Datenschutzbeauftragter des Kantons Basel-Stadt

Bericht an den Grossen Rat

2016

Inhaltsübersicht

Einleitung

Themen

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

Fotokonzept: «Videoüberwachung»

Aus dem Alltag

Fälle

Anhang

Einleitung

2016: Die Herausforderungen der Digitalisierung angehen

Fast 10% mehr Geschäfte, mehr Medienanfragen – keine herausragenden Vorfälle, aber ein stetes Bemühen, die öffentlichen Organe zu unterstützen in der Aufgabe, die Herausforderung der Digitalisierung zu meistern. Dabei gibt es durchaus Verbesserungsbedarf, etwa bei den datenschutzrelevanten Vorhaben, die dem Datenschutzbeauftragten zur Vorabkontrolle vorzulegen sind.

Jahresrückblick

Keine dramatischen Schlagzeilen Was gibt es über 2016 zu berichten? Ein Jahr wie andere auch. Kein überragendes Thema wie die Enthüllungen von Edward Snowdon. Kein spektakulärer Hackerangriff auf das Datennetz Basel-Stadt, bei dem alle Daten von Unbekannten gestohlen oder vernichtet wurden. Kein Spital, das durch einen Angriff wie von WannaCry lahmgelegt wurde. Und doch – von allem ein bisschen: Da ein bisschen mehr (Video-)Überwachung – ein paar neue Anwendungen, die der Polizei die Suche nach ausgeschriebenen Personen oder Fahrzeugen erleichtert, aber natürlich auch Unverdächtige erfassen – Mitarbeitende, die auf Phishing-Mails oder Trojaner hereinfallen, SAP, das ankündigt, dass in ein paar Jahren wichtige Komponenten ihrer Dienstleistungen ausschliesslich als Cloud-Dienste angeboten werden ...

Abhängig Viele sind sich wohl gar nicht bewusst, wie gross unsere Abhängigkeit von der Informationstechnologie schon ist. Es ist nicht das Schlimmste, was passieren kann, wenn einmal die Büroanwendung am Arbeitsplatz nicht funktioniert oder der Zugriff auf die Datenablage für eine Stunde nicht möglich ist. Unsere Abhängigkeit ist viel stärker – und sie nimmt zu. Damit wir unsere Zukunft mitgestalten können, müssen wir uns alle diesbezüglich laufend informieren, die Entwicklungen neu beurteilen und uns orientieren.

Chancen Dabei bietet die Digitalisierung natürlich hervorragende Chancen. Abläufe können vereinfacht, beschleunigt, verbilligt werden – aber noch viel mehr: Es werden neue Dienstleistungen möglich, die bisher undenkbar waren. Auch der Staat soll sich solchen Chancen nicht verschliessen – oder genauer: Er kann die Digitalisierung gar nicht aufhalten. Also gilt es, die Chancen zu nutzen.

E-Anwendungen

Mehrwert Nun ist aber nicht jede E-Anwendung einfach an sich erstrebenswert. «Me too» reicht als Begründung nicht. E-Anwendungen machen für die öffentliche Verwaltung vor allem da Sinn, wo sie den Bürgerinnen und Bürgern einen Mehrwert bringen, die Abläufe für sie vereinfachen, transparenter, zuverlässiger, schneller und/oder günstiger machen. Wo bringt E-Voting mehr als zum Beispiel die bisherige briefliche Stimmabgabe? Von der Erwartung, dass es eine höhere Stimmbeteiligung bringen soll, hat man sich ja bereits verabschiedet. Wo bringt E-Government Verbesserungen oder Erleichterungen für die Bürgerinnen und Bürger? Wo vermeidet es einen Gang zu einer Amtsstelle während der Schalteröffnungszeiten, ohne dass die erforderliche Qualität der staatlichen Dienstleistung leidet? Solche Anwendungen müssen gut überlegt sein, bevor sie – in der Regel mit nicht geringen Kosten – eingeführt werden, einfach weil es modern ist.

Checks and Balances

Auch Risiken Wer von Chancen redet, darf auch die Risiken nicht ausser Acht lassen. Die schöne neue Welt ist natürlich nicht nur schön. Die Digitalisierung bringt unweigerlich auch neue Gefahren mit sich. Wer die Vorteile der Digitalisierung nachhaltig nutzen will, tut deshalb gut daran, nicht blindlings den Marketingversprechen von Anbietern aufzusitzen, sondern genau hinzuschauen, die Zukunft bewusst mitzugestalten, zu prüfen, worauf man sich einlässt, und für einen Ausgleich zu sorgen – «Checks and Balances» eben.

Risikomanagement Eine Anwendung darf nun aber auch nicht einfach verteufelt werden, nur weil sie Risiken in sich birgt – es gilt vielmehr, die Risiken zu erkennen, sie zu bewerten, angemessene Schutzmassnahmen zu treffen, um untragbare Risiken zu vermeiden oder sie auf ein erträgliches Mass zu vermindern, um dann das Restrisiko zu kennen und es bewusst zu übernehmen. Jede Schutzmassnahme hat ein Preisschild, darauf wird der Leistungserbringer unweigerlich hinweisen. Das Restrisiko kostet auch, mindestens dann, wenn der unerwünschte Fall eintritt. Es trägt aber normalerweise kein Preisschild – das sollte es aber! Und eines muss uns bewusst sein: Wenn wir das Risiko ausschliesslich über die Eintretenswahrscheinlichkeit senken, dann entspricht das Schadensausmass im Eintrittsfall gleichwohl demjenigen ohne Schutzmassnahmen!

Beispiel Cloud Künftig stehen, mehr noch als bisher, Entscheidungen an, die grosse Auswirkungen haben werden. Welche Cloud-Strategie soll der Kanton zum Beispiel fahren? Alles in die Cloud, weil es verspricht, weniger zu kosten? Nur bestimmte Prozesse oder Daten in die Cloud? Mit welchen konkreten Schutzmassnahmen? Können diese Massnahmen (z.B. die Verschlüsselung) halten, was man sich davon verspricht? Sollen jene Prozesse und Daten, die für das Funktionieren der Verwaltung entscheidend sind oder deren Schadenspotenzial für die Rechte der Bürgerinnen und Bürger gross sind, nicht in die Cloud? Das kann logischerweise nicht einfach jede Dienststelle für sich beurteilen und entscheiden. Entscheidend wird sein, dass eine seriöse Risikoabwägung stattfindet. Letztlich wird der Regierungsrat hinstehen und klar deklarieren müssen, nach welchem Massstab Risiken bewertetet werden und welche Restrisiken er für das Funktionieren des Staates und für die Grundrechte der Bürgerinnen und Bürger als betroffene Personen als tragbar erachtet. Und der Grosse Rat wird über seine Oberaufsicht diesen Entscheid gutheissen müssen – oder Korrekturen verlangen.

Funktion und Instrumente Der Datenschutzbeauftragte hat in diesen Checks and Balances eine Funktion, und das Datenschutzrecht stellt wirksame Instrumente dafür zur Verfügung. Schon bisher mussten Vorhaben mit einer gewissen Datenschutz-Relevanz dem Datenschutzbeauftragten zur Vorabkontrolle vorgelegt werden. Er hat eine Prüfung vorzunehmen und eine Beurteilung abzugeben – allenfalls verbunden mit einer Empfehlung für Verbesserungen. Das Datenschutzrecht, wie es die modernisierte Europaratskonvention verlangt und auch aufgrund der Schengen-Assoziierung geschaffen werden muss, behält dieses Instrument unter dem (treffenderen) Namen «Vorabkonsultation» bei und fasst seine Vorbereitung unter dem Begriff «Datenschutzfolgenabschätzung» zusammen. Diese beiden Instrumente des präventiven Datenschutzes leisten einen wichtigen Beitrag, damit dereinst von den Vorteilen der Digitalisierung profitiert werden kann – sie müssen aber (noch besser) genutzt werden und der Datenschutzbeauftragte muss die erforderlichen Ressourcen dafür besitzen. Unter anderem zu diesem Zweck wird 2017 eine bisher juristisch besetzte Stelle in eine IT-Stelle umgewandelt werden.

Zum Schluss

Danke! Unsere Aufgabe zum Schutz der Privatheit der Bürgerinnen und Bürger, über welche die öffentlichen Organe Daten bearbeiten, und im Interesse ihres Informationszugangsrechts nach dem Öffentlichkeitsprinzip könnten wir nicht erfolgreich erfüllen ohne die Unterstützung vieler Menschen und Institutionen. Mein Dank gilt deshalb

— allen, die sich mit Fragen zum Datenschutz und zum Öffentlichkeitsprinzip vertrauensvoll an uns wenden;
— den 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;
— den Volontärinnen Cora Dubach und Sarah Salzmann für ihre kritische Neugier und ihre aktive Mitarbeit und
— last but not least meinem Team – Markus Brönnimann, Katja Gysin, Daniela Waldmeier (bis 31. Dezember 2016) und Barbara Widmer –, das mit unverändert grossem Engagement, mit spannenden Diskussionen und konstruktiven Anregungen unsere Arbeit bereichert und vorangebracht hat. Nach über fünfeinhalb Jahren verlässt uns die Juristin Daniela Waldmeier, um, nach bestandenem Advokaturexamen (bravo!), in ein Anwaltsbüro einzutreten. Besten Dank für den tollen und erfolgreichen Einsatz und viel Erfolg und Befriedigung in der weiteren beruflichen Laufbahn!

Beat Rudin, Datenschutzbeauftragter

1 Die in den Texten erwähnten Rechtsquellen und Materialien sind in einem Verzeichnis am Schluss des Berichts detailliert aufgeführt (Seite 54 f.).

Themen

Thema 1 Transparenz bei der Videoüberwachung

Thema 2 Vorabkontrolle – das Instrument des präventiven Datenschutzes

Thema 3 Auswirkungen der europäischen Datenschutz-reform

Thema 1

Transparenz bei der Videoüberwachung

Mit der gesetzlichen Grundlage für Videoüberwachungssysteme im IDG ist der Transparenz für die Betroffenen noch nicht Genüge getan. Die öffentlichen Organe müssen die Reglemente, welche die Details der einzelnen Videoüberwachungssysteme regeln, der Öffentlichkeit leicht zugänglich machen. Der Datenschutzbeauftragte hat 2016 geprüft, inwiefern diese Pflicht eingehalten wird.

Die Regelung der Videoüberwachung

Die DSG-Regelung von 2005 Das frühere Datenschutzgesetz (DSG) verlangte seit der Revision von 2005 eine spezialgesetzliche Grundlage für den Betrieb eines Videoüberwachungssystems[1]. Jedes einzelne System bedurfte einer Autorisierung durch den Datenschutzbeauftragten. Dieses Konzept hatte sich allerdings nicht bewährt. Die verlangte spezialgesetzliche Grundlage wurde im Kanton soweit ersichtlich einzig für die Industriellen Werke Basel (IWB) geschaffen[2]. Trotzdem wurde aber eine Vielzahl von Videoüberwachungssystemen betrieben. Ausserdem wurde die Verantwortlichkeit, die ja letztlich beim Betreiber des Systems liegen muss, durch die Autorisierung verwischt.

Damit diese gesetzliche Grundlage der Bundesgerichtspraxis genügen kann, ist jedes Videoüberwachungssystem auf eine tragfähige Rechtsgrundlage in Form eines Reglements zu stellen.

Neue Regelung im IDG Nachdem in der IDG-Vernehmlassung sehr widersprüchliche Stellungnahmen zur Regelung der Videoüberwachung eingegangen waren, wurde die Videoüberwachungsnorm neu konzipiert. Im Ratschlag schrieb der Regierungsrat dazu:

— «Es wird nicht mehr eine (spezial-)gesetzliche Grundlage verlangt, sondern die Bestimmung im IDG stellt die aus rechtsstaatlichen Gründen erforderliche gesetzliche Grundlage dar.

— Für jedes Videoüberwachungssystem muss vor der Inbetriebnahme ein Reglement erlassen werden; das Reglement ist zeitlich zu befristen und vor der Verlängerung muss die Wirksamkeit evaluiert werden.

— Im Mittelpunkt der Regelung eines Videoüberwachungssystems steht die Festlegung des konkreten Zwecks, der mit dem Einsatz des Systems erreicht werden soll.

— Es wird nicht mehr zwingend eine einheitliche Löschungsfrist festgelegt; sie kann im Reglement, wenn es der konkrete Zweck des Videoüberwachungssystems erfordert, über die ‹Regellänge› von einer Woche verlängert werden»[3].

Konkretisierung in Reglementen § 17 IDG stellt somit neu die (formell-)gesetzliche Grundlage für Videoüberwachungssysteme dar (statt, wie es früher das DSG tat, jeweils eine spezialgesetzliche Grundlage zu verlangen). Damit diese gesetzliche Grundlage der neueren Bundesgerichtspraxis[4] genügen kann, ist jedes Videoüberwachungssystem auf eine tragfähige Rechtsgrundlage in Form eines Reglements zu stellen. Je unpräziser die Regelungen im konkreten Videoüberwachungsreglement sind, desto eher riskiert das Vorhaben, am Bestimmtheitserfordernis zu scheitern, falls die Gerichte angerufen werden sollten[5].

Erlass Erlassen werden muss das Reglement durch

— die Departemente bei Systemen im Verantwortungsbereich kantonaler öffentlicher Organe;
— den Gemeinderat bei Systemen im Verantwortungsbereich kommunaler öffentlicher Organe;
— den Gerichtsrat bei Systemen im Verantwortungsbereich von Gerichten;
— die Direktion selbständiger Anstalten und Körperschaften des öffentlichen Rechts bei Systemen in ihrem Verantwortungsbereich[6].

Reglementsinhalt Der Mindestinhalt der Reglemente ist in der IDV festgelegt[7]. Insbesondere muss festgehalten werden, welches öffentliche Organ für das Videoüberwachungssystem verantwortlich ist, welchem Zweck die konkrete Videoüberwachung dienen soll, welche Räume und Personen durch die Videoüberwachung erfasst werden und nach welcher Dauer der Aufbewahrung die Aufnahmen gelöscht werden. Ausserdem ist zu regeln, welche Massnahmen getroffen werden, um die Wirksamkeit der Videoüberwachung zu evaluieren.

Veröffentlichungspflicht Die Rechtsetzung soll es Bürgerinnen und Bürger erlauben zu sehen, was die Verwaltung tut, inwiefern sie ihre Grundrechte einschränken darf. Darum müssen Gesetze und Verordnungen auch in der Gesetzessammlung publiziert werden. Aus der generellen Regelung des IDG könnten Bürgerinnen und Bürger in keiner Weise erkennen, wo und wie ihr Grundrecht auf informationelle Selbstbestimmung durch staatlich betriebene Videoüberwachung eingeschränkt wird. Ein «geheimes» Reglement könnte natürlich die erforderliche Transparenz für die Betroffenen nicht sicherstellen. Deshalb hat der Verordnungsgeber klar festgelegt: Die Reglemente sind der Öffentlichkeit leicht zugänglich zu machen[8]. Einzig wenn durch die Bekanntgabe der Kamerastandorte die Zweckerreichung unmöglich würde, soll auf deren Veröffentlichung verzichtet werden können[9].

Der Datenschutzbeauftragte hat 2016 erfasst, welche Reglemente der Öffentlichkeit leicht zugänglich gemacht sind.

Rolle des Datenschutzbeauftragten

Vorabkontrolle Was ist die Rolle des Datenschutzbeauftragten? Er führt bei den ihm vorgelegten Videoüberwachungsvorhaben eine Vorabkontrolle durch[10]. Er hat nicht zu entscheiden, ob eine Videoüberwachungsanlage tatsächlich in Betrieb genommen werden soll – das obliegt dem verantwortlichen öffentlichen Organ und der Stelle, die das Reglement zu erlassen hat, also, wie oben erwähnt, dem vorgesetzten Departement, dem Gemeinderat, dem Gerichtsrat bzw. der Direktion selbständiger Anstalten und Körperschaften des öffentlichen Rechts.

Prüfung und Einwirkungsinstrument Der Datenschutzbeauftragte prüft, ob die gesetzlichen Vorgaben eingehalten sind, ob das Videoüberwachungssystem – nicht die einzelne Kamera – gesetzmässig und verhältnismässig ist. Bei Mängeln gibt er gegenüber dem verantwortlichen öffentlichen Organ eine Empfehlung[11] ab. Das öffentliche Organ hat sodann zu erklären, ob es der Empfehlung folgen will oder nicht. Falls es erklärt, der Empfehlung nicht folgen zu wollen, oder tatsächlich der Empfehlung nicht folgt, kann der Datenschutzbeauftragte die Empfehlung oder Teile davon als Weisung in Form einer Verfügung erlassen[12]. Der Adressat kann die Verfügung sodann beim Appellationsgericht anfechten[13].

Veröffentlichung der Reglemente

Prüfung Der Datenschutzbeauftragte hat 2016 erfasst, welche Reglemente der Öffentlichkeit leicht zugänglich gemacht sind. Wo im Internet kein Reglement oder keine Umschreibung des Reglementsinhalts zu finden war, wurden die für den Betrieb der Videoüberwachungsanlagen verantwortlichen öffentlichen Organe angeschrieben.

Resultat Das Resultat dieser Prüfung erscheint in der Tabelle auf den Seiten 12 f. Anfangs 2016 waren nur acht Videoüberwachungsreglemente (oder die wesentlichen Inhalte daraus) über das Internet zugänglich, bei insgesamt 29 bestehenden, dem Datenschutzbeauftragten bekannten, Videoüberwachungsanlagen. Bei 15 weiteren Videoüberwachungssystemen sind die Reglemente bis zum Redaktionsschluss des Tätigkeitsberichts zugänglich gemacht worden, insgesamt sind heute 23 Reglemente bzw. deren wesentlicher Inhalt grundsätzlich publik gemacht worden. Einige Reglemente sind zurzeit in Revision bzw. in Bearbeitung und deshalb nicht veröffentlicht. Bei vier Systemen fehlt die Publikation weiterhin; der Datenschutzbeauftragte hat die verantwortlichen Stellen auf ihre Pflicht aufmerksam gemacht.

Einschränkungen Die IDV sieht vor, dass auf die Veröffentlichung der Kamerastandorte verzichtet werden kann, wenn durch deren Bekanntgabe die Zweckerreichung unmöglich wird. Davon haben etliche Betreiber Gebrauch gemacht. Oft werden die Lagepläne nicht mitveröffentlicht. Allerdings kann die Zweckerreichung nicht nur durch die Bekanntgabe von Kamerastandorten vereitelt werden, sondern auch durch andere Informationen, etwa von Betriebszeiten. Es wird bei der nächsten Revision des IDG zu prüfen sein, ob die Ausnahme von der Veröffentlichungspflicht nicht etwas weiter umschrieben werden könnte.

Form der Publikation Zum Teil werden auf einer Website auch bloss die wesentlichsten Informationen zur Videoüberwachung wiedergegeben, nicht das gesamte Reglement veröffentlicht[14]. Das widerspricht dem Wortlaut der IDV, kann aber dem Transparenzgebot trotzdem genügen. Möglicherweise sind mindestens bei «kleinen» Anlagen die Betroffenen mit einer kurzen und prägnanten Umschreibung ebenso gut informiert wie mit einem Reglement. Im Rahmen einer Revision des IDG kann überlegt werden, ob die Pflicht zur Transparenz nicht in diesem Sinne etwas offener umschrieben werden könnte. >

Erfasste und nicht erfasste Videoüberwachungssysteme

Private Videoüberwachung nicht erfasst Vorweg ist festzuhalten, dass durch Private – Einzelpersonen wie Vermieterinnen und Ladenbesitzer oder Unternehmen – betriebene Videoüberwachungsanlagen nicht erfasst sind. Sie unterstehen nicht dem kantonalen IDG, sondern dem Bundesdatenschutzgesetz. Es besteht auch keine kantonale Bewilligungspflicht[15]. Wenn sich betroffene Personen – ein Mieter, eine Kundin oder Mitarbeitende – gegen eine ihrer Meinung nach ungerechtfertigte oder unverhältnismässige Videoüberwachungsanlage zur Wehr setzen wollen, dann müssen sie – nachdem sie hoffentlich versucht haben, eine Lösung auf dem Gesprächsweg zu finden – den Weg über das Zivilgericht beschreiten. Der kantonale Datenschutzbeauftragte hat gegenüber privaten Datenbearbeiterinnen und Datenbearbeitern nichts zu sagen (und der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte darf nur intervenieren, wenn es sich um einen sog. Systemfehler handelt[16]). Aus diesem Grund gibt es auch keinerlei Anhaltspunkte für die Zahl privater Videoüberwachungen.

Nicht mitgezählte Systeme In der Tabelle nicht aufgeführt sind von öffentlichen Organen betriebene Anlagen, die nicht in den Geltungsbereich des IDG fallen. Nicht enthalten sind demnach:

— die Videoüberwachungssysteme der Basler Verkehrsbetriebe BVB (Tram, Bus, Depots); für die ist aufgrund des Personenbeförderungsgesetzes des Bundes (PBG)[17] nicht mehr der kantonale Datenschutzbeauftragte, sondern der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) zuständig; das gilt im Übrigen natürlich erst recht für die von den SBB betriebenen Videoüberwachungsanlagen (z.B. im Bahnhof SBB);

— die Videoüberwachungssysteme in den staatlichen Parkhäusern; sie werden zwar durch ein öffentliches Organ betrieben (Immobilien Basel-Stadt), hingegen handelt es sich dabei um die Verwaltung von Finanzvermögen, was sich ausserhalb des Geltungsbereichs des kantonalen IDG abspielt;

— allfällige Videoüberwachungssysteme der Basler Kantonalbank; zwar ist die Kantonalbank eine Anstalt des kantonalen öffentlichen Rechts[18], weshalb ihr Datenbearbeiten eigentlich in den Geltungsbereich des kantonalen IDG fällt[19]; da sich aber die BKB am wirtschaftlichen Wettbewerb mit anderen (Universal) Banken teilnimmt und dabei privatrechtlich handelt, fällt sie aus dem Geltungsbereich des IDG;

— die Kameras, die von der Kantonspolizei gestützt auf das Polizeigesetz[20] eingesetzt werden (Bild- und Tonaufnahmen mit z.T. mobilen Kameras zur Beweissicherung bei öffentlichen Veranstaltungen, sofern die konkrete Gefahr besteht, dass Straftaten begangen werden);

— Kameras, die zeitlich begrenzt zum Zweck einer nichtpersonenbezogenen Evaluation eingesetzt werden (z.B. bei einem Versuch zur Velozulassung auf einem Fussgängersteg);

— blosse «Türspione», also in Gegensprechanlagen eingebaute Kameras, die sich beim Klingeln automatisch einschalten und nachher wieder abschalten und bei denen keine Aufzeichnungen gemacht werden.

Unbestreitbar hat die Zahl der erfassten Videoüberwachungssysteme seit der Einführung der Videoüberwachungsbestimmung im DSG zugenommen. Allerdings heisst das nicht, dass so viele Systeme neu in Betrieb genommen worden sind.

Zunahme Unbestreitbar hat die Zahl der erfassten Videoüberwachungssysteme seit der Einführung der Videoüberwachungsbestimmung im DSG zugenommen. Allerdings heisst das nicht, dass so viele Systeme neu in Betrieb genommen worden sind. Vielfach wurde bei schon bestehenden Systemen erst mit der Zeit erkannt, dass sie in den Geltungsbereich des IDG fallen – etwa bei selbständigen öffentlich-rechtlichen Anstalten oder «Aussenbetrieben» der Verwaltung. Es sind also nicht alles neue Systeme, sondern oft bloss neu erfasste. Aus diesem Grund sind früher veröffentlichte und heute vorliegende Zahlen schlicht nicht direkt miteinander vergleichbar. Diese Entwicklung dürfte noch weitergehen: Der Datenschutzbeauftragte nimmt Reglemente z.B. von privaten Listenspitälern[21] oder Wohnheimen zur Vorabkontrolle entgegen, hat aber die anderen Listenspitäler und weitere Private, denen eine öffentliche Aufgabe übertragen worden ist, nicht systematisch kontaktiert. Es ist für die Zukunft zu prüfen, ob mindestens für den Bereich der Zentralverwaltung Vollständigkeitserklärungen eingeholt werden können.

Überwachungshölle oder Sicherheitsparadies?

Was heisst das? Werden die Bürgerinnen und Bürger in Basel auf Schritt und Tritt überwacht? Oder sind die Bürgerinnen und Bürger in Basel wegen der Videoüberwachung sicherer als anderswo? Wohl weder noch.

