Datenschutzbeauftragter des Kantons Basel-Stadt

Bericht an den Grossen Rat

’17
’18
’19

Inhaltsübersicht

Einleitung

Trends

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

Fotokonzept: Cloud(s)
Fotos: B. Rudin

Jahresüberblick

Fälle

Anhang

Einleitung

2017–2019: Ein Drei-Jahresbericht

Sie suchen die Tätigkeitsberichte 2017 und 2018 des Datenschutzbeauftragten des Kantons Basel-Stadt? Vergebens. Aus Ressourcengründen ist die Berichterstattung nicht mit solchen gedruckten Berichten erfolgt, sondern mündlich. Das soll jetzt aber mit diesem Drei-Jahresbericht nachgeholt werden: Was hat der Datenschutzbeauftragte in diesen Jahren getan? Was hat ihn herausgefordert? Worauf hat er den Finger gelegt?

Lücken in Ihrer Sammlung

Keine gedruckten Berichte Sie, sehr geehrte Leserin, sehr geehrter Leser, haben völlig recht, wenn Sie unsere Tätigkeitsberichte für die Jahre 2017 und 2018 in Ihrer Sammlung nicht gefunden haben. Es gibt sie gar nicht. Die Geschäftslast und die Einführung neuer Mitarbeiterinnen und Mitarbeiter haben jeweils dazu geführt, dass wir unsere Ressourcen auf die Abarbeitung der Geschäfte konzentriert und notgedrungen irgendwo reduziert haben.

Nicht gar keine Rechenschaft Nun war es ja nicht so, dass wir den Grossen Rat als das Organ, dem wir als eine der «Kleeblattdienststellen» zugeordnet sind, gar nicht informiert haben. Die Verspätung und schliesslich der Verzicht auf die beiden schriftlichen Tätigkeitsberichte war gegenüber der Datenschutzdelegation des Ratsbüros offengelegt, und in den ein bis zwei Hearings pro Jahr bei der grossrätlichen Geschäftsprüfungskommission wurde über die Kennzahlen, die wichtigsten Geschäfte und Erkenntnisse informiert, insbesondere aus Bereichen, in denen Handlungsbedarf bestand. Aber – das schleckt keine Geiss weg – die gedruckten Berichte blieben aus.

Neugestaltung Ein Grund dafür, warum die Kommunikation in Form des Tätigkeitsberichts ausblieb, war auch die Konzeption der früheren Tätigkeitsberichte. Sie waren sehr umfangreich und sehr aufwändig zu erstellen. Wir haben zwar viele sehr positive Rückmeldungen erhalten, weil die Berichte die Breite der Datenschutzthemen anschaulich zum Ausdruck gebracht und im Sinne eines Multiplikators geholfen haben, praktikable Lösungen für datenschutzrechtliche Probleme aufzuzeigen, die auch für andere als die direkt betroffenen öffentlichen Organe hilfreich sein konnten. Mit einer sanften Neukonzeption sollen nun Umfang und Aufwand reduziert werden, ohne dass die Stärken der bisherigen Tätigkeitsberichte verloren gehen.

Keine Datenschutzthemen mehr?

Im Gegenteil Gibt es keine Datenschutzthemen mehr? Ist das mit ein Grund für das Ausbleiben der zwei letzten Tätigkeitsberichte? Im Gegenteil! Mit der zunehmenden Digitalisierung werden es immer mehr – und immer dringendere. Digitale Lösungen basieren auf Daten, auch häufig auf Personendaten. Für das Vertrauen in die staatlichen Institutionen ist es unerlässlich, dass die Verwendung von immer mehr Daten nicht einfach zu Lasten der Persönlichkeits- und Grundrechte der betroffenen Personen geht – und betroffene Personen sind wir in unserem Leben immer häufiger und umfassender. Eine Polizistin etwa ist während ihrer Arbeitszeit zwar Datenbearbeiterin, also Subjekt einer (behördlichen) Datenbearbeitung; im ganzen übrigen Leben ist sie aber Objekt von unzähligen (behördlichen und privaten) Datenbearbeitungen – und damit sehr wohl auch daran interessiert, dass ihre Daten durch die anderen Datenbearbeiterinnen nur so bearbeitet werden, dass ihre Rechte gewahrt bleiben.

Zum Beispiel der Drang in die Cloud Die «Cloud» kommt, ob wir das wollen oder nicht. Ja, sie ist an vielen Orten schon da. Wenn Sie, liebe Leserin, lieber Leser, Ihre privaten Daten auf OneDrive von Microsoft ablegen oder in der iCloud von Apple – schon sind sie in der Cloud. Wenn Sie das als Privatperson tun, um die Daten auf all Ihren Geräten verfügbar zu haben oder um von einer vielleicht höheren Sicherheit zu profitieren, dann liegt es an Ihnen zu entscheiden, ob der Kontrollverlust, der unweigerlich damit verbunden ist, dies wert ist oder nicht. Nicht so beim Staat: Die öffentlichen Organe dürfen nicht beliebig Risiken eingehen – insbesondere nicht Risiken

