handelns. Dies verlangt vom Gesetzgeber eine sorgfältige Auseinandersetzung mit der Materie – auch wenn die Öffentlichkeit nach tragischen oder aufsehenerregenden Ereignissen reflexartig nach einer sofortigen Regelung ruft. Nur mit wohlüberlegten und hinreichend bestimmten gesetzlichen Regelungen lässt sich das staatliche Handeln (und damit auch das Datenbearbeiten) wirksam steuern.

Der Ruf nach sofortiger Regelung

Warm anziehen! Kaum wurde in den Medien über den Verdacht berichtet, ein Co-Pilot mit Depressionen habe ein Flugzeug absichtlich zum Absturz gebracht, erhielt eine Mitarbeiterin des Datenschutzbeauftragten einen Telefonanruf einer Bekannten: «Jetzt muss sich der Datenschutz aber warm anziehen!». Stunden später schon kursierte in den Medien die Forderung, der Gesetzgeber müsse sofort die Ärztinnen und Ärzte verpflichten, Gesundheitsdaten an die Arbeitgeberin zu leiten. Es dürfe nicht sein, dass «der Datenschutz» höher gewichtet werde als das Leben von 150 Passagieren.

Anderes Szenario Kaum hat ein «Saubannerzug» in Zürich Verwüstungen angerichtet, wird die Forderung laut, jetzt müssten sofort die gesetzlichen Grundlagen geschaffen werden, damit alle Polizistinnen und Polizisten mit Bodycams ausgerüstet werden können. Es dürfe nicht sein, dass «der Datenschutz» höher gewichtet werde als die Sicherheit.

Gemeinsamkeit Was ist den beiden geschilderten Situationen gemeinsam? Aufgrund eines tragischen oder aufsehenerregenden Vorkommnisses wird reflexartig nach neuen gesetzlichen Regeln gerufen: Der Gesetzgeber soll sofort die notwendigen Massnahmen erlauben, so dass ähnliche Vorkommnisse künftig verhindert werden könn(t)en. Nun hat das Gesetz im Rechtsstaat tatsächlich eine wichtige Funktion: Es ist Grundlage und Schranke staatlichen Handelns. Von da her betrachtet ist es richtig, eine gesetzliche Regelung zu verlangen – als Grundlage staatlichen Handelns. Gleichzeitig muss das Gesetz staatlichem Handeln aber auch Schranke sein.

Qualität der Rechtsetzung

Reflexion statt Reflex Gesetzgebung darf deshalb nie Reflex, sondern muss vielmehr Reflexion sein. Der Gesetzgeber muss sich gut überlegen, welche Regeln er aufstellen will. In den erwähnten Beispielen: Soll das ärztliche Berufsgeheimnis gegenüber der Arbeitgeberin generell aufgehoben werden? Oder nur unter bestimmten engen Voraussetzungen? Gegenüber der Arbeitgeberin – oder gegenüber einem vertrauensärztlichen Dienst? Sollen Polizistinnen und Polizisten generell alles aufnehmen dürfen, was um sie herum geschieht, also auch alle Bürgerinnen und Bürger, die sie sehen, die sich aber nichts haben zuschulden kommen lassen? Nur in bestimmten definierten Situationen? Wer entscheidet darüber – die einzelne Polizistin? Erfolgt die Aufnahme in Bild und Ton? Verdeckt oder offen? Unter welchen Voraussetzungen, zu welchem Zweck und durch wen dürfen die Daten ausgewertet werden? Sollen die Daten gelöscht werden oder müssen sie aufbewahrt werden?

Hinreichende Bestimmtheit Wenn die Gesetzgebung staatliches Handeln wirksam steuern soll, dann darf sie nicht zu «dünn» sein. Gerade wenn aus Datenschutzsicht die Zulässigkeit eines behördlichen Datenbearbeitens beurteilt werden soll, ist es entscheidend, wie bestimmt eine gesetzliche Regelung ausgefallen ist. Zu allgemeine gesetzliche Regelungen entwickeln nicht die Steuerungskraft, die ihnen nach dem Legalitätsprinzip abverlangt wird. Das Gesetz schützt Bürgerinnen und Bürger vor Willkür – zu offene, zu vage Bestimmungen geben weder den Betroffenen noch den mit der Rechtsanwendung betrauten öffentlichen Organen die notwendige Sicherheit.

Tätigkeitsbericht 2014

Überblick In Erfüllung des gesetzlichen Auftrages (§ 50 IDG[1]) informieren wir mit diesem Bericht über unsere Tätigkeit im Jahr 2014. Ein besonderes Augenmerk richten wir auf die Qualität der gesetzlichen Grundlagen (Seiten 8 ff.), auf die Verantwortlichkeit der Dateneignerin bei Onlinezugriffen (Seiten 12 ff.) und auf die IT-Governance (Seiten 15 ff.). Anschliessend gewähren wir einen Blick auf das «Tagesgeschäft» – einen Einblick in den bunten Strauss der behandelten Beratungsthemen (Seiten 20 ff.) und in die Kontrolltätigkeit (Seiten 28 ff.). Es folgt ein Überblick über besondere Berichtpunkte: Pilotversuche, Informationszugangsgesuche und die Geschäftslast (Seiten 32 ff.). Einen detaillierten Überblick über die Zahlen des Jahres 2014 bietet die Statistik (Seiten 36 f.). Und schliesslich runden sechs illustrative Fälle die Berichterstattung ab (Seiten 40 ff.).

Zum Schluss

Danke! Unsere Aufgaben im Bereich des Datenschutzes und des Öffentlichkeitsprinzips könnten wir nicht erfolgreich erfüllen ohne die Unterstützung vieler Menschen und Institutionen. Mein Dank gilt deshalb

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

— allen, die sich mit Fragen zum Datenschutz und zum Öffentlichkeitsprinzip 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;

— dem Grossen Rat für das mit meiner Wahl für eine zweite Amtsperiode (2015-2020) zum Ausdruck gebrachte Vertrauen;

— den Volontären Nicolas Hochstrasser und Lorenz Overhage für ihre kritische Neugier und ihre aktive Mitarbeit und

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

Beat Rudin, Datenschutzbeauftragter

1 Die in den Texten erwähnten Rechtsquellen und Materialien sind in einem Verzeichnis am Schluss des Berichts detailliert aufgeführt (Seite 46).

Themen

Thema 1 Gesetzliche Grundlage – nicht beliebig vage!

Thema 2 Onlinezugriffe und Verantwortung der Dateneignerin: Leichen im Keller?

Thema 3 IT-Governance – kein blosses Schlagwort

Thema 1 Gesetzliche Grundlage – nicht beliebig vage!

Das verfassungsrechtliche Legalitätsprinzip verlangt für behördliches Datenbearbeiten eine gesetzliche Grundlage. Was nützt eine solche Grundlage, wenn die Bürgerinnen und Bürger daraus nicht entnehmen können, welche Amtsstelle welche Aufgabe zu erfüllen hat und deshalb welche Personendaten über sie bearbeiten darf?

Annäherung

Verfassungsrechtliche Vorgabe Das Erfordernis der gesetzlichen Grundlage für staatliches Handeln – und damit auch für staatliches Datenbearbeiten – ist ein Ausfluss des verfassungsrechtlichen Legalitätsprinzips. «Grundlage und Schranke staatlichen Handelns ist das Recht», sagen übereinstimmend die Bundesverfassung[1] und die Kantonsverfassung[2]. Ebenfalls halten beide Verfassungen übereinstimmend fest: «Einschränkungen von Grundrechten bedürfen einer gesetzlichen Grundlage»[3]. Das Legalitätsprinzip erlaubt und beschränkt also das staatliche Handeln. Es weist dabei zwei Aspekte auf: einen demokratischen und einen rechtsstaatlichen.

Demokratischer Aspekt Der demokratische Aspekt – vom Recht Betroffene sollen auch beim Rechtsetzen mitwirken können – führt zum Erfordernis der *Gesetzesform:* Schwerwiegende Eingriffe in Grundrechte müssen in Form eines Gesetzes vorgesehen werden – das bedeutet, dass das Parlament diesen Beschluss fassen muss und dass ihn allenfalls, über das fakultative Referendum, auch die Stimmberechtigten gutheissen müssen. Eine tiefere Normstufe reicht nicht aus. Leichtere Eingriffe in die Grundrechte dürfen hingegen auch in Verordnungen vorgesehen werden[4].

Grundlage und Schranke staatlichen Handelns ist das Recht.

Rechtsstaatlicher Aspekt Der rechtsstaatliche Aspekt soll Rechtsgleichheit und Rechtssicherheit schaffen; dazu dient das Erfordernis der *Rechtsnorm*. Es verlangt, dass die Grundlage für staatliches Handeln in Form von generell-abstrakten Rechtsnormen geschaffen wird: generell – d.h. für nicht zum vorneherein bestimmte Personen, abstrakt – d.h. für nicht zum vorneherein bestimmte Sachverhalte. Generell-abstrakte Normen sind etwa das Gesetz oder die Verordnung.

Konkret: Gesetzliche Grundlage im Datenschutzrecht

Differenzierung Bei der gesetzlichen Grundlage für das Bearbeiten von Personendaten wird nicht nur zwischen den verschiedenen Normstufen unterschieden, sondern auch danach, wie «direkt» ein Gesetz oder eine Verordnung das Datenbearbeiten regeln.

Unmittelbare gesetzliche Grundlage Wenn das Gesetz (oder bei «gewöhnlichen» Personendaten allenfalls die Verordnung) das Datenbearbeiten selber umschreibt und ein öffentliches Organ verpflichtet oder ermächtigt, bestimmte Personendaten zu bearbeiten, sprechen wir von einer unmittelbaren gesetzlichen Grundlage für das Datenbearbeiten[5]. So umschreibt beispielsweise § 15 Aufenthaltsgesetz den Inhalt einer Meldung der Bewohnerinnen und Bewohner in sog. Kollektivhaushalten: AHV-Versichertennummer, amtlicher Name, Vorname, Geburtsdatum, Geschlecht, Zivilstand, Staatsangehörigkeit, Zuzugsdatum, Datum des Einzugs in den Kollektivhaushalt, Gemeinde des Hauptwohnsitzes, Wohnadresse. Das öffentliche Organ, die Einwohnerkontrollbehörde, wird damit verpflichtet, diese Personendaten zu bearbeiten.

Mittelbare gesetzliche Grundlage Von einer (bloss) mittelbaren gesetzlichen Grundlage für das Datenbearbeiten sprechen wir, wenn das Gesetz (oder allenfalls die Verordnung) nicht das Datenbearbeiten selber regelt, sondern einem öffentlichen Organ bloss eine Aufgabe überträgt, die dieses nur mit der Bearbeitung von Personendaten erfüllen kann[6]. Art. 123 DBG verpflichtet beispielsweise die kantonale Veranlagungsbehörde, zusammen mit dem Steuerpflichtigen die für eine vollständige und richtige Besteuerung massgebenden tatsächlichen und rechtlichen Verhältnisse festzustellen; die Steuerverwaltung kann die Veranlagungsaufgabe nur erfüllen, wenn sie z.B. bei der Einkommenssteuerveranlagung die dafür massgeblichen Steuerfaktoren nach Art. 16 ff. DBG bearbeiten darf.

Hinreichende Bestimmtheit Inhaltlich muss sich aus der gesetzlichen Grundlage hinreichend bestimmt ergeben:

— das *öffentliche Organ,* das die Aufgabe erfüllen muss (und dazu die Personendaten bearbeiten darf),

— der *Zweck*, zu dessen Erreichung die Personendaten bearbeitet werden sollen, und

— die *Personendaten*(kategorien), welche zur Zweckerreichung bearbeitet werden dürfen[7].

Zudem: Verhältnismässigkeit

Verfassungsprinzip Das verfassungsrechtliche Verhältnismässigkeitsprinzip[8] verlangt, dass staatliches Handeln – hier: behördliches Bearbeiten von Personendaten – zur Zweckerreichung *geeignet, erforderlich* und den betroffenen Personen *zumutbar* ist[9].

Verantwortung für die Verhältnismässigkeit Wenn der Gesetzgeber in der unmittelbaren gesetzlichen Grundlage präzis festlegt, welche Information über die Klientinnen und Klienten einer Amtsstelle bearbeitet werden müssen, dann übernimmt *er* die Verantwortung für die Verhältnismässigkeit. Bei der mittelbaren gesetzlichen Grundlage obliegt es aber dem öffentlichen Organ, dafür zu sorgen, dass die Datenbearbeitung verhältnismässig ist[10]: Es hat zu prüfen, ob die Aufgabe nicht auch ohne Personendaten, mit weniger Personendaten, mit Daten über weniger Personen, mit weniger «sensitiven» Daten oder mit weniger lange aufzubewahrenden Personendaten erfüllt werden kann.

Bedeutung der gesetzlichen Grundlage

Steuerungsinstrument Mit der gesetzlichen Grundlage steuert der Gesetzgeber das staatliche Handeln – in unserem Fall: das staatliche Datenbearbeiten. Je «klarer» die gesetzliche Grundlage, umso klarer ist das Datenbearbeiten gerechtfertigt: Einerseits *für die betroffene Person*, die so weiss, womit sie zu rechnen hat, andererseits aber auch *für das öffentliche Organ*, das damit klare Leitplanken für sein Handeln bekommt. Die informations- und datenschutzrechtliche Verantwortung für das Datenbearbeiten[11] liegt bei der Dateneignerin – wenn sich nicht klar bestimmen lässt, wer eine Aufgabe zu erfüllen hat, ist für die Amtsstellen (bzw. ihre Leiterinnen und Leiter) auch unklar, wofür sie die Verantwortung tragen.

Umsetzung in den Kantonen Anders als der Bund, der häufig unmittelbare gesetzliche Grundlagen schafft[12], zeigen sich die Kantone generell «sparsamer» mit unmittelbaren gesetzlichen Regelungen: Hier werden häufiger nur mittelbare gesetzliche Grundlagen geschaffen, es wird nur die Aufgabe im Gesetz geregelt – das Datenbearbeiten ist deshalb weniger präzis umrissen, die Verantwortung für die Verhältnismässigkeit des Datenbearbeitens wird häufiger den Verwaltungsbehörden überlassen.

Problematisch? Das ist nicht unbedingt problematisch. Wenn sich aus der Aufgabennorm die nötigen Anhaltspunkte entnehmen lassen, dann erfüllt das Gesetz seine Aufgabe als «Grundlage und Schranke staatlichen Handelns». Das ist aber in unserem Kanton nicht immer der Fall. Der Blick in die Gesetzessammlung zeigt, dass Basel-Stadt bezüglich der hinreichenden Bestimmtheit seiner gesetzlichen Grundlagen alles andere als ein Muster ist. Das fehlende Organisationsrecht und eine Vernachlässigung der Normdichte finden sich leider nicht selten in der baselstädtischen Rechtslandschaft.

Wenn der Gesetzgeber eine unmittelbare gesetzliche Grundlage schafft, trägt er die Verantwortung für die Verhältnismässigkeit der geregelten Datenbearbeitung.

Fehlendes Organisationsrecht

Organisationsautonomie der Kantone Der Kanton Basel-Stadt ist im Vergleich mit dem Bund und anderen Kantonen[13] ausgesprochen zurückhaltend bei der Schaffung von Organisationsrecht[14]: Wenn der Bund den Vollzug den Kantonen überlässt, dann spricht er in den entsprechenden Regelungen logischerweise oft nur vom «Kanton», der beispielsweise Daten bearbeiten darf. Welche Stelle dann im Kanton konkret diese Aufgabe erfüllt, muss der Kanton festlegen. Oft ist dies nicht schwierig und liegt auf der Hand: Aufgaben im Zusammenhang mit der Bundesstatistik erfüllt in der Regel das Statistische Amt, mit der Invalidenversicherung die IV-Stelle, mit der Arbeitslosenversicherung das Amt für Wirtschaft und Arbeit. Es bleibt aber gleichwohl den Kantonen überlassen im entsprechenden Fachgesetz festzulegen, welche Stelle *welche* Aufgabe erfüllt. Weil aber der Regierungsrat für die zweckmässige Organisation der Verwaltung zuständig ist, lässt er sich ungern vom Grossen Rat via Gesetz vorschreiben, wie die Organisation auszusehen hat. Eine Regelung der kantonalen Organisation könnte aber auch mittels Verordnung erfolgen.>

Unklare Verantwortung Zwei Beispiele mögen verdeutlichen, zu welchen Unklarheiten das Fehlen eines klaren Organisationsrechts führen kann:

— So lässt sich aus dem Sozialhilfegesetz unter dem Titel «Organisation und Finanzierung» entnehmen, dass «(d)ie Einwohnergemeinden, bzw. in der Stadt Basel der Kanton, (…) ihre Sozialhilfe selber (organisieren und finanzieren)»[15]. Welche Stelle das in der Stadt Basel ist, lässt sich zwar anhand des Namens erraten – aber weder das Sozialhilfegesetz noch eine Verordnung enthalten die entsprechende Zuweisung der Aufgabe an die Dienststelle «Sozialhilfe».

— Weitaus komplexer wird es in jenen Fällen, in denen mehrere Stellen gemeinsam eine Aufgabe erfüllen: Sowohl in den Bereichen der (bundesrechtlich geregelten) Invalidenversicherung und der Arbeitslosenversicherung als auch im Bereich der Sozialhilfe gibt es die (Teil)Aufgabe Arbeitsintegration. In Basel-Stadt wurden 2007 die drei Organisationseinheiten, die in den drei Bereichen diese Aufgabe erfüllt haben, im AWA zusammengefasst als Arbeitsintegrationszentrum (AIZ)[16]. Erst mit Wirkung ab April 2012 wurden die Aufgaben des AIZ in einer Verordnung[17] festgehalten. Zuvor hatte eine Bürgerin oder ein Bürger keine Chance, herauszufinden, wer im Kanton Basel-Stadt im Zusammenhang mit der Arbeitsintegration welche Daten über sie/ihn erhebt, von anderen Stellen erhält und an andere Stelle oder Personen weitergibt. Auch der Datenschutzbeauftragte, der die Datenbearbeitungen kontrollieren soll, fand keine Rechtsgrundlage für die Datenbearbeitungen.

Das fehlende Organisationsrecht und eine Vernachlässigung der Normdichte finden sich leider nicht selten in der baselstädtischen Rechtslandschaft.

Vernachlässigte Normdichte

Allzu viel Interpretationsspielraum Wenn sich – wie oben erwähnt – aus der Aufgabennorm die nötigen Anhaltspunkte entnehmen lassen, dann erfüllt das Gesetz seine Aufgabe als «Grundlage und Schranke staatlichen Handelns». Es muss jedoch festgestellt werden, dass sogar Bereiche, in welchen schwere Eingriffe in die Persönlichkeitsrechte der Bürgerinnen und Bürger erfolgen können, immer wieder mit ausgesprochen vagen Bestimmungen geregelt werden[18].

Allgemeine Aufgabennormen Wenn sich bestimmte Teile der Aufgaben, welche die Psycho-Sozialen Dienste (PSD) der Kantonspolizei erfüllen, nur auf die allgemeine Aufgabenumschreibung der Polizei in § 2 PolG stützen lassen, dann lassen sich dieser gesetzlichen Grundlage kaum Schranken für das Datenbearbeiten entnehmen – weder weiss eine betroffene Person beispielsweise, ob, unter welchen Voraussetzungen und zu welchem Zweck die PSD Fotoaufnahmen ihrer Wohnung herstellen oder von einer anderen Stelle erhalten dürfen, noch können sich die PSD sicher sein, ob ihr Bearbeiten von (teilweise besonderen) Personendaten recht- und verhältnismässig ist und an welche anderen Stellen die Bilder weitergereicht werden dürfen. Aus diesen Gründen arbeitet die Kantonspolizei gemeinsam mit dem Datenschutzbeauftragten an der Verbesserung der gesetzlichen Grundlage.