Äpfel und Birnen Die Zahl der in den Reglementen dokumentierten Videokameras – über 1 100 – erscheint hoch – gerade im interkantonalen Vergleich, der gelegentlich in den Medien erscheint. Ohne diese Zahl kleinreden zu wollen: Der Vergleich hinkt aus mehreren Gründen:

— Die im vergangenen Jahr in den Medien publizierten Zahlen aus anderen Kantonen und/oder Städten erscheinen zum Teil wenig glaubwürdig. Wo kein Melde-, Genehmigungs- oder mindestens Vorabkontrollsystem existiert, sind die Zahlen wohl nicht mehr als grobe Schätzungen und damit wenig zuverlässig.

— Von 20 in einem definierten Prozess beschlossenen und in einem Reglement reglementierten Kameras geht wohl eine kleinere Gefahr der Grundrechtsverletzung aus als von 20 «wilden» Kameras.

— Die Zahl der Kameras allein ist wenig aussagekräftig. Allein schon aus Versicherungsgründen muss ein grosses Kunstmuseum eine Vielzahl von Kameras installiert haben. Sind nun die 200 Kameras bei einem solchen Museum gleich «schlimm», wie wenn an 100 anderen Orten je zwei Kameras betrieben werden?

— Kameras mit einem engen, genau eingeschränkten Aufnahmebereich und –zweck (z.B. beim Lieferanteneingang zu einer Spitalapotheke) beeinträchtigen die Grundrechte von weniger Personen als solche, die Personen im allgemein zugänglichen öffentlichen Raum erfassen.

Einsatzschwerpunktgebiete Wenn man dann die Verteilung der Kameras in Basel-Stadt ansieht, dann relativiert sich die «Überwachungshölle» doch rasch. Mehr als zwei Drittel aller Kameras sind in den folgenden vier Bereichen im Einsatz:

— Fast jede vierte Kamera hängt in einem Museum.
— Mehr als jede fünfte Kamera wird in einem Gefängnis betrieben.
— Etwas mehr als jede siebte Kamera ist in öffentlichen Sportanlagen und Bädern im Einsatz.
— Mehr als jede elfte Kamera wird in einer Gesundheitseinrichtung betrieben.

Einsatzparameter Ausserdem ist Videoüberwachung nicht Videoüberwachung. Von grossem Einfluss sind etwa die folgenden Einsatzparameter:

— Ist die Anlage permanent in Betrieb oder nur, wenn beispielsweise ein Alarmknopf gedrückt wird oder ein Sensor ein bestimmtes Auslösekriterium feststellt?
— Werden die Aufnahmen in Echtzeit ausgewertet (in einer Sicherheitszentrale)?
— Dient die Anlage der Auslösung einer Intervention (akustische Intervention, Aussenden eines Interventionsteams, Alarmierung der Polizei) oder bloss der Beweissicherung?
— Ist die Kamera steuerbar? Besteht eine Zoommöglichkeit?
— Werden die Aufnahmen gespeichert oder nicht? In einem Ringspeicher, der nach einer bestimmten Aufnahmedauer automatisch wieder überschrieben wird, oder auf einem grösseren Speichermedium?
— Wie lange werden die Aufnahmedaten aufbewahrt?
— Wer entscheidet über den Ausbau eines Speichermediums (z.B. eines Ringspeichers) – im Sinne eines Herausnehmens des Speichermediums und die Aufbewahrung zur Beweissicherung?
— Wer entscheidet über die Auswertung gespeicherter Aufnahmen (z.B. die Strafverfolgungsbehörden in einer Strafuntersuchung)?

1 § 6a DSG (in Kraft bis 31. Dezember 2011).
2 § 35 IWB-Gesetz.
3 Ratschlag 08.0637.01, 30 f.
4 BGE 136 I 87, 111 ff. E. 8 zum Polizeigesetz des Kantons Zürich.
5 So der Regierungsrat im IDV-Mantelbericht, S. 6 f.
6 § 18 Abs. 2 lit. a-d IDG; vgl. dazu PK-IDG/BS-Husi, § 18 N 26.
7 § 5 IDV; vgl. dazu PK-IDG/BS-Husi, § 18 N 2 ff.
8 § 6 Abs. 1 IDV; vgl. dazu auch PK-IDG/BS-Husi, § 18 N 46.
9 § 6 Abs. 2 IDV; vgl. dazu auch PK-IDG/BS-Husi, § 18 N 47.
10 Vor dem erstmaligen Erlass und vor einer Verlängerung: § 18 Abs. 4 IDG, §§ 8 und 9 IDV; vgl. dazu PK-IDG/BS-Husi, § 18 N 34 ff.
11 Im Sinne von § 46 IDG; vgl. dazu auch PK-IDG/BS-Schilling, § 46 N 2 ff.
12 § 47 Abs. 1 IDG; vgl. dazu PK-IDG/BS-Schilling, § 47 N 2 ff.
13 § 47 Abs. 5 IDG; vgl. dazu PK-IDG/BS-Schilling, § 47 N 9 ff.
14 Auf Anfrage hin müsste das verantwortliche öffentliche Organ das Reglement aber sicher zugänglich machen – allenfalls mit den gleichen Einschränkungen wie bei der Publikation (Kamerastandorte, evtl. weitere Informationen, deren Bekanntgabe die Zweckerreichung der Videoüberwachungsanlage vereiteln könnte (z.B. Betriebszeiten).
15 Interpellationsantwort 14.5049.02, S. 3.
16 Art. 29 Abs. 1 lit. a DSG.
17 Art. 54 Abs. 1 und 3 PBG; vgl. dazu TB 2010, S. 10 f. und PK-IDG/BS, § 2 N 37 ff.
18 § 1 Kantonalbankgesetz.
19 § 2 Abs. 1 i.V.m. § 3 Abs. 1 lit. b IDG; vgl. dazu PK-IDG/BS-Rudin § 3 N 7.
20 § 58 PolG.
21 Soweit ihnen eine öffentliche Aufgabe übertragen wurde (hier: ein im Leistungsauftrag umschriebener Teil der kantonalen Spitalversorgungsaufgaben), werden sie zu einem öffentlichen Organ des Kantons (§ 3 Abs. 1 lit. c IDG); vgl. dazu PK-IDG/BS-Rudin § 3 N 10 f., Bernhard Rütsche, Datenschutzrechtliche Aufsicht über Spitäler/Surveillance de la protection des données dans les hôpitaux, digma-Schriften Band 6, Zürich 2012, Rz. 116 ff. (Zusammenfassung).

Videoüberwachungsanlagen öffentlicher Organe im Kanton Basel-Stadt: Links zu den Reglementen

Wo?	Wer?	Was?	Link zum Reglement oder zur Information	Bemerkungen
mehr als 200 Kameras				
Kunstmuseum	PD, Kunstmuseum	Überwachung innen und aussen der fünf Gebäude	https://kunstmuseumbasel.ch/	Publikation des Reglements ohne Lagepläne
101-200 Kameras				
Sportanlagen und Bäder	ED	Überwachung der verschiedenen Sportanlagen und Bäder	http://www.ed.bs.ch/ueber-das-departement/interne-dienste/rechtsabteilung/videoueberwachung.html	Publikation des Reglements und der Anhänge ohne Lagepläne
Waaghof	JSD und Staats-anwaltschaft	Überwachung des gesamten Gebäu-dekomplexes innen und aussen		Reglement in Revision
51-100 Kameras				
Polizeiwachen und Polizeiposten	JSD, Kantonspolizei	Überwachung von Polizeiwachen und –posten (ohne Waaghof und Spiegelhof)		Reglement in Revision
Bässlergut	JSD, Amt für Justizvollzug	Überwachung des Innenbereichs, der Aussenhaut des Gebäude-komplexes und der unmittelbaren Umgebung	http://www.bdm.bs.ch/Ueber-uns/Organisation/Amt-fuer-Justizvollzug/Gefaengnis-Baesslergut	Publikation des Reglements ohne Lagepläne
Dreispitzareal	Christoph Merian-Stiftung	Überwachung des gesamten Areals, insbesondere Parkierungsanlagen	http://www.dreispitz.ch/de/wirtschaftspark/informationen-fuer-bauberechtigte.html	Publikation des Reglements ohne Kamerastandorte
IWB-Infrastruktur	IWB, Industrielle Werke Basel	Überwachung der Infrastruktur an verschiedenen Standorten	https://www.iwb.ch/Service/Kontakt/Adressen---Oeffnungs-zeiten/Videoueberwachung.html	Publikation des Reglements ohne Lagepläne
Universitätsspital	Universitätsspital Basel USB	Überwachung des gesamten Areals	https://www.unispital-basel.ch/das-universitaetsspital/umgang-mit-personendaten/	Publikation des Reglements ohne Lagepläne
21-50 Kameras				
Betreibungsamt	Betreibungs- und Konkursamt Basel-Stadt	Überwachung der Schalter	http://www.bka.bs.ch/ueber-uns/betreibungsamt.html	Publikation des Reglements und generelle Information auf der Webseite
Museum der Kulturen	PD, Museum der Kulturen	Überwachung der Ausstellungs-räume, des Museumsshops und des Eingangs- und Aussenbereichs	http://www.mkb.ch/de/Informationen_Services.html	Publikation von genereller Infor-mation zur Video-überwachung
Spiegelhof	JSD	Überwachung der Kundenzone des Handelsregisteramtes und des Polizeipostens Spiegelhof		Reglement in Revision
Universitäre Psychiatrische Kliniken	Universitäre Psychiatrische Kliniken Basel UPK	Überwachung der Eingangs- und Aussenbereiche	http://www.upkbs.ch/ueber-uns/standorte/videoreglement/Seiten/default.aspx	Publikation des Reglements ohne Lagepläne
Universität	Universität Basel	Überwachung verschiedener Standorte	https://www.unibas.ch/de/Universitaet/Rechtserlasse.html	Reglement und Anhänge publiziert

Wo?	Wer?	Was?	Link zum Reglement oder zur Information	Bemerkungen
11-20 Kameras				
Bau- und Verkehrs-departement, Dufour-strasse 40 und 50, Münsterplatz 10-12	BVD	Überwachung der Gebäude-eingänge und des Stadtmodells	http://www.bvd.bs.ch/ueber-uns/regelement.html	Publikation des Reglements ohne Lagepläne
Berufsfeuerwehr Lützelhof	JSD, Rettung, Berufsfeuerwehr	Überwachung des Innenhofes, der Ausfahrtsbereiche und der Zugänge der Berufsfeuerwehr	http://www.bs.ch/publikationen/rettung/reglement-videou-eberwachung-fw-luezelhof.html	Publikation mit Lageplänen
Historisches Museum HMB, Museum für Wohnkultur / Haus zum Kirschgarten	PD, Historisches Museum HMB	Überwachung des Eingangs- und Kassenbereichs und gewisser Ausstellungsräume	http://www.hmb.ch/fileadmin/user_upload/Inhalte/PDF/UEber_das_Museum/Videoueberwachung__HMB.pdf	Publikation eines Informationsblatts zur Videoüberwachung
REHAB Basel	REHAB Basel	Überwachung des Therapie-Tiergartens, der Nebenzugänge und der Tiefgarage	http://www.rehab.ch/patienten-angehoerige/besucher/videoueberwachung.html	Publikation aller drei Reglemente mit Lageplänen
Sanität	JSD, Rettung, Sanität	Überwachung des Areals und der Innenräume der Rettungswagen		Reglement in Revision
5-10 Kameras				
Antikenmuseum Basel & Sammlung Ludwig	PD, Antikenmuseum Basel & Sammlung Ludwig	Überwachung des Kunstlicht- und des Ägyptensaals	http://www.antikenmuseumbasel.ch/de/footer/videoueber-wachung.html	Publikation eines Informationsblatts zur Videoüberwachung
Fachhochschule	Fachhochschule Nordwestschweiz FHNW	Überwachung der Campusgebäude an der Peter Merian-Strasse 86		Reglement in Revision
Steuerverwaltung	FD, Steuerverwaltung	Überwachung des Empfangs und der Schalter	http://www.steuerverwaltung.bs.ch/ueber-uns/leitbild.html	Publikation des Reglements mit Lageplan
Strafgericht	Strafgericht	Überwachung des Eingangs-bereichs und des Weibelgebäudes	http://www.strafgericht.bs.ch/verhandlungen/verhand-lungsbesuch/reglement-videoueberwachung.html	Publikation des Reglements ohne Lageplan
Wohnmodul-Anlage Asyl Dreispitz	WSU, Sozialhilfe	Überwachung der Zugänge zur Anlage	http://www.sozialhilfe.bs.ch/asyl/unterbringung.html	Publikation des Reglements mit Lageplan
Zentrale Informatik-dienste (ZID), Rechenzentren	FD, ZID	Überwachung der kantonalen Rechenzentren bei den IWB und der EBM	http://www.zid.bs.ch/themen/it-plattformen.html	Publikation des Reglements ohne Lagepläne
1-4 Kameras				
Heilsarmee, Wohnen Basel	WSU, Amt für Sozialbeiträge	Überwachung des Eingangsbereichs der Wohnhäuser	http://www.wohnen.heilsarmee-basel.ch	Publikation des Reglements ohne Lageplan
Historisches Museum HMB, Barfüsserkirche	PD, Historisches Museum HMB	Überwachung des Eingangsbereichs und des Sonderausstellungsraums	http://www.hmb.ch/fileadmin/user_upload/Inhalte/PDF/UEber_das_Museum/Videoueberwachung__HMB.pdf	Publikation eines Informationsblatts zur Videoüberwachung
Historisches Museum HMB, Musikmuseum	PD, Historisches Museum HMB	Überwachung des Eingangsbereichs	http://www.hmb.ch/fileadmin/user_upload/Inhalte/PDF/UEber_das_Museum/Videoueberwachung__HMB.pdf	Publikation eines Informationsblatts zur Videoüberwachung
Vollzugszentrum Klosterfiechten	JSD	Überwachung des Empfangsbereichs		Reglement in Bearbeitung
Naturbad Riehen	Gemeinderat Riehen	Überwachung des Haupteingangs und des Cafés	http://www.riehen.ch/aktuell/news/gemeinderatsbe-schluss-betreffend-die-bewilligung-einer-videoueberwa-chungsanlage-im	Publikation des Gemeinderatsbe-schlusses
Naturhistorisches Museum	PD, Naturhistorisches Museum	Überwachung des Eingangstors		
Notschlafstelle	WSU, Sozialhilfe	Überwachung des Eingangsbereiches	http://www.sozialhilfe.bs.ch/notwohnen/notschlafstelle.html	Publikation des Reglements ohne Lageplan
Storchen	FD, General-sekretariat	Überwachung des Eingangs zum Fischmarkt 10		
Zentrale Informatik-dienste (ZID), Be-triebsräumlichkeiten	FD, ZID	Überwachung der Warenanlieferung und der IT Werkstatt		

Thema 2

Vorabkontrolle – das Instrument des präventiven Datenschutzes

Das Informations- und Datenschutzgesetz verpflichtet die öffentlichen Organe, Datenbearbeitungsprojekte mit Risiken für die Rechte und Freiheit der betroffenen Personen dem Datenschutzbeauftragten zur Vorabkontrolle vorzulegen. Damit wird bereits in der Projektphase dazu beigetragen, dass sichere und datenschutzkonforme Lösungen entstehen.

Ausgangslage

Vorabkontrolle Nach dem Informations- und Datenschutzgesetz[1] hat die Dateneignerin[2] die Pflicht, Vorhaben und Projekte, die aufgrund der Art der Bearbeitung oder der zu bearbeitenden Daten geeignet sind, besondere Risiken für die Rechte und Freiheit der betroffenen Personen mit sich zu bringen, dem Datenschutzbeauftragten zur Vorabkontrolle vorzulegen. Hiervon betroffen sind Vorhaben und Projekte, mit welchen Lösungen entstehen, in denen Personendaten bearbeitet werden oder einen massgeblichen Einfluss auf bestehende Lösungen haben. Zu diesen Vorhaben und Projekten zählen beispielsweise auch konzeptionelle Grundlagen oder IT-Basis-Komponenten.

Die öffentlichen Organe sollen die Auswirkungen ihrer Rechtsetzungs- oder IT-Vorhaben auf den Datenschutz und die Informationssicherheit präventiv anschauen, sollen die entsprechenden Risiken bezüglich der Rechte und Freiheiten der betroffenen Personen beurteilen und angemessene Massnahmen zur Vermeidung oder Verminderung der Risiken vorschlagen.

Funktion und Konzept Die Vorabkontrolle ist bei genauerer Betrachtung- trotz des Wortbestandteils «Kontrolle» – keine (nachträgliche) Kontrolle, sondern (vorgängige) Beratung[3]. Vergleichbar ist das Vorgehen bei der Pflicht, dem Datenschutzbeauftragten Erlasse, die für den Umgang mit Informationen oder den Datenschutz erheblich sind, zur Stellungnahme vorzulegen[4]. Die Idee hinter diesen Instrumenten: Die öffentlichen Organe sollen die Auswirkungen ihrer Rechtsetzungs- oder IT-Vorhaben auf den Datenschutz und die Informationssicherheit präventiv anschauen, sollen die entsprechenden Risiken bezüglich der Rechte und Freiheiten der betroffenen Personen beurteilen und angemessene Massnahmen zur Vermeidung oder Verminderung der Risiken vorschlagen. Der Datenschutzbeauftragte prüft die Risikobeurteilung und die vorgeschlagenen Massnahmen und empfiehlt allenfalls zuhanden des verantwortlichen öffentlichen Organs Änderungen[5]. Dieses Konzept bleibt auch bei der europäischen Datenschutzreform unverändert, ja, es wird sogar verstärkt: Vor der «Vorabkonsultation»[6], wie die bisherige Vorabkontrolle neu zutreffender genannt wird, kommt eine «Datenschutz-Folgenabschätzung»[7]. Das ist nichts anderes als die Vorbereitung der Vorabkonsultation: Das verantwortliche öffentliche Organ soll sein Vorhaben daraufhin beurteilen, ob es datenschutzrelevant ist, welche Risiken es aus dem Blickwinkel des Datenschutzes und der Informationssicherheit beinhaltet und wie diese Risiken auf ein zulässiges und angemessenes Mass heruntergefahren werden können, so dass das öffentliche Organ das Restrisiko verantworten kann.

Voraussetzungen

Kriterien Für den Entscheid, ob ein Projekt dem Datenschutzbeauftragten vorgelegt werden muss, legt die Informations- und Datenschutzverordnung Kriterien fest[8]. Ein Vorhaben ist dem Datenschutzbeauftragten vorzulegen:

- wenn ein Abrufverfahren vorgesehen ist,
- wenn besondere Personendaten bearbeitet werden,
- wenn damit der Einsatz einer neuen Technologie verbunden ist,
- wenn eine grosse Anzahl Personen betroffen ist[9],
- wenn ein Datenpool im Sinn von § 1a IDV errichtet werden soll, oder
- wenn ein Gesetz oder eine Verordnung es vorsieht[10].

Abrufverfahren Als Datenbekanntgabe im Abrufverfahren[11] gelten:

- die Bekanntgabe über Daten via eine Benutzungsoberfläche (Onlinezugriff),
- das Zurverfügungstellen von Daten via einen Webservice und
- das periodische und automatisierte Zurverfügungstellen von Listen[12].

Besondere Personendaten Unter besonderen Personendaten[13] sind sensitive Personendaten und Persönlichkeitsprofile zu verstehen. Sensitive Personendaten[14] sind Personendaten, bei deren Bearbeitung eine besondere Gefahr der Grundrechtsverletzung besteht, insbesondere Angaben über a. die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, b. die Gesundheit, das Erbgut, die persönliche Geheimsphäre oder die ethnische Herkunft, c. Massnahmen der sozialen Hilfe und d. administrative oder strafrechtliche Verfolgungen und Sanktionen. Persönlichkeitsprofile[15] sind Zusammenstellungen von Informationen, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlauben.

Neue Technologien Beim Einsatz von neuen Technologien muss berücksichtigt werden, dass hierunter auch Ablösungsprojekte fallen – selbst wenn die neue Lösung auf einer bewährten Technologie basiert[16]. Es geht nicht bloss darum, die Risiken «neuer» Technologie abzufangen, sondern zu beurteilen, ob bei einem Technologiewechsel die erforderlichen Massnahmen getroffen werden, um die (neuen oder alten) Risiken zu vermeiden oder so weit zu vermindern, dass das verantwortliche öffentliche Organ das Restrisiko übernehmen kann.

Eine möglichst frühe Kontaktaufnahme durch die Verantwortlichen ermöglicht eine gute Planung und Definition der Rahmenbedingungen für die jeweilige Vorabkontrolle.

Vorlagepflicht Trifft nach der Beurteilung durch die Dateneignerin mindestens eine dieser Voraussetzungen zu, muss das verantwortliche öffentliche Organ das Projekt dem Datenschutzbeauftragten vorlegen. Dieser entscheidet in der Folge eigenständig darüber, ob und mit welcher Prüfungstiefe er eine Beurteilung vornimmt und eine Empfehlung abgibt.

Durchführung

Zeitpunkt Zu welchem Zeitpunkt, also in welcher Phase des Projekts eine Vorabkontrolle stattfindet, sollte abhängig vom Projekt und im Zusammenspiel mit den Verantwortlichen definiert werden. Eine möglichst frühe Kontaktaufnahme durch die Verantwortlichen ermöglicht eine gute Planung und Definition der Rahmenbedingungen für die jeweilige Vorabkontrolle. Die Vorabkontrolle kann auch gestaffelt erfolgen. So ist möglich, dass verschieden Aspekte eines Vorhabens jeweils einzeln beurteilt werden. Die Vorabkontrolle findet in jedem Fall während der Laufzeit des Projektes statt. Wichtig ist, dass die Vorabkontrolle zu einem Zeitpunkt stattfinden, bei welchem die Empfehlungen berücksichtigt werden können. Eine zu späte Konsultation und Durchführung der Vorabkontrolle kann zur Folge haben, dass die Empfehlungen nur mit erheblichen Mehrkosten oder im schlechtesten Fall gar nicht mehr berücksichtigt werden können. Somit hätte die Dateneignerin eine neue Lösung angeschafft, die unter Umständen den Anforderungen an den Datenschutz und die Informationssicherheit nicht genügt. Es liegt in der Natur von Projekten, dass sie eine Entwicklung durchmachen, dass mit zunehmendem Fortschritt die Konzepte immer konkreter werden und dass schliesslich eine Lösung entsteht, die operativ eingesetzt werden kann und sowohl den fachlichen als auch den nicht fachlichen und qualitativen Anforderungen genügt. Selbstverständlich wird dieser Umstand auch bei der Vorabkontrolle berücksichtigt. So wird sich beispielsweise eine Risikoanalyse im Verlauf eines Projektes verändern, sie soll konkreter werden und neue Erkenntnisse berücksichtigen.

Umfang und Tiefe Wie der Zeitpunkt der Durchführung ist auch der Umfang sowie die Tiefe der Vorabkontrolle abhängig vom Umfang des Projektes, von den bearbeiteten (Personen-)Daten, von der Art des Projektes, der Projektgrösse und der Projektmethode: Ein Projekt, das beispielsweise nach der «Wasserfall-Methode» durchgeführt wird, kann auch bei der Vorabkontrolle nicht gleich behandelt werden wie ein Projekt, das mit einem «iterativen Ansatz» durchgeführt wird. Bezüglich des Umfangs und der Tiefe der Vorabkontrolle ist u.a. die Risikoeinschätzung bezüglich den besondere Risiken für die Rechte und Freiheit der betroffenen Personen treibend. Ziel muss es aber in jedem Fall sein, dass der Aufwand sowohl für das Projekt als auch für den Datenschutzbeauftragten so optimal wie möglich gehalten wird. Kosten und Nutzen sollen so gut wie möglich in Einklang gebracht werden. >

Gerade bei grösseren Projekten erscheint die Kombination einer Projektbegleitung und möglicherweise eine gestaffelte Vorabkontrolle als geeignetes Vorgehen.

Unterlagen Die Informationen und Unterlagen, welche vom Datenschutzbeauftragten für die Beurteilung benötigt werden, sollten weitgehend denen entsprechen, welche für die fertige Lösung und den Betrieb der Lösung vorhanden sein müssen, die für eine zuverlässige Durchführung eines Projektes unerlässlich sind – und vom Datenschutzbeauftragten bei einer Kontrolle als vorhanden vorausgesetzt werden. Hierbei spielt es für den Datenschutzbeauftragten letztlich keine Rolle, in welcher Form, in welchem Dokument, die Angaben festgehalten werden. Je umfangreicher ein Projekt ist, umso sinnvoller erscheint es, die Grundlagen im persönlichen Kontakt, möglicherweise gar im Rahmen einer Projektbegleitung zu klären. In der Regel ist diese Vorgehen sowohl für die Verantwortlichen der entstehenden Lösung (die Dateneignerin oder Gesamtverantwortliche) und das Projekt-Team als auch für den Datenschutzbeauftragten effizienter und führt zu qualitativ besseren Rückmeldungen.