für die Grundrechte der Einwohnerinnen und Einwohner, deren Daten sie bearbeiten. Es braucht somit eine umfassende Risikoanalyse und Schutzmassnahmen, welche die Risiken ausschliessen bzw. soweit vermindern, dass das Restrisiko tragbar ist. Für welche Anwendungen und mit welchen Schutzmassnahmen Cloud-Lösungen überhaupt in Frage kommen, muss differenziert entschieden werden: Eine Lösung, die für harmlose Datenbearbeitungen in Frage kommt, passt möglicherweise nicht für Gesundheits- oder Steuerdaten. Letztlich muss das verantwortliche öffentliche Organ – d.h. die Leitung dieses öffentlichen Organs! – bestätigen, dass es die verbleibenden Risiken (das Restrisiko für die behördliche Aufgabenerfüllung und für die betroffenen Personen, das durch Schutzmassnahmen nicht weiter minimiert werden kann oder soll) kennt und sie übernimmt. Es trägt der Öffentlichkeit und den betroffenen Personen gegenüber die Verantwortung für den Gang in die Cloud. Das gilt generell bei allen Projekten – doch mit der Nutzung von Cloud-Technologien kommen neue Risiken hinzu oder akzentuieren sich.

Achtung Preisschild Jede Schutzmassnahme hat ein Preisschild und ist darum vielleicht nicht so «sympatisch». Jedes nicht durch eine Schutzmassnahme beseitigte Risiko hat aber ebenfalls ein Preisschild. Damit der kumulierte Risikoappetit von Dienststellen nicht gefährlich gross wird, werden die Departementsvorsteherinnen und -vorsteher und schliesslich der Gesamtregierungsrat gefordert sein, sich einen Überblick zu verschaffen – oder sogar bestimmte weitreichende Entscheide selber zu treffen.

Der Bericht

Drei Teile Mit dem Hinweis auf das Beispiel der Cloud-Problematik (siehe dazu S. 11 ff.) sind wir bereits mitten im Bericht. Er fasst die drei Jahre zusammen und gliedert sich – ähnlich wie bisher – in drei Teile:

— Im ersten Teil (S. 8 ff.), gleich nach der Einführung, zeigen wir Trends auf, die uns in den vergangenen drei Jahren beschäftigt haben.

— Im zweiten Teil (S. 24 ff.) stellen wir dar, was wir in dieser Zeit in der Beratungs- und Kontrolltätigkeit getan haben und was uns dabei besonders herausgefordert hat. Abgeschlossen wird dieses Kapitel durch die Statistik (S. 34 f.).

— Im dritten Teil schliesslich (S. 38 ff.) illustrieren wir ein paar spezifische Fragestellungen in Form von Fällen.

Wir wünschen Ihnen eine erspriessliche Lektüre!

Zum Schluss

Danke! Unsere Aufgabe nach dem Informations- und Datenschutzgesetz (IDG)[1] ist es, für den Schutz der Privatheit der Einwohnerinnen und Einwohner, über welche die öffentlichen Organe Daten bearbeiten, und ihres Informationszugangsrechts nach dem Öffentlichkeitsprinzip zu sorgen. Diese Aufgabe könnten wir nicht erfolgreich erfüllen ohne die Unterstützung vieler Menschen und Institutionen. Mein Dank gilt deshalb:

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

— allen, die sich mit Fragen zum Datenschutz und zum Öffentlichkeitsprinzip vertrauensvoll an uns wenden;

— den Mitarbeiterinnen und Mitarbeitern der Verwaltung von Kanton und Gemeinden, der öffentlich-rechtlichen Anstalten und der Gerichte, die mithelfen, datenschutzkonforme Lösungen zu finden und umzusetzen;

— den Kolleginnen und Kollegen der «Kleeblattdienststellen» für die gute Zusammenarbeit;

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

— den Volontärinnen und Volontären Meltem Aslan, Cäcilia Dürdoth, Lucas Maciejewski, Simone Mäder, Larissa Meyer und Tobias Schwaller für ihre kritische Neugier und die aktive Mitarbeit in ihrem jeweils sechsmonatigen Volontariat und

— last but not least meinem Team[2], Rüdiger Bachmann, Eva Maria Bader, Markus Brönnimann, Katja Gysin, Nicole Kuster, Pascal Lachenmeier, Sarah Salzmann, Sukhwant Singh, Thomas Sterchi, Ines Weihrauch und Barbara Widmer, das in den drei Berichtsjahren mit grossem Engagement, mit spannenden Diskussionen und konstruktiven Anregungen unsere Arbeit bereichert und vorangebracht hat.

Beat Rudin, Datenschutzbeauftragter

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

2 Ein riesiges Team – aber nur scheinbar: Eine einzige Mitarbeiterin war über die ganze Zeit im Team des Datenschutzbeauftragten. Die genauen Daten finden Sie im Impressum (S. 47).

Trends

Trend 1 Digitalisierung: «intelligente Fahrzeuge»

Trend 2 Digitalisierung: Cloud, Software as a Service (SaaS)

Trend 3 Von unangenehmen Kunden bis zu den Gefährdern

Trend 4 Europäische Datenschutz-reformen und das IDG

Trend 1 Digitalisierung: «intelligente Fahrzeuge»

Künftig werden immer mehr «intelligente Fahrzeuge» beschafft werden – nicht nur Alarmpikettfahrzeuge für die Kantonspolizei, sondern auch «gewöhnliche» Personenwagen für andere öffentliche Organe, Fahrzeuge für die Rettung, Kehricht- und Reinigungsfahrzeuge usw. Wie kann die Verwaltung dafür sorgen, dass beim Betrieb der Fahrzeuge die Datenschutzregeln eingehalten werden?