Schein-Lösungen Ein anderes Beispiel ist das im Dezember 2014 beschlossene Kinder- und Jugendgesetz (KJG): An ihm lässt sich illustrieren, wie ein Gesetz seine Aufgabe, eine belastbare Grundlage für behördliches Handeln abzugeben und für die betroffenen Personen transparent zu machen, womit sie zu rechnen haben, verfehlen kann. Das betrifft insbesondere folgende Punkte:

— Die allgemeinen Aufträge nach § 4 KJG sind nicht hinreichend bestimmt, um als gesetzliche Grundlagen für Datenbearbeitungen zu dienen.

— § 7 KJG regelt gemäss Titel die «Mitwirkung» – der Blick in den Ratschlag zeigt aber, dass mit der Bestimmung eigentlich nicht die Mitwirkung der Kinder und Jugendlichen bzw. ihrer Eltern geregelt wird; die Bestimmung soll vielmehr den mit der Kinder- und Jugendhilfe betrauten Stellen den Zugang zu Adressen usw. ermöglichen – was nun beim besten Willen nicht in den Wortlaut der Bestimmung hineininterpretiert werden kann.

— Die in § 20 KJG enthaltene Regelung zur Datenbearbeitung bleibt inhaltsleer: Weder sind die zuständigen Stellen klar umschrieben noch lassen sich die Aufgaben, zu deren Erfüllung Personendaten bearbeitet werden dürfen, hinreichend bestimmt dem Gesetz entnehmen. Hier zeigt sich erneut, wie wichtig eine klare Regelung der Aufgaben in § 4 KJG gewesen wäre.

Der Datenschutzbeauftragte äussert sich im Rahmen einer Vernehmlassung nicht politisch, sondern beschränkt sich auf informations- und datenschutzrechtliche Aspekte.

Berücksichtigung der Stellungnahme

Nein Der Datenschutzbeauftragte hat sich im Rahmen der Vernehmlassung dezidiert kritisch zu den nun immer noch festgestellten Unzulänglichkeiten geäussert – leider vergeblich. Er äussert sich nicht politisch, z.B. ob die Statuierung einer bestimmten Aufgabe politisch erwünscht sei oder nicht. Seiner gesetzlichen Aufgabe entsprechend beschränkt er sich auf informations- und datenschutzrechtliche Aspekte. Ob die ausarbeitenden Stellen die Bedeutung einer sorgfältigen Rechtsetzung nicht verstanden haben oder ob sie die Stellungnahme des Datenschutzbeauftragten als politische Stellungnahme angesehen haben, der man je nach politischem Standpunkt folgen mag oder nicht, kann nicht beantwortet werden. Anders als bei Rechtsetzungsprojekten in anderen Departementen hat anschliessend niemand das Gespräch gesucht, um Lösungsansätze zu besprechen. Dass in der Zusammenarbeit sachdienliche und datenschutzkonforme Lösungen gefunden werden können, zeigen die Beispiele des Statistikgesetzes[19] (und in der Fortsetzung des dazugehörenden Verordnungsrechts) oder der Rechtsgrundlagen für die Psycho-Sozialen Dienste der Kantonspolizei. Der Datenschutzbeauftragte prüft zurzeit, ob er gestützt auf § 20 IDG künftig alle Stellungnahmen im Rahmen von Vernehmlassungen auf seiner Website publizieren will.

—

1 Art. 5 Abs. 1 BV.
2 § 5 Abs. 1 KV.
3 Art. 36 Abs. 1 BV; § 13 Abs. 1 KV.
4 Nach der (neuen) Kantonsverfassung sind andere staatliche Handlungsformen, insbesondere Grossratsbeschlüsse und Regierungsratsbeschlüsse, keine Formen der Rechtsetzung mehr.
5 § 9 Abs. 1 lit. a IDG; vgl. dazu PK-IDG/BS-Rudin 2014, § 9 N 16.
6 § 9 Abs. 1 lit. b IDG; vgl. dazu PK-IDG/BS-Rudin 2014, § 9 N 17.
7 PK-IDG/BS-Rudin 2014, § 9 N 21 ff. und (für besondere Personendaten) N 33 ff.
8 § 5 Abs. 2 BV; § 5 Abs. 2 KV.
9 § 9 Abs. 3 IDG; vgl. dazu PK-IDG/BS-Rudin 2014, § 9 N 51 ff.
10 § 6 IDG.
11 § 6 IDG.
12 Dies insbesondere dort, wo Datenbanken im Einsatz sind, auf welche unterschiedliche Behörden Zugriff haben (z.B. N-SIS, RIPOL, ZEMIS, MOFIS, ISA, ISR).
13 Vgl. im Bund etwa das RVOG und die dazugehörenden Verordnungen; im Kantons Basel-Landschaft das Gesetz vom 6. Juni 1983 über die Organisation des Regierungsrates und der kantonalen Verwaltung (Verwaltungsorganisationsgesetz, VwOG), SGS 140, und die gestützt darauf erlassenen Dienstordnungen; im Kanton Zürich das Gesetz 6. Juni 2005 über die Organisation des Regierungsrates und der kantonalen Verwaltung (OG RR), LS 172.1, und die dazu gehörenden Organisationsverordnungen.
14 Vgl. dazu PK-IDG/BS-Rudin 2014, § 6 N 2, § 9 N 37.
15 § 24 SHG.
16 Regierungsratsbeschluss vom 6. Februar 2007, Nr. 07/05/20. Dieser RRB enthält Regelungen über die Verschiebung von Stellen und die Finanzierung der Leistungen, aber keinerlei Bestimmungen zum Datenbearbeiten.
17 Verordnung vom 15. November 2011 betreffend Zuständigkeit und Organisation beim Vollzug der Arbeitslosenversicherung im Kanton Basel-Stadt, SG 835.150.
18 Zu den Anforderungen an die Bestimmtheit der gesetzlichen Grundlage vgl. PK-IDG/BS-Rudin 2014, § 9 N 2 ff. und 33 ff.
19 TB 2012, 24.

Thema 2

Onlinezugriffe und Verantwortung der Dateneignerin: Leichen im Keller?

Die Dateneignerin trägt die informations- und datenschutzrechtliche Verantwortung für ihre Datenbearbeitungen. Besonders wichtig ist dies, wenn sich andere öffentliche Organe mittels Onlinezugriff bei den Daten der Dateneignerin «bedienen» können. Hier tun die verantwortlichen Leitungsorgane gut daran, zu überprüfen, ob sie diesbezüglich nicht Leichen im Keller haben, von denen sie nichts wissen.

Verantwortlichkeit nach IDG

Regelung im IDG 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]. Es hat dafür zu sorgen, dass die Anforderungen aus dem IDG umfassend eingehalten werden. Damit ist es – wie im Praxiskommentar zum IDG festgehalten wird[2] – insbesondere dafür verantwortlich, dass:

— der Umgang mit Informationen so gestaltet ist, dass das öffentliche Organ rasch, umfassend und sachlich informieren kann (§ 4 IDG);

— die Informationen nach den Vorschriften über die Aktenführung gemäss dem Archivgesetz verwaltet werden (§ 5 IDG);

— die Grundsätze für das Bearbeiten von Personendaten nach §§ 9 bis 16 IDG (Gesetzmässigkeit, Verhältnismässigkeit, Treu und Glauben, Richtigkeit, Zweckbindung, Vorabkontrolle, Datenvermeidung und Datensparsamkeit, Erkennbarkeit bei der Beschaffung, Vernichtung) eingehalten werden;

— das Bearbeiten von Informationen nur unter den Voraussetzungen von § 7 IDG Dritten übertragen und dabei sichergestellt wird, dass der Dritte die Informationen nur so bearbeitet, wie es das öffentliche Organ selbst tun dürfte[3];

— die Voraussetzungen für das Bekanntgeben von Personendaten nach §§ 21 bis 23 IDG beachtet werden, insbesondere auch, wenn einem anderen öffentlichen Organ ein Onlinezugriff auf die «eigenen» Personendaten eingeräumt werden soll, und bei der grenzüberschreitenden Datenbekanntgabe (§ 23 IDG);

— die Informationssicherheit nach § 8 IDG gewährleistet ist;

— der Eintrag ins Verzeichnis der Verfahren, bei denen Personendaten bearbeitet werden, nach § 24 IDG erfolgt;

— Gesuche auf Zugang zu Informationen i.S.v. § 25 IDG korrekt behandelt werden;

— Gesuche auf Zugang zu den eigenen Personendaten i.S.v. § 26 IDG korrekt behandelt werden;

— die Rechtsansprüche der betroffenen Personen nach § 27 IDG gewährleistet werden und

— in angemessener Weise auf das Sperrrecht der betroffenen Personen nach § 28 IDG hingewiesen und das ausgeübte Sperrrecht beachtet wird.

Insbesondere bei Datenbekanntgaben Wenn das öffentliche Organ A dem öffentlichen Organ B Personendaten übermittelt, dann stellt dies datenschutzrechtlich eine Datenbekanntgabe im Sinne von § 21 IDG dar. Ob die Voraussetzungen für die Datenbekanntgabe erfüllt sind, insbesondere ob die erforderliche gesetzliche Grundlage besteht und die Datenbekanntgabe verhältnismässig ist, hat das bekanntgebende Organ A, die Dateneignerin, zu prüfen. Die Dateneignerin trägt damit die Verantwortung für die Rechtmässigkeit und Verhältnismässigkeit der Datenbekanntgabe im konkreten Fall.

Konsequenzen bei Verletzung Wenn die oben erwähnten Pflichten verletzt werden, dann stehen den betroffenen Personen die Rechtsansprüche nach § 27 IDG zu[4]. Ausserdem kann die betroffene Person, wenn die entsprechenden Voraussetzungen erfüllt sind, auch Anspruch auf Schadenersatz[5] bzw. Genugtuung[6] geltend machen. Die Verletzung der informations- und datenschutzrechtlichen Verantwortung kann für die fehlbare Person allenfalls auch disziplinarrechtliche Folgen nach sich ziehen[7].

Trägerinnen und Träger der Verantwortung

Verantwortung der Leitungsorgane Verantwortlich ist «das öffentliche Organ». Verantwortung übernehmen und tragen können natürlich nur Menschen. Damit kommt die Verantwortung den Leitungsorganen zu: Sie, die Leiterinnen und Leiter, tragen – rechtlich und politisch – die Verantwortung für den gesamten Betrieb jeweils in ihrem Zuständigkeitsbereich[8]. Sie haben ihre Organisationseinheit so zu organisieren, dass sie die Verantwortung tragen können.

Umsetzung Daraus ergeben sich verschiedene Handlungspflichten[9]. Die Leitungsorgane haben dafür zu sorgen, dass es in ihrem Verantwortungsbereich «richtig» zu und her geht. Sie erreichen das:

— durch ein Bekenntnis zu Datenschutz und Informationssicherheit;
— durch eine zweckmässige Organisation;
— durch den Erlass der erforderlichen Vorschriften;
— durch die Anordnung der erforderlichen organisatorischen und technischen Massnahmen und
— durch eine sorgfältige Auswahl der Mitarbeitenden, ihre eingehende Instruktion und angemessene Beaufsichtigung.

Bei Onlinezugriffen

Einräumung eines Onlinezugriffs Bei einem Onlinezugriff kann die Dateneignerin die Rechtmässigkeit und Verhältnismässigkeit der Datenbekanntgabe im konkreten Fall nicht beurteilen; das zugriffsberechtigte Organ «bedient sich» direkt bei den Daten. Deshalb muss die Dateneignerin bei der Einräumung des Onlinezugriffs generell prüfen, ob die Datenbekanntgabe (bzw. das «Sich-bedienen» des zugreifenden Organs) rechtmässig und verhältnismässig ist. Dazu ist insbesondere zu prüfen, ob die erforderlichen Rechtsgrundlagen gegeben sind und ob die Datenbekanntgabe zur Aufgabenerfüllung verhältnismässig, d.h. zur Aufgabenerfüllung geeignet und erforderlich sowie den betroffenen Personen zuzumuten ist.

Verhältnismässigkeit Bei der Verhältnismässigkeitsprüfung, insbesondere bei der Prüfung, ob die Datenbekanntgabe erforderlich ist, ob also ohne die Daten, mit weniger Daten oder mit weniger sensitiven Daten die Aufgabe nicht erfüllt werden kann (das «mildeste Mittel», mit dem die Aufgabe noch erfüllt werden kann), ist entscheidend, dass der Zugriff nur auf genau die Daten ermöglicht wird, die das empfangende öffentliche Organ braucht (z.B. Namen und Adressen der weiblichen Jugendlichen, die in diesem Jahr 18 Jahre alt werden und das Schweizerbürgerrecht besitzen). Dann können mittels Filtern die Datensätze, auf welche der Zugriff ermöglicht werden soll, oder mittels Masken die Felder, die bei den ausgewählten Datensätzen angezeigt werden sollen, eingeschränkt werden. Wenn diese Einschränkung nicht so präzise gesteuert werden kann, dann ist zu prüfen, ob ein Onlinezugriff überhaupt eingeräumt werden darf oder ob mit anderen Massnahmen dieses Manko gleichsam kompensiert werden kann (z.B. durch die regelmässige Überprüfung der konkret getätigten Zugriffe).

Bei einem Onlinezugriff kann die Dateneignerin die Rechtmässigkeit und Verhältnismässigkeit der Datenbekanntgabe im konkreten Fall nicht beurteilen.

Insbesondere Zugriffshäufigkeit Eine Onlinezugriffs-Möglichkeit ist bequem. Sie ist aber nicht immer auch verhältnismässig. Gerade wenn die Zugriffe nicht mittels Filtern und Masken fein gesteuert werden können, spielt auch die Häufigkeit der Zugriffe eine Rolle. Der Zugriff eines öffentlichen Organs auf die Daten des Betreibungsamtes sollte z.B. so eingeschränkt werden, dass das öffentliche Organ einzig diejenigen Datensätze sieht, bei denen es als Gläubiger involviert ist. Wäre das nicht möglich, hätte also das empfangende öffentliche Organ Zugriff auf mehr als 70000 im Betreibungsregister verzeichnete eingeleitete Betreibungen, obwohl es nur Angaben zu 500 Personen pro Jahr benötigt, dann mag mit kompensierenden Massnahmen das Manko in der Verhältnismässigkeit aufgewogen werden können. Wenn es nur Angaben zu 50 Personen brauchte, wäre die Einräumung des Onlinezugriffs unverhältnismässig. Einmal in der Woche vom Betreibungsamt eine Auskunft zu verlangen, ist zumutbar – und möglicherweise auch günstiger als die Programmierung einer Schnittstelle mitsamt kompensierenden Massnahmen. >

Es ist nicht auszuschliessen, dass öffentliche Organe die eine oder andere Leiche im Keller haben: Sie sind daher aufgerufen, die Onlinezugriffe auf ihre Datenbestände zu prüfen.

Leichen im Keller?

Vorabkontrolle und Befristung Die Dateneignerin (bzw. die Leitungsebene der Dateneignerin) trägt also die Verantwortung für die Einräumung von Onlinezugriffs-Möglichkeiten. Die Einräumung ist vorabkontrollpflichtig, d.h. sie muss der oder dem Datenschutzbeauftragten zur Prüfung vorgelegt werden. Normalerweise wird die Genehmigung des Zugriffs zeitlich begrenzt, muss also periodisch – in der Regel jeweils nach fünf Jahren – wieder geprüft werden.

Überprüfung Der Datenschutzbeauftragte vermutet aufgrund der Unterlagen, die noch aus der Geltungszeit des Datenschutzgesetzes von 1992 stammen, dass etliche Onlinezugriffs-Möglichkeiten bestehen, die in den letzten zehn Jahren nicht von den Dateneignerinnen genehmigt worden sind (oder deren Genehmigung in diesen Jahren nie geprüft und verlängert worden ist). Es ist nicht auszuschliessen, dass öffentliche Organe die eine oder andere Leiche im Keller haben, ohne dass sie (d.h. die Leiterinnen oder Leiter) sich dessen bewusst sind. Deshalb werden alle öffentlichen Organe des Kantons und der Gemeinden aufgerufen, die Onlinezugriffe auf ihre Datenbestände einmal auf ihre Recht- und Verhältnismässigkeit zu prüfen. Der Datenschutzbeauftragte wird in den nächsten Jahren entsprechende Prüfungen vornehmen.

—

1 § 6 Abs. 1 IDG.
2 PK-IDG/BS-Rudin 2014, § 6 N 4-15.
3 Vgl. z.B. TB 2011, 26.
4 PK-IDG/BS-Rudin 2014, § 6 N 32 ff.; PK-IDG/BS-Waldmeier 2014, § 27 N 1 ff.
5 §§ 3 f. HG.
6 § 4a HG.
7 §§ 24 f. PG.
8 PK-IDG/BS-Rudin 2014, § 6 N 3.
9 PK-IDG/BS-Rudin 2014, § 6 N 16 ff.

Thema 3 IT-Governance – kein blosses Schlagwort

Am 1. Januar 2014 wurde im Kanton Basel-Stadt die neue IT-Governance in Kraft gesetzt. Damit ist der Kanton aber keineswegs ein Vorreiter – im Gegenteil: Das Thema Governance und die im Folgenden aufgegriffene IT-Governance sind in Privatwirtschaft und öffentlicher Verwaltung seit geraumer Zeit vieldiskutierte Themen. Was steht aber hinter dem Schlagwort «IT-Governance»?

Ausgangslage

IT-Governance als Framework IT-Governance ist ein strategisches Gesamtkonzept, das auf einer übergeordneten Ebene beschreibt, wie die IT innerhalb einer Organisation gesteuert werden soll. Unter anderem legt die IT-Governance fest, wie beispielsweise die Ausrichtung der IT am operativen Geschäft sichergestellt werden soll, wie die Verantwortlichkeiten geregelt werden, wie der Umgang mit Risiken aussehen soll und wie sichergestellt werden soll, dass die Ziele auch erreicht werden. Die Norm ISO 38500[1] als eines der für die IT-Governance relevanten Frameworks definiert folgende Bereiche für die IT-Governance: Verantwortung (Responsibility), Strategie (Strategy), Beschaffung (Acquisition), Leistung (Performance), Regelkonformität (Conformance) und den Faktor Mensch (Human behaviour). Eines der Herzstücke von COBIT, einem weiteren prominenten Rahmenwerk für IT-Governance, ist eine Zielkaskade, welche ausgehend von den Anspruchsgruppen-Treibern über die Unternehmensziele der Organisation (Strategie) und die IT-Ziele (IT-Strategie) zu den Enabler-Zielen (Umsetzung) einen Zusammenhang abzubilden versucht. Mit dem von COBIT gewählten Vorgehen soll erreicht werden, dass relevante und greifbare Ziele und Zielvorgaben auf verschiedenen Zuständigkeitsebenen vorhanden sind und deren Abhängigkeit und Zusammenhang klar ersichtlich ist. Beiden, ISO 38500 und COBIT, ist gemein, dass die Verantwortung für den Einsatz und den Nutzen der IT nicht ausschliesslich dem IT-Verantwortlichen (CIO) oder den IT-Managern zugeordnet wird. ISO 38500 geht gar so weit, dass sich diese Norm primär an die Unternehmensführung wendet. Dies wird bereits mit dem Titel der Norm(«Corporate governance of information technology» und nicht etwa «IT-Governance») unterstrichen.