Regelungsbedarf

Zu regelnde Punkte Damit ein IT-Projekt als mit dem Informations- und Datenschutzgesetz[17] vereinbar qualifiziert werden kann, müssen mindestens folgende Punkte angemessen geregelt sein:

— (fachliche) Verantwortung (Gesamtverantwortung/Dateneignerin usw.) für die bearbeiteten Informationen;

— Datenmanagement (bearbeitete Informationen/Informationsflüsse/Vernichtung/Archivierung etc.)

— Benutzer- und Zugriffskonzept (Erfassen/Mutieren/Zugreifen/Vernichtung und «wer darf was» unter Berücksichtigung des Verhältnismässigkeitsprinzips [need-to-know]);

— Protokollierung und Auswertung (Zweck, daraus abgeleitet: die zu speichernden Informationen, Zugriffsschutz, Verantwortlichkeit sowie Vernichtung der Protokolldaten);

— Analyse der gesetzlichen Grundlagen (darf mit bestehenden gesetzlichen Grundlagen die Bearbeitung wie geplant durchgeführt werden?);

— Dokumentation der Schnittstellen (gegebenenfalls inklusive Autorisierung durch die Dateneignerinnen bei Abrufverfahren[18]);

— Ermittlung und Dokumentation des Schutzbedarfs inklusive Risikoanalyse zu mindestens den Schutzzielen, bei denen ein erhöhter oder hoher Schutzbedarf ausgewiesen ist;

— Massnahmen (technisch und organisatorisch) zu den Schutzzielen Vertraulichkeit, Integrität, Verfügbarkeit, Zurechenbarkeit und Nachvollziehbarkeit (basierend auf der Risikoanalyse);

— Systemübersicht/Systembeschreibung: Aufbau des Gesamtsystems; Abbildung und Beschreibung der wichtigsten Anforderungen für die Informationssysteme;

— besondere vertragliche Aspekte (bei der Beteiligung externer Dienstleister).

Zusätzliche Unterlagen Je nach Projekt sind zusätzliche Informationen nötig. Ausserdem kann es sinnvoll sein, detaillierter auf die Verantwortlichkeiten nach der Inbetriebnahme einzugehen. Die oben aufgeführten Punkte sind die Grundlage, damit der Datenschutzbeauftragte eine Vorabkontrolle durchführen kann. Alle aufgeführten Themen müssen aber innerhalb des Projektes ohnehin behandelt werden, unabhängig davon, ob eine Vorabkontrolle stattfindet oder nicht. Zudem würden diese Informationen später auch für eine allfällige Prüfung des eingeführten IT-Systems benötigt werden. Es ist dringend zu empfehlen, den obengenannten Punkten bereits in einer frühen Projektphase Aufmerksamkeit zu schenken und laufend zu konkretisieren.

Mit der Vorabkonsultation kann und soll dafür gesorgt werden, dass die Anliegen des Grundrechtsschutzes der von staatlicher Datenbearbeitung betroffenen Personen in den (vor allem IT-)Projekten von Anfang an mitberücksichtigt werden.

Sinnvolles Instrument – zu wenig genutzt

Sinnvoll Mit der Vorabkontrolle (oder künftig eben treffender: mit der Vorabkonsultation[19]) kann und soll dafür gesorgt werden, dass die Anliegen des Grundrechtsschutzes der von staatlicher Datenbearbeitung betroffenen Personen in den (vor allem IT-)Projekten von Anfang an mitberücksichtigt werden. Lieber rechtzeitig den Datenschutz miteinbeziehen als nachher ein frisch beschafftes System teuer reparieren oder feststellen müssen, dass Teile davon nicht genutzt werden dürfen. Die Vorabkontrolle basiert auf Vorarbeiten des öffentlichen Organs, die es ohnehin leisten müsste – im neuen europäischen Recht ist dies als «Datenschutz-Folgenabschätzung» enthalten. Der Erfolg steht und fällt aber mit der rechtzeitigen Vorlage an den Datenschutzbeauftragten.

Leider wenig genutzt Die Vorabkontrolle als Instrument des präventiven Datenschutzes wird aber leider zu wenig genutzt. Im Jahr 2016 hat der Datenschutzbeauftragte zwar (ohne die Vorabkontrollen zu Onlinezugriffs-Autorisierungen[20]) 21 Vorabkontrollen durchgeführt; 13 davon betrafen allerdings Videoüberwachungen. Das heisst: Es blieben netto acht Vorabkontrollen. Dafür muss der Datenschutzbeauftragte hinterher, wenn Detailfragen im Raum stehen, feststellen, dass Projekte eben nicht vorher, rechtzeitig zur Vorabkontrolle vorgelegt worden sind. Wenn dann beispielsweise Verträge mit Externen bereits abgeschlossen sind, ist es sehr aufwändig, nachträglich die notwendigen Klauseln – zum Beispiel betreffend Auftragsdatenbearbeitungen – noch einzubringen.

Damit der präventive Datenschutz nicht bloss eine gute Idee bleibt, muss die Vorabkontrolle besser in die Standardprozesse bei Beschaffungen integriert werden.

Verbesserung in Sicht? Damit der präventive Datenschutz nicht bloss eine gute Idee bleibt, muss die Vorabkontrolle besser in die Standardprozesse bei Beschaffungen integriert werden. Entsprechende Vorarbeiten laufen – sie müssen noch zu einem guten Abschluss gebracht werden.

Zusammenfassung

Rechtzeitige Kontaktaufnahme Die Vorabkontrolle ist ein Instrument des präventiven Datenschutzes. Lieber rechtzeitig den Datenschutz miteinbeziehen als nachher ein frisch beschafftes System teuer reparieren oder feststellen müssen, dass Teile davon nicht genutzt werden dürfen. Die Vorabkontrolle basiert auf Vorarbeiten des öffentlichen Organs, die es ohnehin leisten müsste – im neuen europäischen Recht ist dies als «Datenschutz-Folgenabschätzung» enthalten. Der Erfolg steht und fällt aber mit der rechtzeitigen Vorlage an den Datenschutzbeauftragten. Es empfiehlt sich, möglichst frühzeitig mit ihm Kontakt aufzunehmen, um den Aufwand für die Vorabkontrolle möglichst gering zu halten. Leider wird dieses sinnvolle Instrument des präventiven Datenschutzes noch zu wenig genutzt. Eine Verbesserung könnte erreicht werden, wenn die Vorabkontrolle (oder künftig eben treffender: die Vorabkonsultation) besser in die Standardprozesse integriert würde.

1 § 13 IDG, §§ 2-4 IDV.
2 Das öffentliche Organ, das die Informationen zur Erfüllung seiner gesetzlichen Aufgaben bearbeitet und somit die Verantwortung für den Umgang mit diesen Informationen trägt (§ 6, 8 IDG).
3 Vgl. dazu PK-IDG/BS-Rudin, § 13 N 7.
4 § 44 lit. f IDG; vgl. dazu PK-IDG/BS-Schilling, § 44 N 29 ff.
5 § 13 Abs. 2 IDG; vgl. dazu PK-IDG/BS-Rudin, § 13 N 54 ff.
6 Art. 28 RL 2016/680.
7 Art. 27 RL 2016/680; Art. 8bis Ziff. 2 E-ER-Konv 108.
8 § 2 Abs. 1 IDV; vgl. dazu PK-IDG/BS-Rudin, § 13 N 11 ff.
9 Von einer grossen Anzahl Personen wird gesprochen, wenn über 10000 Personen von einer Datenbearbeitung betroffen sein dürften (PK-IDG/BS-Rudin, § 13 N 24, mit Verweis auf den Mantelbericht IDV).
10 Zum Beispiel bei Pilotversuchen zur Bearbeitung von besonderen Personendaten ohne formellgesetzliche Grundlage (§ 9a Abs. 1 IDG) oder beim Erlass oder der Verlängerung von Videoüberwachungsreglementen (§ 18 Abs. 4 IDG).
11 Vgl. dazu PK-IDG/BS-Rudin, § 13 N 19 f.
12 So soll § 9a Abs. 1 IDV lauten, sobald er durch die Verordnung über den Datenmarkt geändert ist.
13 § 3 Abs. 4 IDG; vgl. dazu PK-IDG/BS-Rudin, § 3 N 33 ff.
14 § 3 Abs. 4 lit. a IDG; vgl. dazu PK-IDG/BS-Rudin, § 3 N 35 ff.
15 § 3 Abs. 4 lit. b IDG; vgl. dazu PK-IDG/BS-Rudin, § 3 N 43 ff.
16 Vgl. dazu PK-IDG/BS-Rudin, § 13 N 22 f.
17 Insbesondere mit §§ 6, 8, 9 und 12 IDG.
18 §§ 9a und 9b IDV.
19 Vgl. unten S. 21.
20 Vgl. dazu unten S. 29.

Thema 3 Auswirkungen der europäischen Datenschutzreform

Seit dem Erlass der europäischen Datenschutz-Regelwerken – 1981 die Europaratskonvention, 1995 die EG-Datenschutzrichtlinie 95/46 – hat die Technologie riesige Fortschritte gemacht. Nun werden diese Regelwerke modernisiert und Bund und Kantone müssen ihr Datenschutzrecht anpassen. Inwiefern besteht Anpassungsbedarf beim Informations- und Datenschutzgesetz des Kantons Basel-Stadt?

Ausgangslage

Europarats-Konvention Die Schweiz hat 1997 die Europaratskonvention 108 (ER-Konv 108) von 1981 (und 2006 das Zusatzprotokoll [ZP zur ER-Konv 108] von 2001) ratifiziert. Darum mussten Bund und Kantone ihre Datenschutzgesetze den Anforderungen anpassen.

EG-Datenschutz-Richtlinie Aufgrund der Schengen-Assoziierung der Schweiz wurde auch die Datenschutz-Richtlinie 95/46/EG (DS-RL 95/46/EG) für die Schweiz verbindlich[1]. Wer Zugang zu den riesigen Datenbeständen des Schengener Informationssystems (SIS) will, muss auch einen Minimalstandard an Datenschutz gewährleisten. Bund und Kantone mussten auch deshalb ihre Datenschutzgesetze anpassen. Ausserdem wurde aufgrund der Schengen-Assoziierung 2010 für die Schweiz auch der Rahmenbeschluss 2008/977/JI, der Datenschutzvorgaben für die justizielle und polizeiliche Zusammenarbeit macht, verbindlich.

Umsetzung Der Kanton Basel-Stadt hat die Anpassungen, die nötig waren, um den Anforderungen der ER-Konv 108 und der EG-DSRL 95/46 zu entsprechen, durch eine Revision des Datenschutzgesetzes[2] vorgenommen. Die revidierten Bestimmungen traten per 1. Juni 2008 bzw. per 1. Februar 2009 in Kraft. Auf Änderungen zur Umsetzung des Rahmenbeschlusses 2008/977/JI wurde verzichtet. Die angepassten DSG-Bestimmungen wurden inhaltlich unverändert in das per 1. Januar 2012 in Kraft getretene Informations- und Datenschutzgesetz übernommen.

Europäische Datenschutzreform

Modernisierung der ER-Konv 108 Der Europarat ist daran, die Europarats-Konvention 108 zu modernisieren. Das ist nötig geworden, weil sich die Technologie seit der Verabschiedung dieser Konvention im Jahre 1981 erheblich verändert hat. Es ist davon auszugehen, dass die Bundesversammlung die modernisierte Konvention, die gleichsam einen globalen Minimalstandard umschreibt, ratifizieren wird, so dass Bund und Kantone verpflichtet sein werden, im Datenschutzrecht die notwendigen Anpassungen vorzunehmen.

EU-Datenschutzreform Am 27. April 2016 hat die Europäische Union nach mehrjährigen Verhandlungen eine Datenschutzreform beschlossen. Sie besteht aus

— der Datenschutz-Grundverordnung 2016/679 (DSGVO), die generell für alle Datenbearbeiter in der EU gilt, also für Private und staatliche Organe, und

— der Datenschutz-Richtlinie 2016/680 (DS-RL 2016/680), die das Datenbearbeiten im Rahmen der justiziellen und polizeilichen Datenbearbeitung regelt.

EU-Datenschutz-Grundverordnung Die DSGVO ist – als Verordnung – für die EU-Mitgliedstaaten unmittelbar verbindlich, nicht aber für die Schweiz, da die Verordnung nicht als schengen-relevant erklärt wurde. Die Schweiz ist auch nicht verpflichtet, sie umzusetzen. Allerdings muss die EU-Kommission nach Art. 45 DSGVO (wie schon bisher nach Art. 15 DS-RL 95/46/EG) darüber entscheiden, ob die Schweiz ein angemessenes Schutzniveau bietet. Nur dann ist eine Datenübermittlung in die Schweiz ohne weitere Massnahmen zulässig. Im Rahmen dieser Prüfung der Angemessenheit des Schutzniveaus wird dann natürlich auch darauf geachtet, wie die Schweiz den Datenschutz sicherstellt.

EU-Datenschutz-Richtlinie Die Datenschutz-Richtlinie 2016/680 wurde hingegen als schengen-relevant erklärt und der Schweiz am 1. August 2016 notifiziert[3]. Innerhalb von zwei Jahren ab diesem Zeitpunkt, also bis August 2018, müssen Bund und Kantone nun die entsprechenden Anpassungen in ihrem Datenschutzrecht vornehmen, wenn sie nicht die Kündigung des Schengen-Assoziierungs-Abkommens riskieren wollen.

Wer Zugang zu den riesigen Datenbeständen des Schengener Informationssystems (SIS) will, muss auch einen Minimalstandard an Datenschutz gewährleisten.

Schweizerische Datenschutzreform

Revisionsbemühungen im Bund Der Bundesrat hat am 21. Dezember 2016 die Vernehmlassung darüber eröffnet, wie er die Bundesgesetzgebung an die europäischen Anforderungen anpassen will. Ebenfalls berücksichtigt werden sollen die Ergebnisse der Evaluation des Bundesdatenschutzgesetzes. Die Vernehmlassungsfrist läuft anfangs April 2017 ab; es ist geplant, dass die Botschaft im Herbst 2017 veröffentlicht wird.

Anpassungsbedarf in den Kantonen Die Kantone müssen ihr Datenschutzrecht ebenfalls an die neuen Anforderungen anpassen[4].

KdK-Leitfaden Um die kantonalen Rechtsetzungsbemühungen zu erleichtern, hat die Konferenz der Kantonsregierungen (wie schon mit der KdK-Wegleitung 2006[5] bei der Schengen-Assoziierung) eine Hilfestellung zugunsten der Kantone verabschiedet: Der Leitfaden wurde in der interdisziplinär zusammengesetzten Arbeitsgruppe Datenschutz der Begleitorganisation Schengen/Dublin (BOSD) der Konferenz der Kantonsregierungen erarbeitet und soll 2017 den Kantonen zugestellt werden[6].

Anpassungsbedarf im Kanton

Die wichtigsten Anpassungen In der Folge soll schon einmal kurz auf die wichtigsten Anpassungen im IDG des Kantons Basel-Stadt hingewiesen werden.

Geltungsbereich Die europäischen Vorgaben sehen keine Ausnahme mehr vor bei hängigen Verfahren der Zivil- und Strafgerichtsbarkeit und der Verwaltungs- und Verfassungsgerichtsbarkeit[7]. Das heisst, dass das IDG künftig auch in diesen Verfahren Anwendung finden soll. Die jetzigen Ausnahmeregelungen stammen aus einer Zeit, als noch unklar war, wie die verschiedenen Ebenen des Datenschutzrechts zusammenwirken: Das IDG enthält (als sog. «allgemeines Datenschutzrecht») nur die Grundsätze, die konkreten Regelungen für das Datenbearbeiten durch die öffentlichen Organe finden sich in den Fachgesetzen, also im Schulgesetz, im Polizeigesetz oder im Sozialhilfegesetz (sog. «besonderes oder bereichsspezifisches Datenschutzrecht»). Und eigentlich sind die Prozessordnungen nichts anderes als eben solches bereichsspezifisches Datenschutzrecht. Ihre Bestimmungen gehen als lex specialis den IDG-Bestimmungen als lex generalis vor, bleiben folglich auch wirksam, wenn das IDG in diesen Verfahren gilt. In einer Strafuntersuchung wird also beispielsweise die Staatsanwaltschaft weiterhin alle Befugnisse haben wie bisher[8].

Die europäischen Vorgaben sehen keine Ausnahme mehr vor bei hängigen Verfahren der Zivil- und Strafgerichtsbarkeit und der Verwaltungs- und Verfassungsgerichtsbarkeit.

Kollisionsvermeidung Kollisionen kann es geben bezüglich der Informationsrechte der Betroffenen und bezüglich der Aufsicht. Diese lassen sich einfach verhindern, indem im IDG ausdrücklich festgehalten wird,

— dass sich die Rechte und Ansprüche der betroffenen Personen während hängigen Verfahren der Zivil- und Strafrechtspflege und während hängigen Verfahren der Verwaltungs- und Verfassungsgerichtsbarkeit ausschliesslich nach dem anwendbaren Verfahrensrecht richten, so dass das Recht auf Zugang zu den eigenen Personendaten (wie bisher) erst nach Abschluss eines Verfahrens geltend gemacht werden kann, und

— dass Datenbearbeitungen in hängigen Verfahren der Zivil- und Strafrechtspflege und in hängigen Verfahren der Verfassungs- und Verwaltungsgerichtsbarkeit nicht der Aufsicht der oder des Datenschutzbeauftragten unterstehen. >

Warum trotzdem? Wenn also – mit den erwähnten Zusatzregelungen – gar nicht viel ändert, warum ist die Korrektur beim Geltungsbereich trotzdem nötig? Die Verfahrensordnungen enthalten eben – zu Recht – nur die verfahrensspezifischen Bearbeitungsregeln. Allgemeine Bestimmungen wie etwa die Pflicht zur Sicherstellung der Informationssicherheit oder die Pflicht, bestimmte datenschutzrelevante Bearbeitungen der oder dem Datenschutzbeauftragten zur Vorabkontrolle vorzulegen, sind darin aber nicht enthalten. Dabei geht es nicht darum, künftig im konkreten Anwendungsfall zu kontrollieren, ob beispielsweise ein IMSI-Catcher oder ein «Staatstrojaner» zu Recht eingesetzt wird – genau das wird mit der zweiten oben genannten Ausnahme ja ausgeschlossen. Aber es soll vorher, generell und unabhängig von einem konkreten Anwendungsfall, dazu Stellung genommen werden können, wie der Einsatz solcher Mittel datenschutzkonform erfolgen kann.

Schutz für natürliche Personen Nur wenige Staaten haben wie die Schweiz den Schutz der Persönlichkeitsrechte auch juristischen Personen zukommen lassen. Das soll nun geändert werden – Personendaten sollen künftig nur noch Informationen über natürliche Personen sein[9]. Trotzdem werden juristische Personen nicht schutzlos: Die Bekanntgabe von oder der Zugang zu Informationen sind auch künftig noch einzuschränken, wenn private Geheimhaltungsinteressen überwiegen, also zum Beispiel Berufs-, Fabrikations- oder Geschäftsgeheimnisse offenbart oder Urheberrechte verletzt würden[10].

Begriffsdefinitionen Im IDG müssen die Begriffsdefinitionen angepasst werden. «Genetische Daten»[11] können allenfalls unter «Daten über das Erbgut»[12] mitverstanden werden, «Daten zum Sexualleben oder zur sexuellen Orientierung» eventuell unter «Daten über Intimsphäre» oder «Daten über die persönliche Geheimsphäre»[13]. Neu sind aber «biometrische Daten» in die Kategorie der besonderen Personendaten aufzunehmen[14]. Biometrische Daten sind mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, welche die eindeutige Identifizierung dieser Person ermöglichen oder bestätigen (biometrische Daten), also etwa Gesichtsbilder (d.h. durch Gesichtserkennungsprogramme gewonnene Daten zu einem Gesicht – also nicht jede Foto eines Gesichts!), daktyloskopische Daten, Stimmmuster, Iris-Muster usw.

Profiling als Datenbearbeitungsart Der Begriff des Persönlichkeitsprofils[15] ist in der Vergangenheit recht vage geblieben. Neu verwendet das europäische Recht den Begriff des «Profilings»[16]. Darunter wird jede Auswertung von Daten oder Personendaten verstanden, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen, insbesondere bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, Intimsphäre oder Mobilität vorherzusagen. Anknüpfungspunkt ist somit nicht mehr die «gefährliche» Datenart, sondern die «gefährliche» Bearbeitungsart. Inhaltlich werden die Anforderungen nicht strenger werden.

Zeitliche Begrenzung Stärker als bisher wird die zeitliche Komponente des Verhältnismässigkeitsprinzips betont. Schon bisher gehörte zur Verhältnismässigkeit[17], dass das Bearbeiten von Personendaten zeitlich befristet sein muss. Neu wird verlangt, dass für die Löschung (oder Anonymisierung) von Personendaten bzw. für eine regelmässige Überprüfung, ob Personendaten zur Aufgabenerfüllung noch erforderlich sind, Fristen vorzusehen sind und dass durch verfahrensrechtliche Vorkehrungen sicherzustellen ist, dass diese Fristen eingehalten werden[18].

Nur wenige Staaten haben wie die Schweiz den Schutz der Persönlichkeitsrechte auch juristischen Personen zukommen lassen. Das soll nun geändert werden – Personendaten sollen künftig nur noch Informationen über natürliche Personen sein.

Nachweis der Compliance Mehrfach wird in den neuen Rechtsgrundlagen verlangt, dass das verantwortliche öffentliche Organ oder die Auftragsdatenbearbeiterin/der Auftragsdatenbearbeiter die Einhaltung der Datenschutzbestimmungen nachweisen können muss[19]. Dieser Nachweis kann in einem Datenschutzmanagementsystem (DSMS) erbracht werden. DSMS basieren auf den ISO-Standards des Qualitätsmanagements (ISO 9001) und der Informationssicherheit (ISO 27001 usw.). Es wird festzulegen sein, wann es ein solches Managementsystem braucht bzw. in welchen Fällen eine andere Form des Nachweises genügen soll.

Auftragsdatenbearbeitung Auftragsdatenbearbeitungen werden immer häufiger und führen dazu, dass die Kontrolle über die Datenbearbeitungen immer mehr aus den Händen gegeben wird. Damit das nicht zulasten der Grundrechte der betroffenen Personen geht, sind die Anforderungen an die Auslagerung von Datenbearbeitungen noch klarer zu regeln[20].

Pflicht zur Information der Betroffenen Schon aufgrund des Rahmenbeschlusses 2008/977 hätte die Pflicht der öffentlichen Organe, die betroffenen Personen aktiv darüber zu informieren, dass Personendaten über sie erhoben werden (nicht nur bei besonderen Personendaten), eingeführt werden müssen – wie es der Bund in seinem DSG gemacht hat[21]. Das wird nun nachzuholen sein[22].

Datenschutz-Folgenabschätzung und Vorabkonsultation Im Grunde genommen nichts Neues ist die «Datenschutz-Folgenabschätzung»[23]: Das «Data Protection Impact Assessment» ist nichts anderes als die Vorbereitung des öffentlichen Organs, damit es die Voraussetzungen für den Nachweis der Einhaltung der Datenschutzvorschriften erbringen kann, und beschlägt dieselben Punkte, die bei Vorhaben, die voraussichtlich zu einem hohen Risiko für die Grundrechte der betroffenen Personen führen, für eine Vorabkonsultation erarbeitet werden müssen: Welche Risiken entstehen? Mit welchen Massnahmen werden die Risiken vermieden oder so weit vermindert, dass das verantwortliche öffentliche Organ das Restrisiko übernehmen kann? «Vorabkonsultation»[24] ist die bisherigen Vorabkontrolle – der neue Name passt besser, da es nicht um eine (nachträgliche) Kontrolle, sondern um eine (vorgängige) Beratung geht, bei welcher die oder der Datenschutzbeauftragte die Risikobeurteilung prüft und zu den vorgeschlagenen Massnahmen Stellung nimmt.

Neu wird verlangt, dass das verantwortliche öffentliche Organ oder die Auftragsdatenbearbeiterin/der Auftragsdatenbearbeiter die Einhaltung der Datenschutzbestimmungen nachweisen können muss.