«Intelligente Fahrzeuge»

Datengetriebene Systeme Ob «intelligente Fahrzeuge» intelligent sind, mag kritisch hinterfragt werden. Auf jeden Fall sind solche Fahrzeuge eine Herausforderung auch für den Datenschutz, da das, was als «intelligent» bezeichnet wird, in der Regel darauf basiert, dass eine Unmenge von Informationen für die Steuerung verwendet werden. Einige dieser Informationen sind auch Personendaten, weil sie sich auf mindestens bestimmbare Personen beziehen lassen und damit Aussagen zu diesen Personen entstehen. Wird die Fahrroute eines solchen Fahrzeugs ausgewertet, sagt das auch etwas über die Fahrerin aus.

Nicht nur der Tesla Solche «intelligente Fahrzeuge» sind nicht nur beispielsweise der Tesla X 100D, das Alarmpikettfahrzeug der Kantonspolizei Basel-Stadt. Auch andere Fahrzeuge sind heute voll mit Assistenz- und Steuerungssystemen, auch lange bevor sie «autonom» fahren können. Auch Fahrzeuge der Stadtreinigung oder der Rettung etwa zeichnen grosse Mengen von Daten auf, bei deren Bearbeitung auf Datenschutzkonformität zu achten ist.

Alarmpikettfahrzeug der Polizei

Digitalisierungsprojekt Das Alarmpikett-Fahrzeug Tesla X der Kantonspolizei hat es nicht nur zu einem Spitzensujet an der Fasnacht 2019 gebracht. Auch wenn zu Beginn der Beschaffung bestimmte Fragen zum Datenschutz noch nicht beantwortet waren – am Schluss war die Behandlung der Fragen rund um den Umgang mit Informationen ein gutes Beispiel für ein Digitalisierungsprojekt. Früher waren Fahrzeuge vor allem Fahrzeuge, heute werden sie je länger desto mehr zu Computern auf Rädern. Deshalb muss sich eine Beschaffung künftig auch um Datenschutzfragen kümmern.

Nie «wegen des Datenschutzes» in der Garage Was eingangs festgehalten werden muss, nachdem eine Tageszeitung auch bei der dritten Publikationswelle immer noch das Gegenteil behauptet hatte: Der Tesla war nie «wegen des Datenschutzes» nicht im Einsatz[1]. Die Datenschutzfragen konnten fundiert abgeklärt werden während der Phase, in der beispielsweise die Ausbildung der Fahrerinnen und Fahrer stattfand.

Der Tesla war nie «wegen des Datenschutzes» nicht im Einsatz.

Vorabkontrolle Vor dem Einsatz der Fahrzeuge wurde die Beschaffung dem Datenschutzbeauftragten zur Vorabkontrolle im Sinne von § 13 IDG vorgelegt. Die Vorabkontrolle konzentrierte sich der gesetzlichen Aufgabe des Datenschutzbeauftragten entsprechend auf die Datenschutzfragen, also auf das Bearbeiten von Personendaten. Es stellte sich die Frage, ob durch den Betrieb der Fahrzeuge Personendaten erhoben und allenfalls bekannt gegeben werden. Falls das der Fall ist, muss geprüft werden, ob die Bearbeitung recht- und verhältnismässig ist. Andere Fragen, ob beispielsweise Unberechtigte herausfinden können, wo sich die Fahrzeuge gerade befinden oder ob sie allenfalls böswillig «gehackt» werden können, sind Fragen, welche sich jede Betreiberin «intelligenter Fahrzeuge» im Lichte der Erfüllung ihrer gesetzlichen Aufgaben selber stellen und beantworten muss.

Prüfung Der Datenschutzbeauftragte hat über die Kantonspolizei bei der Herstellerin Informationen zu den Datenbearbeitungen eingeholt. Mit einer technischen Prüfung durch die cnlab security ag wurden die erhaltenen Informationen soweit möglich verifiziert oder plausibilisiert.

Resultat Im Resultat hat sich gezeigt:

— Die *Bild-/Videodaten*, die alle ausserhalb der Fahrzeuge aufgenommen werden, werden nur temporär auf einem internen flüchtigen Speicher festgehalten.

— Nur im Falle eines *sicherheitsrelevanten Vorfalles* (Auslösung oder Fast-Auslösung des Airbags, was während der Lebensdauer eines Fahrzeuges zwischen nie und sehr selten stattfinden dürfte) werden die Aufnahmen wenige Sekunden vor dem Ereignis auf einem fest eingebauten Speicher festgehalten, verschlüsselt an die Herstellerin übermittelt und danach auf dem Speicher im Fahrzeug gelöscht. Das Risiko einer Persönlichkeitsverletzung erscheint damit sehr gering. Um die Gefahr einer Identifikation gänzlich auszuschliessen, sollte die Kantonspolizei Basel-Stadt prüfen, ob sie diese automatische Übermittlung deaktivieren lassen will.