Der Datenschutzbeauftragte erachtet eine seriöse Umsetzung der neuen IT-Governance in den kommenden Jahren als eine der wichtigsten Aufgaben der kantonalen Verwaltung.

Politisches Commitment Bereits im Tätigkeitsbericht 2012 hat der Datenschutzbeauftragte das Thema IT-Governance aufgegriffen. In der Zwischenzeit hat der Regierungsrat eine «Neuregelung der IT-Governance» beschlossen. So hält er in seiner Antwort auf die Schriftliche Anfrage Urs Müller-Walz betreffend «Alleingang Rechenzentren JSD»[2] fest: «Per 1. Januar 2014 trat die vom Regierungsrat am 12. November 2013 beschlossene Neuregelung der IT-Governance in Kraft. Mit dieser wurden die kantonalen Steuerungsinstrumente und Organisationen zur effizienten und betriebswirtschaftlich orientierten Führung der Informatik gestärkt.» Auch in seiner Stellungnahme zu den Erwartungen der Geschäftsprüfungskommission im Bericht 14.5265.01 zum Jahr 2013[3] verweist er auf diese IT-Governance und deren Nutzen. Die Neubesetzung der Stellen des Leiters der Zentralen Informatikdiensten (ZID) und des Leiters Informatiksteuerung und Organisation (ISO) erfolgte im Verlauf des Berichtsjahres. Ob und welche Auswirkungen die neue IT-Governance hat, lässt sich noch nicht feststellen, zumal auch wesentliche von der IT-Governance geprägte Vorhaben, wie beispielsweise die neue Verordnung über die Informationssicherheit, bislang aufgeschoben wurden.

Erwartungen und Herausforderungen

Erwartungen Der Datenschutzbeauftragte erachtet eine seriöse Umsetzung der neuen IT-Governance in den kommenden Jahren als eine der wichtigsten Aufgaben der kantonalen Verwaltung: Hierbei wird dem Gesamtregierungsrat eine zentrale Rolle zukommen. Der Gesamtregierungsrat trägt nicht nur die Verantwortung für die strategischen Vorgaben, die Sicherstellung deren Umsetzung sowie ein angemessenes >

Risikomanagement, letztlich ist er das oberste Führungsgremium der Exekutive und vor allem auch das Bindeglied zwischen den sieben Departementen. Die Vorgaben, was zentral und was dezentral behandelt werden soll, kann letztlich nur der Gesamtregierungsrat vorgeben und die zielführende Durchsetzung sicherstellen.

IT-Governance kann nur umgesetzt werden, wenn Verantwortlichkeiten geklärt und ernstgenommen werden.

Herausforderungen Gerade für eine föderal strukturierte Organisation wie eine kantonale Verwaltung ergeben sich bezüglich der Verantwortlichkeiten spezielle Herausforderungen. IT-Governance in der öffentlichen Verwaltung ist ein Balanceakt zwischen föderalen Strukturen und zentralen Vorgaben. Dieser Herausforderung muss sich nicht nur der Kanton Basel-Stadt stellen – alle öffentlichen Verwaltungen der Schweiz werden über kurz oder lang um die Verabschiedung einer IT-Governance nicht mehr herumkommen.

Beispiel Bund Der Bund hat bereits mit der Bundesinformatikverordnung (BInfV) einen ersten Schritt getan: So werden dem Bundesrat folgende Zuständigkeiten auferlegt: Er

— bestimmt die IKT-Strategie des Bundes;
— legt die IKT-Standarddienste und deren Marktmodell fest;
— überwacht die Umsetzung der IKT-Strategie des Bundes anhand des strategischen Controllings und beschliesst bei Bedarf Massnahmen;
— legt fest, in welchen Bereichen IKT-Vorgaben nötig sind oder angepasst werden sollen;
— erlässt Weisungen über die IKT-Sicherheit;
— bestimmt im Rahmen des Budgetprozesses über die Zuweisung zentral eingestellter Mittel für IKT-Vorhaben;
— entscheidet bei Differenzen zwischen den Departementen, der Bundeskanzlei und dem ISB und
— bewilligt Abweichungen von seinen Vorgaben.

In Ausübung dieser Kompetenzen verabschiedete der Bundesrat am 30. November 2012 beispielsweise die Weisung für das Strategische Controlling für die Informatik und Telekommunikation (IKT) und setzte diese auf den 1. Dezember 2012 hin in Kraft. In dieser Weisung fordert der Bundesrat unter anderem «aktuelle und stufengerechte Steuerungsinformationen» ein, damit er die «strategischen Kernfragen bezüglich der Bundesinformatik beantworten kann». Der Bundesrat will mit dieser Weisung auch den Umsetzungsstand der IKT-Strategie des Bundes 2012-2015, den Status der IKT-Schlüsselprojekte sowie den Stand bei den IKT-Standarddiensten überwachen und kommt letztlich den verbindlichen Bestimmungen der BInfV nach.

Vergleich Etwas fällt auf: Im Kanton Basel-Stadt hat sich der Regierungsrat in seiner IT-Governance keine vergleichbare Stellung zugeordnet. Diese zentrale Funktion, die der Bundesrat im Bund einnimmt, fehlt im Kanton. Weder das Finanzdepartement noch die Konferenz für Organisation und Information (KOI) oder die Fachstelle Informatiksteuerung und Organisation (ISO) dürften längerfristig in der Lage sein, zentrale Vorgaben gegenüber einzelnen Departementen durchzusetzen. Der Datenschutzbeauftragte befürchtet, dass ohne die Übernahme dieser zentralen Funktion durch die Exekutive die Ziele der IT-Governance nicht erreicht werden können.

Handlungsbedarf

Verantwortung Nach § 6 IDG trägt dasjenige öffentliche Organ die Verantwortung für den Umgang mit Informationen, das die Informationen zur Erfüllung seiner gesetzlichen Aufgaben bearbeitet. Im IT-Kontext liegt diese Verantwortung bei der Dateneignerin. Es muss daher zwingend für alle bearbeiteten Informationen geklärt sein, wie diese Verantwortung ausgestaltet ist. IT-Governance kann nur umgesetzt werden, wenn Verantwortlichkeiten geklärt und ernstgenommen werden: Auch etablierte Standards und Frameworks zur IT und deren Sicherheit kennen die Definition des «fachlich Verantwortlichen». In der Verwaltung fehlt es aber aktuell vielerorts an einer klaren Zuordnung der Verantwortlichkeiten innerhalb der jeweiligen Organisationseinheit. Diese Klärung hat zwar letztendlich dezentral zu erfolgen – im Interesse einer gesamtheitlichen Lösung, eben einer *kantonalen* IT-Governance, erscheint es jedoch sinnvoll, Regelungen zentral zu verabschieden. Derzeit fehlen solche Vorgaben oder Richtlinien jedoch.

Zusammenarbeit In diesem Zusammenhang stellt sich auch die Frage, wie das Zusammenspiel über die Hierarchieebenen hinaus innerhalb der Verwaltung gestaltet werden soll. § 8 IDG gibt vor: «Das öffentliche Organ [also die Dateneignerin] schützt Informationen durch angemessene organisatorische und technische Massnahmen.» Die einzelnen Dateneignerinnen sind aber eingebunden in «ihre» Departemente und die Departemente ihrerseits in die gesamte Verwaltung. Sie können somit beispielsweise nicht frei entscheiden, welches Restrisiko getragen werden kann, geschweige denn, ob die Summe aller Restrisiken im Departement oder gar der gesamten Kantonsverwaltung akzeptiert werden kann. Häufig fehlt auch das Fachwissen, um Aspekte des Datenschutzes und der Informationssicherheit ausreichend fundiert beurteilen zu können. Damit aber nicht genug: Dateneignerinnen beziehen in der Regel IT-Leistungen, die zentral (von einem internen oder externen Anbieter) zur Verfügung gestellt werden. Die Dateneignerinnen können also faktisch nicht nach Belieben über die Angemessenheit der Massnahmen entscheiden und benötigen entsprechende spezifische Unterstützung sowie die Einbindung in die Gesamtorganisation. Damit darf aber ihre teils sogar gesetzlich vorgeschriebene Unabhängigkeit in ihrer Aufgabenerfüllung nicht tangiert werden. Auch diesem Umstand muss bei der Definition und Umsetzung einer tauglichen IT-Governance-Reglung Rechnung getragen werden.

In der Verwaltung fehlt es aktuell vielerorts an einer klaren Zuordnung der Verantwortlichkeiten innerhalb der jeweiligen Organisationseinheit.

Am Ball bleiben Das Thema IT-Governance darf nicht nur für den Datenschutzbeauftragten von zentraler Bedeutung sein. Die Verwaltung und insbesondere der Gesamtregierungsrat sind gefordert. Die Chancen und die Risiken, die mit dem Einsatz von Informatikmitteln bestehen, sind bekannt und müssen entsprechend ernstgenommen werden. Erschwert wird die seriöse Konzeption und Umsetzung der IT-Governance durch die Tatsache, dass zentrale Stellen bezüglich der Umsetzung bereits wieder vakant sind. Auch wenn die unaufhaltsame und immer schneller voranschreitende technische Entwicklung eine langfristige Planung oder gar eine «Patentlösung» verunmöglicht, so birgt der Einsatz von IT-Mitteln zu grosse Risiken, auch für die Persönlichkeitsrechte der Betroffenen und die Reputation der Verwaltung, vor allem aber auch für die Finanzen. Deshalb darf diese Thematik schlicht nicht dem Zufall überlassen werden. Dass Lösungsansätze unter Umständen nach kurzer Zeit revidiert werden müssen, ist unvermeidbar, bedeutet aber nicht, dass aus Angst, dass eine Lösung «falsch» sein könnte, auf die Hoffnung abgestellt werden darf, dass «schon alles gut gehe». Falsch wäre lediglich, die Risiken zu ignorieren und bezüglich der Herausforderungen nicht am Ball zu bleiben. Der Datenschutzbeauftragte steht für Diskussionen zur Verfügung und wird die Verwaltung bei der Umsetzung der IT-Governance fachlich gerne unterstützen.

—

1 ISO/IEC 38500:2008 Corporate governance of information technology.
2 Schriftliche Anfrage Urs Müller-Walz betreffend «Alleingang Rechenzentrum JSD» (14.5144.02 vom 27. Mai 2014).
3 Weitergeleitet an den Grossen Rat mit Schreiben 14.5265.02 der GPK vom 18. Dezember 2014 an den Grossen Rat.

Aus dem Alltag

Einblicke in die Beratungstätigkeit

Einblicke in die Kontrolltätigkeit

Besondere Berichtspunkte

Statistik

Aus dem Alltag

Einblicke in die Beratungstätigkeit

Der Datenschutzbeauftragte wird fast täglich mit neuen und herausfordernden Fragen konfrontiert. Die folgende Darstellung bietet Ihnen ein paar kurze Einblicke in die Vielfalt der behandelten Themen – von A (wie Aufbewahrungsdauer von Informationen) bis Z (wie Zugriffsgesuche). Ausserdem wird ein Blick auf die «Aussenauftritte» des Datenschutzbeauftragten und seiner Mitarbeitenden geworfen, auf Schulungen, Referate und Publikationen.

Verwendung von Fotos auf Werbeplakaten

Authentizität Um möglichst authentische Bilder zu gewinnen, verzichtete der Fotograf der Berufs- und Laufbahnberatung darauf, die Kinder einer Kindergartengruppe (bzw. ihre Eltern) sowie ihre Leiterin um ihre vorgängige Einwilligung zu bitten – er schoss die Fotos, ohne dass die abgelichteten Personen dies gemerkt hätten. Auch nachträglich wurde von den Kindern bzw. ihren Eltern und der Leiterin keine Einwilligung eingeholt[1] – erst per Zufall erkannte die besagte Leiterin sich und ihre Gruppe auf einem Plakat und wandte sich an den Datenschutzbeauftragten.

Nachträgliche Einwilligung Der Datenschutzbeauftragte informierte die Berufs- und Laufbahnberatung darüber, dass dieses Vorgehen widerrechtlich ist: Da keine gesetzliche Grundlage für die Erstellung von Fotos, auf denen Personen erkennbar sind, bestehe, müssten die abgelichteten Kinder und Jugendlichen bzw. deren Eltern, sowie die Leiterin der Gruppe zwingend um ihre Einwilligung in die Aufnahmen gebeten werden. Die Berufs- und Laufbahnberatung versicherte daraufhin, künftig entweder auf die Verwendung von Fotografien, auf welchen Personen erkennbar sind, zu verzichten, oder aber die Einwilligung der abgelichteten Personen oder derer gesetzlichen Vertreter einzuholen. Gegenüber den Eltern der Kinder, die auf den aktuellen Plakaten abgebildet waren, entschuldigte sich die Berufs- und Laufbahnberatung schriftlich und bat nachträglich um die Einwilligung, die Plakate verwenden zu dürfen.

Videoaufzeichnungen zur Massnahmenüberprüfung

Steigerung der Verkehrssicherheit Das Amt für Mobilität hat im vergangen Jahr verschiedene verkehrstechnische Massnahmen im Zusammenhang mit sog. Kaphaltestellen[2] erprobt, um die Verkehrssicherheit vor allem für die Velofahrenden, aber auch für die anderen Verkehrsteilnehmer zu erhöhen. Die erprobten Massnahmen, wozu beispielsweise das Anbringen von Velosymbolen zwischen den Schienen oder das Führen eines Veloweges auf Niveau Trottoir gehörten, sollten mittels Befragungen und Videoaufnahmen ausgewertet werden. Dabei waren insbesondere Blick, Handzeichen, Fahrverhalten etc. von Interesse, weshalb die Velofahrenden von vorne aufgenommen werden sollen.

Bestehen keine gesetzlichen Grundlagen für die Erstellung von Fotos, auf denen Personen erkennbar sind, müssen die Betroffenen zwingend um ihre Einwilligung gebeten werden.

Aufgabenerfüllung Der Datenschutzbeauftragte geht davon aus, dass die durch die erprobten Massnahmen bezweckte Erhöhung der Verkehrssicherheit zu den gesetzlichen Aufgaben des Amtes für Mobilität[3] gehört. Nach § 10 IDG ist auch das Bearbeiten zu einem nicht personenbezogenen Zweck (Statistik, Planung, Wissenschaft und Forschung) in der gesetzlichen Grundlage für die Aufgabenerfüllung mitenthalten[4].

Outsourcing Die Übertragung der Datenbearbeitung an Dritte ist nach § 7 IDG zulässig[5], allerdings darf keine rechtliche Bestimmung oder vertragliche Vereinbarung der Übertragung entgegenstehen. Zudem muss das öffentliche Organ sicherstellen, dass die Personendaten nur so bearbeitet werden, wie es dies selbst tun dürfte.

Fragebogen über Kindergartenkinder

Unklares Befragungsziel Der Fragebogen des Kinder- und Jugendgesundheitsdiensts (vormals Schulärztlicher Dienst), der allen neu in den Kindergarten eingetretenen Kindern verteilt wurde, löste bei einer Mutter Stirnrunzeln aus: Auch wenn der Fragebogen freiwillig auszufüllen sei – weshalb sollte es für den Kinder- und Jugendgesundheitsdienst relevant sein zu wissen, ob die Eltern bzw. die jeweiligen Betreuungspersonen mit dem Kind gemeinsam frühstücken, zu Mittag essen und das Znacht mit ihm einnehmen?

Plausibilisierung Der Datenschutzbeauftragte kontaktierte den Kinder- und Jugendgesundheitsdienst und klärte die Hintergründe für die Befragung ab: Der Kinder- und Jugendgesundheitsdienst verfügt für derartige Befragungen mit den §§ 140 ff. Schulgesetz über die erforderlichen gesetzlichen Grundlagen. Ob die gestellten Fragen bzw. die damit erhobenen Informationen für die Aufgabenerfüllung des Schularztamtes auch tatsächlich geeignet und erforderlich sind, kann der Datenschutzbeauftragte im Sinne einer Plausibilisierung und auf den konkreten Sachverhalt bezogen prüfen: Es erschien im aktuellen Fall nachvollziehbar, dass derartige Angaben für die Erstellung eines Gesamtbilds über das jeweilige Kind erforderlich sind und es dem Schularztamt erlauben einzuschätzen, ob die Angebote zur Gesundheitsversorgung im Kleinkindalter von den Eltern in Anspruch genommen wird bzw. ob das Bewusstsein für eine regelmässige und ausgewogene Ernährung im Familienkreis besteht und ob allenfalls weitere Sensibilisierungsmassnahmen erforderlich sind.

Wiederholung der Durchimpfungsstudie

Vage gesetzliche Grundlage Das Institut für Sozial- und Präventivmedizin der Universität Zürich führte im Auftrag des Kinder- und Jugendgesundheitsdienstes und der Kantonsärztin eine weitere Studie zum Durchimpfungsgrad von Kleinkindern durch. Wie bereits im Jahr 2010 wurde als gesetzliche Grundlage für die Durchführung der Studie Art. 22 Epidemiengesetz (EpG) angeführt. Nach Auffassung des Datenschutzbeauftragten bietet dieser Art. 22 lediglich eine sehr vage gesetzliche Grundlage[6] für das Bearbeiten von besonderen Personendaten.

Strenge Prüfung Entsprechend hohe Anforderungen stellte der Datenschutzbeauftragte an die Verhältnismässigkeit der Datenbearbeitungen, die aber erfüllt wurden: Die erhobenen Daten sind zur Erreichung des Studienzwecks geeignet und erforderlich. Lediglich die personalisierten Reminder (zweites Schreiben, in welchem die Eltern gebeten werden, die Impfnachweise zu erbringen) sowie die geplanten Telefonanrufe (als weitere Reminder) veranlassten den Datenschutzbeauftragten dazu festzuhalten, dass dieses Vorgehen in Anbetracht der Freiwilligkeit der Studienteilnahme doch mindestens problematisch sei.

Datenschutz in Grossraumbüros

Herausforderung Grossraumbüro Telefongespräche, Akten, die offen auf Schreibtischen liegen und die Bildschirme der PC können in Grossraumbüros dazu führen, dass die Mitarbeiterinnen und Mitarbeiter einer Abteilung Kenntnis von Personendaten erlangen, die von einer anderen Abteilung bearbeitet werden und die sie selbst nicht für ihre Aufgabenerfüllung benötigen. Damit wird gegen das IDG verstossen: Öffentliche Organe dürfen nur diejenigen Personendaten bearbeiten, die sie zur Erfüllung ihrer gesetzlichen Aufgabe benötigen.

Öffentliche Organe dürfen nur diejenigen Personendaten bearbeiten, die sie zur Erfüllung ihrer gesetzlichen Aufgabe benötigen.

Lösungen Nun lässt sich aus datenschutzrechtlicher Sicht nicht sagen, Grossraumbüros seien unzulässig. Vielmehr muss zuerst versucht werden, mit geeigneten (z.B. organisatorischen, baulichen, gestalterischen usw.) Massnahmen dafür zu sorgen, dass der Datenschutz eingehalten wird, dass also Personendaten – und ganz besonders besondere Personendaten – nicht an andere Personen gelangen, die sie nicht zur Aufgabenerfüllung benötigen.