Meldepflicht bei Datenschutzverletzungen Die unter dem Namen «Data breach notification» bekannte Meldepflicht[25] soll – anders als bei der zu weiten Umschreibung in der Vernehmlassungsvorlage des Bundes – nur greifen, wenn die Sicherheit so verletzt wird, dass bearbeitete Personendaten unwiederbringlich vernichtet werden oder verloren gehen, unbeabsichtigt oder unrechtmässig verändert oder offenbart werden oder dass Unbefugte Zugang zu solchen Personendaten erhalten. Die Meldung erfolgt an die Datenschutzbeauftragte oder den Datenschutzbeauftragten und unter Umständen an die betroffenen Personen – dann nämlich, wenn diese zur Abwendung des Schadens Massnahmen ergreifen können.

«Vorabkonsultation» ist die bisherigen Vorabkontrolle – der neue Name passt besser, da es nicht um eine (nachträgliche) Kontrolle, sondern um eine (vorgängige) Beratung geht, bei welcher die oder der Datenschutzbeauftragte die Risikobeurteilung prüft und zu den vorgeschlagenen Massnahmen Stellung nimmt.

Privacy by design und Privacy by default Damit der Grundrechtsschutz auch bei weiteren technischen Entwicklungen gewährleistet wird, sind die Prinzipien des «Privacy by design» und «Privacy by default» ins IDG aufzunehmen. Nach dem ersten sind bei Datenbearbeitungen von Anfang an Massnahmen zu treffen, die das Risiko von Verletzungen der Persönlichkeit oder der Grundrechte verringern und solchen Verletzungen vorbeugen. Nach dem zweiten Prinzip ist mittels geeigneter Voreinstellungen sicherzustellen, dass standardmässig nur diejenigen Personendaten bearbeitet werden, die für den jeweiligen Verwendungszweck erforderlich sind.

Nicht notwendige Ergänzungen Der Datenschutzbeauftragte ist der Überzeugung, dass aber verschiedene Vorgaben nicht zu Änderungen im IDG führen sollen:

— Es ist demnach keine Regelung für *automatisierte Einzelentscheidungen* nötig, weil sichergestellt ist, dass bei automatisierten Einzelentscheidungen die betroffene Person informiert wird (z.B. durch Eröffnung der entsprechenden Verfügung) und sie die Möglichkeit hat, sich zur Einzelentscheidung zu äussern (z.B. aufgrund des Anspruchs auf rechtliches Gehör). Auf die Informationspflicht oder das Anhörungsrecht könnte höchstens durch eine klare formellgesetzliche Regelung verzichtet werden, so dass eine entsprechende Regelung im IDG nicht nötig ist. >

— Es sind *Sanktionen* vorzusehen bei Verstössen gegen das IDG. Solche Möglichkeiten bestehen heute schon, zum Beispiel Strafbestimmung für Amtsgeheimnisverletzungen, Strafbestimmung für die auftragswidrige Verwendung oder Bekanntgabe von Personendaten durch die Beauftragten bei einer Datenbearbeitung im Auftrag usw. Auf die Einführung beispielsweise von Bussen gegen öffentliche Organ, die gegen das IDG verstossen, kann getrost verzichtet werden.

Weil der Kanton Basel-Stadt mit der Schengen-Revision des DSG von 2008 und vor allem mit der Schaffung des IDG von 2010 seine Hausaufgaben weitgehend gemacht hat, hält sich der Anpassungsbedarf im interkantonalen Vergleich in Grenzen.

Die Datenschutz-Richtlinie 2016/680 sieht vor, dass das nationale Recht (d.h. des Bundes bzw. der Kantone) die verantwortlichen öffentlichen Organe verpflichten muss, einen *(amtsinternen[26]) Datenschutzbeauftragten* zu benennen. In der Praxis haben die grösseren Dienststellen mit heiklen Datenbeständen auch ohne gesetzliche Pflicht solche Personen bezeichnet; alle Dienststellen dazu zu verpflichten, macht angesichts der Kleinheit vieler Dienststellen keinen Sinn. Allenfalls kann diese Pflicht, die aus der schengen-relevanten Richtlinie stammt, bereichsspezifisch, d.h. für die Kantonspolizei und die Staatsanwaltschaft, umgesetzt werden.

Ausblick

Anpassungsbedarf Weil der Kanton Basel-Stadt mit der Schengen-Revision des DSG von 2008 und vor allem mit der Schaffung des IDG von 2010 seine Hausaufgaben weitgehend gemacht hat, hält sich der Anpassungsbedarf im interkantonalen Vergleich in Grenzen. Es wird am grundsätzlichen Konzept des Datenschutzes und des Öffentlichkeitsprinzips nichts geändert – es sind bloss Ergänzungen und Verdeutlichungen des geltenden Rechts. Sie vorzunehmen ist aber erforderlich, weil andernfalls durch die technologischen und gesellschaftlichen Entwicklungen die Grundrechte der betroffenen Personen – also von uns allen – ausgehöhlt werden.

Zusammenarbeit Der Datenschutzbeauftragte wird in der Vorbereitung die Zusammenarbeit mit dem federführenden Präsidialdepartement suchen.

1 Art. 2 Abs. 2 und Anhang B des Schengen-Assoziierungs-Abkommen (SAA).
2 Grossratsbeschluss vom 16. April 2008.
3 Erläuternder Bericht zum VE-DSG, S. 27.
4 Vgl. ausführlicher dazu: Beat Rudin, Anpassungsbedarf in den Kantonen, digma 2017, S. 58-70.
5 Konferenz der Kantonsregierungen (KdK), Umsetzung Schengen/Dublin in den Kantonen: Datenschutz, Wegleitung, 2006
6 Der Leitfaden wurde am 2. Februar 2017 abgeschlossen und anschliessend den Kantonen zugestellt. Er ist auf der Website des Datenschutzbeauftragten des Kantons Basel-Stadt unter Datenschutz I Neues Datenschutzrecht abrufbar: <http://www.dsb.bs.ch/dam/jcr:8772f3e4-14ce-45ca-aff1-46b00d043d23/KdK%20Leitfaden%20DSG%20Kantone.pdf> (Kurz-URL: <http://bit.ly/2sfj00f>).
7 Vgl. KdK-Leitfaden 2017, Ziff. 2.2-2.4.
8 Vgl. dazu Beat Rudin, Überholte Ausnahmen beim Geltungsbereich, digma 2016, S. 122 ff.
9 Vgl. KdK-Leitfaden 2017, Ziff. 3.2.
10 § 29 Abs. 3 IDG; vgl. dazu PK-IDG/BS-Rudin, § 29 N 39 ff.
11 Vgl. KdK-Leitfaden 2017, Ziff. 3.5.
12 § 3 Abs. 4 lit. a Ziff. 2 IDG; vgl. dazu PK-IDG/BS-Rudin, § 3 N 37.
13 § 3 Abs. 4 lit. a Ziff. 2 IDG; vgl. dazu PK-IDG/BS-Rudin, § 3 N 37.
14 Vgl. KdK-Leitfaden 2017, Ziff. 3.6.
15 § 3 Abs. 4 lit. b IDG; vgl. dazu PK-IDG/BS-Rudin, § 3 N 43.
16 Vgl. KdK-Leitfaden 2017, Ziff. 3.8 und 4.2.
17 § 9 Abs. 3 IDG und § 16 IDG; vgl. dazu PK-IDG/BS-Rudin, § 9 N 51 und § 16 N 1 ff.
18 Vgl. KdK-Leitfaden 2017, Ziff. 4.6.
19 Vgl. KdK-Leitfaden 2017, Ziff. 4.10.
20 Vgl. KdK-Leitfaden 2017, Ziff. 4.12.
21 Art. 18a und 18b DSG.
22 Vgl. KdK-Leitfaden 2017, Ziff. 5.2 und 5.3.
23 Vgl. KdK-Leitfaden 2017, Ziff. 6.2.
24 Vgl. KdK-Leitfaden 2017, Ziff. 6.3.
25 Vgl. KdK-Leitfaden 2017, Ziff. 6.4.
26 Die oder der Datenschutzbeauftragte im Sinne des IDG heisst in der Richtlinie 2016/680 «die Aufsichtsbehörde»; gemeint ist hier ein amtsinterner Datenschutzberater.

Aus dem Alltag

Einblicke in die Beratungstätigkeit

Einblicke in die Kontrolltätigkeit

Pilotversuche, Informationszugangsgesuche und Geschäftslast

Statistische Auswertungen 2016 (mit Vorjahresvergleichen)

Aus dem Alltag

Einblicke in die Beratungstätigkeit

Fast täglich wird der Datenschutzbeauftragte mit neuen und herausfordernden Fragen kontaktiert. Diese «Einblicke in die Beratungstätigkeit» lassen die Breite der behandelten Themen erahnen: von der Datenbekanntgabe an die Unfallversicherung über die Adresssammelbekanntgabe für politische Zwecke, die Begründung von Neufestsetzungen des Eigenmietwertes oder Zugriffe auf Daten anderer öffentlicher Organe im Abrufverfahren bis hin zu Medienanfragen zu Themen aus der gesamten Verwaltungstätigkeit.

Bekanntgabe von Personendaten

Fragestellungen Der Datenschutzbeauftragte hat eine Checkliste «Bekanntgabe von Personendaten»[1] auf seiner Website veröffentlicht. Idealtypisch betrachtet sind bei einer Datenbekanntgabe auf Anfrage die folgenden Fragen zu stellen (bei einer Datenbekanntgabe «von sich aus» entfallen natürlich die ersten beiden Fragen):

— Darf das öffentliche Organ, das Personendaten erhalten will, die verlangten Daten überhaupt bearbeiten (erheben) (§ 9 IDG)?

— Darf das empfangende öffentliche Organ die Frage nach den verlangten Personendaten stellen? Oder ist diese Datenbekanntgabe (mit der Fragestellung wird implizit auch die Information bekannt gegeben, dass die betroffene Person Klientin des fragenden öffentlichen Organs ist) im Sinne von § 29 IDG einzuschränken?

— Bearbeitet das öffentliche Organ, das die verlangten Personendaten bekannt geben soll, diese überhaupt zu Recht (§ 9 IDG)? Unrechtmässig bearbeitete Personendaten dürfen nicht bekannt gegeben werden.

— Darf das öffentliche Organ, von dem die Bekanntgabe von Personendaten verlangt wird, diese bekannt geben (§§ 21 und 29 IDG)?

In der Praxis Die Frage, ob Personendaten von einem öffentlichen Organ an ein anderes oder an Privatpersonen bekannt gegeben werden dürfen, stellen sich im Praxisalltag der Verwaltung immer wieder. In der Folge sollen einzelne Fragen, die dem Datenschutzbeauftragten unterbreitet worden sind, dargestellt werden.

Der Datenschutzbeauftragte hat eine Checkliste «Bekanntgabe von Personendaten» auf seiner Website veröffentlicht.

Datenbekanntgabe an eine Unfallversicherung?

Medizinische Unterlagen Die Unfallversicherung eines Geschädigten prüfte die Frage des Regresses auf ein Kind mit einer Erziehungsbeistandschaft, das mutmasslich einen Unfall verursacht hatte, und verlangte vom Kinder- und Jugenddienst (KJD) die Herausgabe der medizinischen Unterlagen über das Kind, gestützt auf eine Bestimmung im ATSG[2]. Der KJD war im Besitz mehrerer Berichte verschiedener Ärzte, hatte jedoch nur einen davon selbst in Auftrag gegeben. Über weitere medizinische Akten verfügte er nicht.

Umfang der Herausgabe Zum einen stellte sich für den KJD die Frage, ob er diejenigen Berichte, die er nicht selbst in Auftrag gegeben hatte, überhaupt herausgeben dürfe. Zum anderen war er unsicher, wie er mit darin enthaltenen Informationen, welche die Mutter und das Verfahren bei der Kindes- und Erwachsenenschutzbehörde (KESB) betreffen, umgehen solle. In Absprache mit dem Datenschutzbeauftragten sandte der KJD alle ärztlichen Berichte an die Unfallversicherung, aber nicht ohne vorher alle Stellen, die nicht das Kind selber betrafen, einzuschwärzen.

Bekanntgabe zu einem nicht personenbezogenen Zweck?

Daten über FU-Rekursfälle Die Rekurskommission für Fürsorgerische Unterbringungen war unsicher, ob sie eine Exceltabelle mit den Daten über die Fälle von Patientinnen und Patienten der Universitären Psychiatrischen Kliniken (UPK), die von der Rekurskommission entschieden worden sind, an die UPK weitergeben darf. Die UPK wollte empirisch untersuchen, welche Gründe bei einem Rekurs angegeben wurden, wie die Rekurse jeweils entschieden wurden bzw. ob sich daraus Erkenntnisse für die Zukunft gewinnen lassen.

Nicht personenbezogener Zweck Ein öffentliches Organ darf «seine» Personendaten, die es personenbezogen zur Erfüllung seiner gesetzlichen Aufgabe bearbeitet, unter bestimmten Bedingungen bzw. Auflagen auch zu einem nicht personenbezogenen Zweck (weiter-)bearbeiten[3]. Als nicht personenbezogene Zweck erscheinen insbesondere Statistik, Planung und Forschung[4].

In casu Die UPK verfügen über die Krankengeschichten ihrer Patientinnen und Patienten. Ausserdem erhalten sie alle Entscheide der Rekurskommission, soweit sie ihre Patientinnen und Patienten betreffen. Gestützt auf § 10 IDG dürfen sie unter den entsprechenden Bedingungen bzw. Auflagen «ihre» Daten nicht personenbezogen zu Forschungszwecken bearbeiten. Die Rekurskommission darf gestützt auf § 22 IDG den UPK die Daten aus Rekursverfahren, die deren Patientinnen und Patienten betreffen, für den nicht personenbezogenen Zweck der Forschung bekannt geben. Da die UPK die Daten zum Zweck der personenbezogenen Bearbeitung ja bereits besitzen (einzig nicht in der strukturierten Form, wie sie bei der Rekurskommission festgehalten werden), sind an die (erneute) Bekanntgabe in strukturierter Form keine hohen Anforderungen zu stellen.

Sammeladressauskünfte

Rechtliche Grundlage im Aufenthaltsgesetz Das kantonale Aufenthaltsgesetz erlaubt es der Einwohnerkontrolle, beispielsweise die Adressdaten von in der Gemeinde wohnhaften Personen an Private bekannt zu geben[5]. Diese sogenannte Listenauskunft ist nur erlaubt, wenn die Daten ausschliesslich für schützenswerte ideelle Zwecke verwendet werden. Bis anhin sah das kantonale Einwohneramt in konstanter Praxis die politische Werbung nicht als schützenswerten ideellen Zweck im Sinne des Aufenthaltsgesetzes an[6]. Aufgrund eines Verwaltungsgerichtsurteils im Kanton Zug hat es seine Praxis überprüft; das Justiz- und Sicherheitsdepartement hat die daraus folgende Praxisänderung in einem Bericht an den Regierungsrat umschrieben. Der Bericht wurde vom Regierungsrat am 6. Dezember 2016 zur Kenntnis genommen und mit folgender Begründung veröffentlicht: «Das Einwohneramt ändert seine Praxis bei Sammeladressauskünften gegenüber Parteien. Gestützt auf Art. 30 Abs. 6 Aufenthaltsgesetz werden solche Auskünfte gegen Gebühr künftig erteilt, sofern die gesetzlich aufgelisteten Kriterien erfüllt sind und die Zielgruppe des Versandes derart definiert ist, dass die angeschriebene Person nur einmal mit persönlich adressierter Parteiwerbung bedient wird»[7].

In Vorfeld zum Regierungsratsbeschluss über die Praxisänderung bezüglich politischer Werbung hat der Datenschutzbeauftragte darauf hingewiesen, dass bei der Umsetzung darauf zu achten ist, dass eine konstante und rechtsgleiche Praxis entwickelt wird.

Zu beachten In Vorfeld zu diesem Regierungsratsbeschluss hat der Datenschutzbeauftragte darauf hingewiesen, dass bei der Umsetzung dieser Bestimmung – bzw. zu § 11 Abs. 2 lit. d NAG, der diese Bestimmung per 1. Juli 2017 ablöst – darauf zu achten ist, dass eine konstante und rechtsgleiche Praxis entwickelt wird. Es wird beispielsweise zu klären sein, was «nur einmal mit persönlich adressierter Parteiwerbung bedient» meint: Einmal pro Wahlgang? Einmal pro Wahl? Einmal pro Jahr? Von jeder Kandidatin, jedem Kandidaten? Von jeder Partei? Unbestreitbar und unbestritten ist, dass andere als die im Gesetz aufgelisteten Kriterien (Alter, Geschlecht, Adresse, Stimmberechtigung und Zuzug) nicht für die Selektion verwendet werden dürfen (z.B. Personen mit einem steuerbaren Einkommen von über oder unter …, nur mit bestimmten Berufen usw.). >

Abgrenzung Gestützt auf das Aufenthaltsgesetz können nicht nur zur Verfolgung eines schützenswerten ideellen Zwecks Personendaten Privaten bekanntgegeben werden, sondern gestützt auf § 30a AufenthG – bzw. auf § 12 NAG, der diese Bestimmung per 1. Juli 2017 ablöst – auch im Rahmen von Forschungs- und Präventionsprojekten.

Anfragen im Zuge der Neufestsetzung der Eigenmietwerte durch die Steuerverwaltung

Ausgangslage Die Steuerverwaltung Basel-Stadt hat die Eigenmietwerte bei Liegenschaften neu festgesetzt – sie muss dies periodisch tun. Das hat dieses Mal zu heftigen Diskussionen geführt. Der Datenschutzbeauftragte wurde im Vorfeld der Bewertung bzw. der Verfügung der neuen Werte nicht beigezogen. Hingegen haben sich verschiedene betroffene Personen an ihn gewandt. Sie haben bemängelt, dass ihnen «aus Datenschutzgründen» die Vergleichswerte nicht bekannt gegeben werden, die als Berechnungsgrundlage gedient haben. Als Berechnungsgrundlage des Eigenmietwertes dienten (unter anderem) Kaufpreise der im Kantonsgebiet verkauften Grundstücke in den Jahren 2013 und 2014.

Entgegenstehende Ansprüche In dieser Konstellation prallen zwei einander entgegenstehende Ansprüche aufeinander:

— Einerseits haben alle Personen einen aus dem verfassungsrechtlichen Anspruch auf rechtliches Gehör[8] hergeleiteten Anspruch auf Begründung von Verfügungen, die sie betreffen.

— Andererseits aber haben die Verkäuferinnen und Verkäufer bzw. die Käuferinnen und Käufer von Grundstücken den Anspruch, dass der bezahlte Kaufpreis nicht öffentlich gemacht wird. Bei der letzten Revision der Grundbuchverordnung (VOBG) stand die Frage zur Debatte, ob die Kaufpreise künftig publiziert werden sollen. Das wurde abgelehnt, was einen Entscheid für die (relative) Geheimhaltung darstellt; mindestens die Öffentlichkeit soll nicht erfahren, wer wieviel für welches Grundstück bezahlt oder bekommen hat[9].

Lösungsvorschlag Der Datenschutzbeauftragte hat für das Einspracheverfahren[10] angeregt, dass die für die Berechnung in einem bestimmten Raum zugrundeliegenden Verkäufe pseudonymisiert und mit kategorisierten Attributen mindestens den Einsprecherinnen und Einsprechern zugänglich gemacht werden. Wenn in einem bestimmten Raum z.B. drei Verkaufsfälle ausgewertet worden sind, dann werden diese als A bis C bezeichnet und mit den relevanten Informationen (in Kategorien dargestellt) aufgelistet. In Kategorien (z.B. 150-250m^2) deshalb, weil z.B. anhand der Quadratmeterzahl eines Grundstückes (z.B. 198m^2), das innerhalb eines Zeitraums von zwei Jahren in einem bestimmten in der Regel nicht sehr grossen Bezugsraumes verkauft worden ist, in aller Regel das konkrete Grundstück bestimmt werden kann – es sind oft nur sehr wenige vergleichbare Verkaufsfälle. Weiter müssten möglicherweise andere preisbestimmende Faktoren mitgeliefert werden, z.B. für eine Überbauung ungünstige Grundstückform, die Nähe zu Lärmquellen, die noch nicht ausgeschöpfte Ausnutzung usw. Welche Informationen dies sind und wie die Kategorien zu bilden sind, müsste von den Fachbehörden bestimmt werden. Falls nach dem Einspracheverfahren ein Rekursverfahren folgt, könnte die Steuerrekurskommission dann mit den entpseudonymisierten Daten entscheiden. Damit könnten die beiden eingangs erwähnten Ansprüche so miteinander in Einklang gebracht werden, dass einerseits die von der Eigenmietwerterhöhung betroffenen Grundeigentümer nicht «im Blindflug» Einsprache und Rekurs einreichen müssen und andererseits die Verkäufer- und Käuferschaft nicht erleben muss, dass der bezahlte Preis nicht doch öffentlich zugänglich wird.

Es wird interessant sein, wie die allenfalls angerufenen Gerichte die für die Betroffenen nicht kontrollierbare Begründung der Eigenmietwertfestsetzung, mithin also die Verletzung des verfassungsrechtlichen Begründungsanspruches beurteilen werden.

Abgelehnt Die angeregte Lösung wurde von der Steuerverwaltung und der Bodenbewertungsstelle als zu aufwändig verworfen, was rein aus verwaltungsökonomischer Sicht nachvollziehbar ist. Es wird allerdings interessant sein, wie die allenfalls angerufenen Gerichte die für die Betroffenen nicht kontrollierbare Begründung der Eigenmietwertfestsetzung, mithin also die Verletzung des verfassungsrechtlichen Begründungsanspruches beurteilen werden.

Vorabkontrolle zu Onlinezugriffs-Gesuchen

AWS Die Zentralen Informatikdienste (ZID) haben – in enger Zusammenarbeit mit dem Datenschutzbeauftragten und unter Einbezug von Vertreterinnen und Vertretern der wichtigsten Dateneignerinnen – den elektronischen Workflow für die Onlinezugriffs-Gesuche AWM («Autorisierungs-Workflow-System») erarbeitet. Das System soll in der zweiten Hälfte 2017, nach der Schulung der Dateneignerinnen, aufgeschaltet werden. Es löst das bisherige, eher aufwändige papierbasierte System ab und wird hoffentlich den Prozess zur Stellung und Verlängerung von Onlinezugriffen vereinfachen und für alle Beteiligten übersichtlicher gestalten.

Sich «bedienen» können Wenn ein öffentliches Organ im Abrufverfahren auf Personendaten eines anderen öffentlichen Organs zugreifen können will – sich quasi bei den Daten eines anderen öffentlichen Organs «bedienen» will –, muss es ein sog. Onlinezugriffs-Gesuch stellen. Bevor der Onlinezugriff freigeschaltet wird, muss die Dateneignerin der Daten, auf welche zugegriffen werden können soll, dieses Gesuch bewilligen, den künftigen Onlinezugriff also «autorisieren». Ausserdem müssen diese Genehmigungen vorab dem Datenschutzbeauftragten zur Stellungnahme unterbreitet werden.

Datenbekanntgabe im Abrufverfahren Die meisten dieser Onlinezugriffe erfolgen über den kantonalen Datenmarkt. Dieser stellt einen Datenpool im Sinne von § 1a IDV dar und bedarf nach § 1b IDV einer gesetzlichen Grundlage mindestens auf Verordnungsstufe. Im Berichtsjahr liefen die Vorbereitungsarbeiten an der neuen Datenmarktverordnung (DMV), welche die alte von 2005 ablösen sollte. Im Rahmen der DMV (bzw. der durch die Schlussbestimmungen der DMV geänderten IDV) soll nun einerseits der Begriff des Abrufverfahrens definiert werden. Als *Datenbekanntgabe im Abrufverfahren* gelten:

- die Bekanntgabe über Daten via eine Benutzungsoberfläche (Onlinezugriff),
- das Zurverfügungstellen von Daten via einen Webservice und
- das periodische und automatisierte Zurverfügungstellen von Listen[11].

Onlinezugriff Bei der Datenbekanntgabe im Abrufverfahren über eine Benutzeroberfläche (Onlinezugriff) greift eine berechtigte Person (oder greifen berechtigte Personen einer Verwaltungseinheit) mittels eines Webportals auf die «fremden» Daten zu (Mensch-zu-Maschine-Interaktion). Dies betrifft z.B. Auskünfte über Personen, Gebäude oder Motorfahrzeuge[12].

Wenn ein öffentliches Organ im Abrufverfahren auf Personendaten eines anderen öffentlichen Organs zugreifen können will – sich quasi bei den Daten eines anderen öffentlichen Organs «bedienen» will, muss es ein sog. Onlinezugriffs-Gesuch stellen.