— Optional ist die Funktion einer *Dashcam* verfügbar; sie muss aber von der Fahrzeughalterin oder vom Fahrzeughalter eigens aktiviert werden. Die Kantonspolizei Basel-Stadt hat darauf verzichtet und will die Dashcams auch in Zukunft nicht einrichten. Falls sie darauf zurückkommen möchte, ist dieses Vorhaben dem Datenschutzbeauftragten zur Vorabkontrolle vorzulegen.

— *Sprach-/Audiodaten* werden nur aufgenommen, wenn der Sprachbefehlsknopf am Lenkrad aktiviert wird. Sie werden in Echtzeit verschlüsselt an einen von der Herstellerin beauftragten Drittanbieter für die Umwandlung von Sprach- zu Textbefehlen weitergeleitet und als umgewandelter Text am Armaturenbrett angezeigt. Die Sprachbefehle werden nur temporär im Fahrzeug gespeichert und nach der Bearbeitung gelöscht. Die Messung des Datenverkehrs zwischen Fahrzeug und Internet ergab, dass das beobachtete Aufkommen und Datenvolumen für den Dienst plausibel erscheint. Ein allfälliger Personenbezug ist im Falle der Alarmpikettfahrzeuge nicht direkt herstellbar, da Aussenstehende grundsätzlich keine Kenntnis haben, wer sich zu einem bestimmten Zeitpunkt im Fahrzeug befindet.

— Durch weitere Sensoren werden *Informationen zum Fahrzeugzustand* (inkl. Fahrverhalten) und zu den Fahrzeuginsassen erhoben, auf internen Speichermedien festgehalten und anschliessend an die Herstellerin übermittelt. Die Herstellerin kann die Personen höchstens singularisieren, aber allein aufgrund der Fahrzeugidentifikationsnummer nicht bestimmen, wer die Person ist. Für die Kantonspolizei Basel-Stadt sind diese Daten zur Person der Fahrerin oder des Fahrers zuordenbar, weil die Kantonspolizei aufgrund der Einsatzplanung bzw. Einsatzleitung ohnehin weiss, wer ihrer Mitarbeitenden als Fahrerin oder Fahrer oder als weiteres Teammitglied eingeteilt ist. Ausserdem müssen Blaulichtfahrzeuge nach der bundesrätlichen Verordnung über die technischen Anforderungen an Strassenfahrzeuge (VTS) mit einem Datenaufzeichnungsgerät ausgerüstet sein[2], so dass im Fall von Kollisionen auch weitere Informationen aus den 30 Sekunden vor dem Ereignis bekannt sind. Die Kantonspolizei Basel-Stadt muss (z.B. in einer Dienstvorschrift) die notwendigen Rechtsgrundlagen für die Bearbeitung der auf Mitarbeitende beziehbaren Daten schaffen und durch organisatorische Massnahmen sicherstellen, dass die Daten auch nur so bearbeitet werden, wie dies gerechtfertigt und verhältnismässig ist.

— Die *Geolokalisierung* (z.B. durch Nutzung eines Navigationssystems) ist datenschutzrechtlich nur relevant, wenn die Daten einen Personenbezug aufweisen. Das darf in Bezug auf die Herstellerin und die Dienstanbieterinnen ausgeschlossen werden.

Nur im Falle eines sicherheitsrelevanten Vorfalles werden die Aufnahmen wenige Sekunden vor dem Ereignis auf einem fest eingebauten Speicher festgehalten, verschlüsselt an die Herstellerin übermittelt und danach auf dem Speicher im Fahrzeug gelöscht.

— Wenn die Datenübermittlungen an die Herstellerin und von ihr beauftragte Drittanbieter recht- und verhältnismässig sind, ist es unerheblich, mit welchen Mitteln die Datenübertragung stattfindet (über Mobilfunk, WLAN oder durch Auslesen des Speichers). Um das Risiko einer (ungerechtfertigten) Übertragung besser kontrollieren zu können, ist der Ersatz der Tesla-SIM-Card durch die *SIM-Card eines Schweizer Providers* zu begrüssen.

— Es ist dafür zu sorgen, dass künftige *Änderungen in der Konfiguration* der Hard- und Software auf ihre datenschutzrechtliche Relevanz überprüft und gegebenenfalls dem Datenschutzbeauftragten zur Vorabkontrolle vorgelegt werden. >

Empfehlungen Der Datenschutzbeauftragte hat der Kantonspolizei den Schlussbericht der Vorabkontrolle[3] zugestellt und acht Empfehlungen abgegeben[4]. Werden diese Empfehlungen angenommen, steht einem Einsatz der Alarmpikettfahrzeuge aus datenschutzrechtlicher Sicht nichts entgegen. Eine Prüf-Empfehlung war Ende 2019 noch in Arbeit; alle anderen Empfehlungen wurden von der Kantonspolizei angenommen und bereits umgesetzt.

Andere «intelligente Fahrzeuge»

Überarbeitung des Fragebogens Als Lehre aus der Alarmpikett-Fahrzeug-Vorabkontrolle hat der Datenschutzbeauftragte den Fragebogen zu den Datenbearbeitungen in «intelligenten Fahrzeugen» überarbeitet und dem Justiz- und Sicherheitsdepartement (JSD) im Hinblick auf weitere Fahrzeugbeschaffungen zur Verfügung gestellt. Er wurde vom JSD bei einer Ausschreibung anfangs 2020 in diesem Sinne verwendet.