Empfehlungen Der Datenschutzbeauftragte empfiehlt beispielsweise, einzelne und themenverwandte Abteilungen zusammen zu platzieren: Eine Abteilung, welche sich mit Bauten beschäftigt, kann neben einer Abteilung, welche die Planung von Veranstaltungen vornimmt, platziert werden – beide werden in der Regel nur wenige bzw. weniger heikle Personendaten bearbeiten, wohingegen das Care Management möglichst getrennt von anderen Abteilungen untergebracht werden sollte. Verschiedene Abteilungen können hintereinander so platziert werden, dass nicht alle Mitarbeiterinnen und Mitarbeiter jedesmal an den Arbeitsplätzen jener Abteilung vorbeigehen müssen, >

bei der die heikelsten Dossiers auf dem Tisch liegen. Aber auch innerhalb einer Abteilung kann es zu unzulässigen Situationen kommen: Wenn beispielsweise eine Mitarbeiterin der Bewährungshilfe ein «heikles» Telefongespräch mit einem Klienten führt, dann ist es unzulässig, dass der Klient, der mit ihrem Büronachbarn telefoniert oder mit diesem in einer Besprechung ist, den Inhalt des Gesprächs mitbekommt. Möglicherweise kann mit Headsets telefoniert werden, so dass Umgebungsgeräusche (und damit auch das Gespräch der Büronachbarin) nicht aufgenommen werden. Auch mit einer geschickten Positionierung von Mobiliar (Aktenschränken oder mobilen Trennwänden) kann erreicht werden, dass sowohl die Sicht auf die einzelnen Arbeitsplätze eingeschränkt wie auch die Akustik gedämpft wird. Die Sicht auf die Bildschirme kann mittels spezieller Folien eingeschränkt werden: Nur wer in einem bestimmten Winkel auf den Bildschirm blickt, kann wirklich erkennen, woran gerade gearbeitet wird.

Sensibilisierung Und schliesslich gilt es, die Mitarbeiterinnen und Mitarbeiter für den Umgang mit Personendaten in Grossraumbüros zu sensibilisieren. Der Datenschutzbeauftragte kann für entsprechende Schulungen gerne beigezogen werden.

Aufbewahrung und Vernichtung von Dokumenten

Lebenszyklus Wie lange müssen Dokumente, die ein öffentliches Organ zu seiner Aufgabenerfüllung benötigt hat, aufbewahrt werden, wenn ein Geschäft abgeschlossen ist? § 16 IDG hält fest, dass «nicht mehr benötigte Personendaten, die von der gemäss Archivgesetz zuständigen Stelle als nicht archivwürdig beurteilt werden, (…) vom öffentlichen Organ zu vernichten (sind).» § 21 Abs. 1 der Registratur- und Archivierungsverordnung verpflichtet die öffentlichen Organe wiederum «die Unterlagen, die sie nicht mehr benötigen, aus(zusondern) und (…) dem Staatsarchiv an(zubieten), und zwar in der Regel spätestens zehn Jahre nach Abschluss der Unterlagen».

Einzelfallbeurteilung Damit wird deutlich, dass es – ausser in einzelnen Fällen, in denen ein Gesetz eine Aufbewahrungsfrist explizit vorsieht – keine fixe «Standardaufbewahrungsdauer» gibt, sondern lediglich eine *in der Regel* anwendbare Maximalaufbewahrungsfrist: Es muss also von Fall zu Fall entschieden werden. Das öffentliche Organ selbst muss abschätzen, wie lange es einen Informationsbestand regelmässig benötigt, um seine gesetzlichen Aufgaben erfüllen zu können. Ein paar Beispiele, welche die unterschiedlichen Aufbewahrungsfristen illustrieren:

— Ein Universitätsinstitut, das Personendaten für eine bestimmte wissenschaftliche Studie erhoben und ausgewertet hat, kann die Daten nicht unmittelbar nach dem Abschluss dem Archiv anbieten oder vernichten, da während einer bestimmten Frist – die von der Art der Studie und den dafür verwendeten Daten abhängt – zum Beweis der Wissenschaftlichkeit aufbewahren.

Es gibt keine fixe «Standardaufbewahrungsdauer»: Es muss von Fall zu Fall entschieden werden, ob ein Informationsbestand zur Aufgabenerfüllung noch benötigt wird.

— Die Sanität Basel-Stadt erstellt von jedem Rettungseinsatz ein Protokoll. Unabhängig davon, ob die Patientin bzw. der Patient in eine Klinik gebracht wird oder nicht, bewahrt die Sanität die Dokumentation des jeweiligen Einsatzes auf. Für die Sanität Basel-Stadt ist in diesem Kontext das kantonale Gesundheitsgesetz (GesG) einschlägig: § 21 Abs. 1 GesG definiert Fachpersonen im Gesundheitswesen als «alle Personen, die berufsmässig diagnostisch, therapeutisch, pflegend oder betreuend tätig sind und über eine entsprechende Ausbildung verfügen.» Damit fällt die Sanität klar in den Anwendungsbereich des GesG. Entsprechend gelangt die in § 29 Abs. 2 GesG vorgesehene Aufbewahrungsfrist von zehn Jahren auch auf die Sanität Basel-Stadt zur Anwendung.

— Die Sozialhilfe Basel-Stadt prüft die Ersuchen von Personen, die sich in einer persönlichen Notsituation befinden oder nicht in der Lage sind, für den Lebensunterhalt für sich oder ihrer Familie aufzukommen, anhand von Unterstützungsrichtlinien. Kommt die Sozialhilfe Basel-Stadt zum Schluss, dass kein Anspruch auf Unterstützung besteht, so wird das jeweilige Dossier nach ungenutztem Verstreichen der Rekursfrist nach Ablauf eines Jahres dem Staatsarchiv angeboten bzw. vernichtet.

Angebot Der Datenschutzbeauftragte berät die öffentlichen Organe gerne bei der Festlegung der jeweiligen Aufbewahrungsfristen und -modalitäten.

Sperrung der Bekanntgabe von Personendaten an Private

Teil des Persönlichkeitsrechts Jede Person hat das Recht, bei einem öffentlichen Organ die Bekanntgabe ihrer Personendaten an Private schriftlich sperren zu lassen[7]. In diesem Zusammenhang geben verschiedene Punkte immer wieder Anlass zu Fragen an den Datenschutzbeauftragten.

Einzelne Aspekte Im einzelnen kann festgehalten werden:

— Es gibt kein generelles Sperrbegehren. Eine Person, welche die Bekanntgabe ihrer Daten sperren lassen will, muss an jedes öffentliche Organ – konkret: an jede Dienststelle – einzeln ein Gesuch richten[8].

— Das Recht auf Sperrung steht jeder Person voraussetzungslos zu. Welches Interesse sie mit ihrem Gesuch verfolgt, ist irrelevant. Das Sperrrecht muss deshalb auch nicht begründet werden[9].

— Das Sperrrecht richtet sich gegen die Bekanntgabe der Personendaten durch das öffentliche Organ an Private generell. Wird das Sperrecht geltend gemacht, gilt es gegenüber allen Privaten, es kann nicht bloss gegenüber bestimmten Privatpersonen ausgeübt werden[10].

— Die Sperrung nach § 28 IDG betrifft die Datenbekanntgabe an Private. Sie hat keinen Einfluss auf die Datenbekanntgabe an andere öffentliche Organe oder auf andere Bearbeitungsvorgänge als der Bekanntgabe.

— Die Ausübung des Sperrrechts ist kostenlos[11].

— Die betroffene Person hat jederzeit das Recht, um Aufhebung der Sperre zu ersuchen[12].

Durchbrechung der Bekanntgabesperrung

Grundrechtseingriff Die Durchbrechung der Sperre ist ein erheblicher Grundrechtseingriff. Eine Bekanntgabe der Personendaten an Private trotz Sperrung ist nach § 28 Abs. 3 IDG nur zulässig, wenn:

— eine gesetzliche Pflicht besteht, Daten an Private bekannt zu geben[13];

— die Bekanntgabe der Personendaten an Private zur Erfüllung einer gesetzlichen Aufgabe eines öffentlichen Organs zwingend notwendig ist[14] oder

— die um Bekanntgabe ersuchende Person glaubhaft macht, dass die Personendaten zur Durchsetzung ihrer Rechtsansprüche erforderlich sind[15].

Rechtliches Gehör Ist im letztgenannten Fall ein Gesuch nicht von vornherein abzuweisen, ist der betroffenen Person das rechtliche Gehör zu gewähren, d.h. sie ist zur Stellungnahme innert angemessener Frist einzuladen[16]. Trifft innert der eingeräumten Frist keine Stellungnahme ein, muss das öffentliche Organ ohne Kenntnis der Gegenargumente, aber im Bewusstsein, dass einmal bekannt gegebene Informationen nicht wieder zurückzuholen sind, eine Interessenabwägung vornehmen[17].

Der Entscheid, ob ein öffentliches Organ einem anderen einen Onlinezugriff auf seine Informationen einräumen will, trifft die Dateneignerin in eigener Verantwortung.

Entscheid Auf Begehren der betroffenen Person, entgegen deren Stellungnahme die Sperrung durchbrochen werden soll, oder auf Begehren des gesuchstellenden Person, deren Gesuch auf Durchbrechung der Bekanntgabesperrung abgewiesen werden soll, ist der Entscheid in Form einer anfechtbaren Verfügung zu erlassen, womit der Adressatin der Rechtsweg offensteht[18]. Vor dem rechtskräftigen Entscheid dürfen die Daten nicht bekannt gegeben werden.

Onlinezugriffs-Gesuche

Pflicht zur Vorabkontrolle Wenn ein öffentliches Organ einem anderen öffentlichen Organ einen Onlinezugriff auf seine Informationen einräumen will (Abrufverfahren), muss dieses Vorhaben dem Datenschutzbeauftragten zur *Vorabkontrolle* vorgelegt werden[19]. Der Entscheid hingegen, ob ein öffentliches Organ einem anderen einen Onlinezugriff auf seine Informationen einräumen will, trifft nicht der Datenschutzbeauftragte, sondern die Dateneignerin in eigener Verantwortung. Dabei müssen vor allem die gesetzlichen Grundlagen und die Verhältnismässigkeit geprüft werden.

Formalisiertes Verfahren Die Vorabkontrolle eines Onlinezugriffs eines öffentlichen Organs auf Datenbestände eines anderen öffentlichen Organs, ob als Datenansicht oder als Schnittstelle, kann in einem formalisierten Verfahren abgewickelt werden. Dafür haben die Zentralen Informatikdienste (ZID) zusammen mit dem Datenschutzbeauftragten einen Prozess definiert. Das Schema, die Gesuchsformulare sowie ein Leitfaden sind im Intranet abrufbar[20]. Der Datenschutzbeauftragte hat schon vor längerer Zeit vorgeschlagen, das ganze Verfahren ohne Medienbruch elektronisch abzuwickeln, was hoffentlich in absehbarer Zeit möglich werden wird.>

Gesuchsformen Beim formalisierten Abrufverfahren zwischen öffentlichen Organen[21] existieren drei Arten von Gesuchen: das Hauptgesuch, das Erweiterungsgesuch sowie das Verlängerungsgesuch:

— Handelt es sich um ein *Hauptgesuch,* muss der Gesuchsteller die Datenart sowie die Dateneignerin benennen, rechtliche Grundlagen, die den Zugriff rechtfertigen, vorweisen, die Verhältnismässigkeit der Datenbekanntgabe aufzeigen sowie den Zweck des Zugriffs erklären. Des Weiteren wird der Zugriff auf technische und organisatorische Aspekte, insbesondere auf Filtermöglichkeiten hin geprüft.

— Ein *Verlängerungsgesuch* basiert inhaltlich auf den Angaben des Hauptgesuchs. Es werden deshalb nur jene Punkte (nochmals) abgefragt, die für die Genehmigung einer Verlängerung von Bedeutung sind. Voraussetzung für die Zulässigkeit eines Verlängerungsgesuchs ist, dass das diesem zugrunde liegende Hauptgesuch nach dem 1. Mai 2009 genehmigt wurde und sowohl die darin angegebenen rechtlichen Grundlagen als auch die darin angegebenen Filterkriterien im Vergleich zum Hauptgesuch keine Veränderungen erfahren haben. Sollten diese Voraussetzungen nicht erfüllt sein, ist ein neues Gesuch um Zugriff auf Personendaten anderer öffentlicher Organe im Abrufverfahren (Hauptgesuch) zu stellen.

Der Entscheid, ob ein öffentliches Organ einem anderen einen Onlinezugriff auf seine Informationen einräumen will, trifft die Dateneignerin in eigener Verantwortung.

Auch das *Erweiterungsgesuch* basiert inhaltlich auf den Angaben des Hauptgesuchs. Wie beim Verlängerungsgesuch werden nur noch jene Punkte geprüft, die für die Genehmigung einer Erweiterung von Bedeutung sind. Voraussetzung für die Zulässigkeit eines Erweiterungsgesuchs ist auch hier, dass das diesem zugrunde liegende Hauptgesuch nach dem 1. Mai 2009 genehmigt wurde und sich die darin angegebenen rechtlichen Grundlagen im Vergleich zum Hauptgesuch nicht verändert haben.

Sonderfall Wenn Private, denen von Kanton oder Gemeinde eine öffentliche Aufgabe übertragen worden ist und die deshalb datenschutzrechtlich zu einem öffentlichen Organ i.S.v. § 3 Abs. 1 lit. c IDG werden, einen Onlinezugriff auf Datenbestände eines öffentlichen Organs beantragen, kann die Vorabkontrolle nicht in diesem formalisierten Verfahren abgewickelt werden. In solchen Fälle findet eine «gewöhnliche» Vorabkontrolle[22] statt. Dann sind weitere Punkte zu prüfen – etwa die Frage der Informationssicherheit ausserhalb des DANEBS, der Risikoanalyse usw.

Gesetzliche Grundlage für die Psycho-Sozialen Dienste der Kapo

Betriebskonzept Die Psycho-Sozialen Dienste der Kantonspolizei haben im Jahr 2014 mit der Erstellung eines Betriebskonzepts begonnen. Dieses Betriebskonzept bildet in einem zweiten Schritt die Grundlage für die Schaffung der aus rechtstaatlicher Sicht dringend erforderlichen Rechtsgrundlagen für die Tätigkeiten der Psycho-Sozialen Dienste[23]. Der Datenschutzbeauftragte berät den Rechtsdienst der Kantonspolizei und die Leitung der Psycho-Sozialen Dienste bei der Ausarbeitung dieser Bestimmungen (siehe dazu auch Seiten 10 f.).

Gefährderansprache im Kontext häuslicher Gewalt

Neuer Ansatz Die Fachstelle Häusliche Gewalt hat den Datenschutzbeauftragten im Jahr 2014 in die Diskussion um die Ausgestaltung eines Pilotprojekts zur erweiterten Gefährderansprache im Kontext häuslicher Gewalt miteinbezogen. Dabei ging es in einem ersten Schritt um die Klärung der Frage, ob § 37a PolG allenfalls auch die Bekanntgabe von Daten über die Gefährderinnen oder Gefährder bzw. die Opfer an Beratungsstellen zulässt, wenn keine Wegweisung verfügt wurde. Der Wortlaut und die Materialien zu § 37a PolG lassen jedoch keinen Spielraum zu: § 37a PolG kann nur im Falle einer Wegweisung zur Anwendung kommen. Damit fehlt es aktuell an einer gesetzlichen Grundlage, welche eine erweiterte Gefährderansprache zulassen würde – ob diese erweiterte Gefährderansprache jedoch überhaupt die erhofften Resultate bringen kann, ist noch offen.

Pilotversuch Bevor also die notwendige (formell-) gesetzliche Grundlage geschaffen wird, drängt sich ein Pilotversuch auf. Im zweiten Schritt musste daher eruiert werden, wie das Pilotprojekt ausgestaltet werden soll: Unter welchen Voraussetzungen (beispielweise nach der Schwere der Tat, der Häufigkeit von Vorfällen im fraglichen Haushalt, dem Verhalten des Täters/der Täterin gegenüber den Polizistinnen und Polizisten vor Ort usw.) sollen welche Stellen zu welchen Zwecken welche Daten erhalten dürfen, wie soll mit den Daten umgegangen werden, wie soll die Gefährderansprache aussehen, usw.? Wie ist das Pilotprojekt sodann zu evaluieren, wie lange soll das Projekt dauern usw.? Die Arbeiten sind noch immer im Gange, der Datenschutzbeauftragte wird die Arbeitsgruppe auch im Jahr 2015 in datenschutzrechtlichen Fragen beraten. Zu Pilotversuchen generell vgl. Seiten 32 f.

Adressbekanntgaben für Studien

Gesetzliche Grundlage Am 6. Juli 2014 ist der neue § 30a Aufenthaltsgesetz in Kraft getreten. Er ermächtigt die Einwohnerkontrolle, «die zur Kontaktaufnahme für ein bestimmtes Forschungs- oder Präventionsprojekt notwendigen Adressdaten ausgewählter Einwohnerinnen und Einwohner bekannt (zu) geben an: a) öffentliche und private Stellen und Organisationen, die vom Bund oder einer Gemeinde mit der Durchführung eines bestimmten Forschungs- oder Präventionsprojekts beauftragt worden sind oder (an) b) öffentlich-rechtliche Forschungseinrichtungen für ihre Forschungsprojekte.»

Rückgang Im Gegensatz zum Vorjahr wurde der Datenschutzbeauftragte lediglich einmal um seine Beurteilung einer Adressbekanntgabe für Studien gebeten.

Videoüberwachung

Vorabkontrolle Dem Datenschutzbeauftragten wurden im Jahr 2014 zehn Projekte (2013: acht) für den Einsatz von Videoüberwachungsanlagen zur Vorabkontrolle vorgelegt.

Breites Spektrum Davon handelte es sich in neun Fällen um neue Anlagen, wie beispielsweise um die Überwachungskameras im und um das Naturbad Riehen, um die Überwachung des Eingangs des Storchen (Finanzdepartement Basel-Stadt) oder der Berufsfeuerwehr Basel-Stadt und in einem Fall um eine Erweiterung einer bestehenden Anlage. Die Reglemente zum Betrieb der jeweiligen Anlagen finden sich auf den Homepages der verantwortlichen Amtsstellen.

Vernehmlassungen

Vorlagepflicht Nach § 44 lit. f IDG hat der Datenschutzbeauftragte Stellung zu Erlassen zu nehmen, die für den Umgang mit Informationen oder den Datenschutz erheblich sind. Damit er dies tun kann, ist es erforderlich, dass ihm von den verantwortlichen Stellen die Erlassentwürfe vorgelegt werden[24]. 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[25].

Unterschiedlich Die Vorlagepflicht wird in unterschiedlichem Mass eingehalten. Dem Datenschutzbeauftragten wurden im Jahr 2014 15 Erlassentwürfe (2013: 18) zur Stellungnahme vorgelegt. Besondere Erwähnung sollen im Folgenden die Vernehmlassung zur Publikation von Erwachsenenschutzmassnahmen[26] und zum Vorentwurf für ein Bundesgesetz über Medizinialberufe sowie die Vernehmlassungen zu den Schengen-Weiterentwicklungen finden:

Publikation von Erwachsenenschutzmassnahmen

Vergessen Obschon der Datenschutzbeauftragte bei dieser wichtigen Thematik vom zuständigen Departement nicht zur Stellungnahme zuhanden der kantonalen Vernehmlassung eingeladen wurde, konnte via privatim, der Vereinigung der schweizerischen Datenschutzbeauftragten, eine Beurteilung der Bundesvorlage abgegeben werden.

Dem Datenschutzbeauftragten wurden zehn Projekte für den Einsatz von Videoüberwachungsanlagen zur Vorabkontrolle vorgelegt.