Webservice Bei der Datenbekanntgabe im Abrufverfahren mittels Webservice werden Daten eines Systems über eine Schnittstelle einem anderen, berechtigten und eindeutig identifizierten System zur Verfügung gestellt (Maschine-zu-Maschine-Interaktion). Das maschinenlesbare Format ist jeweils in einer Schnittstellenbeschreibung spezifiziert. Es bestehen zahlreiche Webservices vom Datenmarkt zu den kantonalen Fachanwendungen. Beispiele dafür sind die Steuerlösung NEST, die MFK-Lösung Avedris, die Einwohnerlösung Loganto sowie die Baubegehrenlösung BBG[13].

Automatisiertes Zurverfügungstellen von Listen Schliesslich kann auch die Auslieferung von Listen im Auftrag der Dateneignerinnen eine Datenbekanntgabe im Abrufverfahren darstellen, dann nämlich, wenn sie periodisch und automatisiert erfolgt, wenn also die Dateneignerin in Bezug auf die konkrete Auslieferung faktisch nicht mehr selber die Rechtmässigkeit der Datenbekanntgabe und die Richtigkeit der bekanntzugebenden Daten prüft. Beispiele sind die monatliche Auflistung und Lieferung der Zuzüge und Wegzüge im Kanton als Basis für den Versand des kantonalen Abfuhrkalenders durch Gebäude- und Abwasserreinigung, die jährliche Lieferung der Gebäudedaten an das Hochbau- und Planungsamt, die jährliche Lieferung der Steueratlas-Daten an die Steuerverwaltung und die jährliche Aufbereitung der Daten für die Auszahlung der Gutschriften im Zusammenhang mit dem Stromsparfonds. In diesen Fällen muss dasselbe Autorisierungsverfahren durchlaufen werden wie bei der Einräumung eines Onlinezugriffs oder eines Datenbezuges mittels Webservice. >

Vorabkontrollen Im Berichtsjahr hat der Datenschutzbeauftragte in enger Zusammenarbeit mit den Zentralen Informatikdiensten (ZID) 57 Vorabkontrollen zu Onlinezugriffsgesuchen (2015: 17) durchgeführt. 39 davon konnten im Berichtsjahr abgeschlossen werden, 18 waren Ende 2016 noch in Arbeit. Ausserdem gab es 12 Geschäfte mit den Vorabkontrollen vorausgehenden Anfragen und Vorabklärungen. Der Grund für diese wiederum sehr hohe Zahl von Vorabkontrollen liegt in der Tatsache, dass einzelne Dateneignerinnen aktiv ihre Verantwortung wahrgenommen und systematisch die laufenden Bekanntgabe ihrer Daten im Abrufverfahren unter die Lupe genommen haben. Mit der Einführung des eingangs erwähnten AWS wird es für die Dateneignerinnen einfacher, den Überblick zu behalten, welche Abrufverfahren bezüglich ihrer Daten laufen.

Videoüberwachung

Vorabkontrollen Nach § 18 Abs. 4 IDG sind die Videoüberwachungsreglemente vor dem Erlass und der Verlängerung dem Datenschutzbeauftragten zur Vorabkontrolle vorzulegen. Im Berichtsjahr wurden 21 solche Vorabkontrollen (2015: 10) durchgeführt. Abgeschlossen werden konnten 18 Geschäfte, 3 waren Ende Jahr noch hängig. Die eher hohe Zahl von Vorabkontrollen rührt daher, dass im Jahr 2012 mit dem Inkrafttreten des neuen Videoüberwachungsregelung im IDG für viele Anlagen die Reglemente geschaffen werden musste – und 2016 sind damit die vier Jahre der Befristung[14] abgelaufen.

Weitere Beratungen Ausserdem behandelten je zwei Geschäfte Vorhaben videobasierter Verkehrsauswertung und Baufortschrittskameras.

Vernehmlassungen

Eingeladen Der Datenschutzbeauftragte hat die Aufgabe, zu Erlassen, die für den Umgang mit Informationen oder den Datenschutz erheblich sind, Stellung zu nehmen[15]. Bei 20 solcher Vorlagen (2015: 15) wurde der Datenschutzbeauftragten zur Stellungnahme eingeladen; elf betrafen kantonale Erlasse, neun Bundesvorlagen. Sie betrafen u.a.:

- die Verordnung über das Informatiksystem der Staatsanwaltschaft;
- die Totalrevision des Tagesbetreuungsgesetzes;
- die Revision der Smart Metering-Bestimmung des IWB-Gesetzes;
- die Ausführungsgesetzgebung zum Bundesgesetz über das elektronische Patientendossier (EPDG).

Der Datenschutzbeauftragte hat die Aufgabe, zu Erlassen, die für den Umgang mit Informationen oder den Datenschutz erheblich sind, Stellung zu nehmen. Auch weiterhin ist nicht garantiert, dass ihm alle Erlasse rechtzeitig vorgelegt werden.

Unvollständig Von den Departementen, die regelmässig Vorlagen ausarbeiten, die für den Umgang mit Informationen oder den Datenschutz erheblich sind, klappt der Einbezug beim Justiz- und Sicherheitsdepartement und beim Gesundheitsdepartement recht gut, wenn auch manchmal zeitlich etwas spät. In anderen Fällen wenden sich Dienststellen oder selbständige Anstalten des öffentlichen Rechts (beispielsweise die IWB) an den Datenschutzbeauftragten. Bei den Vorlagen, die fälschlicherweise dem Datenschutzbeauftragten nicht vorgelegt werden, ist teilweise anzunehmen, dass die Departemente die Relevanz für das Öffentlichkeitsprinzip oder den Datenschutz nicht erkennen. Aus diesem Grund empfiehlt es sich, alle Vorlagen dem Datenschutzbeauftragten zukommen zu lassen[16] mit Ausnahme jener, die offensichtlich keinerlei Berührungspunkte mit dem Umgang mit Informationen oder dem Datenschutz haben. Wenn der Datenschutzbeauftragte zur Überzeugung gelangt, es bestehe kein Bezug zu seinem Aufgabenbereich oder die Änderungen seien unterhalb einer Wesentlichkeitsschwelle, dann wird er rasch, und ohne weiteren Aufwand zu betreiben, auf eine Stellungnahme verzichten.

Schengen-Weiterentwicklungen

Schengen-Besitzstand Aufgrund der Natur der Schengen- und Dublin-Assoziierung als «dynamische Abkommen» ist die Schweiz verpflichtet, die Weiterentwicklungen des Schengener und Dubliner Besitzstands zu übernehmen. Im Berichtsjahr hat der Datenschutzbeauftragte sich mit acht Weiterentwicklungen (2015: 8) befasst; einzig zur Weiterentwicklung aufgrund der EU-Datenschutzreform hat er sich geäussert.

Datenschutzreform der EU und des Europarates Die Europäische Union hat der Schweiz am 1. August 2016 die Richtlinie (EU) 2016/680 als Schengen-Weiterentwicklung notifiziert. Die Schweiz muss der EU mitzuteilen, ob sie die Weiterentwicklung übernehmen will, und gegebenenfalls innert zwei Jahren die nötigen Gesetzesanpassungen vornehmen. Ausserdem steht die Ratifizierung der modernisierten Datenschutzkonvention des Europarates an. Der Datenschutzbeauftragte hat dazu gegenüber dem kantonsintern zuständigen Justiz- und Sicherheitsdepartement festgehalten, er gehe aus den folgenden Gründen davon aus, dass Bund und Kantone nicht darum herumkommen werden, die Weiterentwicklung des Datenschutzrechts der Europäischen Union zu übernehmen:

— Die neue Richtlinie (EU) 2016/680, die anstelle des Rahmenbeschlusses 2008/977 treten wird, ist schengen-relevant. Falls die Schweiz nicht das Risiko eingehen will, dass die Schengen-Assoziierung der Schweiz aufgelöst wird, wird sie nicht darum herumkommen, die Richtlinie zu übernehmen. Das betrifft nicht nur den Bund, sondern auch die Kantone.

— Auch wenn die Datenschutz-Grundverordnung (DSGVO), die anstelle der bisherigen Richtlinie 95/46/EG treten wird, nicht schengen-relevant ist, ist sie trotzdem nicht bedeutungslos für die Schweiz. Nach ihrem Art. 41 Ziff. 1 darf eine Übermittlung personenbezogener Daten an ein Drittland (wie die Schweiz) vorgenommen werden, wenn die EU-Kommission festgestellt hat, dass das betreffende Drittland ein angemessenes Schutzniveau bietet. Für diese Beurteilung der Angemessenheit des gebotenen Schutzniveaus werden insbesondere berücksichtigt: die Rechtsstaatlichkeit, die Achtung der Menschenrechte und Grundfreiheiten, die in entsprechenden Land geltenden einschlägigen Rechtsvorschriften, die Anwendung dieser Rechtsvorschriften, die Datenschutzbestimmungen, Berufsvorschriften und Sicherheitsvorschriften einschliesslich der Vorschriften für die Weitergabe personenbezogener Daten an ein anderes Drittland und die Existenz und die wirksame Funktionsweise einer oder mehrerer unabhängiger Aufsichtsbehörden. Die öffentliche Verwaltung, erst recht aber die Privatwirtschaft haben ein erhebliches Interesse, dass die EU-Kommission auch das in der Schweiz gebotene Schutzniveau als angemessen beurteilt. Ausserdem gilt die DSGVO nach ihrem Art. 3 Ziff. 2 lit. a unmittelbar auch für Datenbearbeitungen durch Schweizer Unternehmen, die Dienstleistungen in EU-Mitgliedstaaten anbieten – sie müssen also ohnehin diese Regelungen einhalten.

— Die modernisierte Europaratskonvention verlangt inhaltlich nichts, was weiter geht als die Weiterentwicklung des Datenschutzrechts in der Europäischen Union. Die Europaratskonvention gilt weit über Europa hinaus als Datenschutzstandard. Sowohl die öffentliche Verwaltung als auch die Privatwirtschaft haben ein gewichtiges Interesse daran, diesen Standard zu übernehmen.

— Das baselstädtische Informations- und Datenschutzgesetz wird angepasst werden müssen. Aber es muss nicht in seinem Grundkonzept überarbeitet werden. Der Grundaufbau kann bestehen bleiben, es braucht nur Ergänzungen bzw. detaillierte Präzisierungen.

Aufgrund der Natur der Schengen- und Dublin-Assoziierung als «dynamische Abkommen» ist die Schweiz verpflichtet, die Weiterentwicklungen des Schengener und Dubliner Besitzstands zu übernehmen.

— Inwiefern Mehrkosten entstehen werden, kann vom Datenschutzbeauftragten nicht abschliessend beurteilt werden. Es wird sicher z.B. aufgrund von zusätzlichen Informationspflichten ein gewisser Mehraufwand entstehen. Die grössten Kosten dürften wohl bei der technischen Umsetzung anfallen, etwa bei der Protokollierung (Logging). Das sind allerdings Aufwendungen, die unabhängig von der Umsetzung der hier behandelten Weiterentwicklungen in näherer Zukunft zur Gewährleistung der Informationssicherheit ohnehin getätigt werden müssen.

— Der Datenschutzbeauftragte hat angeregt, dass die KdK wiederum (wie 2006 im Hinblick auf die (damals neue) Assoziierung der Schweiz an Schengen) zuhanden der Kantons eine «Handreichung» für die Umsetzung der neuen Richtlinie ins kantonale Recht verfassen zu lassen[17]. >

Unterstützung Der Datenschutzbeauftragte war schon an der Ausarbeitung des KdK-Leitfaden beteiligt und wird bei der Vorbereitung der notwendigen IDG-Revision seine Unterstützung anbieten (vgl. auch vorne Seiten 18 ff.).

Die Europaratskonvention gilt weit über Europa hinaus als Datenschutzstandard. Sowohl die öffentliche Verwaltung als auch die Privatwirtschaft haben ein gewichtiges Interesse daran, diesen Standard zu übernehmen

Medienanfragen

Gesteigertes Medieninteresse 31 Medienanfragen hat der Datenschutzbeauftragte im Jahr 2016 erhalten (2015: 16). Die Anfrage der nationalen Medien dürften ihren Grund zum Teil in der privatim-Präsidentschaft haben.

Themen Die Medienanfragen befassten sich mit einer sehr breiten Themenpalette. Sie betrafen u.a.:

— die Erfahrungen mit dem Öffentlichkeitsprinzip;
— die politische Forderung, zur Ermittlung von Straftätern die Analyse codierender Abschnitte der DNA zuzulassen («Aufweichung» des DNA-Profil-Gesetzes);
— den eHealth-Modellversuch Basel;
— den Einsatz von IMSI-Catchern, d.h. von Geräten, mit denen die auf der SIM-Karte eines Mobiltelefons gespeicherte International Mobile Subscriber Identity (IMSI) ausgelesen und der Standort eines Mobiltelefons innerhalb einer Funkzelle eingegrenzt werden kann;
— mehrmals die Wahl des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten;
— mehrmals die Videoüberwachung;
— die Resultate der Datenschutz-Audits des Datenschutzbeauftragten (im Nachgang zur Veröffentlichung des Tätigkeitsberichtes 2015);
— den (nicht erhärteten) Verdacht, dass Immobilien Basel-Stadt auf Daten des Betreibungs- und Konkursamtes zugreifen kann und diese Daten zur Auswahl von Mietinteressentinnen und Mietinteressenten verwendet;
— den Vertrag zwischen dem Erziehungsdepartement und Nestlé betreffend Glacé-Verkauf in Sportanlagen;
— den Einsatz von BodyCams bei den Polizeikorps;
— die Weitergabe des Sperrvermerks bei der Bekanntgabe von Einwohnerdaten via Datenmarkt;
— die Rechtsgrundlagen zu Smart Grid/Smart Metering;
— das Radikalisierungs-Profiling-Tool «Ra-Prof».

Schulungen, Referate und Publikationen

Anhaltendes Interesse Auch in diesem Jahr blieb das Interesse an bereichsspezifischen datenschutz- und öffentlichkeitsrechtlichen Schulungen sowie an Referaten gross: Der Datenschutzbeauftragte hat im Berichtsjahr acht[18] (2014: 7) Schulungen für öffentliche Organe durchgeführt; hinzu kommen noch fast doppelt so viele Referate und Weiterbildungsbeiträge, die ebenfalls der Sensibilisierung dienen.

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

— zweimal das Seminar «Datenschutz und Öffentlichkeitsprinzip: kurz erklärt» im Rahmen des kantonalen Weiterbildungsangebotes;
— zwei Schulungen für den Sozialdienst der Universität;
— eine Schulung für die Mitarbeiterinnen und Mitarbeiter der Kindes- und Erwachsenenschutzbehörde (KESB);
— eine Schulung für die Mitarbeiterinnen und Mitarbeiter des Schulpsychologischen Dienstes und
— eine Schulung für Mitarbeiterinnen und Mitarbeiter von Einwohnerdiensten im Rahmen des Weiterbildungsangebotes des Verbandes der Schweizerischen Einwohnerdienste (VSED).
— das Modul «Datenschutz, Amtsgeheimnis und Archivierung», das Teil des Lehrplans der KV-Lehre in der öffentlichen Verwaltung bildet.

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

— ein Referat zum Datenschutz in Behindertenorganisationen (interkantonale ERFA-Gruppe der IT-Leitungen);
— ein Referat für die Auszubildenden an der Höheren Fachschule Kindererziehung;
— ein Datenschutz-Update für das Kader der Sozialhilfe Basel;
— ein Referat zu «Datenschutz – neue Herausforderungen: Verfassungsrechtliche Grundlegung und EU-Datenschutzreform als Schengen-Weiterentwicklung» an der Schengen-Tagung der Juristischen Fakultät der Universität Basel;

— eine Schulung zu Datenschutzfragen in der Zusammenarbeit zwischen den kantonalen Brustkrebs-Früherkennungsprogrammen (Mammographie-Screening-Programm MSP Basel-Stadt) und Swiss Cancer Screening SCS, dem Zusammenschluss der kantonalen Krebs-Screening-Programme);

— ein Referat zu «Das vernetzte Automobil und der Datenschutz» an der Strassenverkehrs-Tagung 2016;

— ein Referat zum «Intelligenten Verkehr und Datenschutz» an der Tagung «Intelligenter Verkehr – Rechtsfragen im Kontext» der Juristischen Fakultät der Universität Basel;

— eine Referat «Aktuelle Herausforderungen für das Datenschutzrecht» vor dem Basler Juristenverein;

— ein Referat zu «Europas Datenschutzreformen und ihre Auswirkungen auf den öffentlichrechtlichen Datenschutz in der Schweiz» am 21. Symposium on Privacy and Security;

— ein Referat zu «‹Wer nichts zu verbergen hat, hat nichts zu befürchten› – wirklich?» vor dem Kiwanis Club Basel.

Auch 2016 blieb das Interesse an bereichsspezifischen datenschutz- und öffentlichkeitsrechtlichen Schulungen sowie an Referaten gross.

Datenschutz-Basilisk Mit der Kolumne in «BS intern» bzw. auf der Website des Datenschutzbeauftragten hat der «Datenschutz-Basilisk» die folgenden Themen angesprochen:

— *«Proleete» in der Öffentlichkeit*: Ein Staatsangestellter darf über seinen Departementsvorsteher denken, was er will. Er darf es auch im Zug seine Kollegin anvertrauen. «Anvertraut» ist es aber nicht mehr, wenn andere zuhören und sich ihren Reim auf das Gehörte machen können, sondern vielleicht sogar strafbar.

— *Einsicht in meine Notizen*: Notizen als «persönliches Arbeitsmittel» gehen niemanden etwas an, auch nicht die Betroffenen – eine unrichtige Ansicht, die sich hartnäckig hält. Eine solche Ausnahme wurde in der Vernehmlassung zum Informations- und Datenschutzgesetz ausdrücklich abgelehnt.

— *Das Ohr an den Kundinnen und Kunden*: Befragungen von Kundinnen und Kunden einer Amtsstelle? Um unsere Dienstleistungen besser auf deren Bedürfnisse abzustimmen, reicht in der Regel eine anonyme Umfrage. Um nur bestätigt zu bekommen, dass wir sowieso die Besten sind – damit sind heute keine Lorbeeren zu verdienen.

— *«Die Regierungspräsidentin* [redacted] *verdient …»*: Wer Personendaten bearbeitet, muss das Datenschutzrecht einhalten. Das gilt nicht mehr, wenn die Daten anonymisiert worden sind. Anonymisieren ist aber mehr als bloss den Namen entfernen! Was denn?

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. weiterhin Mitherausgeber und Redaktor von «digma»[19], der Zeitschrift für Datenrecht und Informationssicherheit aus dem Haus Schulthess Juristische Medien AG, und der «digma-Schriften zum Datenrecht» aus dem gleichen Verlag. In dieser Funktion verfasst er regelmässig Einführungsartikel[20] sowie den «schlusstakt»[21]. Barbara Widmer publiziert regelmässig in der digma-Rubrik «Der Blick nach Europa und darüber hinaus»[22]; von ihr erschien ausserdem ein Aufsatz zum «vernetzten Automobil»[23]. Ausserdem sind von Sandra Husi-Stämpfli und dem Datenschutzbeauftragten im Kommentar zum Energierecht eine Kommentierung zum Datenschutzartikel im Bundesgesetz über die Stromversorgung[24] erschienen. Und schliesslich hat der Datenschutzbeauftragte einen Artikel zu «Psychiatrie und Datenschutz»[25] zum Buch beigetragen, das anlässlich der Eröffnung des neuen Therapie- und Ökonomiegebäudes der Klinik Sonnenhalde präsentiert wurde.

Veranstaltungen

Europäischer Datenschutztag Wie gewohnt hat der Datenschutzbeauftragte aus Anlass des Europäischen Datenschutztages zu einem Apéro eingeladen. Der Anlass bietet Gelegenheit, mit den Grossrätinnen und Grossräten aus dem Grossratsbüro, der Geschäftsprüfungs- und der Justiz-, Sicherheits- und Sportkommission, mit den Präsidien der anderen Grossratskommissionen, mit den Leiterinnen und Leitern und den Ansprechpersonen aus den Dienststellen, mit denen der Datenschutzbeauftragte regelmässig zu tun hat, ungezwungen ins Gespräch zu kommen. >

Spätherbstapéro mit Fachreferat In einem unregelmässigen Rhythmus lädt der Datenschutzbeauftrage die Mitglieder der Grossratskommissionen, mit denen er häufig in Kontakt ist (Büro, GPK, JSSK), sowie die Präsidien aller anderen Grossratskommissionen, die Mitglieder des Regierungsrates und Dienststellenleiterinnen und Dienstellenleiter der Verwaltung zu einer Veranstaltung mit einem Fachreferat ein. 2016 kamen die etwa 50 geladenen Gäste in den Genuss eines Referates von Prof. Dr. Marc Langheinrich von der Università della Svizzera Italiana zu «IoT – was erwartet uns im Internet der Dinge?». Er hat in sehr unterhaltsamer Weise die aktuellen und absehbaren technischen Entwicklungen und ihre Auswirkungen auf unsere Gesellschaft aufgezeigt und zum Nachdenken und Diskutieren angeregt.

Zusammenarbeit

Gesetzlicher Auftrag Der Datenschutzbeauftragte arbeitet zur Erfüllung seiner Aufgaben mit den Organen der anderen Kantone, des Bundes und des Auslandes, welche die gleichen Aufgaben erfüllen, zusammen[26]. Dank dieser Zusammenarbeit lassen sich Synergien nutzen.

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

Kantonsübergreifend Die kantonsübergreifende Zusammenarbeit stellte auch im Jahr 2016 ein wesentliches Element der Tätigkeit des Datenschutzbeauftragten dar. So arbeiteten der Datenschutzbeauftragte und seine Mitarbeiterinnen und Mitarbeiter nicht nur aktiv im privatim-Büro (dazu unter dem nächsten Zwischentitel gleich mehr), sondern auch in den privatim-Arbeitsgruppen «Gesundheit» (Daniela Waldmeier) und «ICT» (Markus Brönnimann) mit. Auch in den neu zusammengestellten privatim-Arbeitsgruppen «Digitale Verwaltung» (Beat Rudin, Markus Brönnimann) und «Sicherheit» (Katja Gysin) wird der Datenschutzbeauftragte mitarbeiten und von den Erfahrungen der anderen Datenschutzaufsichtsstellen profitieren. Barbara Widmer war aktiv beteiligt am Aufbau von «TerrAudit». In diesem Verein können sich die Grundbuchämter und Datenschutzbeauftragte der Kantone, die sich an «Terravis» beteiligen, zusammenschliessen, um eine interkantonal koordinierte wirksame Aufsicht über die Plattform «Terravis» sicherzustellen. «Terravis» ist ein elektronisches Grundbuch-Informationssystem (eGRIS), über welches die angeschlossenen kantonalen Grundbuchämter Grundbuchinformationen mit Berechtigten austauschen. Basel-Stadt ist (noch?) nicht an «Terravis» angeschlossen – das Vorhandensein einer wirksamen Aufsicht ist aber auf jeden Fall Voraussetzung für einen allfälligen Beitritt. Schliesslich ist der Datenschutzbeauftragte (zusammen mit Daniela Waldmeier als Stellvertreterin) Mitglied der Ethikkommission der Pädagogischen Hochschule der FHNW.

Da internationale Entwicklungen auch Auswirkungen auf die Schweiz haben, ist auch der Austausch über die Landesgrenzen hinweg wichtig.

National Im Bereich von eHealth vertrat Barbara Widmer die kantonalen Datenschutzbeauftragten in den Arbeitsgruppe «Standards & Architektur» und «Aufbau & Vernetzung» von eHealth suisse. Katja Gysin vertritt Basel-Stadt in der Koordinationsgruppe der Schweizerischen Datenschutzbehörden für die Schengen-Aufsicht. Zwar wurde auch 2016 keine koordinierte Kontrolle durchgeführt; Katja Gysin arbeitete jedoch in einer Arbeitsgruppe mit, die einen Leitfaden für die koordinierte Kontrolle der Nutzung des Schengener Informationssystems (SIS) erarbeitet; sie konnte die reiche Basler Erfahrung mit solchen Kontrollen einbringen. Der Leitfaden soll im Sommer 2017 verabschiedet und künftig umgesetzt werden. Beat Rudin wiederum ist – im Rahmen einer starken Basler Delegation – Mitglied im Beirat der Fondation CH2048 für das Reformprojekt «Digitale Revolution: Reformvorschläge für eine global wettbewerbsfähige und verantwortliche Schweiz». Damit will die Stiftung die Schweizer Politik für die digitale Zukunft fit machen. Beat Rudin vertritt die Anliegen des Persönlichkeitsschutzes im Rahmen des Teilprojekte «Datennutzung und Datenschutz», in dem es darum geht, den Wert der Daten für die digitale Gesellschaft mit den Persönlichkeitsrechten der Betroffenen vereinbar zu machen.