Der Datenschutzbeauftragte empfiehlt bei künftigen Fahrzeugbeschaffungen zu verlangen, dass die offerierenden Unternehmen auch verpflichtet werden, den erwähnten Fragebogen zur Erhebung und Bearbeitung von Informationen auszufüllen.

Weitere Fragestellungen Bei Fahrzeugen anderer öffentlicher Organe hat sich die Frage gestellt, wie aufgrund der gewonnenen Informationen eine Prozessoptimierung (z.B. eine Verbesserung der Toureneinteilung oder Routenwahl) vorgenommen werden kann, ohne dass es zu einer unerlaubten Überwachung von Mitarbeiterinnen oder Mitarbeitern führt. Weil einem bestimmten Fahrzeug auf einer bestimmten Tour eine bestimmte Fahrerin zugeteilt ist, sind Angaben über das Fahrverhalten, die Routenwahl, die Pausen usw. immer personenbezogen. Für die Auswertung sind deshalb immer genügend lange Auswertungszeiträume zu wählen. Falls bestimmte Auswertungen personenbezogen vorgenommen werden sollen, müssen die entsprechenden Rechtsgrundlagen dies erlauben und muss dies den Mitarbeiterinnen und Mitarbeitern vorgängig transparent gemacht werden. Bestimmte Optimierungen, etwa ein fahrzeug- und umweltschonendes Fahren, können auch durch Schulungen und Informationskampagnen erreicht werden.

Beschaffungen in der Zukunft

Fragebogen und technische Prüfung In Zukunft werden zunehmend «intelligente Fahrzeuge» beschafft werden. Der Datenschutzbeauftragte empfiehlt von den offerierenden Unternehmen zu verlangen, den erwähnten Fragebogen zur Erhebung und Bearbeitung von Informationen auszufüllen. Um nicht von den Beurteilungen der offerierenden Firmen abhängig zu sein (die zum Beispiel meinen, es würden gar keine Personendaten bearbeitet, weil sie nicht realisieren, dass Informationen schon zu Personendaten werden, wenn sie «personenbeziehbar» sind, also etwa mit Daten über die Fahrerin verknüpfbar sind), empfiehlt es sich auch, durch eine (externe) technische Prüfung die Angaben der Herstellerinnen zu verifizieren / falsifizieren oder wenigstens plausibilisieren zu lassen.

1 Medienmitteilung des JSD und des DSB vom 20. Dezember 2018: <https://www.jsd.bs.ch/nm/2018-inbetriebnahme-der-neuen-alarmpikett-fahrzeuge-der-kantonspolizei-verzoegert-sich-nicht-jsd.html> (Kurz-URL: <https://bit.ly/2C6soxi>).
2 Art. 102 VTS.
3 Schlussbericht: <https://www.dsb.bs.ch/dam/jcr:be059e63-d032-4817-9381-5227de60c7f3/Schlussbericht_Vorabkontrolle_Intelligente_Fahrzeuge_final_20190426_(Web).pdf> (Kurz-URL: <https://bit.ly/3e26NmE>).
4 Medienmitteilung des Datenschutzbeauftragten vom 26. April 2019 zur Vorabkontrolle der Alarmpikett-Fahrzeuge der Kantonspolizei: <https://www.dsb.bs.ch/medienmitteilungen-und-stellungnahmen/medienmitteilung-zur-tesla-vorabkontrolle.html>. (Kurz-URL: <https://bit.ly/3dWqZX7>).

Trend 2 Digitalisierung: Cloud, Software as a Service (SaaS)

Es gibt – auch bei der staatlichen Verwaltung – als Megatrend einen starken Drang «in die Cloud». Bei Clouddiensten wird oft etwas «wolkig», wer dort mit welchen Daten was tun kann. Weniger «wolkig» ist, wer die Verantwortung dafür trägt. Diese bleibt von Gesetzes wegen beim öffentlichen Organ, auch wenn es die Daten durch Dritte bearbeiten lässt. Es braucht eine umfassende Risikoanalyse und -abwägung. Selbst wenn Schweizer Recht anwendbar und vor einem Schweizer Gericht durchsetzbar ist, wird nicht «alles» in die Cloud verschoben werden können.

Der Drang in die Cloud

Megatrend In den vergangenen drei Jahren gab es einen Megatrend: den Drang in die Cloud. Es gibt Anbieterinnen von Anwendungen, die ankündigen, dass sie diese in ein paar Jahren nur noch als Cloud-Anwendungen anbieten würden. Andere Anbieterinnen versuchen die Nutzerinnen und Nutzer, die bisher Softwarepakete gekauft haben, in Abonnementslösungen (häufig Clouddienste) zu verschieben, welche die Updates von Software vereinfachen, vor allem aber auch regelmässige Abonnementseinnahmen generieren.