Fragwürdige Änderungen Nach altem Recht verfügte Schutzmassnahmen werden in den kantonalen Amtsblättern veröffentlicht. Diese Praxis fiel mit dem neuen Erwachsenenschutzrecht, welches seit dem 1. Januar 2013 in Kraft ist, zur Verhinderung von Stigmatisierungen dahin. Heute werden solche Erwachsenenschutzmassnahmen nicht mehr öffentlich bekannt gegeben. Doch hat jede Person die Möglichkeit, bei der Erwachsenenschutzbehörde Auskunft über das Vorliegen einer Erwachsenenschutzmassnahme zu verlangen, sofern sie ein Interesse glaubhaft machen kann. Die parlamentarische Initiative forderte nun, dass die KESB neu die *Betreibungsämter* über das Vorhandensein einer die Handlungsfähigkeit einschränkenden oder aufhebenden Massnahme informiert. Sodann sollten die Betreibungsämter befugt werden, im Rahmen der Ausstellung von Betreibungsregisterauszügen interessierte Personen über bestehende Erwachsenenschutzmassnahmen, welche gegenüber einer bestimmten Person verfügt wurden, zu informieren.

Unverhältnismässig Der Datenschutzbeauftragte machte in seiner Vernehmlassungsantwort darauf aufmerksam, dass die geplante Änderung des ZGB den Grundsatz der Verhältnismässigkeit verletzen würde. Im Betreibungsregisterauszug dürfen lediglich Aussagen enthalten sein, die sich auf die Handlungsfähigkeit beziehen. Ein möglicher Passus im Betreibungsregisterauszug im Sinne von «Wird die Handlungsfähigkeit beschränkt oder entzogen? Ja, vollständig / Ja, >

teilweise / Nein» wäre jedoch unter Umständen für den Empfänger der Information ungeeignet: Anhand der Aussage «Person ist teilweise handlungsunfähig» lässt sich nicht ableiten, ob die fragliche Person für das konkrete Geschäft handlungsfähig oder eben handlungsunfähig ist. Erforderlich wären hier weitere Informationen wie beispielsweise die Begründung des Entscheids der zuständigen Behörde – was aber wiederum zu stark in die Persönlichkeit der betroffenen Person eingreifen würde.

Vorentwurf Bundesgesetz über Gesundheitsberufe

Politischer Entscheid Obschon der Vorentwurf für ein Bundesgesetz über Gesundheitsberufe keine Regelungen über den Umgang mit Informationen oder den Datenschutz enthielt, zu denen der Datenschutzbeauftragte Änderungen vorschlagen musste, machte der Datenschutzbeauftragte darauf aufmerksam, dass der Entscheid über die Einführung eines aktiven Registers für die vom Gesundheitsberufegesetz geregelten Berufe letztlich politischer Natur sei – dass bei der Ausgestaltung eines solchen Registers aber darauf zu achten sei, dass dieses sich bezüglich der zu erfassenden Daten und den differenzierten Zugriffsberechtigungen mindestens an den Parametern des Medizinalberuferegisters[27] orientiert. Die Veröffentlichung der Daten zu Disziplinarmassnahmen wäre beispielsweise sehr problematisch, ebenso müssten zwingend Fragen zur Übertragung der Registerführung an Dritte geklärt werden.

Das Interesse an bereichsspezifischen datenschutz- und öffentlichkeitsrechtlichen Schulungen blieb erfreulicherweise auf demselben Niveau wie im Vorjahr.

Schengen-Weiterentwicklungen

Anstieg Im Jahr 2014 wurden der Schweiz zwölf Schengen-Weiterentwicklungen (2013: sieben) notifiziert, welche kantonsintern vom Datenschutzbeauftragten geprüft werden konnten. Die Weiterentwicklungen betrafen grösstenteils Anpassungen der Visa-Bestimmungen und warfen unseres Erachtens keine datenschutzrechtlichen Fragestellungen auf.

Medienanfragen

Erfreuliches Medieninteresse Das Medieninteresse an Datenschutzfragen hat im Berichtsjahr leicht abgenommen: Zu 20 Themen (2013: 27) wurde der Datenschutzbeauftragte von Zeitungen und Radiostationen um Stellungnahmen gebeten: Die Durchsuchung von zur Unzeit bereit gestellten Bebbisäcken, der Internetpranger für Hooligans, das Datenleck bei der Universität Basel oder die Frage, ob ein Recht auf Zugang zu den Informationen über alle Aufträge von Departementen an Kommunikationsbüros bestehe – das Interesse der Medien und der Öffentlichkeit an Datenschutz- und Informationsrechtlichen Themen war auch im Jahr 2014 erfreulich gross.

Schulungen, Referate und Publikationen

Stabiles Interesse Das Interesse an bereichsspezifischen datenschutz- und öffentlichkeitsrechtlichen Schulungen hat sich auf dem bisherigen Niveau eingependelt: Der Datenschutzbeauftragte hat im Berichtsjahr sechs (2013: sieben) Schulungen für öffentliche Organe durchgeführt; hinzu kommen noch anderthalb mal so viele Referate und Weiterbildungsbeiträge, die dem gleichen Zweck dienen.

Schulungen Der Datenschutzbeauftragte hat im Berichtsjahr die folgenden sechs Schulungen durchgeführt:

— zwei spezifische Schulungen für die Einwohnerkontrolle, das Pass- und das Fundbüro Basel-Stadt,
— eine Schulung für die Abteilung Prävention der Kantonspolizei,
— einen Workshop anlässlich der 12. Weiterbildungsveranstaltung für ophthalmologisches Assistenzpersonal,
— die Schulung «Das IDG kurz erklärt» und
— das Modul «Datenschutz, Amtsgeheimnis und Archivierung», das Teil des Lehrplans der KV-Lehre in der öffentlichen Verwaltung ist.

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

— am Forum für Suchtfragen zu den datenschutzrechtlichen Fragestellungen im Kontext von Online-Beratungsportalen,
— an der Hochschule für Gestaltung und Kunst zum Thema «un-privacy»,
— an der Konferenz der Archivdirektorinnen und –direktoren zum Thema «Archivierungs- und Datenschutzrecht in den Kantonen»,
— am Symposium on Privacy and Security zum Thema «Schutz durch das Gesetz – berechtigte oder übertriebene Hoffnung» oder
— an der Universität Basel zum Thema «Dublin, Schengen und die EU-Datenschutzrechtsrevision» und
— an einer gemeinsam mit der Juristischen Fakultät der Universität Basel (Prof. Dr. Herbert Zech) durchgeführten Tagung «Wem gehören meine Daten? – ‹Smarte Dinge› als Herausforderung für den Datenschutz» zu den Fragestellungen im Zusammenhang mit dem «intelligenten Haus».

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», der Zeitschrift für Datenrecht und Informationssicherheit aus dem Haus Schulthess Juristische Medien AG[28], und der «digma-Schriften» für Datenrecht aus dem gleichen Verlag. In dieser Funktion verfasst er regelmässig Einführungsartikel[29] sowie den «schlusstakt»[30]. Barbara Widmer hat eine vierteilige, ausführliche Artikelreihe zum Thema «Auftragsdatenbearbeitung»[31] veröffentlicht und publiziert regelmässig in der Rubrik «Der Blick nach Europa und darüber hinaus». Sandra Husi verfasst vierteljährlich die News aus den Datenschutzbehörden[32]. Ausserdem sind in diesem Jahr Beiträge zum Datenschutz in der grenzüberschreitenden Zusammenarbeit[33] und zu vier Artikeln des Bundesdatenschutzgesetzes im entsprechenden Basler Kommentar[34] erschienen.

Dank der Mitarbeit in der Datenschutz-Arbeitsgruppe der KdK und in der Schengen Coordination Group ist sichergestellt, dass die Entwicklungen im EU-Datenschutzrecht zeitnah beurteilt werden können.

Zusammenarbeit

Kantonsübergreifend Die Zusammenarbeit stellte auch im Jahr 2014 ein wesentliches Element der Tätigkeit des Datenschutzbeauftragten dar. So engagierten sich der Datenschutzbeauftragte und seine Mitarbeiterinnen und Mitarbeiter aktiv im privatim-Büro und in den privatim-Arbeitsgruppen «Gesundheit», «Schule» und «ICT». Ausserdem vertraten sie privatim in den Arbeitsgruppen «Standards und Architektur» sowie «Aufbau und Vernetzung» von eHealth Suisse sowie in verschiedenen Gremien zu eGRIS. Schliesslich wurde der Datenschutzbeauftragte auch zu einem Hearing der Nationalen Ethikkommission im Bereich der Humanmedizin eingeladen.

International Weiterhin intensiv beschäftigt hat den Datenschutzbeauftragten auch die Revision des Datenschutzrechts auf EU-Ebene[35] und die Kontrolle der Umsetzung des Schengen-Besitzstandes (SCH-Eval) in der Schweiz, welche im Jahr 2014 durchgeführt wurde[36]. Die Interessen der Kantone in der Datenschutz-Arbeitsgruppe der Konferenz der Kantone, in der SCH-Eval-Vorbereitungsgruppe und in der Schengen Coordination Group (SCG), welche die Joint Supervisory Authority of Schengen (JSA) abgelöst hat, werden ebenfalls vom Datenschutzbeauftragten des Kantons Basel-Stadt vertreten. Damit ist auch sichergestellt, dass die laufenden Entwicklungen im Bereich des Datenschutzes in der EU konzentriert und zeitnah beurteilt werden können.

—

1 Zu den Voraussetzungen, unter welchen Fotos von öffentlichen Organen verwendet werden dürfen, die die Identifikation von einzelnen Personen erlauben, vgl. Seite 41 (Fall 2).
2 Bei Kaphaltestellen wird das Trottoir näher an die Tramschiene «herangezogen», damit ein barrierefreier Einstieg ins Tram möglich wird.
3 § 7 Abs. 1 StVO.
4 PK-IDG/BS-Rudin 2014, § 10 N 9.
5 Vgl. dazu PK-IDG/BS-Rudin 2014, § 7 N 4 ff.
6 Das EpG wurde inzwischen revidiert (BBl 2012 8157); die revidierte Fassung soll nach heutigem Kenntnisstand per 1. Januar 2016 in Kraft treten (<http://www.bag.admin.ch/themen/medizin/03030/03209/03210/index.html?lang=de>, zuletzt besucht am 07.04.2015).
7 § 28 Abs. 1 IDG.
8 PK-IDG/BS-Waldmeier 2014, § 28 N 8.
9 PK-IDG/BS-Waldmeier 2014, § 28 N 9.
10 Eine Einwilligung nach § 21 Abs. 1 lit. c und 2 lit. c IDG durchbricht aber die Sperrung im konkreten Einzelfall; vgl. PK-IDG/BS-Waldmeier 2014, § 28 N 32.
11 PK-IDG/BS-Waldmeier 2014, § 28 N 16.
12 PK-IDG/BS-Waldmeier 2014, § 28 N 31.
13 § 28 Abs. 3 lit. a IDG.
14 § 28 Abs. 3 lit. b IDG.
15 § 28 Abs. 3 lit. c IDG.
16 § 28 Abs. 4 IDG; PK-IDG/BS-Waldmeier 2014, § 28 N 28.
17 PK-IDG/BS-Waldmeier 2014, § 28 N 29.
18 PK-IDG/BS-Waldmeier 2014, § 28 N 30.
19 § 13 IDG in Verbindung mit § 2 Abs. 1 lit. a IDV. Vgl. dazu PK-IDG/BS-Rudin 2014, § 13 N 54 ff.
20 <http://informatik.intranet.bs.ch/verbindliche-vorgaben> unter Informationssicherheit, gültig in der gesamten Verwaltung | Leitfaden: Autorisierungsgesuch für Datenbezug via Kantonalen Datenmarkt gemäss § 6 IDG.
21 I.S.v. § 3 Abs. 1 lit. a und b IDG.
22 I.S.v. § 13 IDG und §§ 2-4 IDV.
23 Siehe dazu bereits TB 2012, 22.
24 PK-IDG/BS-Schilling 2014, § 44 N 29 ff.
25 PK-IDG/BS-Schilling 2014, § 44 N 32.
26 Parlamentarische Initiative 11.449 «Publikation von Erwachsenenschutzmassnahmen».
27 <http://www.bag.admin.ch/themen/berufe/00411/> (zuletzt besucht am 08.04.2015).
28 2014 mit den Schwerpunktthemen Datenschutz in der Schule (Heft 1), Personalisierte Medizin (Heft 2), Internet-Governance (Heft 3) und Tracking (Heft 4).
29 Beat Rudin, «Non scholae sed vitae discimus», digma 2014, 4 f.; ders., Tracking – und was man dagegen tun kann, digma 2014, 136 f.
30 Beat Rudin, Bewahre uns vor dem Bösen – technisch?, digma 2014, 48; ders., Mein Auto – meine Nanny, digma 2014, 132; ders., Big Mother im Kinderzimmer, digma 2014, 188.
31 Barbara Widmer, Auftragsdatenbearbeitung – zum Ersten, digma 2014, 26 ff.; dies., Auftragsdatenbearbeitung – zum Zweiten, digma 2014, 76 ff.; dies., Auftragsdatenbearbeitung – zum Dritten, digma 2014, 112 ff., und dies., Auftragsdatenbearbeitung – zum Vierten, digma 2014, 168 ff.
32 digma 2014, 46 f., 86 f., 131,
33 Sandra Husi-Stämpfli/Beat Rudin, Datenschutz, in: Hans Martin Tschudi/Benjamin Schindler/Alexander Ruch/Eric Jakob/Manuel Friesecke (Hrsg.), Die Grenzüberschreitende Zusammenarbeit der Schweiz, Juristisches Handbuch zur Grenzüberschreitenden Zusammenarbeit von Bund und Kantonen, Zürich 2014, 623 ff.
34 Beat Rudin/Sandra Husi-Stämpfli, Art. 36-39 DSG, in: Urs Maurer-Lambrou/Gabor-Paul Blechta (Hrsg.), Basler Kommentar Datenschutzgesetz (DSG)/Öffentlichkeitsgesetz (BGÖ), Basel 2014.
35 TB 2012, 26 f.
36 Siehe dazu Seiten 30 f.

Aus dem Alltag

Einblicke in die Kontrolltätigkeit

Der Datenschutzbeauftragte – so sieht es § 44 lit. a IDG vor – kontrolliert nach einem autonom aufzustellenden Prüfprogramm die Anwendung der Bestimmungen über den Umgang mit Informationen. Im Jahr 2014 wurden fünf Datenschutz-Prüfungen abgeschlossen und drei neue begonnen. Die umfassenden Prüfberichte gingen an die involvierten öffentlichen Organe. Hier werden die wichtigsten Erkenntnisse zusammengefasst dargestellt.

Übersicht

Abgeschlossen Der Datenschutzbeauftragte hat im Berichtsjahr fünf Prüfungen (2013: 4) abschliessen können:

— eine Datenschutz-Prüfung bei der IV-Stelle Basel-Stadt,

— eine Datenschutz-Prüfung beim Kinder- und Jugenddienst (KJD),

— ein Prüfung zur Passwortqualität und

— zwei «SIS-Kontrollen» bei der Abteilung Verkehr der Kantonspolizei und beim Amt für Justizvollzug, Abteilung Strafvollzug.

Begonnen Mit drei weiteren Datenschutz-Prüfungen konnte begonnen werden – sie werden aber erst im Folgejahr abgeschlossen werden können:

— eine Datenschutz-Prüfung beim Bereich Gesundheitsdienste im Gesundheitsdepartement,

— eine Querschnittsprüfung zum Löschen und Vernichten von Personendaten und

— eine Datenschutz-Prüfung zu Konsul.

Abgeschlossen: Datenschutz-Prüfung bei der IV-Stelle

Sensitive Daten Der Datenschutzbeauftragte hat im Berichtsjahr die 2013 begonnene Datenschutz-Prüfung bei der IV-Stelle Basel-Stadt[1] abgeschlossen. Im Zentrum der Prüfung standen die Zugriffe auf die sensitiven und umfassenden Informationen, die von der IV-Stelle Basel-Stadt zur Erfüllung ihrer gesetzlichen Aufgabe bearbeitet werden. Für die Bearbeitung kommt die Fachanwendung OSIV zum Einsatz. Diese Anwendung wird in sieben Kantonen genutzt. Der Datenschutzbeauftragte hat bezüglich der OSIV-Kontrolle mit den Datenschutzbeauftragten der anderen Kantone zusammengearbeitet. Die IV-Stelle Basel-Stadt ist sich der Sensitivität der von ihr bearbeiteten Informationen bewusst. Teilweise wurde bereits während der Durchführung der Prüfung mit der Umsetzung von Massnahmen seitens der IV-Stelle begonnen.

Feststellungen Der Datenschutzbeauftragte hat innerhalb des von ihm definierten Prüfbereichs unter anderem bei den folgenden Themenbereichen wesentliche Feststellungen gemacht:

— Es besteht Optimierungsbedarf bei den strategischen und taktischen Vorgaben (teilweise mit der entsprechenden operativen Umsetzung) im Bereich der Informationssicherheit.

— Beim Löschen von Informationen sowie bei der Steuerung des Zugriffs durch Mitarbeitende wurde ebenfalls ein Optimierungsbedarf festgestellt.

Abgeschlossen: Datenschutz-Prüfung beim Kinder- und Jugenddienst

Datenschutz-Bewusstsein Der Datenschutzbeauftragte hat im Berichtsjahr beim Kinder- und Jugenddienst (KJD) einen Audit durchgeführt. Das Thema Datenschutz wird beim KJD sehr ernst genommen – verschiedene Prozesse regeln den Umgang mit den sensitiven Personendaten und beim Erstgespräch wird den Klienten immer ein Merkblatt ausgehändigt, welches darlegt, wie die Stelle mit den persönlichen Daten umgeht.

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

— Es besteht Optimierungsbedarf bei den strategischen und taktischen Vorgaben (teilweise mit der entsprechenden operativen Umsetzung) sowie bei den Zuweisungen von Aufgaben, Kompetenzen und Verantwortlichkeiten.

— In Bezug auf die eingesetzte Fachanwendung Tutoris sind Mängel bei der Steuerung der Zugriffsberechtigungen sowie im Bereich Löschung (Vernichtung) der Daten festgestellt worden.

— Obwohl das Zusammenspiel mit der IT-ED gut funktioniert, fehlen hier verbindliche Vereinbarungen und eine klare Zuteilung der Verantwortlichkeiten.

Abgeschlossen: Prüfung zur Passwortqualität

Ausstehende Rückmeldung Die Prüfung im Bereich der Passwort-Qualität[2] wurde im Berichtsjahr abgeschlossen. Die Empfehlungen des Datenschutzbeauftragten sind an die damalige IK (Informatik-Konferenz) und ihre Vorsitzende, Frau Regierungsrätin Eva Herzog, gerichtet. Zu diesem Zeitpunkt war die IK für die übergreifenden gesamtkantonalen Informatikleistungen, die sog. IKT-Basisleistungen, zuständig. Bis zum Ende des Berichtsjahres hat der Datenschutzbeauftragte noch keine Rückmeldung erhalten. Er geht davon aus, dass alle hängigen Geschäfte der IK von der Nachfolgeorganisation, der Konferenz für Organisation und Informatik (KOI), und der Fachstelle Informatiksteuerung und Organisation (ISO) übernommen werden.

Abgeschlossen: Zwei SIS-Kontrollen

Regelmässige Kontrolle Der Datenschutzbeauftragte führte im Jahr 2014 je eine Kontrolle der Nutzung des Schengener Informationssystems (SIS) bei der Abteilung Verkehr der Kantonspolizei sowie beim Amt für Justizvollzug, Abteilung Strafvollzug, durch. 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 Abteilung Verkehr bzw. der Abteilung Strafvollzug benötigt werden und ob entsprechende Berechtigungskonzepte bestehen.