International Da internationale Entwicklungen auch Auswirkungen auf die Schweiz haben, ist auch der Austausch über die Landesgrenzen hinweg wichtig. Der Datenschutzbeauftragte war deshalb an der Konferenz der Europäischen Datenschutzbehörden in Budapest und an der Internationalen Konferenz der Datenschutzbehörden in Marrakesch vertreten. Der Fokus der ersten Konferenz war auf die neue Europäische Datenschutz-Grundverordnung und die Modernisierung der Europarats-Konvention 108 gerichtet. An der zweiten Konferenz unter dem Titel «Opening new territories for privacy» standen (u.a.) die Themenbereiche Datenschutz und Bildung, Künstliche Intelligenz, Verschlüsselung, Fragen der Aufsicht im Sicherheitsbereich im Vordergrund.

Aber auch kantonsintern Die Mitarbeiterinnen und Mitarbeiter des Datenschutzbeauftragten wirken kantonsintern in etlichen verwaltungsinternen Arbeitsgruppen und Steuerungs-Gremien mit, oftmals nur in beratender Funktion, um die Unabhängigkeit nicht zu gefährden. Der Datenschutzbeauftragte hat ausserdem mitgeholfen, die Basler Expertengruppe «Datenschutz im Gesundheitswesen», in der sich regelmässig Vertreterinnen und Vertretern des Universitätsspital, der Schweizerischen Akademie der Medizinische Wissenschaften (SAMW), von Novartis und Roche und einem auf diesem Gebiet stark engagierten Advokaturbüro und eben der Datenschutzbeauftragte über aktuelle Datenschutzfragen im Gesundheitsbereich austauschen, wiederzubeleben.

privatim, die Konferenz der schweizerischen Datenschutzbeauftragten

Wechsel im Präsidium Nach zwölf Jahren ist Bruno Baeriswyl, der Datenschutzbeauftragte des Kantons Zürich, als Präsident von privatim, der Konferenz der schweizerischen Datenschutzbeauftragten, zurückgetreten. Die Suche nach einer Nachfolgerin oder einem Nachfolger hatte rund vier Jahre gedauert. Verschiedene Lösungsvorschläge mit extern vergebener Geschäftsstelle wurden als nicht nachhaltig und zu teuer verworfen. Schliesslich hat sich Beat Rudin bereit erklärt, das Präsidium zu übernehmen, wenn der Aufwand dafür reduziert werden kann.

Reorganisation Die Entlastung des Präsidiums konnte durch die folgenden Reorganisationsansätze erreicht werden:

— Verteilung der Aufgaben auf mehr Schultern (Chargen im Büro: Präsidium, Vizepräsidium, Mitarbeit im Büroausschuss, Kommunikation (Kommunikation mit den Mitgliedern, nach aussen, Betreuung der Website), Arbeitsgruppenleitung;
— Einsetzung eines Büro-Ausschusses (Tagesgeschäft, Vorbereitung der Arbeit im Büro, Telefonkonferenz im Zweiwochenrhythmus);
— finanzielle Kompensation für die Übernahme von Chargen im Büro;
— Entschädigung für Sekretariatsaufgaben beim Präsidium.

Neubeginn Mit diesen Änderungen konnten neue Mitglieder für das Büro gewonnen werden. Dank der Entschädigung war es beispielsweise Datenschutzbeauftragten mit einem Teilzeitpensum möglich, die Leitung einer Arbeitsgruppe zu übernehmen, ohne dafür ihr Pensum als Datenschutzbeauftragte in Anspruch zu nehmen. Im Berichtsjahr hat sich das privatim-Büro aus den Datenschutzbeauftragten der Kantone Aargau, Basel-Stadt, Bern, Freiburg, Neuenburg/Jura, Zug und Zürich zusammengesetzt.

Ehrung

Wissenschaftspreis der Stadt Basel Der Regierungsrat hat am 20. September 2016 den Wissenschaftspreis der Stadt Basel verliehen[27]. In einer von Colette Greder und Andrej Ichtschenko wunderschön baslerisch umrahmten Preisverleihung im Grossratssaal überreichte Regierungspräsident Dr. Guy Morin den Preis an Beat Rudin,

— «der als kantonaler Datenschutzbeauftragter für eine differenzierte Umsetzung des Datenschutzes in die Praxis sorgt und die kantonalen Amtsstellen insbesondere durch seine Beratungstätigkeit mit Augenmass unterstützt sowie auch auf nationaler Ebene ein sehr grosses Engagement für den Datenschutz zeigt;
— der über den beruflichen Alltag hinaus als Autor und Herausgeber von einschlägigen Publikationen zur wissenschaftlichen Bearbeitung und Reflexion seines Fachgebiets wichtige Beiträge von nationaler und internationaler Bedeutung leistet;
— der als Titularprofessor an der Universität Basel für eine wissenschaftlich verankerte Vermittlung des Datenschutz- und Informationsrechts an die künftige Generation von Juristinnen und Juristen besorgt ist;

>

— der mit der Abhaltung von Tagungen wie auch mit Stellungnahmen in den Medien zu aktuellen Fragen wichtige Beiträge für den gesellschaftlichen Diskurs zu Datenschutz und Datenzugang leistet und damit in der rasanten Entwicklung der modernen Gesellschaft hin zu einer Informations- und Kommunikationsgesellschaft die relevanten Fragen aus dem Spannungsfeld zwischen Datenschutz und offenem Informationszugang/Transparenzanliegen thematisiert;

Die Auseinandersetzung mit unserer digitalen Zukunft beginnt erst. Dazu braucht es auch mehr als bloss Datenschutzbeauftragte: Es ist eine Diskussion, die wir als *freiheitliche Gesellschaft* führen müssen – als Gesellschaft, die freiheitlich bleiben will.

— dem es durch sein vielfältiges Wirken auf ausserordentliche Weise gelingt, Personen aus Wirtschaft, Wissenschaft, Politik und Verwaltung zusammen zu bringen und zur ganzheitlichen Betrachtung der Entwicklungstendenzen beiträgt, indem rechtliche, technische, wirtschaftliche, politische und nicht zuletzt auch ethische Aspekte in die Wissenschaft und die sozialpolitische Debatte einfliessen.»

Dank Der Geehrte dankte darauf den Damen und Herren der Wissenschaftspreis-Kommission für die Zuerkennung des Preises, der ihn ansporne, den eingeschlagenen Weg weiterzugehen, und dem Regierungsrat des Kantons Basel-Stadt für die Verleihung des Preises – dessen Wertschätzung freue ihn erst recht, weil seine Aufgabe es mit sich bringe, dass er mit seinem Team der Verwaltung gegenüber ab und zu auf Handlungsbedarf hinweisen muss, was der Exekutive – das verstehe er voll und ganz – nicht immer nur Freude bereite. Mit diesem Preis sei der Datenschutz endgültig angekommen, habe er mehr als einmal gehört. Ob wir also am Ziel seien? Wer am Morgen der Preisverleihung in der bz Basel das Interview mit dem Schriftsteller Tom Hillenbrand zu seinem Roman «Drohnenland»[28] gelesen habe, wisse: Nein – die Auseinandersetzung mit unserer digitalen Zukunft beginnt erst. Dazu brauche es auch mehr als bloss Datenschutzbeauftragte: Es ist eine Diskussion, die wir als *freiheitliche Gesellschaft* führen müssen – als Gesellschaft, die freiheitlich bleiben will. Wissenschaftler und Datenschutzbeauftragte könnten diese Diskussion nur anstossen und alimentieren. Führen müssten sie wir alle. Der Regierungspräsident habe die Verleihung des Preises mit dem gelungenen Brückenschlag begründet. Brücken könne man nur schlagen, wenn der Boden, auf dem die Brückenpfeiler stehen sollen, stark genug sei. Dass er, der Geehrte, diesen Preis in Empfang nehmen dürfe, habe also viel mit den Menschen zu tun, die diesen Boden gelegt hätten. Etlichen von diesen «Bodenlegern» hat er anschliessend gedankt, von seinen Förderern, die ihn zum öffentlichen Recht und zum Datenschutz gebracht haben (René Rhinow, Andreas Koellreuter), seinen früheren und aktuellen Kolleginnen und Kollegen für den FLöhlichen Austausch, für die gute Zusammenarbeit in privatim, für die Aufnahme in der Juristischen Fakultät, den ehemaligen und aktuellen Mitgliedern der Datenschutz-Delegation des Ratsbüros für die wohlwollende Begleitung und den Schutz der Unabhängigkeit des Datenschutzbeauftragten, und – last but not least – seinem Team, ohne das der Brückenschlag zwischen Theorie und Praxis nicht so gut gelingen würde, und seiner Familie – er schätze sich glücklich, aus dieser Ressource schöpfen zu dürfen.

1 <http://www.dsb.bs.ch/Merkblaetter/checkliste-bekanntgabe.html>.
2 Art. 32 Abs. 1 lit. d ATSG.
3 § 10 IDG; vgl. dazu PK-IDG/BS-Rudin, § 10 N 2 ff.
4 Die in § 10 Abs. 1, § 22 Abs. 1 und 4 IDG ebenfalls noch erwähnte «Wissenschaft» beschreibt im Grunde genommen nicht den Bearbeitungszweck, sondern die Methode. Ihre Erwähnung hat deshalb keine eigenständige Bedeutung (PK-IDG/BS-Rudin, § 10 N 7).
5 § 30 Abs. 6 AufenthG.
6 Anders aber schon PK-IDG/BS-Husi, § 30 AufenthG N 34.
7 RRB vom 6. Dezember 2016, Sammeladressauskünfte an Parteien durch das Einwohneramt, P161833.
8 Art. 29 Abs. 2 BV; § 12 KV.
9 Vgl. dazu z.B. auch § 3 Abs. 1 des Gesetzes vom 20. Juni 1968 über die Ermittlung von Grundstückwerten, SGS 717.100, wonach das Ergebnis der Preisauswertung nur in einer Art bekanntgegeben werden darf, die keinen Aufschluss über die für bestimmte Grundstücke bezahlten Preise gibt.
10 Das Problem besteht allerdings schon bei der Begründung der Verfügung, nicht erst bei der Einsprache (oder bei einem Rekurs). Allerdings waren, als die Frage dem Datenschutzbeauftragten unterbreitet wurde, ein Grossteil aller Verfügungen bereits eröffnet.
11 § 9a Abs. 1 lit. a-c IDV (in der durch die inzwischen vom Regierungsrat verabschiedete DMV geänderten Fassung); vgl. ebenso § 5 Abs. 1 lit. a-c DMV.
12 Erläuterungen zur Verordnung über den Datenmarkt, S. 6.
13 Erläuterungen zur Verordnung über den Datenmarkt, S. 6.
14 § 18 Abs. 3 IDG.
15 § 44 lit. f IDG; vgl. dazu PK-IDG/BS-Schilling, § 44 N 29 ff.
16 So auch PK-IDG/BS-Schilling, § 44 N 29.
17 Was in der Folge auch geschehen ist: Die KdK hat am 7. Februar 2017 den KdK-Leitfaden (<http://www.dsb.bs.ch/dam/jcr:8772f3e4-14ce-45ca-aff1-46b00d043d23/KdK%20Leitfaden%20DSG%20Kantone.pdf>, Kurz-URL: <http://bit.ly/2sfj00f>) allen Kantonen zugestellt.
18 Im Jahresbericht 2016 (des Regierungsrates), S. 410, wurden fälschlicherweise nur 7 Schulungen erwähnt.
19 2016 mit den Schwerpunktthemen «Whistleblowing» (2016.1), «Quantified Self» (2016.2) und «Outsourcing durch Gemeinwesen» (2016.3); die vierte Nummer erschien zusammen mit der Nummer 2017.1 als Doppelnummer zu «Datenschutzreform».
20 Beat Rudin, Unbefriedigender Whistleblower-Schutz (digma 2016, S. 4 f.); ausserdem ders, Überholte Ausnahmen im Datenschutzrecht (digma 2016, S. 122 ff.).
21 Beat Rudin, Gebt dem Auto mehr Daten zum Rechnen! (digma 2016, S. 44); ders., Wer schaut dem Trojaner ins Maul? (digma 2016, S. 96); ders., Datenschutzaufsicht ohne Ressourcen? (digma 2016, S. 140).
22 Barbara Widmer, Stimmen Sie mit Nichtwissen zu? (digma 2016, S. 42 f.); dies., Pay as you drive – bezahlen mit Daten (digma 2016, S. 92 f.); dies., Wer entscheidet – Sie oder der Algorithmus? (digma 2016, S. 134); dies., Microsoft vs. US-Justizbehörden (digma 2016, S. 139).
23 Barbara Widmer, Das vernetzte Automobil und der Datenschutz, in: Thomas Probst/Franz Werro (Hrsg.), Strassenverkehrs-Tagung 21.-22. Juni 2016, Bern 2016, S. 143 ff.
24 Beat Rudin/Sandra Husi-Stämpfli, Art.27, in: Brigitta Kratz/Michael Merker/Renato Tami/Stefan Rechsteiner/Kathrin Föhse (Hrsg.), Kommentar zum Energierecht, Band I: WRG/EleG/StromVG/RLG, Bern 2016, S. 1695-1723.
25 Beat Rudin, Psychiatrie und Datenschutz, in: Anja Oswald (Hrsg.), Psychiatrie und Gesellschaft im Wandel der Zeit 1900–2016, Basel 2016, S. 172 ff.
26 § 48 IDG.
27 Medienmitteilung des Regierungsrates: <http://www.medien.bs.ch/nm/2016-06-14-rrbs-003.html> (Kurz-URL: <http://bit.ly/2vboSfv>); Medienmitteilung der Universität: <https://www.unibas.ch/de/Aktuell/News/Uni-People/Beat-Rudin-erhaelt-den-Wissenschaftspreis-der-Stadt-Basel-2016.html>. (Kurz-URL: <http://bit.ly/2u9qSAC>).
28 bz Basel vom 20. September 2016, S. 6: «Es ist gruseliger als bei Orwell».

Aus dem Alltag

Einblicke in die Kontrolltätigkeit

Der Datenschutzbeauftragte kontrolliert nach einem autonom aufzustellenden Prüfprogramm die Anwendung der Bestimmungen über den Umgang mit Informationen. Im Jahr 2016 konnten eine Datenschutz-Prüfung abgeschlossen werden, vier sind noch am Laufen, eine in Vorbereitung. Ausserdem arbeitet der Datenschutzbeauftragte mit dem Staatsschutzkontrollorgan zusammen.

Übersicht

Abgeschlossen Wie bereits im Jahresbericht erwähnt, konnte dieses Jahr eine Prüfung abgeschlossen werden: die Prüfung, inwiefern die öffentlichen Organe, die Videoüberwachungsanlagen betreiben, ihrer Pflicht nachgekommen sind, die Videoüberwachungsreglemente der Öffentlichkeit leicht zugänglich zu machen. Diese Prüfung war relativ aufwändig, wie sogleich unten zu sehen ist. Dass nicht mehr Prüfungen abgeschlossen werden konnten, lag am erhöhten Geschäftsaufkommen (hinten Seite 43 f.), an der Aufwändigkeit der abgeschlossenen und laufenden Prüfungen und schliesslich auch an personellen Engpässen – eine neuen Mitarbeiterin musste erst in die Kontrolltätigkeit eingeführt werden und der Wechsel von einer juristischen zu einer weiteren IT-Stelle war noch im Gange, eine Stelle somit vakant.

Begonnen Mehrere Prüfungen waren aber am Laufen, konnten jedoch im Berichtsjahr noch nicht abgeschlossen werden:

- eine Prüfung bei der Kantonspolizei;
- eine Prüfung beim Universitätsspital;
- eine Prüfung bei den Volksschulen im Erziehungsdepartement;
- eine Prüfung bei der Steuerverwaltung

In Vorbereitung Statt für eine eigene SIS-Kontrolle wurden die Ressourcen in die Vorbereitung einer mit dem Bund und anderen Kantonen koordinierten SIS-Kontrolle investiert.

Abgeschlossen: Prüfung Publikation der Videoüberwachungsreglemente

Prüfgebiet Die Informations- und Datenschutzverordnung (IDV) sieht vor, dass Reglemente der Öffentlichkeit leicht zugänglich gemacht werden müssen[1]. Auf die Veröffentlichung der Kamerastandorte kann verzichtet werden, wenn durch deren Bekanntgabe die Zweckerreichung unmöglich wird[2]. Der Datenschutzbeauftragte hat 2016 geprüft, ob und wie die Reglemente der Videoüberwachungsanlagen von den öffentlichen Organen im Kanton Basel-Stadt der Öffentlichkeit zugänglich gemacht wurden.

Durchführung der Prüfung Die Prüfung startete auf der Basis der bekannten Videoüberwachungsanlagen. Wo der Datenschutzbeauftragte keine Hinweise auf eine Publikation des Reglements fand, wurden die für den Betrieb der Videoüberwachungsanlagen verantwortlichen öffentlichen Organe angeschrieben, mit der Bitte um Angaben zur Publikation, insbesondere zu allfälligen Gründen, warum keine Veröffentlichung des Reglements vorgenommen worden war[3].

Wesentliche Feststellungen Die Prüfung ergab die folgenden wesentlichen Feststellungen:

— Bei Prüfungsbeginn im Sommer 2016 lagen dem Datenschutzbeauftragten 29 Reglemente für Videoüberwachungsanlagen vor. Davon waren im Zeitpunkt der Kontrolle acht publiziert, für 21 Reglemente fehlten Angaben zur Publikation und eine Suche auf den relevanten Webseiten ergab keine Resultate.

— Mehrere Anlagenverantwortliche veranlassten im Nachgang zur Anfrage die erneute Publikation ihres Reglements und machten geltend, dass ihre Webseite in Überarbeitung sei bzw. überarbeitet worden sei und das Reglement erneut aufgeschaltet werden musste.

— Einige nahmen die Nachfrage zum Anlass, den Stand der Anlagen in ihrem Bereich generell zu prüfen, eventuell eine Überarbeitung der Reglemente in die Wege zu leiten und organisatorische Zuständigkeiten zu überarbeiten bzw. neu zuzuweisen.

— Nur wenige stellten die Publikationspflicht generell in Frage, z.B. weil ihre Anlage die Öffentlichkeit nur am Rande betreffe oder weil sie die Existenz und Details ihrer Anlage als «geheim» erachteten.

Stand Mitte 2017 Der heutige Stand der Videoüberwachungsreglemente präsentiert sich wie folgt (vgl. dazu auch die Tabelle vorne auf den Seiten 12 f.):

— Zurzeit liegen dem Datenschutzbeauftragten 31 verabschiedete Videoüberwachungsreglemente vor; davon sind zum Zeitpunkt des Redaktionsschlusses dieses Berichts 25 publiziert.

— Bei den nicht publizierten Reglementen handelt es sich zur Hälfte um Reglemente, die noch in Revision sind.

— Bei drei Anlagen fehlt die Publikation trotz mehrfacher Nachfrage bei der verantwortlichen Stelle.

Es hat sich erfreulicherweise gezeigt, dass die Mehrzahl der öffentlichen Organe der Publikationspflicht nachkommt und fehlende Publikation meist unwillentlich bzw. unwissentlich geschieht.

Empfehlungen Es hat sich erfreulicherweise gezeigt, dass die Mehrzahl der öffentlichen Organe der Publikationspflicht nachkommen und fehlende Publikation meist unwillentlich bzw. unwissentlich geschieht. Einige grundsätzliche Anmerkungen ergeben sich trotzdem aus der Prüfung:

— In der Regel dürfte die Publikation im Internet auf der Webseite der verantwortlichen Behörde die einfachste und wirksamste Lösung sein. Aus Sicherheitsgründen kann dabei – wie oben bereits erwähnt – auf die Veröffentlichung der Pläne oder von Details zu den Kamerastandorten verzichtet werden; diese Option wurde bei 13 von 25 Publikationen gewählt. Auch in diesen Fällen gibt es aber zumindest eine Umschreibung im Reglement selber, wo wie viele Kameras aktiv sind.

— Keine genügende Publikation ist im Regelfall erreicht, wenn die Publikation nur auf einem internen Netz (Intranet) veröffentlich wird. Auch wenn die Anlage zum Beispiel nur Innenräume ohne Publikumsverkehr überwacht, sind doch auch potentiell Personen betroffen, die keinen Zugang zum Intranet haben, zum Beispiel Lieferantinnen und Handwerker. Eine Publikation ist auch nötig, wenn theoretisch nur sehr wenige Personen von der Videoüberwachung betroffen sind, beispielweise die Überwachung eines Entsorgungscontainers mit nur einer Kamera. Auch in diesem Fall kann nicht zum Vorneherein bestimmt werden, wer von einer Überwachung erfasst wird; potentiell Beeinträchtigte sollen die Möglichkeit haben, sich eigenständig darüber zu informieren wann, wo und von wem sie möglicherweise gefilmt werden.

— Fraglich bleibt auch, ob eine Publikation den Ansprüchen genügt, wenn sie nicht mit einer einfachen Suche auf der relevanten Webseite aufgefunden werden kann. Gewisse Reglemente wurden zwar publiziert, sind aber nur auffindbar, wenn man den Link zur Publikation kennt. Andere findet man nur mit einer generellen Suche auf der Webseite des Kantons, nicht aber auf der Webseite der Betreiberin. Es bleibt fraglich, warum gewisse Stellen sich nur widerstrebend auf eine Veröffentlichung des Reglements einlassen. Gerade die präventive Wirkung der Videoüberwachungsanlagen – oftmals ein Hauptgrund für die Installation – entfaltet sich ja nur bei Kenntnis einer Überwachung. Zum einen weisen dabei Piktogramme oder Hinweisschilder vor Ort auf die Überwachung hin[4], zum andern entfaltet eben gerade das publizierte Reglement eine ähnliche Wirkung. Dass dabei ein Gefängnis oder eine Polizeiwache nicht die Detailpläne ihrer Installationen und damit ihrer Gebäude veröffentlichen möchten, ist verständlich. Aber die Tatsache, dass Kameras genutzt werden, wie viele es davon gibt, wer die Aufnahmen in welchen Fällen anschauen darf und an wen sie weitergegeben werden dürfen, betreffen die persönlichen Rechte der Betroffenen und sollten diesen leicht zugänglich gemacht werden.

— Oftmals sind Publikationen nicht mehr auffindbar, weil die Webseite überarbeitet wurde und das Reglement nicht mehr neu aufgeschaltet wurde oder ein bestehender Link führt nun ins Leere. Es ist Sache der Anlageverantwortlichen sicherzustellen, dass die Veröffentlichung des Reglements jederzeit den gesetzlichen Anforderungen genügt. Links und Webseiten sind also zu überprüfen und bei Änderungen ist dem Reglement wieder der nötige Platz zuzuweisen. >

In Vorbereitung: SIS-Kontrolle

Erste koordinierte Kontrolle Im Berichtsjahr wurden die Ressourcen statt einmal mehr in eine Logfile-Kontrolle betreffend die Nutzung des Schengener Informationssystem (SIS)5 in die Vorbereitung von Grundlagen für eine erste koordinierte Kontrolle zusammen mit den anderen Kantonen und dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) gearbeitet. Während der Amtszeit des letzten EDÖB fand bekanntlich keine einzige koordinierte SIS-Kontrolle statt. Nun wurde zum einen am Leitfaden für die koordinierte Kontrolle im Rahmen der Schengen-Koordinationsgruppe der schweizerischen Datenschutzbeauftragten aktiv mitgewirkt; zum andern wurden Vorabklärungen zur kantonsinternen Organisation der Zugriffsberechtigungen im SIS vorgenommen.

Die Schweiz wird 2018 zum dritten Mal das Schengen-Evaluierungsverfahren durchlaufen. Expertinnen und Experten aus anderen Schengen-Staaten sowie der EU werden prüfen, ob die Schweiz – und diesmal konkret auch Basel-Stadt – die Schengener Vorschriften korrekt anwendet.

Kontrolltätigkeit im Bereich des Staatsschutzes

Koordination Auch 2016 trafen sich das Staatsschutzkontrollorgan und der Datenschutzbeauftragte zu einer koordinierenden Sitzung, wo Fragen zu Berührungspunkten zwischen der Fachgruppe 9 und anderen öffentlichen Organen des Kantons Basel-Stadt behandelt wurde. Vorgängig hat der Datenschutzbeauftragte die Liste der Ämterkontakte der Fachgruppe 9 mit dem Migrationsamt auf ihre Richtigkeit und Vollständigkeit geprüft und verifizieren können.