Cloud und Datenschutz Was hat Cloud mit Datenschutz zu tun? Mit der Inanspruchnahme von Cloud-Technologien geht ein gewisser Kontrollverlust einher. Nicht dass mit einer «on premise»-Lösung – der Betrieb einer Anwendung auf den eigenen Servern – sozusagen von alleine alle Datenschutz- und Sicherheitsprobleme gelöst wären, beileibe nicht. Aber die Auslagerung in die Cloud bringt zusätzliche Risiken, und die Verantwortung dafür bleibt beim auftraggebenden öffentlichen Organ!

Verantwortung beim auftraggebenden öffentlichen Organ

Auftragsdatenbearbeitung Anders als bei der Aufgabenübertragung (oder Funktionsübertragung), wo die Privaten (Privatpersonen oder private Unternehmen), denen die öffentliche Aufgabe übertragen wird, selber zu einem öffentlichen Organ werden[1] und damit selber für die Einhaltung aller datenschutzrechtlichen Pflichten und Obliegenheiten verantwortlich sind[2], bleibt das öffentliche Organ, das zur Erfüllung seiner gesetzlichen Aufgabe Informationen durch einen Dritten bearbeiten lässt, vollumfänglich verantwortlich[3]. Es muss vertraglich[4] dafür sorgen, dass – vereinfacht gesagt – die Auftragnehmerin das tut, was ihr das öffentliche Organ aufträgt, und alles unterlässt, was ihr vom öffentlichen Organ nicht aufgetragen wird. Die Person, deren Rechte durch die Auftragsdatenbearbeiterin verletzt werden, kann sich an das auftraggebende öffentliche Organ halten: Dieses bleibt ihr gegenüber verantwortlich und allenfalls haftbar. Es liegt deshalb im ureigensten Interesse des auftraggebenden öffentlichen Organs, dass es dafür sorgt, dass die Auftragnehmerin die Informationen ausschliesslich so bearbeitet, wie es selber es auch tun dürfte[5].

Zulässigkeit der Auftragsdatenbearbeitung Bevor ein öffentliches Organ Informationen (und insbesondere Personendaten) durch Dritte bearbeiten lässt, muss es prüfen, ob eine Auftragsdatenbearbeitung überhaupt zulässig ist. Das IDG lässt die Auslagerung schon gar nicht zu, wenn eine rechtliche Bestimmung (zum Beispiel ein besonderes Amtsgeheimnis oder ein Berufsgeheimnis) oder eine vertragliche Vereinbarung entgegenstehen[6]. Ob eine Auftragsdatenbearbeitung zulässig ist, bestimmt sich nach den entsprechenden Rechtsgrundlagen (nach dem IDG und den spezifischen Fachgesetzen, wo beispielsweise die besonderen Amtsgeheimnisse statuiert sind).

Leitfaden Auftragsdatenbearbeitung Wenn eine Auslagerung grundsätzlich zulässig ist, dann muss das öffentliche Organ durch Vertrag sicherstellen, dass die Auftragsdatenbearbeiterin die Informationen nur so bearbeitet, wie es selber das auch tun dürfte. Der Datenschutzbeauftragte hat dafür einen Leitfaden Auftragsdatenbearbeitung veröffentlicht[7]. Je nach Art der Daten und der Bearbeitung sind einzelne der aufgeführten Aspekte wichtiger als andere.

Inanspruchnahme von Cloud-Technologie Die von Dritten zur Verfügung gestellten Datenbearbeitungsdienstleistungen basieren heute immer mehr auf der Verwendung von *Cloud-Technologie*: Ressourcen für die Datenbearbeitungen werden dynamisch zur Verfügung gestellt, und eine konkrete Lokalisation von Datenbearbeitungen und Daten ist nicht vorgesehen: Sie befinden sich eben in der «Cloud». >

Auch bei der Inanspruchnahme solcher Cloud-Dienstleistungen bleibt das auftraggebende öffentliche Organ vollumfänglich verantwortlich. Es muss deshalb zusätzlich die Cloud-spezifischen Risiken beurteilen und die zur Vermeidung oder Minimierung dieser Risiken notwendigen Massnahmen vorkehren. Dazu muss es eine umfassende Risikoanalyse und -abwägung vornehmen. Für diese Herausforderung hat privatim, die Konferenz der schweizerischen Datenschutzbeauftragten, ein Merkblatt zu Cloud-spezifischen Risiken und Massnahmen[8] veröffentlicht.

privatim-Merkblatt zu Cloud-spezifischen Risiken und Massnahmen

Zweck Mit diesem Merkblatt soll aufgezeigt werden, welche Risiken bei Cloud-Dienstleistungen *zusätzlich zu denen einer Auftragsdatenbearbeitung* hinzukommen oder sich akzentuieren und wie die Verantwortung diesbezüglich von den öffentlichen Organen konkret wahrgenommen werden kann. Diese Risiken sind durch angemessene Massnahmen auszuschliessen oder auf ein tragbares Mass zu reduzieren. Bei der *umfassenden Risikoanalyse* für die konkrete Datenbearbeitung sind die cloud-spezifischen Risiken mit zu berücksichtigen und es sind entsprechende Vorkehrungen zu treffen. Im Vordergrund stehen drei Risikobereiche: das anwendbare Recht und der Gerichtsstand, der Ort der Datenbearbeitung (Serverstandorte) und der Geheimnisschutz bzw. das Schlüsselmanagement.