Zweifelhafte Verknüpfung Im Rahmen der Stichprobenkontrollen musste festgestellt werden, dass den wenigsten Mitarbeiterinnen und Mitarbeitern überhaupt bewusst ist, dass mit jeder von ihnen getätigten RIPOL, FABER- oder ZEMIS-Abfrage automatisch auch ein Abgleich mit dem SIS erfolgt. Dieser Umstand rührt daher, dass das SIS für die Aufgabenerfüllung der kontrollierten Stellen keine wesentliche Rolle spielt. Der Datenschutzbeauftragte empfahl daher, die Verknüpfung des SIS mit den nationalen Informationssystemen auf Bundesebene prüfen zu lassen. Weiter konnte festgehalten werden, dass das Datenschutzbewusstsein der Mitarbeiterinnen und Mitarbeiter sehr gross ist, dass aber teilweise die Praxis für die Nutzung des SIS (bzw. der nationalen Informationssysteme) fehlt. Entsprechende Schulungen wurden vom Datenschutzbeauftragten angeregt.

Berechtigungskonzept In organisatorischer Hinsicht musste festgestellt werden, dass noch Defizite bezüglich der Berechtigungskonzepte bestehen. Die beiden kontrollierten Stellen haben nun innerhalb der nächsten zwei Jahre die erforderlichen Arbeiten vorzunehmen.

Keine koordinierte Kontrolle Die Schengen-Koordinationsgruppe der schweizerischen Datenschutzbeauftragten hat auch im Jahr 2014 keine koordinierte Kontrolle durchgeführt[3].

Es konnte festgehalten werden, dass das Datenschutzbewusstsein der Mitarbeiterinnen und Mitarbeiter sehr gross ist.

Begonnen: Datenschutz-Prüfung beim Bereich Gesundheitsdienste

Erste Arbeiten Der Datenschutzbeauftragte hat im Berichtsjahr bei den Gesundheitsdiensten des Gesundheitsdepartements mit der Planungsphase einer Datenschutz-Prüfung begonnen. In der Planungsphase werden aufgrund der jeweils spezifischen Ausgangslage der geprüften Stelle die Prüfgebiete und der Prüfumfang festgelegt. Wie in den meisten Fällen wird hierbei auf erste kurze Gespräche mit den Verantwortlichen und auf vorhandene Dokumentationen zurückgegriffen.

Begonnen: Datenschutz-Prüfung Konsul

Querschnittsprüfung Das Geschäftsverwaltungssystem CMI Konsul hat in der Verwaltung des Kantons Basel-Stadt eine grosse Verbreitung. Bei dieser Querschnittsprüfung werden ausschliesslich die Mandanten für die Geschäftsverwaltung der Departemente und der Regierung berücksichtigt. Die Prüfung hat im Berichtsjahr begonnen und wird im ersten Quartal 2015 abgeschlossen werden.

Begonnen: Prüfung zu Datenlöschung und -vernichtung

Lebenszyklus Aufgrund der Erfahrungen aus den Datenschutz-Prüfungen bei den Dienststellen und Ämtern hat der Datenschutzbeauftragte mit dieser Querschnittsprüfung zur Vernichtung von Personendaten (und Daten, die auf eine Person beziehbar sind) im Berichtsjahr begonnen. Mittels einer Umfrage wird eruiert, ob ein gesamtkantonaler Handlungsbedarf besteht. Bei der Umfrage wird von den Verantwortlichen der jeweiligen (Personen-) Daten mittels einer Selbsteinschätzung der aktuelle Stand erhoben. Die Resultate dieser Selbsteinschätzung erwartet der Datenschutzbeauftragte im ersten Quartal 2015. >

Kontrolltätigkeit im Bereich des Staatsschutzes

Gewohnter modus operandi Die Koordination mit dem Staatsschutzkontrollorgan fand dieses Jahr in Form von informellen Kontakten zu spezifischen Fragestellungen statt.

Begleitet: Schengen-Evaluation der EU in der Schweiz (SCH-Eval)

EU-Kontrolle Die Schweiz wurde im Jahr 2014 zum zweiten Mal im Rahmen des Schengen-Evaluierungsverfahrens daraufhin überprüft, ob die EU-Vorgaben des Schengen-Acquis von den hiesigen Behörden eingehalten werden[4]. Untersucht wurden insbesondere die Bereiche Datenschutz, Aussengrenzschutz (Flughäfen), Schengener Informationssystem, polizeiliche Zusammenarbeit und Visa.

Ablauf Die Schengen-Evaluierung fand in drei Etappen statt.

— In einer ersten Phase im Jahr 2013 verschafften sich die Expertinnen und Experten einen Überblick über die Umsetzung und Anwendung der Schengen-Vorschriften in der Schweiz.

— In der zweiten Phase im ersten Halbjahr 2014 wurden vier Evaluierungsbesuche in der Schweiz sowie ein Evaluierungsbesuch bei zwei Schweizer Vertretungen im Ausland durchgeführt. Die Expertinnen und Experten aus anderen Schengen-Staaten sowie der EU prüften vor Ort, ob die Schweiz die Schengen-Bestimmungen korrekt umsetzt und anwendet. Die Besuche fanden zwischen März und Juli 2014 statt und betrafen im Bereich Datenschutz den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten, den Datenschutzbeauftragten des Kantons Bern sowie den Datenschutzbeauftragten der Kantone Jura und Neuenburg. Der Datenschutzbeauftragte des Kantons Basel-Stadt bereitete für den Fall, dass die Kontrolle in den Kantonen Jura und Neuenburg aus personellen Gründen nicht hätte stattfinden können, als «backup» einen Kontrollbesuch im Kanton Basel-Stadt vor. Im Anschluss an diese Besuche haben die Expertenteams Evaluierungsberichte verfasst, die in der Ratsarbeitsgruppe «SCH-Eval» gutgeheissen wurden.

— Die Schweiz muss in der dritten Phase in der Ratsarbeitsgruppe über allfällige Massnahmen, die sie aufgrund der Empfehlungen getroffen hat, Bericht erstatten.

Abschluss Die Evaluierung wurde mit der Annahme von Schlussfolgerungen durch den Rat der EU auf Ministerebene formell abgeschlossen[5].

Mitwirkung Der Datenschutzbeauftragte vertrat die Interessen der kantonalen Datenschutzbeauftragten in der Arbeitsgruppe, welche die Kontrollen organisierte. Während es im Jahr 2013 galt, die Antworten der kantonalen Datenschutzbeauftragten zu sammeln und zu konsolidieren, mussten im ersten Halbjahr 2014 die Kontrollbesuche sorgfältig vorbereitet und im zweiten Halbjahr 2014 die Kontrollberichte akribisch durchgearbeitet und annotiert werden.

Empfehlungen Das Expertenteam gab (in Bezug auf die beiden kontrollierten Datenschutzbehörden Bern und Neuenburg/Jura) die folgenden Empfehlungen ab[6]:

— Die im Datenschutzgesetz verankerte Unabhängigkeit der Aufsichtsstelle zur Budgetierung müsse noch verstärkt umgesetzt werden;

— gegenüber der Geschäftsprüfungskommission des Grossen Rates sei die verankerte Unabhängigkeit dahin zu verstehen, dass kein Einfluss auf Entscheide erfolgen dürfe;

— die Kontrolle der Abrufe der Kantonspolizei im SIS solle häufiger als bisher und periodisch erfolgen;

— künftig sei diese Kontrolle durch die Aufsichtsstelle selbst und nicht durch externe Beauftragte durchzuführen;

— ebenfalls seien die vom Polizeikommando in Zusammenarbeit mit der Aufsichtsstelle durchgeführten Kontrollen ein gutes Hilfsmittel, dürften jedoch nicht darüber hinwegtäuschen, dass es sich um eine ungenügende Selbstkontrolle handle;

Die Auswirkungen der Empfehlungen der Schengen-Evaluation dürften für den Kanton Basel-Stadt gering, aber gleichwohl nicht zu vernachlässigen sein.

— für den Beizug externer Kontrollbeauftragter sei in Zusammenarbeit mit der Schengener Koordinationsgruppe eine eigene gesetzliche Grundlage zu schaffen und die Unabhängigkeit der Kontrolleure gegenüber der kontrollierten Stelle müsse garantiert sein;

— eine Erhöhung des Personalbestandes der Aufsichtsstelle sei den zuständigen Instanzen vorzuschlagen;

— auf der Internetseite der Aufsichtsstelle seien Informationen über die Rechtsgrundlagen des SIS und Musterschreiben zur Ausübung des Auskunfts- und Berichtigungsrechts aufzunehmen.

Bedeutung der Schengen-Evaluationsempfehlungen für Basel-Stadt

Gering, aber nicht zu vernachlässigen Bezüglich des Kantons Basel-Stadt dürften die Auswirkungen der Empfehlungen gering sein:

— Die gesetzliche Regelung bezüglich der Unabhängigkeit des Datenschutzbeauftragten bei der Budgetierung[7] erscheint uns hinreichend; unzulässig wäre eine materielle Einflussnahme (z.B. im Sinne von: weniger Kontrollen durchführen!).

— Die Unabhängigkeit (auch gegenüber der GPK) ist durch das IDG garantiert[8] und wird auch in der Zusammenarbeit zwischen der GPK und dem Datenschutzbeauftragten so gelebt. Schwächer als bei der Leitung der Finanzkontrolle[9] und bei der Ombudsfrau bzw. beim Ombudsmann[10] ist allerdings die Sicherung der Unabhängigkeit bezüglich der Stellung der oder des Datenschutzbeauftragten[11].

— Der Datenschutzbeauftragte des Kantons Basel-Stadt kontrolliert seit längerem jährlich die SIS-Abrufe von zwei Dienststellen.

— Der Datenschutzbeauftragte des Kantons Basel-Stadt führt seit zwei Jahren die SIS-Kontrollen selber durch, also weder unter Beizug externer Kontrolleure noch gemeinsam mit der Kantonspolizei. Ein Beizug externer Kontrolleure käme nur in Frage, wenn spezifisches, beim Datenschutzbeauftragten nicht vorhandenes (technisches) Knowhow nötig wäre.

— Eine Erhöhung des Personalbestandes drängt sich zurzeit nicht auf.

— Der Datenschutzbeauftragte hat auf seiner Homepage bereits Hinweise zum Zugang zu den in den Informationssystemen des Bundes enthaltenen Personendaten veröffentlicht[12].

—

1 TB 2013, 26.
2 Vgl. TB 2013, 27.
3 Siehe dazu schon TB 2011, 14.
4 Siehe dazu schon TB 2013, 27 f.
5 Siehe dazu auch die Medienmitteilung des Bundesamtes für Justiz unter <https://www.bj.admin.ch/bj/de/home/aktuell/news/2014/2014-11-18.html> (zuletzt besucht am 08.04.2015).
6 Bericht 2014 der Datenschutzaufsichtsstelle des Kantons Bern, 1 f.
7 § 42 IDG i.V.m. § 18 Abs. 2 lit. f GO.
8 § 37 Abs. 1 und § 38 Abs. 1 und 2 IDG.
9 § 4 Abs. 1 Satz 2 FVKG.
10 § 2 Abs. 3 OmbG.
11 § 41 Abs. 1 IDG. Vgl. dazu auch Bericht 12.1046.02,4 (Ziff. 3.1. am Ende).
12 <www.dsb.bs.ch/ihre-rechte.html> (zuletzt besucht am 08.04.2015).

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 Der Grosse Rat hat mit Beschluss vom 13. Oktober 2013 das IDG um § 9a (Voraussetzungen für das Bearbeiten von besonderen Personendaten im Rahmen von Pilotversuchen) ergänzt[1]. Diese Bestimmung ist seit dem 29. Dezember 2013 wirksam.

Zweck Mit § 9a 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 der neuen Regelung in § 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 zwingend vorher im Rahmen einer Vorabkontrolle die Beurteilung der oder des Datenschutzbeauftragten eingeholt werden[4].

§ 9a IDG erlaubt, dass unter engen Voraussetzungen im Rahmen von Pilotversuchen besondere Personendaten bearbeitet werden dürfen, ohne dass die erforderliche formellgesetzliche Rechtsgrundlage besteht.

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 war, 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.

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].

Der JSSK war es ausserordentlich wichtig, dass alle Pilotversuche korrekt im Hinblick auf den Zweck, zu dem sie durchgeführt werden, ausgewertet werden.

Laufende Pilotversuche Der Datenschutzbeauftragte hält fest, dass per 31. Dezember 2014 *kein Pilotversuch* im Sinne von § 9a IDG lief. In Vorbereitung ist, wie bereits im Ratschlag angekündigt, ein Pilotversuch, der bestimmte Aspekte des elektronischen Datenaustauschs zwischen Leistungserbringern im Gesundheitswesen testen soll – als eHealth-Modellversuch im Hinblick auf die Schaffung eines elektronischen Patientendossiers. Eine abschliessende Beurteilung hat der Datenschutzbeauftragte aber noch nicht abgeben können; bis Ende 2014 lag noch kein definitiver Entwurf der Verordnung vor. Zu möglichen Pilotversuchen in anderen Bereichen wurden verschiedene Behörden beraten – es liegen aber noch keine spruchreifen Projekte vor.

Informationszugangsgesuche nach dem Öffentlichkeitsprinzip

Berichtspflicht Nach § 31 Abs. 2 IDV stellt die Staatskanzlei die Statistik über die eingereichten Informationszugangsgesuche der oder dem Datenschutzbeauftragten zur Berichterstattung nach § 50 IDG zu.

Statistik Die Zahlen finden sich – über die gesamte kantonale Verwaltung zusammengefasst – im Statistikteil dieses Tätigkeitsberichts (Seite 36 f.). Aufgeschlüsselt nach Departementen veröffentlicht der Regierungsrat sie in seinem Verwaltungsbericht[8]. >

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.

Rückläufige Gesuchszahlen Die Zahl der schriftlich bei der kantonalen Verwaltung eingereichten Gesuche (18; 2013: 30) ist gegenüber dem Vorjahr um 40% zurückgegangen, gegenüber dem ersten Jahr, in welchem das Öffentlichkeitsprinzip galt, sogar um über 60%. Der Rückgang 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 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 stellen, 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.

Erledigung Im Berichtsjahr wurden 39% der Gesuche ganz oder teilweise gutgeheissen (2013: 77%). 50% der Gesuche (2013: 13%) wurden ganz abgewiesen. Über 11% der Gesuche (2013: 10%) war Ende des Berichtsjahres noch nicht rechtskräftig entschieden. Diese Zahlen stimmen eher nachdenklich, doch auch sie sind ohne weitere Abklärungen schwierig zu interpretieren:

— Hat die Bereitschaft der öffentlichen Organe, sich in die Karten blicken zu lassen, abgenommen?

— Waren die Gesuche «schlechter», 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?

Entwicklung beobachten Der Datenschutzbeauftragte wird die weitere Entwicklung im Auge behalten. Es stellt sich längerfristig die Frage, ob der Paradigmenwechsel vom Geheimhaltungsprinzip mit Öffentlichkeitsvorbehalt zum Öffentlichkeitsprinzip mit Geheimhaltungsvorbehalt stattgefunden hat. Auf eine Pendenz hat der Datenschutzbeauftragte schon hingewiesen[9]: Die absolute Anonymisierungspflicht nach § 30 IDG ist deutlich strenger als die Regelungen in anderen Kantonen und im Bund: Dort dürfen ausnahmsweise Personendaten in nicht anonymisierter Form zugänglich gemacht werden, wenn daran ein überwiegendes öffentliches Interesse besteht[10]. Der Datenschutzbeauftragte wird entsprechende Anpassungsbemühungen aktiv unterstützen.

Es stellt sich längerfristig die Frage, ob der Paradigmenwechsel vom Geheimhaltungsprinzip mit Öffentlichkeitsvorbehalt zum Öffentlichkeitsprinzip mit Geheimhaltungsvorbehalt stattgefunden hat.

Statistik zu den Geschäften des Datenschutzbeauftragten

Statistik Die Statistik zu den Geschäften des Datenschutzbeauftragten im Jahr 2014 (mit Vorjahresvergleich) findet sich auf den Seiten 36 f.

Stabile Geschäftszahl Im Berichtsjahr sind 400 Geschäfte neu eröffnet worden (2013: 403); die Zahl ist damit minim geringer als im Vorjahr (-3 Geschäfte, -0.75%).

Komplexere Fälle Der Anteil komplexer Geschäfte an allen Beratungen ist auf 15% (2013: 11%) gestiegen. Gegenüber dem Vorjahr entspricht dies einer Zunahme um 4 Prozentpunkte. Darunter fallen insbesondere grössere Vorabkontrollen.

Rasche Erledigung Von den nicht-komplexen Beratungsgeschäften konnten 58% (2013: 54%) innert 14 Tagen seit Eingang abgeschlossen werden.

Audits Die Zahl der im Berichtsjahr abgeschlossenen Audits stieg auf 5 (2013: 4). Weitere Details dazu finden sich auf den Seiten 28 ff.

Schulungen Im Berichtsjahr wurden 6 Schulungen für öffentliche Organe durchgeführt (2013: 7). Hinzu kommen noch anderthalb mal 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. Auch weiterhin werden über die Hälfte der Geschäfte durch eine Anfrage kantonaler öffentlicher Organe initiiert. Details dazu finden sich auf Seite 37.

Involvierte Stellen Bei den in die Geschäfte involvierten Stellen gab es einzig eine Verschiebung vom Finanzdepartement (-8 Prozentpunkte) zum Justiz- und Sicherheitsdepartement (+8 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 2014, § 9a N 1 ff., insb. N 6 ff.
4 § 9a Abs. 1 IDG (Einleitungssatz); zur Vorabkontrolle: § 13 IDG, §§ 2-4 IDV; PK-IDG-Rudin 2014, § 13 N 1 ff.
5 § 9a Abs. 5 IDG.
6 PK-IDG/BS-Husi 2014, § 9a N 23.
7 Bericht 13.0739.02, 5 f.
8 Zahlen aufgeschlüsselt nach Departementen: Jahresbericht 2014 (noch nicht publiziert), Vorabdruck, Ziff. [4.2.1], Präsidialdepartement, Staatskanzlei, Öffentlichkeitsprinzip, S. 161.
9 PK-IDG/BS-Rudin 2014, § 30 N 21 ff.
10 Art. 9 BGÖ i.V.m. Art. 19 Abs. 1bis DSG.

Aus dem Alltag

Statistische Auswertungen 2014 (mit Vorjahresvergleichen)

A Geschäfte

	2014		2013		2012		2011	
	Anzahl	%	Anzahl	%	Anzahl	%	Anzahl	%
Anzahl eröffnete Geschäfte	400		403		366		341	
prozentuale Veränderung gegenüber Vorjahr		-1		10		7		6

B Indikatoren gemäss Budget

	2014		2013		2012		2011	
	Anzahl	%	Anzahl	%	Anzahl	%	Anzahl	%
Anteil komplexer Beratungen								
prozentualer Anteil an allen Beratungen		15		11		9		7
Innert 14 Tagen abgeschlossene nicht-komplexe Beratungen								
prozentualer Anteil an allen nicht-komplexen Beratungen		58		54		50[1]		61[1]
Durchgeführte Audits/Assessments								
Anzahl durchgeführte Audits/Assessments	5		4		2		2	
Durchgeführte Schulungen für öffentliche Organe								
Anzahl durchgeführte Schulungen	6		7		11		12	

[1]Die Zahlen für 2012 und 2011 waren im Tätigkeitsbericht 2012 leider vertauscht worden.