Ausblick: Schengen-Evaluation (Sch-Eval) 2018

Regelmässige Überprüfung Die Schweiz wird 2018 zum dritten Mal das Schengen-Evaluierungsverfahren durchlaufen. Expertinnen und Experten aus anderen Schengen-Staaten sowie der EU werden prüfen, ob die Schweiz die Schengener Vorschriften korrekt anwendet. Untersucht werden insbesondere die Bereiche Datenschutz, Aussengrenzen, Polizeikooperation, SIS/SIRENE, Rückkehr und Visa. In Vorbereitung für die Schengen-Evaluation wurde bereits unter der Federführung des Bundesamtes für Justiz ein Fragebogen mit einem Überblick zur rechtlichen und praktischen Umsetzung der Vorgaben in den verschiedenen Bereichen vorbereitet.

Ortstermin in Basel Im Frühling 2018 wird dann eine Expertengruppe verschiedene Evaluierungsbesuche vornehmen. Im Bereich Datenschutz werden traditionellerweise auch zwei Kantone von der Kommission besucht, um die Umsetzung der datenschutzrechtlichen Vorgaben zu prüfen. Der Datenschutzbeauftragte ist erfreut, dass Basel-Stadt zu den vorgeschlagenen Kantonen für einen Ortstermin gehört.

1 § 6 IDV; zur Begründung dieser Veröffentlichungspflicht vgl. vorne Seite 9.
2 § 6 Abs. 2 IDV; vgl. dazu PK-IDG/BS-Husi, § 18 N 46 ff.
3 Anzumerken ist, dass eine grosse Zahl von Reglementen 2016 erstmals ihre vierjährige Geltungsdauer erreichte. Allfällige Verlängerungen mussten dem Datenschutzbeauftragten im Laufe des Jahres zur Vorabkontrolle vorgelegt werden. Im Rahmen dieser Verlängerungen kam es zu Veränderungen im Vergleich zu den bestehenden Reglementen – bisherige Reglemente, die Anlagen an mehreren Standorten betrafen, wurden aufgeteilt, andere wurden zusammengelegt, neue Anlagen kamen hinzu. Die hier zitierten Zahlen beziehen sich auf den jeweiligen Stand zum angegebenen Zeitpunkt.
4 § 17 Abs. 3 IDG; vgl. dazu PK-IDG/BS-Husi, § 17 N 34 ff.
5 Vgl. dazu (u.a.) TB 2015, S. 33 f.; TB 2014, S. 29; TB 2013, S. 27 f.; TB 2012, S. 29; TB 2011, S. 14 f.

Besondere Berichtspunkte

Pilotversuche, Informationszugangsgesuche und Geschäftslast

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

Pilotversuche mit besonderen Personendaten

IDG-Ergänzung Ende 2013 wurde das Informations- und Datenschutzgesetz um den § 9a (Bearbeiten von besonderen Personendaten im Rahmen von Pilotversuchen) ergänzt[1]. Mit § 9a IDG soll ermöglicht werden, dass unter engen Voraussetzungen[2] und zeitlich befristet im Rahmen von Pilotversuchen besondere Personendaten bearbeitet werden dürfen, ohne dass die nach § 9 Abs. 2 IDG erforderliche formellgesetzliche Grundlage besteht. Der Regierungsrat muss die Modalitäten eines Pilotversuchs in einer Verordnung regeln[3]. Ausserdem sind Pilotversuche zwingend zu evaluieren[4].

Funktion des Datenschutzbeauftragten Der Datenschutzbeauftragte hat nach § 9a Abs. 1 IDG das Projekt eines Pilotversuchs im Rahmen einer Vorabkontrolle vorgängig zu beurteilen. Ausserdem hat die Justiz-, Sicherheits- und Sportkommission des Grossen Rates (JSSK) bei der Behandlung der IDG-Ergänzung grossen Wert darauf gelegt, dass die Umsetzung des § 9a IDG eng begleitet wird[5]. Er soll jährlich darüber berichten, welche Pilotversuche laufen. Insbesondere soll er auch kontrollieren, ob Pilotversuche nach Ablauf der fünfjährigen Versuchsphase, falls die notwendige formellgesetzliche Grundlage nicht geschaffen wurde, tatsächlich definitiv eingestellt worden sind. Nicht ausdrücklich vorgesehen ist, dass der Datenschutzbeauftragte die Evaluation begleitet. Er hat nicht zu entscheiden, ob ein Pilotversuch erfolgreich war oder nicht – das obliegt der Fachbehörde und dem vorgesetzten Departement. Er hat aber zu den datenschutzrechtlichen Aspekten Stellung zu nehmen. Ausserdem ist es sinnvoll, ihn frühzeitig einzubeziehen, da ja – wenn für die Fortsetzung der Datenbearbeitung die notwendige formellgesetzliche Grundlage geschaffen werden soll – dazu Stellung zu nehmen hat[6]. Und es ist davon auszugehen, dass die beratende Grossratskommission zum Gesetzgebungsprojekt eine datenschutzrechtliche Beurteilung voraussetzt.

Laufende Pilotversuche Ende 2016 waren zwei Pilotversuche i.S.v. § 9a IDG ein Thema – in unterschiedlichen Phasen: Der Pilotversuch «Erweiterte Gefährderansprache» war während eines Jahres gelaufen und ging in die Verlängerung; für den Pilotversuch «eHealth-Modellversuch Basel» (früher: «eHealth am Rhy») hat der Regierungsrat am 19. April 2016 die Verordnung erlassen, die Bearbeitung von Personendaten im Rahmen des Pilotversuchs hat aber noch nicht begonnen.

Pilotversuch «Erweiterte Gefährderansprache»

Ziel Am 1. Januar 2016 trat die Verordnung über die Meldung von gefährdenden Personen im Rahmen eines Pilotversuchs («Erweiterte Gefährderansprache») (PPV-Erweiterte Gefährderansprache) in Kraft. Der Pilotversuch sollte aufzeigen, ob durch die Meldung von gefährdenden Personen an die Beratungsstelle mehr gefährdende Personen angesprochen und zur freiwilligen Teilnahme an geeigneten Massnahmen motiviert werden können, als wenn nur, wie im Polizeigesetz[7] vorgesehen, Gefährderinnen und Gefährder angesprochen werden, gegenüber denen eine Wegweisung ausgesprochen worden ist.

Einbezug des Datenschutzbeauftragten Der Datenschutzbeauftragte wurde vom Justiz- und Sicherheitsdepartement sowohl zur Erarbeitung der Pilotversuchs-Verordnung als auch zur Evaluation und zur Ausarbeitung des Antrags zur Verlängerung des Pilotversuchs einbezogen. Dazu nahm er in beratender Funktion an fünf Sitzungen der «Arbeitsgruppe Evaluation» teil. Zur Halbzeit des ursprünglich auf eine Laufzeit von einem Jahr angelegten Pilotversuchs >

führte der Datenschutzbeauftragte eine Vor-Ort-Prüfung der aktuellen Datenbearbeitung durch die Beratungsstelle durch. Dabei wurden die Datenflüsse im Rahmen der Gefährderansprache zusammen mit der Leiterin Fachreferat und der Beratungsstelle nachvollzogen. Der Beratungsstelle konnte dabei ein gutes Zeugnis ausgestellt werden. Zwei Anpassungen der Datenschutzrichtlinie wurden aufgrund der Evaluation vorgenommen. Die Details der Evaluation wurden im Zwischenbericht zum Pilotprojekt festgehalten.

Evaluation Der Zwischenbericht zum Pilotprojekt zog eine positive Bilanz, und der Regierungsrat hat in seiner Sitzung vom 20. Dezember die Verlängerung des Pilotversuchs um zwei Jahre (bis Ende 2018) genehmigt. In dieser Zeit soll nun die entsprechende Normierung auf Verordnungsstufe in das Polizeigesetz übergeführt werden, also die für die Fortsetzung der Datenbearbeitung der besonderen Personendaten notwendige formellgesetzliche Grundlage geschaffen werden.

Pilotversuch «eHealth-Modellversuch Basel»

Pilotversuch Der eHealth-Modellversuch Basel ist im Lichte von § 9a IDG ein atypischer Pilotversuch. Hier geht es (inzwischen) nicht mehr darum, gestützt auf eine Verordnungsgrundlage eine Datenbearbeitung von besonderen Personendaten «auszuprobieren», um dann gestützt auf diesen Versuch die «richtige» formellgesetzliche Grundlage schaffen zu können. Der Bund hat nämlich mit dem Bundesgesetz über das elektronische Patientendossier (EPDG) die erforderliche Rechtsgrundlage schon geschaffen (und inzwischen per 15. April 2017 in Kraft gesetzt). Die Listenspitäler nach KVG müssen innert drei Jahren ab Inkrafttreten (also bis 15. April 2020) das elektronische Patientendossier anbieten[8]. Voraussetzung dafür ist, dass sie sich einer zertifizierten Gemeinschaft oder Stammgemeinschaft nach Art. 11 EPDG anschliessen.

Ziel Der Regierungsrat hat am 19. April 2016 die eHealth-Verordnung erlassen. Mit dem Pilotversuch soll nun – vereinfacht gesagt – das Funktionieren einer Stammgemeinschaft getestet werden. Zu diesem Zweck erarbeiten das Gesundheitsdepartement, das nach der Verordnung die Gesamtverantwortung für den Pilotversuch trägt[9], das Universitätsspital Basel sowie weitere Listenspitäler und Leistungserbringer die Grundlagen für die Schaffung einer Stammgemeinschaft, die sich dann zertifizieren lassen kann[10]. Der Pilotversuch ist offen für die Ausweitung auf weitere Kantone, deren Leistungserbringer sich dann gemeinsam zu einer Stammgemeinschaft zusammenschliessen könnten.

Einbezug des Datenschutzbeauftragten Der Datenschutzbeauftragte wurde bereits seit den ersten Vorbereitungen im Jahre 2010 regelmässig beigezogen – so auch im Vorfeld des Erlasses der Verordnung über den Pilotversuch. Der weitere Einbezug, z.B. im Zusammenhang mit der Schaffung eines regionalen Master-Patient-Indexes, sind geplant.

Stand Festzuhalten ist nochmals, dass zwar am Pilotversuch gearbeitet wird, dass aber im Rahmen des Pilotversuchs (noch) keine besonderen Personendaten bearbeitet werden und insbesondere keine elektronischen Patientendossiers geführt werden.

Informationszugangsgesuche nach dem Öffentlichkeitsprinzip

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

Statistik Die Zahlen finden sich – über die gesamte kantonalen Verwaltung zusammengefasst – im Statistikteil dieses Tätigkeitsberichts (Seite 44). Aufgeschlüsselt nach Departementen veröffentlicht der Regierungsrat sie in seinem Jahresbericht[11].

Der Zwischenbericht zum Pilotprojekt zog eine positive Bilanz, und der Regierungsrat hat in seiner Sitzung vom 20. Dezember die Verlängerung des Pilotversuchs um zwei Jahre (bis Ende 2018) genehmigt.

Höhere Zahl Die Zahl der schriftlich bei der kantonalen Verwaltung eingereichten Gesuche ist nach zwei Jahren mit einer «Gesuchsflaute» wieder angestiegen (33; 2016:19) – ungefähr auf das Niveau von 2013. Ob das eine Trendwende gegenüber den letzten Jahren darstellt, lässt sich aufgrund der dünnen Faktenlage nicht sagen.

Aussagekraft Insider aus Departementen stellen auch die Aussagekraft der erfassten Zahlen in Frage. Wichtig für die Interpretation der Daten ist zu wissen,

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

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

Zwei Drittel aller Geschäfte wurden durch eine Anfrage kantonaler öffentlicher Organe initiiert. Der Anteil der von Privatpersonen initiierten Geschäfte nahm um rund einen Drittel ab, derjenige von Medien hat sich mehr als verdoppelt.

Erledigung 58% der Gesuche wurden ganz oder teilweise gutgeheissen (2015: 45%). 39% der Gesuche (2015: 35%) wurden ganz abgewiesen. Die Abweisungsgründe sind dem Datenschutzbeauftragten nicht bekannt. Über 3% der Gesuche (2015: 20%) der Gesuche war Ende des Berichtsjahres noch nicht rechtskräftig entschieden.

Aufhebung der Pflicht zur Anonymisierung Der Ratschlag mit der in den letzten beiden Tätigkeitsberichten angesprochenen geplanten Anpassung von § 30 IDG12 wurde vom Regierungsrat im Berichtsjahr noch nicht verabschiedet[13].

Statistik zu den Geschäften des Datenschutzbeauftragten

Statistik Die Statistik zu den Geschäften des Datenschutzbeauftragten im Jahr 2016 (mit Vorjahresvergleich) findet sich auf den Seiten 44 f.

Höhere Geschäftszahl Im Berichtsjahr sind 447 Geschäfte neu eröffnet worden (2015: 411); die Zahl ist markant höher als im Vorjahr (+36 Geschäfte, +9%). Zum Teil ist diese Erhöhung erklärbar durch die Vorabkontrollen im Zusammenhang mit der Verlängerung der im Jahr 2012 verabschiedeten Videoüberwachungsreglemente, deren vierjährige Geltungsdauer abgelaufen ist, und durch Vorabkontrollen im Zusammenhang mit Onlinezugriffs-Gesuchen.

Komplexere Fälle Der Anteil komplexer (und damit ressourcenintensiver) Geschäfte an allen Beratungen hat sich in den vergangenen Jahren bei rund einem Achtel eingependelt. Im Berichtsjahr betrug ihr Anteil an allen Beratungen 14% (2015: 13%).

Rasche Erledigung Von den nicht-komplexen Beratungsgeschäften konnten 53% (2015: 61%) innert 14 Tagen seit Eingang abgeschlossen werden. Der etwas tiefere Anteil dürfte seine Begründung in der höheren Geschäftslast finden.

Audits Wie bereits im Jahresbericht[14] erwähnt, konnte im Berichtsjahr nur ein Audit (2015: 4) abgeschlossen werden. Weitere Details dazu finden sich auf den Seiten 38 ff.

Schulungen Im Berichtsjahr wurden sieben Schulungen für öffentliche Organe durchgeführt (2015: 6). Hinzu kommt eine noch grössere Zahl von Referaten und Weiterbildungsbeiträgen, die dem gleichen Zweck dienen; Details finden sich auf den Seiten 32 f.

Initianten Die Stellen bzw. Personen, welche die Geschäfte veranlasst haben, verteilen sich im Berichtsjahr nur geringfügig anders als in den Vorjahren. Zwei Drittel aller Geschäfte wurden durch eine Anfrage kantonaler öffentlicher Organe initiiert. Der Anteil der von Privatpersonen initiierten Geschäfte nahm um rund einen Drittel ab, derjenige von Medien hat sich mehr als verdoppelt. Details zu den Medienanfragen finden sich auf Seite 32.

Involvierte Stellen Bei den in die Geschäfte involvierten Stellen sind die Zahlen stabil. Die im Jahr zuvor beobachtete Verschiebung vom Justiz- und Sicherheitsdepartement zum Departement für Wirtschaft, Soziales und Umwelt wurde wieder rückgängig gemacht (+7 Prozentpunkte bzw. -3 Prozentpunkte; 2015: -5 bzw. +4). Auch diese Schwankungen 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 Vgl. dazu PK-IDG/BS-Husi, § 9a N 7 ff., insb. 12 ff.; TB 2015, S. 35.
3 § 9a Abs. 5 IDG; vgl. dazu PK-IDG/BS-Husi, § 9a N 23; TB 2015, S. 35.
4 § 9a Abs. 4 IDG; vgl. dazu PK-IDG/BS-Husi, § 9a N 21 f.; TB 2015, S. 36.
5 Bericht 13.0739.02, 5 f.
6 § 44 lit. f IDG; vgl. dazu vgl. dazu PK-IDG/BS-Schilling, § 44 N 29 ff.
7 § 37a Gesetz vom 13. November 1996 betreffend die Kantonspolizei des Kantons Basel-Stadt (Polizeigesetz, PolG), SG 610.500.
8 Übergangsbestimmung zur Änderung des KVG vom 19. Juni 2015 i.V.m. Art. 39 Abs. 1 lit. f KVG.
9 § 7 Abs. 1 eHealth-Verordnung.
10 Art. 11 ff. EPDG.
11 Jahresbericht 2016 (des Regierungsrates), Staatskanzlei, Informationszugangsgesuche nach Departementen im Jahre 2016, S. 173.
12 TB 2015, S. 38; TB 2014, S. 34, und PK-IDG/BS-Rudin, § 30 N 21 ff.
13 Vgl. aber inzwischen Ratschlag 17.0998.01 vom 5. Juli 2017.
14 Jahresbericht 2016 (des Regierungsrates), S. 409.

Statistische Auswertungen 2016 (mit Vorjahresvergleichen)

A Geschäfte

	2016		2015		2014		2013	
	Anzahl	%	Anzahl	%	Anzahl	%	Anzahl	%
Anzahl eröffnete Geschäfte	447		411		400		403	
prozentuale Veränderung gegenüber Vorjahr		9		3		-1		10

B Indikatoren gemäss Budget

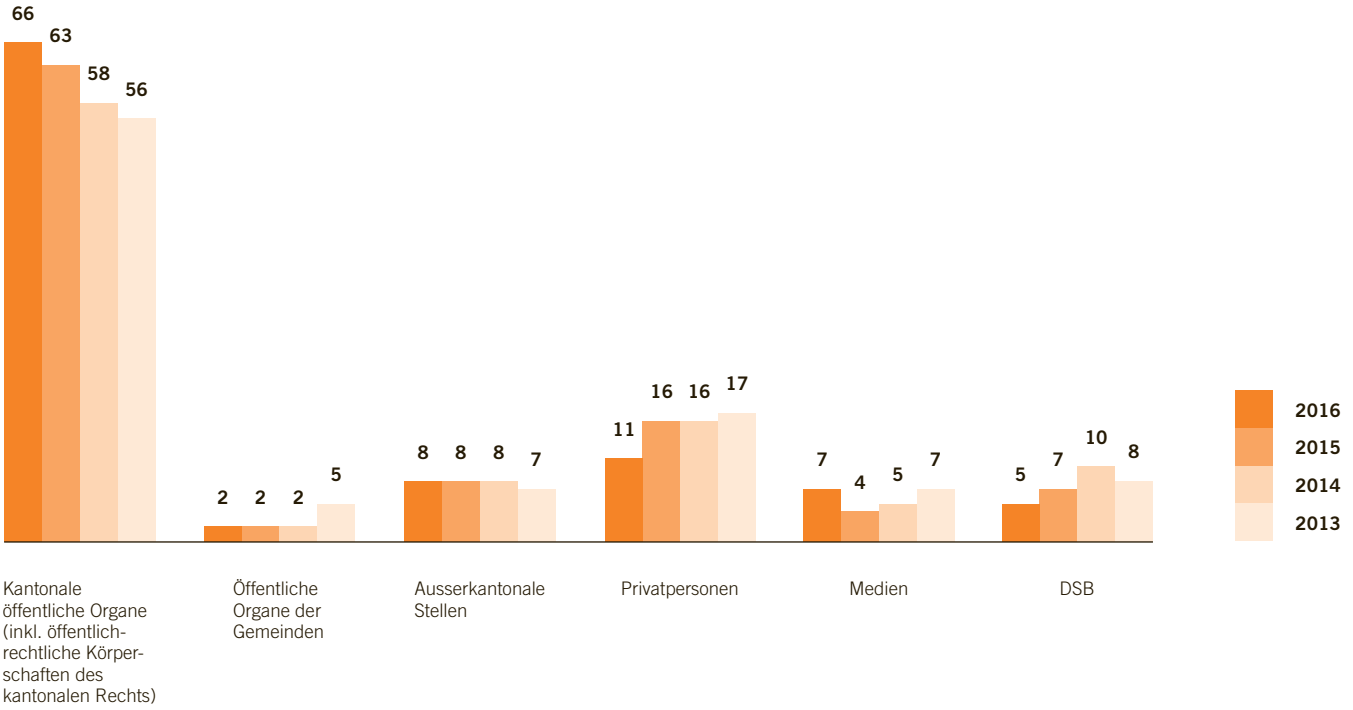
	2016		2015		2014		2013	
	Anzahl	%	Anzahl	%	Anzahl	%	Anzahl	%
Anteil komplexer Beratungen								
prozentualer Anteil an allen Beratungen		14		13		15		11
Innert 14 Tagen abgeschlossene nicht-komplexe Beratungen								
prozentualer Anteil an allen nicht-komplexen Beratungen		53		61		58		54
Durchgeführte Audits								
Anzahl durchgeführte Audits	1		4		5		4	
Durchgeführte Schulungen für öffentliche Organe								
Anzahl durchgeführte Schulungen	7		7		6		7	

C Öffentlichkeitsprinzip

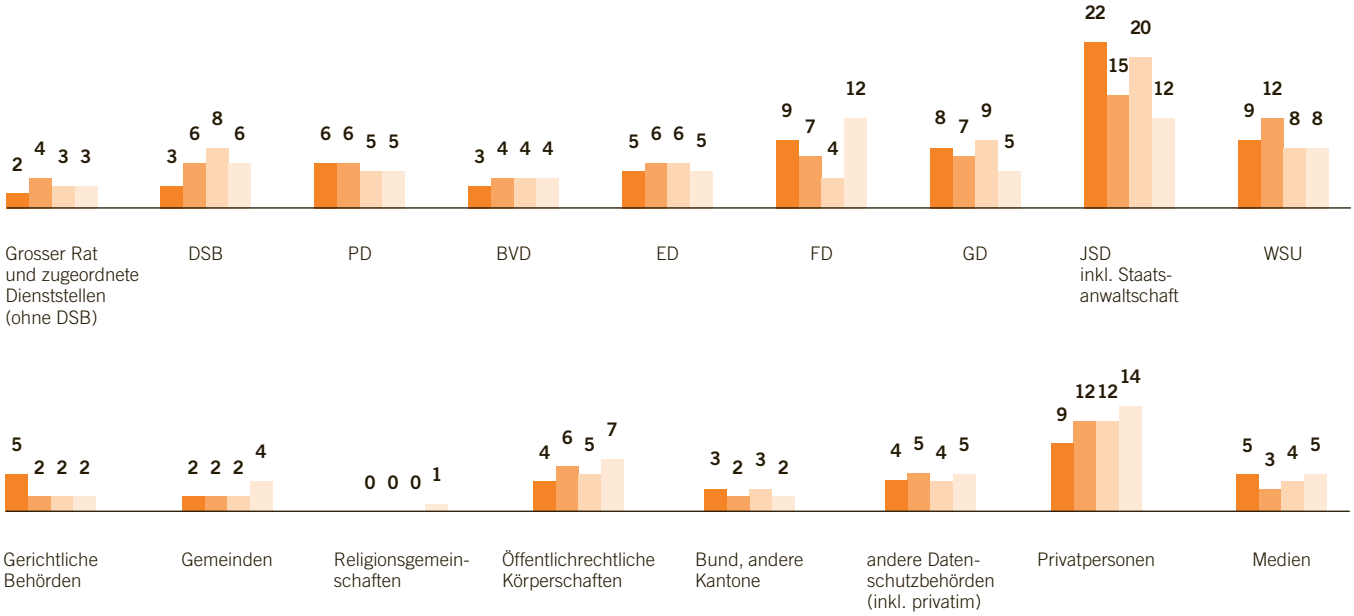
	2016		2015		2014		2013	
	Anzahl	%	Anzahl	%	Anzahl	%	Anzahl	%
Eingereichte Gesuche nach § 25 IDG								
Anzahl eingereichte Gesuche	33		19		18		30	
prozentuale Veränderung gegenüber Vorjahr		74		6		-40		-38
Behandlung der Gesuche nach § 25 IDG								
Anzahl gutgeheissener Gesuche		52		35		28		37
Anzahl teilweise gutgeheissener Gesuche		6		10		11		17
Anzahl ganz abgewiesener Gesuche		39		35		50		37
Anzahl noch nicht rechtskräftig entschiedener Gesuche		3		20		11		10

Öffentlichkeitsprinzip ab 2012.
Zahlen erfasst durch die Staatskanzlei aufgrund der Meldungen der Departemente (§ 31 IDV).
Zahlen aufgeschlüsselt nach Departementen: Jahresbericht 2016 (des Regierungsrates), Staatskanzlei, Informationszugangsgesuche nach Departementen im Jahre 2016, S. 173.

D Initianten: Veranlasser der Geschäfte (A) in %



E In die Geschäfte (A) involvierte Stellen in %



Fälle

Fall 1 Nach Bewerberinnen und Bewerbern googeln? Die tun das ja auch ...