Anwendbares Recht und Gerichtsstand

Es geht primär um Vertragsrecht, nicht um Datenschutzrecht Das anwendbare Recht und der Gerichtsstand[9] sind zentrale Punkte bei Streitigkeiten aus dem Vertrag. Ein Privatunternehmen, ob im Inland oder im Ausland, untersteht als Auftragsdatenbearbeiterin nicht dem IDG, sondern dem DSG (oder als Unternehmen in einem EU-Mitgliedstaat der DSGVO). Anders ist das, wenn ihm vom Kanton oder einer Gemeinde eine gesetzliche Aufgabe übertragen wird, womit es selber zum öffentlichen Organ wird, dessen Datenbearbeiten dem IDG untersteht[10]. Einer Auftragsdatenbearbeiterin hingegen kann nicht einfach auferlegt werden: «Es gilt das baselstädtische Informations- und Datenschutzgesetz», sondern es ist *im Auftrag klar und verständlich festzulegen*, was die Auftragnehmerin tun muss und nicht tun darf, damit sie nur das tut, was auch das auftraggebende öffentliche Organ tun dürfte – also insbesondere:

— die Personendaten nur so bearbeitet, wie es das öffentliche Organ aufgrund seiner gesetzlichen Grundlage bearbeiten dürfte[11];

— die Personendaten nur nach Treu und Glauben und verhältnismässig bearbeitet[12];

— die Personendaten zu keinem anderen Zweck[13] bearbeitet als zu dem, zu dem die Auftragnehmerin vom auftraggebenden öffentlichen Organ beauftragt worden ist, also insbesondere nicht zu einem eigenen Zweck;

— die Informationssicherheit so gewährleistet, wie es das IDG verlangt[14],

— nur richtige Personendaten bearbeitet[15];

— die Personendaten, die es bearbeitet hat, nach den Vorgaben des auftraggebenden öffentlichen Organs an dieses zurückgibt und die gespeicherten Daten vernichtet, sobald der Auftrag erledigt (und die Erledigung kontrolliert) ist[16].

Das auftraggebende öffentliche Organ muss zusätzlich die Cloud-spezifischen Risiken beurteilen und die zur Vermeidung oder Minimierung dieser Risiken notwendigen Massnahmen vorkehren. Dazu muss es eine umfassende Risikoanalyse und -abwägung vornehmen.

Erhebliches Risiko Ein öffentliches Organ muss gegenüber den Personen, deren Daten es bearbeiten lässt, geradestehen. Eine betroffene Person kann ihre *Ansprüche aus dem IDG[17] gegenüber dem öffentlichen Organ* geltend machen und allenfalls sogar nach dem Haftungsgesetz Schadenersatz verlangen[18]. Sieht der Vertrag einer Anbieterin von Onlinediensten nun beispielweise die Geltung des irischen Rechts und Dublin als Gerichtsstand vor, dann geht das öffentliche Organ mit einem solchen Vertrag ein erhebliches Risiko ein. Im Falle einer Verletzung der Vertraulichkeit von Kundendaten in Clouddiensten richtet sich die Haftung der Anbieterin/Auftragsdatenbearbeiterin gegenüber dem öffentlichen Organ nach irischem Recht und kann im dort erlaubten Umfang – z.B. auch für grobe Fahrlässigkeit – ausgeschlossen werden. Wenn dann ein öffentliches Organ die vertraglichen Zusicherungen nach einer ihm nicht bekannten Rechtsordnung vor einem für das Organ nicht einfach zugänglichen Gericht durchsetzen muss, dann kann es faktisch nicht sicherstellen, «dass die Informationen nur so bearbeitet werden, wie es das öffentliche Organ tun dürfte»[19].

Scheinlösung Wenn eine Anbieterin von Clouddiensten dem Kanton – als «Lösung» – die folgende Vertrags-Zusatzbestimmung vorschlägt: «Für Klagen und Begehren gestützt auf das schweizerische Bundesgesetz über den Datenschutz und die schweizerische Verordnung zum Bundesgesetz über den Datenschutz sind die Gerichte in der Schweiz zuständig»,

dann blenden deren Juristen die Rechtsetzungs-Kompetenzordnung im Datenschutzbereich aus – oder – das darf man aber einer Anbieterin nicht unterstellen – man versucht den Kanton als Vertragspartner über den Tisch zu ziehen. Die auftraggebenden kantonalen und kommunalen Organe können Klagen und Begehren nicht auf das Bundesdatenschutzgesetz stützen, weil das für sie schlicht nicht gilt: Für sie gilt das entsprechende kantonale Informations- und Datenschutzgesetz. Und die Betroffenen, die Personen, deren Daten von der Auftragsdatenbearbeiterin allenfalls vertragswidrig bearbeitet worden sind, können sich wie erwähnt an das verantwortliche öffentliche Organ halten, das ihnen für die datenschutzkonforme Bearbeitung ihrer Personendaten verantwortlich ist – und auch sie haben deshalb keine Ansprüche aus dem Bundesdatenschutzgesetz, sondern ebenfalls aus dem kantonalen Informations- und Datenschutzgesetz.