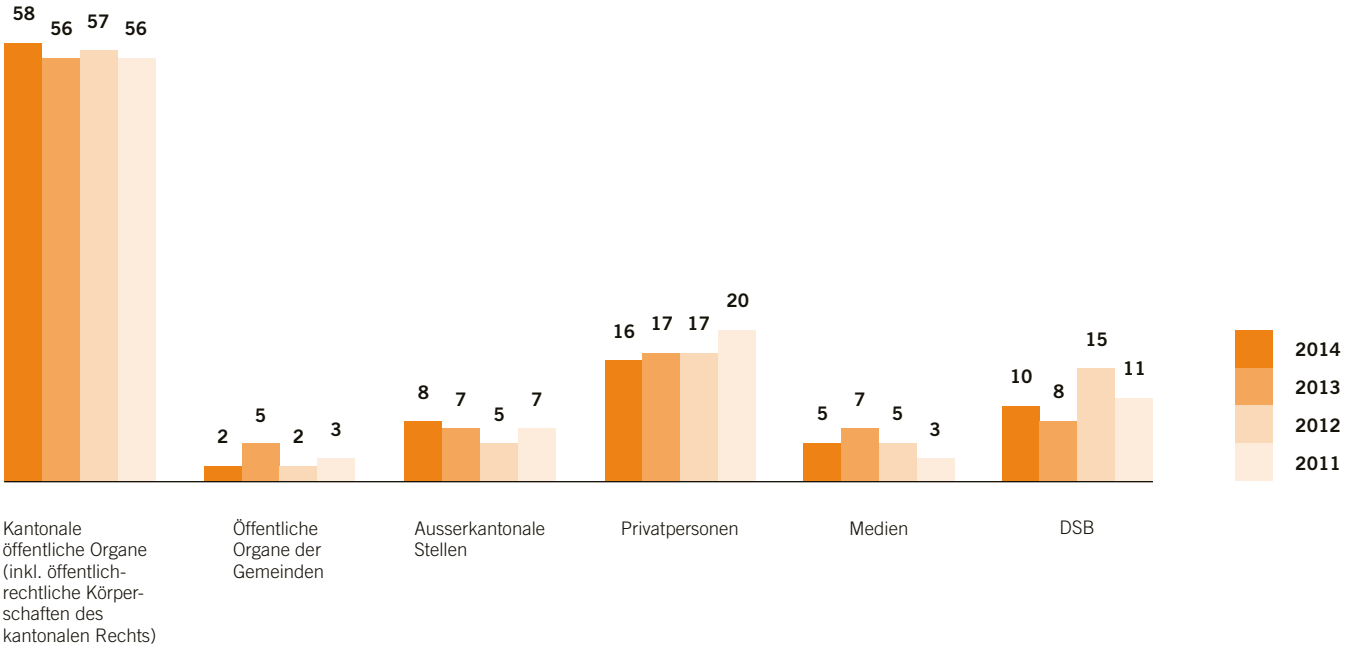
Indikatoren erfasst ab 2011.

C Öffentlichkeitsprinzip

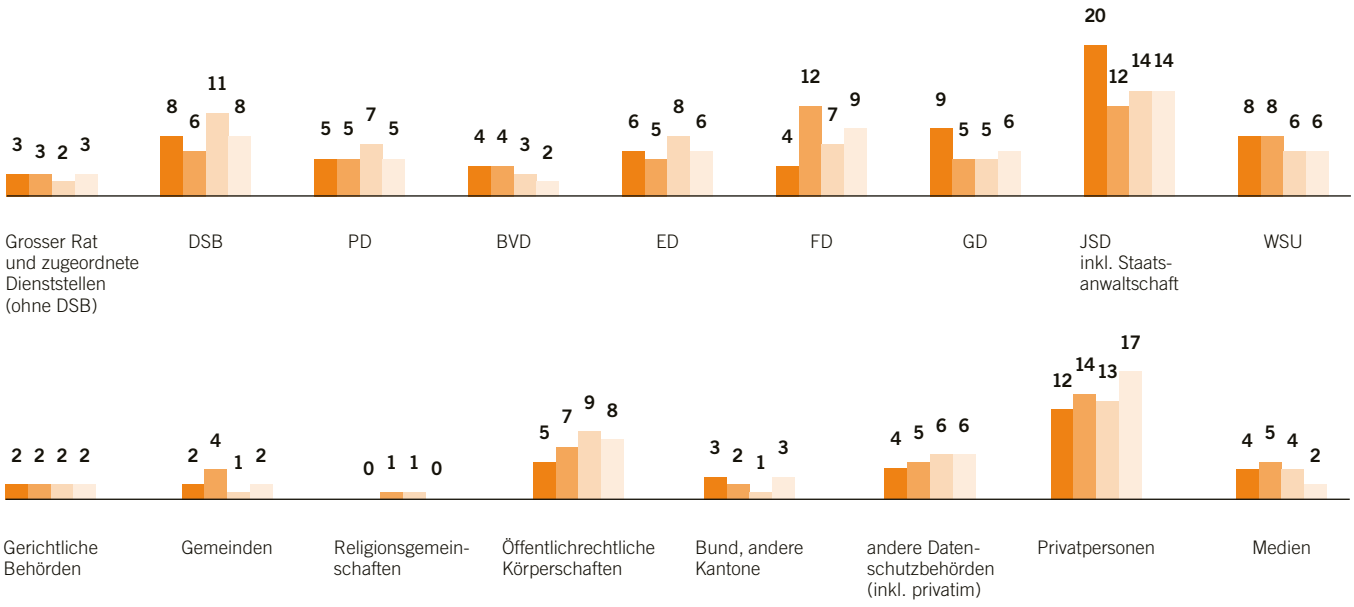
	2014		2013		2012	
	Anzahl	%	Anzahl	%	Anzahl	%
Eingereichte Gesuche nach § 25 IDG						
Anzahl eingereichte Gesuche	18		30		48	
prozentuale Veränderung gegenüber Vorjahr		-40		-38		100
Behandlung der Gesuche nach § 25 IDG						
Anzahl gutgeheissener Gesuche		28		37		60
Anzahl teilweise gutgeheissener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

Öffentlichkeitsprinzip ab 2012.
Zahlen erfasst durch die Staatskanzlei aufgrund der Meldungen der Departemente (§ 31 IDV).
Zahlen aufgeschlüsselt nach Departementen: Jahresbericht 2014 (noch nicht publiziert), Vorabdruck, Ziff. [4.2.1], Präsidialdepartement, Staatskanzlei, Öffentlichkeitsprinzip, S. 161.

D Initianten: Veranlasser der Geschäfte (A) in %



E In die Geschäfte (A) involvierte Stellen in %



Fälle

Fall 1 Der Betreibungsregisterauszug des Taxihalters

Ein Taxihalter erhält vom Taxibüro die Aufforderung, seine Betreibungen in der Höhe von rund CHF 350000 auf maximal CHF 100000 zu reduzieren. Andernfalls müsse ihm per Ende Jahr die Taxihalterbewilligung entzogen werden. Der Taxihalter ist empört: Er habe weder Auskunft über seine Schulden gegeben noch eingewilligt, dass das Taxibüro Auskünfte über seine Betreibungen einholen dürfe. Bearbeiten das Taxibüro und/oder das Betreibungsamt widerrechtlich Personendaten?

Die Daten über die Betreibungen des Taxihalters stammen vom Betreibungsamt. Waren also die rechtlichen Voraussetzungen erfüllt, dass das Betreibungsamt die zur Diskussion stehenden Daten an das Taxibüro bekanntgeben durfte?

Das IDG erlaubt die Bekanntgabe von Personendaten, wenn eine gesetzliche Bestimmung dazu verpflichtet oder ermächtigt, oder, wenn dies zur Erfüllung einer gesetzlichen Aufgabe erforderlich ist oder, wenn (im Einzelfall) die betroffene Person der Bekanntgabe ausdrücklich zugestimmt hat[1].

Das Taxibüro erteilt die Bewilligung für die Erbringung von Taxi-Dienstleistungen[2]. Die Erteilung einer Taxihalterbewilligung ist an die Voraussetzung geknüpft, dass keine Verlustscheine aus den letzten fünf Jahren und keine «Betreibungen in bedeutendem Umfang»[3] bestehen. Was unter «bedeutendem Umfang» zu verstehen ist, konkretisiert die Taxiverordnung: Danach können offene Betreibungen in der Gesamthöhe eines Viertels des durch den Taxibetrieb voraussichtlich erzielbaren Jahresumsatzes zur Verweigerung der Bewilligung bzw. zum Entzug der Bewilligung führen[4].

Damit das Taxibüro die gesetzlich vorgesehene Prüfung, welche der Erteilung bzw. der Aufrechterhaltung einer Taxihalterbewilligung vorangehen muss, durchführen kann, ist es auf die Daten des Betreibungsamtes angewiesen.

Möglich wäre es zwar, dass das Taxibüro vom Taxihalter verlangt, dass er einen aktuellen Betreibungsregisterauszug beibringt. Das wäre aber mit Umtrieben und Kosten für den Taxihalter verbunden – und wenn er den Auszug nicht beibringt, müsste wohl das Betreibungsamt die Daten bekannt geben dürfen, da ein Bewilligungsentzug bloss wegen der Nichteinhaltung der Mitwirkungspflicht wohl unverhältnismässig wäre.

Die Bekanntgabe der Daten vom Betreibungsamt an das Taxibüro erscheint somit für dessen gesetzliche Aufgabenerfüllung erforderlich, die Voraus-setzungen von § 21 Abs. 1 lit. b IDG sind damit erfüllt.

Das Einholen einer Einwilligung der von der Bekanntgabe der Betreibungsregister Daten betroffenen Person ist in diesem Fall nicht angezeigt, ja wäre sogar trügerisch: Selbst wenn die betroffene Person ihre Einwilligung in den Informationsaustausch zwischen Betreibungsamt und Taxibüro verweigern würde, könnte das Taxibüro gestützt auf die Rechtsgrundlagen im Taxigesetz bzw. in der Taxiverordnung die Daten trotzdem vom Betreibungsamt herausverlangen. Die Einwilligung würde damit bloss zum pro forma-Akt degradiert werden[5].

Ergebnis

Damit das Taxibüro prüfen kann, ob ein Bewerber die gesetzlich vorgesehenen Voraussetzungen für die Erbringung von Taxi-Dienstleistungen erfüllt, muss es auch die Höhne allfällig bestehender Betreibungen in Erfahrung bringen können. Das Taxibüro verfügt mit § 6 Taxigesetz und § 4 Abs. 2 Taxiverordnung über die von § 21 Abs. 1 lit. b IDG vorgesehenen gesetzlichen Grundlagen, damit das Betreibungsamt dem Taxibüro die fraglichen Personendaten bekannt geben kann.

1 § 21 IDG.
2 § 4 Taxigesetz i.V.m. § 1 Taxiverordnung.
3 § 6 Abs. 3 Taxigesetz.
4 § 4 Abs. 2 Taxiverordnung.
5 Siehe dazu schon TB 2012, 36.

Fall 2 Gemütlicher Feierabend am Rheinbord – im Internet?

Eine Website kann auf den ersten Blick attraktiver gemacht werden, wenn auf der ersten Seite ein passendes Bild die Leserin oder den Leser begrüsst. Wie wär's mit einer Aufnahme vom Rheinbord, wo sich fröhliche Menschen am Feierabend niedergelassen haben? Eine Fotografie mit Menschen drauf – im Internet? Darf ein öffentliches Organ solche Bilder auf seiner Website publizieren?

Ein öffentliches Organ darf ohne gesetzliche Grundlage keine Personendaten veröffentlichen. Eine gesetzliche Grundlage, die das Publizieren von solchen Fotos mit Personen erlaubt, liegt nicht vor[1]. Ebensowenig ist eine gesetzliche Aufgabe ersichtlich, die das öffentliche Organ nur erfüllen kann, indem es solche Fotos im Internet – also zugänglich für eine Weltöffentlichkeit – veröffentlicht[2]. Eine Rechtfertigung könnte schliesslich durch die Zustimmung der betroffenen Personen erfolgen[3]. Ausser wenn mit «Models» gearbeitet wird, liegt eine solche Einwilligung meistens nicht vor (und kann faktisch in fast allen Fällen auch nicht nachträglich eingeholt werden).

Wenn die abgebildeten Personen nicht identifizierbar sind, liegen keine Personendaten vor[4] – dann ist die Veröffentlichung aus Datenschutzsicht kein Problem. *Wann* eine Person nicht mehr identifiziert werden kann, kann aber nicht in absoluten Zahlen bestimmt werden (etwa im Sinne von: «Kopf kleiner als 40×20 Pixel»). Es kommt also darauf an, in welcher Grösse und mit welcher Auflösung das öffentliche Organ ein Bild auf seiner Website publiziert und wie die Person abgebildet ist (von vorne, von der Seite, von hinten, halb verdeckt, mit weiteren identifizierenden Merkmalen…).

Wenn ein öffentliches Organ ein Bild veröffentlicht, dann trägt es dafür die informations- und datenschutzrechtliche Verantwortung[5] (wenn der Fotograf das Bild vorher schon publiziert hat, trägt er dafür die Verantwortung – das befreit das öffentliche Organ aber nicht von seiner Verantwortung für die erneute Publikation). Das heisst: Die Leitung des öffentlichen Organs muss das Risiko übernehmen, dass jemand geltend macht, sein Recht am eigenen Bild werde durch die Publikation verletzt, weil er erkennbar sei. Dabei steht wohl in der Regel weniger ein Schadenersatzanspruch im Vordergrund als vielmehr der Reputationsverlust, wenn jemand (unter Umständen medial verstärkt) geltend macht, dass der Kanton die Rechte seiner Bürgerinnen und Bürger mit Füssen trete. Denkbar ist natürlich auch mehr: Grösser würde das Problem beispielsweise, wenn eine Frau aufgrund der Publikation feststellt, dass ihr Partner sich an der Rheinpromenade nicht mit ihr, sondern mit einer Nebenbuhlerin «abgibt», und den Mann aus ihrer Wohnung weist …

Es kann sein, dass sich niemand an einem Bild stört – Glück gehabt. Es kann aber durchaus auch sein, dass jemand auf seine Rechte pocht. Dieses Risiko ist reduzierbar, indem das öffentliche Organ Ausschnitt, Grösse und Auflösung so wählt, dass möglichst keine Personen erkennbar sind.

Ergebnis

Ein öffentliches Organ darf das Bild einer Person nur veröffentlichen, wenn es dafür über eine Rechtfertigung verfügt: über eine gesetzliche Grundlage oder über die ausdrückliche Einwilligung der betroffenen Person. Ohne eine solche Rechtfertigung dürfen Bilder nur so publiziert werden, dass ohne spezifisches Zusatzwissen keine Personen erkennbar sind.

1 Sog. unmittelbare gesetzliche Grundlage im Sinne von § 21 Abs. 1 (bzw. bei besonderen Personendaten: Abs. 2) lit. a IDG; vgl. dazu PK-IDG-BS-Rudin 2014, § 21 N 5 bzw. 36.

2 Sog. mittelbare gesetzliche Grundlage im Sinne von § 21 Abs. 1 (bzw. bei besonderen Personendaten: Abs. 2) lit. b IDG; vgl. dazu PK-IDG-BS-Rudin 2014, § 21 N 6 ff. bzw. 37.

3 § 21 Abs. 1 (bzw. bei besonderen Personendaten: Abs. 2) lit. c IDG; vgl. dazu PK-IDG-BS-Rudin 2014, § 21 N 21 ff. bzw. 50 ff.

4 § 3 Abs. 3 IDG; vgl. dazu PK-IDG-BS-Rudin 2014, § 3 N 17 ff., insb. 26 ff.

5 § 6 IDG; vgl. dazu PK-IDG-BS-Rudin 2014, § 6 N 4 ff.

Fall 3 Wenn die Staatsanwaltschaft beim Unispital nach Daten fischt …

Das Universitätsspital wird von der Staatsanwaltschaft kontaktiert: Man fahnde nach mutmasslichen Beteiligten an einem Raufhandel bzw. nach den Tätern einer schweren Körperverletzung. Das Spital solle alle Personen melden, die an drei bestimmten Tagen eine Handverletzung behandeln liessen. Darf das Unispital einfach alle diese Personen melden?

Ein mutmasslicher «Mit-Raufhändler» solle sich während des Tathergangs eine Verletzung an der Hand (die Staatsanwaltschaft vermutet einen Bruch) sowie eine Schnittwunde zugezogen haben. Die Staatsanwaltschaft bittet um Bekanntgabe aller Personen, die sich im Zeitraum von drei bestimmten Tagen im letzten Monat mit einer Handverletzung im Universitätsspital in Behandlung begeben haben.

Das Unispital darf Personendaten bekannt geben, wenn es dafür über eine gesetzliche Grundlage[1] verfügt. Das Gesundheitsgesetz erlaubt die Datenbekanntgabe an die Strafuntersuchungs- und Strafverfolgungsbehörden bei Verdacht auf die Erfüllung von bestimmten Straftatbeständen[2], u.a. bei schwerer Körperverletzung[3]. Zu beachten gilt es aber Folgendes:

Der Tatbestand beim Raufhandel ist im Strafgesetzbuch wie folgt umschrieben: «Wer sich an einem Raufhandel beteiligt, der den Tod oder die Körperverletzung eines Menschen zur Folge hat, wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft. Nicht strafbar ist, wer ausschliesslich abwehrt oder die Streitenden scheidet»[4]. Damit kann ein Raufhandel schon bei einer einfachen Körperverletzung gegeben sein, während die Befreiung vom Berufsgeheimnis nach dem Gesundheitsgesetz erst bei einem Verdacht auf Begehung einer *schweren* Körperverletzung greift[5]. Das Unispital ist verpflichtet, bei solchen Anfragen genau zu prüfen, ob die Voraussetzungen für die Befreiung vom Berufsgeheimnis nach dem Gesundheitsgesetz erfüllt sind (in casu: sich bei der Staatsanwaltschaft zu vergewissern, dass beim verfolgten Raufhandel wirklich eine schwere Körperverletzung begangen worden sei).

Ausserdem muss ein Datenbearbeiten nicht nur auf einer gesetzlichen Grundlage basieren, sondern es muss auch verhältnismässig sein. Gefordert ist u.a., dass die Datenbearbeitung zur Erfüllung der gesetzlichen Aufgabe erforderlich, bei besonderen Personendaten (wie hier) zwingend notwendig sei. In diesem Kontext erscheint das Kriterium «Behandlung einer Person mit Handverletzung (Bruch, Schnittwunde) an drei bestimmten Tagen im letzten Monat» reichlich unbestimmt. Darunter würden jeder Greis oder jede junge Frau fallen, die sich bei einem Sturz eine Handverletzung zugezogen haben – auch wenn sie in keiner Weise ins Täterbild passen würden. Es ist nicht davon auszugehen, dass die Staatsanwaltschaft bei allen ihr durch das Spital gemeldeten Personen – inkl. dem Greis und der jungen Frau – Nachforschungen anstellen würde und insbesondere diesen gegenüber transparent darlegen würde, dass sie solche Nachforschungen über sie anstelle. Das würde sie logischerweise nicht tun, weil sie wohl aufgrund weiterer ihr vorliegender Informationen keinen Greis und keine junge Frau sucht. Das Verhältnismässigkeitsprinzip gebietet es deshalb, dass der Kreis der zu meldenden Patientinnen und Patienten eingegrenzt wird, indem mindestens das Geschlecht und eine Alterskategorie genannt werden.

Ergebnis

Zu allgemeine Anfragen verletzen das verfassungsrechtliche Verhältnismässigkeitsprinzip, das auch in der Strafverfolgung gilt. Das angefragte öffentliche Organ muss deshalb der anfragenden Amtsstelle eine Eingrenzung des Kreises der zu meldenden Personen verlangen.

1 Im Sinne von § 21 Abs. 2 lit. a oder b IDG; die alternativ vorgesehene Rechtfertigung der Datenbekanntgabe durch Einwilligung der betroffenen Personen fällt in dieser Konstellation faktisch wohl ausser Betracht.
2 § 27 Abs. 3 GesG.
3 § 27 Abs. 3 lit. b GesG
4 Art. 133 StGB.
5 § 27 Abs. 3 lit. b GesG.