Fall 2 «Den Medien etwas stecken» – Whistleblowing oder Amtsgeheimnisverletzung?

Fall 3 Logfiles kontrollieren – mal schauen, was Sie angeschaut haben?

Fall 1 Nach Bewerberinnen und Bewerbern googeln? Die tun das ja auch …

Wer sich auf eine Stelle bewirbt, recherchiert vorher über diesen Arbeitgeber. Auch wenn es eine Stelle in der Verwaltung ist. Was tut zum Beispiel ein Generalsekretariat? Wer leitet wohl die verschiedenen Abteilungen? Schliesslich wollen die Bewerberinnen und Bewerber sicher sein, dass sie sich auf eine interessante Stelle mit guten Leuten bewerben. Darf umgekehrt auch die Verwaltung in allen Quellen nach Informationen über ihre Bewerberinnen und Bewerber suchen?

Wenn ein öffentliches Organ eine Stelle besetzen muss, wie verlockend ist es doch da, auch ein wenig nach den Bewerberinnen und Bewerbern zu googeln! Oder ein bisschen mehr: zum Beispiel in sozialen Netzwerken zu recherchieren. Schliesslich sollen – logisch – nur die besten Leute angestellt werden. Interessant, was man da alles findet! Fotos von den Ferien, vielleicht auch Kommentare zu Vorkommnissen oder Äusserungen anderer Personen. Oder Schilderungen anderer Personen zu ihrem Verhalten an früheren Arbeitsstellen, im Sport usw.

Darf man das? Klar, sagen diejenigen, die es tun. Die Bewerberinnen und Bewerber tun es ja auch über die Dienststelle, bei der sie sich bewerben. Also gleich lange Spiesse für beide Seiten!

Nur – das stimmt nicht. Die öffentlichen Organe sind an das öffentliche Recht gebunden. Sie dürfen nur tun, wozu eine Rechtsgrundlage sie ermächtigt und was verhältnismässig ist. Und damit das auch gerade klar ist: Mit der Bewerbung willigen die Interessentinnen und Interessenten nicht einfach in das Erheben von beliebigen Daten über sie aus allen Quellen ein!

Aus dem Personalrecht kann – im Sinne einer mittelbaren gesetzlichen Grundlage[1] – abgeleitet werden, dass öffentliche Organe dafür sorgen müssen, für die Aufgabenerfüllung geeignete Personen anzustellen. Es wäre denkbar, dass das Recherchieren in allen verfügbaren Quellen dazu dienen könnte.

Allerdings ist die Verhältnismässigkeit einer solchen Datenbeschaffung mehr als fraglich. Ausserdem ist die Richtigkeit der Daten alles andere als gewährleistet. Handelt es sich beim «Peter Müller», über den Daten zu finden sind, um denjenigen, der sich bei Ihnen beworben hat? Und ist das, was irgendjemand über diesen Peter Müller hochgeladen hat, auch richtig – oder versucht jemand, ihn schlecht zu machen? Wird schon die Auswahl, wer zum Vorstellungsgespräch eingeladen wird, aufgrund solcher Informationen getroffen, dann haben die Bewerberinnen und Bewerber keine Chance, unrichtige Daten richtigzustellen. Ebenfalls klar ist: Informationen, nach denen in einem Vorstellungsgespräch nicht gefragt werden dürfte, dürfen auch nicht auf anderen Wegen beschafft werden.

Wie könnte eine Lösung aussehen, bei der sowohl die Sorgfaltspflicht des Arbeitgebers bei der Personalauswahl als auch die Persönlichkeitsrechte der Betroffenen miteinander vereinbart werden können? Bei der Recherche ist zwischen berufs- und freizeitorientierten Netzwerken zu unterscheiden:

— In spezifisch beruflichen sozialen Netzwerken wie LinkedIn oder Xing zugänglich gemachte Informationen dürfen miteinbezogen werden. Hier darf davon ausgegangen werden, dass die Bewerberinnen und Bewerber diese Informationen mit einem beruflichen Umfeld teilen wollen.

— Informationen, nach denen auch im Vorstellungsgespräch nicht gefragt werden dürfte, dürfen auch nicht in die Entscheidung über die Begründung eines Arbeitsverhältnisses einfliessen.

— Gefundene Informationen werden den Bewerberinnen bzw. Bewerbern vorgelegt, damit sie zu möglicherweise negativen Informationen direkt Stellung nehmen können.

Die gefundenen Informationen und allfällige Stellungnahmen dazu sind auf jeden Fall im Bewerbungsdossier zu dokumentieren.

Ergebnis

Das Googeln nach Informationen über Stellenbewerberinnen und –bewerber ist nur innerhalb der Grenzen des Persönlichkeitsschutzes zulässig. Es darf in beruflichen Netzwerken wie LinkedIn oder Xing nach Informationen gesucht werden. Die gefundenen Informationen müssen den Bewerberinnen und Bewerbern anlässlich des Vorstellungsgesprächs zur Stellungnahme vorgelegt werden. Die Informationen wie auch die Stellungnahmen dazu sind im Dossier zu dokumentieren.

1 § 9 Abs. 1 und 2, jeweils lit. b IDG.

Fall 2 «Den Medien etwas stecken» – Whistleblowing oder Amtsgeheimnisverletzung?

Darf die Mitarbeiterin oder der Mitarbeiter, die/der das Gefühl hat, in der Dienststelle laufe etwas nicht gut, Informationen dazu «den Medien» stecken? Quasi als Anwendungsfall des Öffentlichkeitsprinzips, weil doch die Öffentlichkeit ein berechtigtes Interesse daran hat, dass alles mit rechten Dingen zugehe?

In den letzten Jahren sind immer wieder Informationen über Unstimmigkeiten oder behauptete Unstimmigkeiten in der Verwaltung an die Medien gelangt. Nun «gelangen» die natürlich nicht einfach dorthin. In den meisten Fällen dürften es auch nicht Versehen gewesen sein, die dazu geführt haben, dass Informationen plötzlich Medienredaktionen zugänglich waren.

Die eine Fragestellung betrifft das, was die Medien daraus machen: Löst eine solche Information Recherchen aus? Werden die Verantwortlichen der betroffenen Amtsstellen zur Stellungnahme eingeladen? Wird schliesslich sachlich und unvoreingenommen über festgestellte Sachverhalte berichtet oder werden eigentliche Kampagnen gefahren? Das zu beurteilen, obliegt der Öffentlichkeit, allenfalls dem Presserat oder schliesslich den Gerichten.

In unserem Fokus steht hingegen die Frage, ob und unter welchen Voraussetzungen es Mitarbeitenden erlaubt ist, an die Medien zu gelangen. Regelmässig wird sich die Frage stellen, ob die Bekanntgabe von Informationen an die Medien eine Amtsgeheimnisverletzung darstellt. Die Verletzung des Amtsgeheimnisses ist strafbar. Das Personalgesetz legt fest, dass Staatsangestellte das Amtsgeheimnis zu wahren haben[1]; das Strafgesetzbuch stellt seine Verletzung unter Strafe[2].

Grundsätzlich untersteht dem Amtsgeheimnis auch die Tatsache, dass ein Vorgesetzter gegen rechtliche Bestimmungen verstösst. Es wäre aber unerträglich, wenn damit verboten würde, entsprechende Informationen weiterzugeben, damit solche Missstände behoben werden können. Deshalb hat der Gesetzgeber das Whistleblowing geregelt – allerdings nicht im Sinne eines Freipasses, Informationen «den Medien zu stecken». Es ist vielmehr eine Kaskade vorgesehen:

— Zuerst soll intern versucht werden, auf die Missstände aufmerksam zu machen; werden sie anschliessend behoben, ist der Zweck ja erreicht.

— Wenn nichts geschieht, dann dürfen Mitarbeitende – ohne das Amtsgeheimnis zu verletzen[3] – Missstände der Ombudsstelle melden[4]. Voraussetzung ist, dass sie in gutem Glauben sind, also aus objektiver Sicht davon ausgehen dürfen, dass tatsächlich ein solcher Verstoss vorliegt, und die Meldung nicht der Erlangung persönlicher Vorteile dienen soll[5].

— Nur wenn diese Meldung erfolgt ist und die Ombudsstelle innert zehn Arbeitstagen nicht reagiert hat, die Weitergabe der Information wiederum im guten Glauben erfolgt und die Allgemeinheit als solche ein Interesse an der Beseitigung des Missstandes hat[6], ist die Information der Öffentlichkeit erlaubt[7]. Wenn aber die Ombudsstelle ein Verfahren einleitet oder kein Verfahren einleitet, weil sie keine Anzeichen für das Vorliegen des gemeldeten Missstandes findet, ist die Information der Öffentlichkeit unzulässig und damit potenziell eine strafbare Amtsgeheimnisverletzung[8].

Wer diese Regeln umgeht, ist kein Whistleblower, den es zu schützen gilt, sondern ein potenzieller Straftäter.

Ergebnis

Über Missstände oder behauptete Missstände in der Verwaltung ist die Ombudsstelle zu informieren. Wenn die Ombudsstelle nicht innert zehn Arbeitstagen reagiert, kann die Information der Öffentlichkeit gerechtfertigt sein. Werden diese Regeln umgangen, dann handelt es sich nicht um Whistleblowing, sondern potenziell um Amtsgeheimnisverletzungen. Whistleblower sind zu schützen. Amtsgeheimnisverletzungen dienen nicht nur der ordentlichen Verwaltungsführung nicht, sondern schaden auch dem Vertrauen in die Verwaltung.

1 § 19 PG.
2 Art. 320 StGB.
3 § 19a Abs. 3 PG.
4 § 19a Abs. 1 PG.
5 § 19a Abs. 1 PG; § 2 Abs. 2 Whistleblowing-Verordnung.
6 § 2 Abs. 3 Whistleblowing-Verordnung.
7 § 4 Abs. 1 Whistleblowing-Verordnung.
8 § 4 Abs. 2 Whistleblowing-Verordnung.

Fall 3 Logfiles kontrollieren – mal schauen, was Sie angeschaut haben?

Viele Mitarbeitende der Verwaltung haben Zugriff auf Datenbanken. Darf der Staat die Nutzung solcher Anwendungen mittels Logfile-Kontrolle prüfen oder verletzt er damit die Persönlichkeitsrechte der Mitarbeitenden?

Viele Mitarbeitende erhalten zur Erfüllung ihrer gesetzlichen Aufgabe – und nur dafür – einen Onlinezugriff zu bestimmten Daten, etwa zu bestimmten Inhalten des kantonalen Datenmarktes, zu polizeilichen Datenbanken des Bundes oder des Kantons usw. Im Grunde genommen müssten die Zugriffsberechtigungen so eng gefasst werden, dass diese Mitarbeitenden nur auf Daten derjenigen Personen zugreifen können, die bei ihnen «als Geschäftsfall anfallen», und bei diesen Personen nur auf diejenigen Datenfelder, die zur Aufgabenerfüllung benötigt werden. Diese Zugriffsbegrenzung, z.B. durch Filtern (bezüglich der Personen) und Masken (bezüglich der Attribute dieser Personen), ist jedoch nicht immer möglich. Wenn die Bewährungshilfe zum Bezug von Betreibungsdaten über ihre Klienten berechtigt ist, dann gibt es im Betreibungsregister (zu Recht!) keinen Eintrag «Klient der Bewährungshilfe», der zum Filtern verwendet werden könnte.

Wenn die Eingrenzung nicht möglich ist, *können* die Mitarbeitenden Daten über Personen abrufen, obwohl sie dies nicht tun *dürfen*. Um das Risiko des Datenmissbrauchs zu verringern, kann es angezeigt sein, die Zugriffe zu loggen und die Logfiles periodisch auszuwerten, also zu prüfen, ob nur dann Daten abgerufen wurde, wenn die Zugriffsvoraussetzungen erfüllt waren.

Nach der Ansicht des Datenschutzbeauftragten können solche Kontrollen angebracht sein,

— wenn es sich bei den abrufbaren Daten um besondere Personendaten[1], also um Personendaten mit einem gewissen Stigmatisierungs- oder Diskriminierungspotenzial, oder um Daten handelt, die einem Berufs-[2] oder besonderen Amtsgeheimnis[3] unterstehen, oder

— wenn der Zugriff auf Daten von sehr viel mehr Personen möglich ist, als zur Aufgabenerfüllung erforderlich wäre, und

— wenn dafür gesorgt ist, dass die Logfile-Auswertung nicht zu einer Mitarbeiterüberwachung führt.

Bei Onlinezugriffen kann die Dateneignerin, auf deren Daten ein anderes öffentliches Organ zugreift, der Leitung dieses anderen öffentlichen Organs die Auflage machen, ein- oder zweimal pro Jahr (je nach Sensitivität oder Menge der abrufbaren Daten) eine Stichprobenkontrolle über einen bestimmten Kontrollzeitraum (Zugriffe während 1-2 Wochen) durchzuführen (also z.B. sich das Geschäft zeigen zu lassen, zu dessen Bearbeitung der Datenabruf erfolgt ist). Damit es keine Mitarbeiterüberwachung wird, kann z.B. der IT-Betreiber (und nicht die kontrollpflichtige Dienststellenleitung) den Zeitpunkt der konkreten Auswertung und nach dem Zufallsprinzip die Stichprobe bestimmen[4]. Das Resultat der Stichprobenkontrolle ist der Dateneignerin zuzustellen; der Datenschutzbeauftragte kann die Kontrolle und die Ergebnisse überprüfen.

Festzulegen sind auch die Konsequenzen bei Missverhalten, wenn auch nur in genereller Art, z.B. dass disziplinarische Massnahmen zu ergreifen sind. In schweren Fällen kann bzw. muss die Dateneignerin ihre Autorisierung des Onlinezugriffs widerrufen.

Anders als beim Mail oder der Internetnutzung können einer Auswertung von Logdaten bei (nicht-öffentlichen) Datenbanken keine privaten Interessen entgegenstehen: Der Onlinezugriff auf solche Datenbanken ist ausschliesslich zum Zweck der behördlichen Aufgabenerfüllung zulässig.

Ergebnis

Wenn die Onlinezugriffsmöglichkeiten nicht so eingegrenzt werden können, dass nur genau diejenigen Daten abgerufen werden können, deren Bearbeitung rechtmässig und verhältnismässig ist, kann es als kompensierende Massnahme angezeigt sein, die Zugriffe zu loggen und die Logfiles periodisch auszuwerten. Voraussetzung ist, dass es sich bei den abrufbaren Daten um besondere Personendaten, also um Personendaten mit einem gewissen Stigmatisierungs- oder Diskriminierungspotenzial, oder um Daten handelt, die einem Berufs- oder besonderen Amtsgeheimnis unterstehen, oder dass der Zugriff auf Daten von sehr viel mehr Personen möglich ist, als zur Aufgabenerfüllung erforderlich wäre. In jedem Fall muss dafür gesorgt sein, dass die Logfile-Auswertung nicht zu einer Mitarbeiterüberwachung führt.

1 § 3 Abs. 4 IDG; vgl. dazu PK-IDG/BS-Rudin, § 3 N 33 ff.

2 Z.B. einem Berufsgeheimnis, dessen Verletzung nach Art. 321 StGB unter Strafe gestellt ist: «Geistliche, Rechtsanwälte, Verteidiger, Notare, Patentanwälte, nach Obligationenrecht zur Verschwiegenheit verpflichtete Revisoren, Ärzte, Zahnärzte, Chiropraktoren, Apotheker, Hebammen, Psychologen sowie ihre Hilfspersonen».

3 Z.B. Sozialhilfegeheimnis, Sozialversicherungsgeheimnis, Schweigepflicht der Opferhilfeberatung, Steuergeheimnis, Stimmgeheimnis nach den entsprechenden Fachgesetzen; ihre Verletzung ist nach Art. 320 StGB strafbar.

4 Dafür braucht es Regeln und Prozesse. Für den Fall, dass Logfile-Kontrollen als kompensatorische Massnahmen für die Nichteingrenzbarkeit von Zugriffsberechtigungen angebracht sind, hat der Datenschutzbeauftragte die Konferenz für Organisation und Informatik auf das Bedürfnis nach klaren Regeln und Prozessen aufmerksam gemacht.

Anhang Verzeichnis der zitierten Gesetze, Materialien und Literatur

Kanton Basel-Stadt:
Rechtsgrundlagen, Materialien

Rechtsgrundlagen

AufenthG Gesetz vom 16. September 1998 über das Aufenthaltswesen (Aufenthaltsgesetz), SG 122.200 (per 1. Juli 2017 abgelöst vom NAG).

DMV Verordnung vom 4. Juli 2017 über den Datenmarkt (Datenmarktverordnung, DMV), SG 153.310.

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

eHealth-Verordnung Verordnung vom 19. April 2016 über den eHealth-Modellversuch Basel (eHealth-Verordnung), SG 300.310.

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

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

IWB-Gesetz Gesetz vom 11. Februar 2009 über die Industriellen Werke Basel (IWB-Gesetz), SR 772.300.

Kantonalbankgesetz Gesetz vom 9. Dezember 2015 über die Basler Kantonalbank, SG 915.200.

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

NAG Gesetz vom 11. Januar 2017 über Niederlassung und Aufenthalt (NAG), SG 122.200 in Kraft seit 1. Juli 2017).

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.

PPV-Erweiterte Gefährderansprache Verordnung vom 25. August 2015 über die Meldung von gefährdenden Personen im Rahmen eines Pilotversuchs («Erweiterte Gefährderansprache»)

VOGB Verordnung vom 16. Dezember 2003 über das Grundbuch (VOGB), SG 214.310.

Whistleblowing-Verordnung Verordnung vom 24. September 2013 betreffend Meldung von Missständen (Whistleblowing-Verordnung), SG 162.600.

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.

Interpellationsantwort 14.5049.02 Schreiben 14.5049.02 des Regierungsrates vom 26. Februar 2014 zur Interpellation Nr. 5 André Auderset betreffend Nichthandeln der Behörden bei illegalen Videoüberwachungen.

KdK-Leitfaden 2017 Leitfaden der Konferenz der Kantonsregierungen (KdK-Leitfaden), EU-Datenschutzreform/Modernisierung der Europarats-Konvention 108: Anpassungsbedarf bei den kantonalen (Informations- und) Datenschutzgesetzen, Bern, 2. Februar 2017, Kurz-URL: <http://bit.ly/2sfj00f>.

KdK-Wegleitung 2006 Konferenz der Kantonsregierungen (KdK), Umsetzung Schengen/Dublin in den Kantonen: Datenschutz, Wegleitung, 2006, Kurz-URL: <http://bit.ly/2mCJaZb>.

Ratschlag 17.0998.01 Ratschlag 17.0998.01 vom 5. Juli 2017 zu einer Änderung des Gesetzes über die Information und den Datenschutz vom 9. Juni 2010 (Informations- und Datenschutzgesetz).

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.

Ratschlag 08.0637.01 Ratschlag 08.0637.01 des Regierungsrates vom 11. Februar 2009 betreffend Gesetz über die Information und den Datenschutz (Informations- und Datenschutzgesetz).

Bund:
Rechtsgrundlagen, Materialien

Rechtsgrundlagen

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

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

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

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

EPDG Bundesgesetz vom 19. Juni 2015 über das elektronische Patientendossier (EPDG), SR 816.1.

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

PBG Bundesgesetz vom 20. März 2009 über die Personenbeförderung (Personenbeförderungsgesetz, PBG), SR 745.1.

SAA Abkommen zwischen der Schweizerischen Eidgenossenschaft, der Europäischen Union und der Europäischen Gemeinschaft über die Assoziierung dieses Staates bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands, SR 0.362.31.

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

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

Materialien

Erläuternder Bericht zum VE-DSG Bundesamt für Justiz, Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz, 21. Dezember 2016, <https://www.admin.ch/ch/d/gg/pc/documents/2826/Totalrevision-des-Datenschutzgesetzes_Erl.-Bericht_de.pdf> (Kurz-URL: <http://bit.ly/2sDZ5YI>).

VE-DSG Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz, Anhang: Bundesgesetz über den Datenschutz (Vernehmlassungsvorlage), 21. Dezember 2016, <https://www.admin.ch/ch/d/gg/pc/documents/2826/Totalrevision-des-Datenschutzgesetzes_Entwurf-DSB_de.pdf> (Kurz-URL: <http://bit.ly/2thnSTS>).

Europarat, Europäische Union: Rechtsgrundlagen

Rechtsgrundlagen

DSGVO Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl L119 vom 4.5.2016, 1 ff.

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

E-ER-Konv 108 Entwurf Übereinkommen (des Europarates) zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten; konsolidierter Wortlaut der Vorschläge zur Modernisierung des Übereinkommens 108 im Anschluss an die Sitzung des CAHDATA (15./16. Juni 2016), <https://www.admin.ch/ch/d/gg/pc/documents/2826/Totalrevision-des-Datenschutzgesetzes_Uebereinkommen_de.pdf>.

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

Rahmenbeschluss 2008/977/JI Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, ABl L 350/60 vom 30. Dezember 2008.

Richtlinie (EU) 2016/680 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl L119 vom 4.5.2016, 89 ff.

RL 2016/680 siehe Richtlinie (EU) 2016/680.

ZP zur ER-Konv 108 Zusatzprotokoll vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung, SR 0.235.11.

Tätigkeitsberichte

TB 2015 Tätigkeitsbericht des Datenschutzbeauftragten des Kantons Basel-Stadt, 2015, abrufbar unter <http://www.dsb.bs.ch/dam/jcr:6aacf6b8-8531-4c88-889c-9ffc5108e6bf/TB_2015_des_DSB_BS.pdf> (Kurz-URL: <http://bit.ly/2viNP98>).

TB 2014 Tätigkeitsbericht des Datenschutzbeauftragten des Kantons Basel-Stadt, 2014, abrufbar unter <http://www.dsb.bs.ch/dam/jcr:dfe74bc4-031e-4583-9814-05bfc9cca763/2014_taetigkeitsbericht.pdf> (Kurz-URL: <http://bit.ly/2u3Ihzr>).

TB 2013 Tätigkeitsbericht des Datenschutzbeauftragten des Kantons Basel-Stadt, 2013, abrufbar unter <http://www.dsb.bs.ch/dam/jcr:cb0b8dc7-bfc5-4113-9511-c79fc3747692/2013_Taetigkeitsbericht.pdf> (Kurz-URL: <http://bit.ly/2ujOsLf>).

TB 2012 Tätigkeitsbericht des Datenschutzbeauftragten des Kantons Basel-Stadt, 2012, abrufbar unter <http://www.dsb.bs.ch/dam/jcr:c0234879-d5d3-4db7-bfd7-05d22169dbeb/2012_Taetigkeitsbericht.pdf> (Kurz-URL: <http://bit.ly/2tZljV7>).

TB 2011 Tätigkeitsbericht des Datenschutzbeauftragten des Kantons Basel-Stadt, 2011, abrufbar unter <http://www.dsb.bs.ch/dam/jcr:fb385ad9-1fbb-4e53-bf63-e2b5f57c148a/2011_taetigkeitsbericht.pdf> (Kurz-URL: <http://bit.ly/2uVRybU>).

TB 2010 Tätigkeitsbericht des Datenschutzbeauftragten des Kantons Basel-Stadt, 2010, abrufbar unter <http://www.dsb.bs.ch/dam/jcr:6a26f5b1-4b92-4146-bf8c-74b20b374da4/2010_Taetigkeitsbericht.pdf> (Kurz-URL: <http://bit.ly/2uVG2gt>).

TB 2009 Tätigkeitsbericht des Datenschutzbeauftragten des Kantons Basel-Stadt, 2009, abrufbar unter <http://www.dsb.bs.ch/dam/jcr:456ed814-2293-49fa-9e54-31a33cc34006/2009_Taetigkeitsbericht.pdf> (Kurz-URL: <http://bit.ly/2vifkQr>).

Literatur

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

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

Datenschutzbeauftragter
Beat Rudin, Prof. Dr. iur., Advokat

Team
Markus Brönnimann, CISA
Katja Gysin, Fürsprecherin
Daniela Waldmeier, Dr. iur.
Barbara Widmer, Dr. iur., LL.M., CIA
Katrin Gisler, MLaw
(befristet bis 30.3.2016)

Volontärinnen:
Cora Dubach, MLaw
(1.1.2016 - 30.6.2016)
Sarah Salzmann, MLaw
(1.7.2016 - 31.12.2016)

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
datenschutz@dsb.bs.ch
www.dsb.bs.ch

Gestaltung
Andrea Gruber,
Gruber Gestaltung, Basel

Druck
Gremper AG, Basel/Pratteln