Fall 4 Ein Datenleck – was tun?

Der Albtraum jedes Verantwortlichen eines IT-Systems: Es wird ein Datenleck entdeckt. Unberechtigte können auf Daten, die nicht öffentlich zugänglich sein sollten, zugreifen. Welche Massnahmen hat das öffentliche Organ in einem solchen Fall zu treffen?

Es wird entdeckt, dass – warum auch immer – Daten eines öffentlichen Organs fälschlicherweise über eine gewisse Zeitdauer öffentlich zugänglich waren. So geschah es etwa bei der Universität, als Bewerbungsunterlagen aus vergangenen Berufungsverfahren über längere Zeit offen im Internet standen[1]. Es ist aber denkbar, dass ein solcher Fehler bei irgendeinem öffentlichen Organ passiert und Personendaten, die nach dem Öffentlichkeitsprinzip nicht zugänglich sein dürf(t)en, trotzdem öffentlich zugänglich sind. Was muss ein öffentliches Organ tun, wenn es einen solchen Fehler selber feststellt oder von jemandem darauf hingewiesen wird?

Ruhe bewahren. Wenn das öffentliche Organ seine Hausaufgaben gemacht hat, sind Notfallpläne für diesen Fall vorbereitet. Dabei sollten mindestens die folgenden Massnahmen vorgesehen sein, wobei über die Reihenfolge im konkreten Einzelfall zu entscheiden ist:

— *Beweissicherung:* Damit eruiert werden kann, was zum Fehler geführt hat, muss eine Beweissicherung stattfinden. Wenn sofort alles gelöscht wird, kann unter Umständen nicht mehr rekonstruiert werden, was passiert ist – und man segelt im Blindflug aufs nächste Leck zu.

— *Information der vorgesetzten Behörden* (Leitung, Kommunikation, IT): Ein Datenleck erweckt grosse mediale Aufmerksamkeit. Die involvierten Stellen dürfen nicht unvorbereitet gelassen werden.

— *Information des Datenschutzbeauftragten:* Werden schutzwürdige Interessen offensichtlich gefährdet oder verletzt, so kann der Datenschutzbeauftragte eine verbindliche Weisung erlassen und als Sofortmassnahme anordnen, dass das öffentliche Organ die Bearbeitung einstellt oder einschränkt[2].

— *Stopfen des Lecks:* Die zuständige IT-Abteilung soll Massnahmen treffen, um zu verhindern, dass das Leck weiterhin besteht (Server vom Netz nehmen, Daten löschen[3]).

— *Schadenbegrenzung:* Auch wenn die eigenen Server vom Netz genommen wurden – Google beispielsweise hat von vielen Daten eine Kopie erstellt und diese auf eigenen Datenträgern gespeichert. Es muss deshalb bei Google[4] die Löschung dieser Kopien (inkl. Google-Cached-Funktion) beantragt werden.

— *Information der Betroffenen:* Nach dem Grundsatz von Treu und Glauben sind die Personen, deren Daten öffentlich zugänglich waren, auch ohne ausdrückliche gesetzliche Verpflichtung[5] zu informieren[6], damit sie ebenfalls Schadensbegrenzungsmassnahmen treffen können. Wenn beispielsweise aus einem Bezahlsystem die Informationen einer grossen Zahl von Kreditkarten zugänglich waren, kann es auch angezeigt sein, Dritte (das Kreditkartenunternehmen) zu informieren, weil nur so eine rasche Sperrung der Karten möglich ist[7].

Nur einer Illusion darf man sich nicht hingeben: Glauben, dass es sicherer sei, den Vorfall zu vertuschen.

Ergebnis

Wenn ein Datenleck festgestellt wird, sind sofort die geeigneten Massnahmen zur Beweissicherung, zur Information der vorgesetzten Behörden und des Datenschutzbeauftragten, zur Schadensbegrenzung und zur Informationen der Betroffenen zu ergreifen. Wenn das öffentliche Organ seine Hausaufgaben gemacht hat, sind entsprechende Notfallpläne vorhanden.

1 «Heikles Datenleck an der Universität Basel», NZZ vom 31. März 2014, 45, <http://campus.nzz.ch/das-grosse-ganze/heikles-datenleck-der-universitaet-basel>; «1526 heikle Datensätze versehentlich publiziert», bz Basel (Nordwestschweiz) vom 1. April 2014, 21.

2 Art. 47 Abs. 4 IDG; vgl. dazu PK-IDG/BS-Schilling 2014, § 47 N 2 ff. und 8.

3 Ohne aber die Beweissicherung (siehe oben beim ersten Spiegelstrich) zu vereiteln.

4 Via Googles Webmastertools (<https://www.google.com/webmasters>): Eröffnung eines Accounts, Registrierung der verwalteten Websites, Eingabe der Originallinks (nicht der Links, die zum Cache-Inhalt führen).

5 Z.B. die ‹data breach laws› von US-Bundesstaaten.

6 PK-IDG/BS-Rudin 2014, § 9 N 50.

7 PK-IDG/BS-Rudin 2014, § 9 N 50; Rosenthal/Jöhri 2008, Art. 4 N 16.

Fall 5 Office 365 datenschutzkonform einsetzbar – ein Freibrief für die Cloud?

privatim hat Microsoft überzeugen können, die Vertragsbestimmungen für die Schweizer Bildungsinstitutionen so anzupassen, dass der Einsatz von Microsoft Office 365, einer Cloud-Lösung, datenschutzkonform möglich ist. Dürfen nun Schulen ohne weiteres beliebige Daten über Schülerinnen und Schüler (und über Lehrpersonen) in der Cloud bearbeiten? Und sollen sie die Cloud-Lösung den Lehrpersonen und Eltern der Schülerinnen und Schüler empfehlen?

privatim, die Vereinigung der schweizerischen Datenschutzbeauftragten, hat zwei Merkblätter zur Cloud-Nutzung durch öffentliche Organe und durch Schulen[1] herausgegeben. Daraufhin hat sich Microsoft an privatim gewandt. Nach zahlreichen Gesprächen hat privatim erreicht, dass Microsoft seine Vertragsbedingungen für Bildungsinstitutionen so anpasst, dass der Einsatz von Office 365 im Schulbereich datenschutzkonform möglich ist. Insbesondere wurde erreicht, dass die Datenbearbeitung in Europa erfolgen muss, dass Kontrollmöglichkeiten bestehen, dass schweizerisches Recht anwendbar und der Gerichtsstand in der Schweiz gegeben ist. Ist damit nun jede beliebige Datenbearbeitung von Schulen in der Cloud ohne weiteres zulässig?

Nein.

Nach dem IDG trägt dasjenige öffentliche Organ, das die Informationen zur Erfüllung seiner gesetzlichen Aufgaben bearbeitet, die Verantwortung für den Umgang mit Informationen[2]. Es muss u.a. seine Informationen durch angemessene organisatorische und technische Massnahmen z.B. vor dem Zugriff von Unberechtigten schützen[3]. Ein öffentliches Organ muss sich also genau überlegen, welche Daten es in einer «public cloud» bearbeitet, z.B. speichert. Dass Lehrpersonen ihre Unterrichtsmaterialien (Lehrstoff, Folien, Bilder usw.) dort ablegen, ist datenschutzrechtlich unbedenklich. Sobald sie (oder die Schulverwaltung) aber Personendaten über Schülerinnen und Schüler (oder auch über Lehrpersonen) bearbeiten, wird es heikler.

Da bei Cloud-Lösungen – mindestens bei sog. «public cloud»-Lösungen – nicht ausgeschlossen ist, dass eben auch Unberechtigte auf die Informationen zugreifen können, müssen zusätzliche Informationssicherheitsmassnahmen getroffen werden. Bei «gewöhnlichen» Personendaten mag es ausreichen, alle Personendaten lokal zu speichern, wenn dies möglich ist, oder eine in der Lösung angebotene Verschlüsselungsmöglichkeit zu nutzen[4]. Da bei Office 365 aber ein Schlüssel bei Microsoft verbleibt, müssen besondere Personendaten oder Daten, die einem Berufsgeheimnis unterstehen, vor der Ablage auf dem Speicher von Microsoft mit einer Zusatzsoftware verschlüsselt werden. Dabei ist zu beachten, dass auch an und für sich nicht sensitive Daten zu besonderen Personendaten werden können, wenn die Menge (z.B. ein über Jahre mit Informationen angereichertes Schülerprofil) sie zu einem Persönlichkeitsprofil[5] werden lässt.

Falls dereinst auch die Schülerinnen und Schüler und Eltern das Software-Paket gratis angeboten bekommen, wenn die Schule bereits Lizenznehmerin ist, dann empfehlen wir der Schule, auch die Eltern darauf aufmerksam zu machen, dass Office 365 eine Cloud-Lösung bleibt und sie besser daran tun, ohne zusätzliche Schutzmassnahmen nur in der Cloud zu speichern, was alle sehen dürften.

Ergebnis

Dass Microsoft die Vertragsbestimmungen so angepasst hat, dass der Einsatz von Office 365 datenschutzkonform möglich ist, befreit die Schulbehörden nicht davor, organisatorische und technische Massnahmen zu ergreifen, um die damit bearbeiteten Personendaten vor dem Zugriff Unberechtigter zu schützen. Bei besonderen Personendaten oder Daten, die einem Berufsgeheimnis unterstehen, müssen die Daten vor der Ablage mit einer Zusatzsoftware verschlüsselt werden.

1 <http://www.privatim.ch/files/layout/downloads_de/privatim+Merkblatt+Cloud+Computing+in+Schulen.pdf>.
2 § 6 Abs. 1 IDG.
3 § 8 IDG.
4 Die von Office 365 angebotene Verschlüsselung entspricht dem gesetzlich geforderten aktuellen Stand der Technik (§ 8 Abs. 3 IDG): Die gewählten Algorithmen und Schlüssellängen gelten zurzeit als sicher, wie der Datenschutzbeauftragte des Kantons Zürich in einer E-Mail am 30. März 2015 bestätigt hat.
5 Persönlichkeitsprofile sind «Zusammenstellungen von Informationen, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlauben» (§ 3 Abs. 4 lit. b IDG).

Fall 6 Quellensteuer: Kontrolle der gemeldeten Arbeitstage von Salonmitarbeiterinnen

Die Abteilung Quellensteuer möchte aufgrund des Verdachtes, dass Betreiber von Etablissements die Löhne ihrer Angestellten nicht oder nicht korrekt angeben, einen regelmässigen Abgleich mit den Daten des Amtes für Wirtschaft und Arbeit vornehmen. Ist dies zulässig und wenn ja, welche Daten dürfen übermittelt werden?

Die Arbeitgeber, in diesem Fall die Salonbetreiber, melden ihre Mitarbeiterinnen über das Meldeverfahren beim Amt für Wirtschaft und Arbeit (AWA) an. Dabei geben sie u.a. die Anzahl Arbeitstage an, welche die Mitarbeiterinnen leisten. Werden nicht die ursprünglich gemeldeten Arbeitstage geleistet, müssen die Mitarbeiterinnen wieder abgemeldet werden. Dadurch stimmen die gemeldeten Arbeitstage in der Regel sehr gut mit den tatsächlich geleisteten Arbeitstagen überein. Quartalsweise haben die Salonbetreiber der Abteilung Quellensteuer eine Abrechnung mit dem Bruttoertrag der Mitarbeiterinnen abzuliefern. Diese Meldung werde jedoch nur von einem Bruchteil aller Salonbetreiber gemacht. Die Abteilung Quellensteuer möchte aufgrund dieses Umstandes einen regelmässigen Abgleich mit den Daten des AWA vornehmen und bat den Datenschutzbeauftragten um eine Beurteilung einer möglichen Lösung.

Ein öffentliches Organ – in diesem Fall das AWA – darf Personendaten bekannt geben, wenn es durch eine gesetzliche Grundlage dazu ermächtigt wird[1]. § 140 Abs. 1 des Steuergesetzes stellt eine derartige Legitimation dar: «Die Verwaltungs- und Gerichtsbehörden des Kantons (...) haben ungeachtet einer allfälligen Geheimhaltungspflicht den Steuerbehörden des Kantons auf Ersuchen hin alle erforderlichen Auskünfte zu erteilen.» Das Bundesgericht beurteilte den Passus «auf Ersuchen hin» sehr offen. So reicht ein einmaliges Ersuchen auf regelmässigen Austausch aus, um der Steuerbehörde periodisch die gewünschten Daten weitergeben zu dürfen[2].

Wie ist der Informationsaustausch jedoch auszugestalten, um dem Erfordernis der Verhältnismässigkeit (Geeignetheit, Erforderlichkeit und Zumutbarkeit)[3] zu genügen? Sollen die Namen der Salon-Angestellten übermittelt werden oder reichen allenfalls auch weniger Informationen?

Die Abteilung Quellensteuer schlug vor, dass das AWA nicht etwa Namen und dazugehörige Arbeitsstunden der Mitarbeiterinnen melde, sondern lediglich das Etablissement und die dort gesamthaft während eines Quartals geleisteten Arbeitstage. Der Vorteil der quartalsweisen Weitergabe liege darin, dass die abzugleichenden Arbeitsstunden einen überschaubaren Rahmen behalten würden. Als weiteres Argument für einen quartalsweisen Abgleich führte die Abteilung Quellensteuer an, dass die Abrechnungen der Salonbetreiber über denselben Zeitrahmen bei der Abteilung Quellensteuer abzuliefern seien.

Der Datenschutzbeauftragte erachtet den von der Abteilung Quellensteuer vorgeschlagenen Umfang des Informationsaustauschs als verhältnismässig: Die gewünschten Daten sind zweifelsohne geeignet, um die Bruttoerträge der einzelnen Etablissements zu überprüfen. Auch erscheint die Übermittlung von Salonname und Gesamtzahl der dort geleisteten Arbeitstage als mildestes Mittel, um die Bruttoerträge der Etablissements zu ermitteln, da insbesondere keine unnötigen Personendaten beispielsweise über die einzelnen Mitarbeiterinnen bekannt gegeben werden müssen.

Die quartalsweise Übermittlung der in einem Etablissement gesamthaft geleisteten Arbeitstage durch das AWA an die Abteilung Quellensteuer stellt damit einen aus datenschutzrechtlicher Sicht gangbaren, d.h. rechtmässigen und verhältnismässigen Lösungsweg dar.

Ergebnis

Damit die Abteilung Quellensteuer überprüfen kann, ob die Salonbesitzer ihrer Pflicht zur Meldung der in ihrem Betrieb geleisteten Bruttoarbeitstage korrekt nachgekommen sind, dürfen Informationen vom AWA eingeholt werden. Für die Überprüfung genügt jedoch die Übermittlung der gesamthaft geleisteten Arbeitstage pro Etablissement – die Bekanntgabe weiterer Informationen wäre nicht verhältnismässig.

1 § 21 IDG
2 BGE 124 II 58, E. 3d. Vgl. dazu aber TB 2010, 36 (Fall 11).
3 § 9 Abs. 3 IDG.

Anhang Verzeichnis der zitierten Gesetze, Materialien und Literatur

Rechtsgrundlagen des Kantons Basel-Stadt

Arbeitslosenversicherungs-Vollzugsverordnung Verordnung vom 15. November 2011 betreffend Zuständigkeit und Organisation beim Vollzug der Arbeitslosenversicherung im Kanton Basel-Stadt, SG 835.150.

DO-LHA Dienstordnung des Lufthygieneamtes beider Basel vom 30. Mai 2005, SG 781.110.

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.

FVKG Finanz- und Verwaltungskontrollgesetz vom 17. September 2003 (FVKG), SG 610.200.

GesG Gesundheitsgesetz vom 21. September 2011, SG 300.100.

GO Gesetz vom 29.06.2006 über die Geschäftsordnung des Grossen Rates (GO), SG 152.100.

HG Gesetz vom 17. November 1999 über die Haftung des Staates und seines Personals (Haftungsgesetz), SG 161.100.

KJG Gesetz vom 10. Dezember 2014 betreffend Förder- und Hilfeleistungen für Kinder und Jugendliche (Kinder- und Jugendgesetz), SG 415.100.

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

OmbG Gesetz vom 13. März 1986 betreffend die Beauftragte/den Beauftragten für das Beschwerdewesen (Ombudsfrau/Ombudsmann) des Kantons Basel-Stadt, SG 152.900.

PG Personalgesetz vom 17. November 1999, SG 162.100.

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

Registratur- und Archivierungsverordnung Verordnung vom 13. Oktober 1998 über die Registraturen und das Archivieren, SG 153.610.

Schulgesetz Schulgesetz vom 4. April 1929, SG 410.100.

SHG Sozialhilfegesetz vom 29. Juni 2000, SG 890.100.

Steuergesetz Gesetz vom 20. April 2000 über die direkten Steuern, SG 640.100.

StVO Verordnung vom 17. Mai 2011 über den Strassenverkehr (Strassenverkehrsverordnung, StVO), SG 952.200.

Taxigesetz Gesetz vom 17. Januar 1996 über den Betrieb von Taxis, SG 563.200.

Taxiverordnung Verordnung vom 3. Dezember 1996 zum Taxigesetz, SG 563.210.

Rechtsgrundlagen des Kantons Basel-Landschaft

VwOG/BL Gesetz vom 6. Juni 1983 über die Organisation des Regierungsrates und der kantonalen Verwaltung (Verwaltungsorganisationsgesetz, VwOG), SGS 140.

Rechtsgrundlagen des Kantons Zürich

OG RR/ZH Gesetz 6. Juni 2005 über die Organisation des Regierungsrates und der kantonalen Verwaltung (OG RR), LS 172.1.

Bundesrecht

BGÖ Bundesgesetz vom 17. Dezember 2004 über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz, BGÖ), SR 152.3.

BInfV Verordnung vom 9. Dezember 2011 über die Informatik und Telekommunikation in der Bundesverwaltung (Bundesinformatikverordnung BinfV), SR 172.010.58.

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

DBG Bundesgesetz vom 14. Dezember 1990 über die direkte Bundessteuer (DBG), SR 642.11.

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

EPG Bundesgesetz vom 18. Dezember 1970 über die Bekämpfung übertragbarer Krankheiten des Menschen (Epidemiengesetz), SR 818.101 (revidierte Fassung: Bundesgesetz vom 28. September 2012 über die Bekämpfung übertragbarer Krankheiten des Menschen [Epidemiengesetz, EpG], BBl 2012 8157, voraussichtlich in Kraft ab 2016).

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 JSSK vom 16. Oktober 2013 Bericht 13.0739.02 der Justiz, Sicherheits- und Sportkommission vom 16. Oktober 2014 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.

Bericht 12.1046.02 Bericht 12.1046.02 des Ratsbüros vom 30. Januar 2013 zum Ratschlag betreffend Änderung von Gesetzen zur rechtlichen Konsolidierung der dem Grossen Rat unterstellten und zugeordneten Dienstabteilungen sowie Bericht zu einer Motion.

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 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

PK-IDG/BS-Autor(in) 2014 Beat Rudin/Bruno Baeriswyl (Hrsg.), Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Basel-Stadt, Zürich/Basel/Genf 2014.

Rosenthal/Jöhri David Rosenthal/Yvonne Jöhri, Handkommentar zum Datenschutzgesetz, Basel 2008.

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

Volontäre:
Nicolas Hochstrasser, MLaw
(1.1.2014 - 30.6.2014)
Lorenz Overhage, MLaw
(1.7.2014 - 31.12.2014)

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

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

Gestaltung
Andrea Gruber,
Visuelle Gestaltung, Basel

Druck
Gremper AG