Ort der Datenbearbeitung (Serverstandort)

Schweiz oder Staat mit angemessenem Datenschutzniveau Der Ort der Datenbearbeitung (Serverstandort)[20] kann insofern von Bedeutung sein, als ein ausländischer Staat unter Umständen nach seinem Recht auf Daten auf Servern in seinem Einflussgebiet zugreifen kann, auch wenn dies nach schweizerischen Recht nicht zulässig wäre. Aus diesem Grund ist als Ort der Datenbearbeitung wenn möglich die Schweiz oder ein Staat mit einem angemessenen Datenschutzniveau zu wählen.

«Übergriffiges» ausländisches Recht Bei Rechtsregimen mit extraterritorialer Wirkung spielt allerdings der Serverstandort keine entscheidende Rolle mehr: So müssen etwa dem US-amerikanischen CLOUD Act – der nichts mit Cloud Computing zu tun hat, sondern die Abkürzung ist für Clarifying Lawful Overseas Use of Data Act[21]– unterstehende Cloud-Anbieterinnen[22] den US-Behörden auch dann *Zugriff auf gespeicherte Daten* gewähren, wenn die Speicherung nicht in den USA, sondern zum Beispiel in einem EU-Mitgliedstaat oder in der Schweiz erfolgt. Da hilft eigentlich nur noch der Verzicht auf Angebote solcher Anbieterinnen oder die Verunmöglichung des Zugriffs durch Verschlüsselung. Der Serverstandort kann auch aus anderen Gründen relevant sein: Einerseits kann die Sicherheit der Infrastruktur z.B. in Bezug auf die Schutzziele Verfügbarkeit und Integrität, Zurechenbarkeit und Nachvollziehbarkeit schwächer sein; und andererseits muss allenfalls ein nach Schweizer Recht am Schweizer Gerichtsstand errungenes Urteil im Ausland durchgesetzt werden, was zusätzlichen Aufwand verursacht. Solche Risiken sind bei der umfassenden Risikobeurteilung ebenfalls in Rechnung zu stellen.

Schutz der Vertraulichkeit: Verschlüsselung, Schlüsselmanagement

Verschlüsselung Zum Schutz insbesondere der Vertraulichkeit der in der Cloud bearbeiteten Daten kann Verschlüsselung[23,24] dienen. Daten (data at rest und data in transit) sind nach dem aktuellen Stand der Technik zu verschlüsseln. Bei besonderen Personendaten – inklusive Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterstehen – sind zusätzliche Anforderungen an die Verschlüsselung und das Schlüsselmanagement zu stellen:

— Die Verschlüsselung soll *durch das öffentliche Organ* erfolgen. Grundsätzlich dürfen die Schlüssel nur für das öffentliche Organ verfügbar sein. Die Schlüssel sind vor Verlust, Entwendung sowie unrechtmässiger Bearbeitung und Kenntnisnahme zu schützen.

— Ist dies nicht möglich, können die Schlüssel – wenn die umfassende Risikoabwägung dies zulässt – bei der Cloud-Anbieterin aufbewahrt werden, wenn sie sich *vertraglich verpflichtet*, sie nur mit der ausdrücklichen Zustimmung des öffentlichen Organs zu verwenden. Zugriffe sind zu protokollieren. Ausserdem muss die Cloud-Anbieterin die Schlüssel vor Verlust, Entwendung sowie unrechtmässiger Bearbeitung und Kenntnisnahme schützen und sicherstellen, dass die Daten beim Verschlüsselungsvorgang nicht kompromittiert werden können. Eine solche Regelung ist aber letztlich rein vertraglicher Art und wird nochmals geschwächt, wenn auf den Vertrag nicht Schweizer Recht anwendbar und nicht ein Schweizer Gerichtsstand vereinbart ist. Auf jeden Fall stellt eine Verschlüsselung, bei welcher die Verschlüsselung nicht durch das öffentliche Organ erfolgt und der Schlüssel nicht ausschliesslich für das Organ verfügbar ist, ein höheres Risiko dar, was bei der Risikoabwägung in Rechnung zu stellen ist.

Verschlüsselung ist nicht gleich Verschlüsselung Es ist schliesslich darauf hinzuweisen, dass Verschlüsselung nicht einfach gleich Verschlüsselung ist[25]. Es ist genau zu prüfen, was wann verschlüsselt ist (bzw. was in welchem Moment nicht verschlüsselt ist und wer dann darauf zugreifen kann) und wer über den Schlüssel verfügt. Eine reine Transportverschlüsselung und Speicherverschlüsselung bringt keinen durchgehenden Schutz, wenn die Daten «in der Cloud» im Klartext bearbeitet werden (z.B. bei Software as a Service, SaaS). >

Glossar Eine Umschreibung der wichtigsten Begriffe im Zusammenhang mit Cloud Computing finden Sie auf unserer Website unter: über <https://www.dsb.bs.ch/handreichungen/privatim-merkblatt-cloud.html>.

Fazit des privatim-Merkblatts[26]

Umfassende Risikoanalyse Öffentliche Organe können für ihre Datenbearbeitungen – wenn ihre Auslagerung nach den allgemeinen Regeln für die Auftragsdatenbearbeitung (also nach Konsultation des Leitfadens Auftragsdatenbearbeitung) zulässig ist – auch Cloud-Dienstleistungen Dritter in Anspruch nehmen. Dafür sind in einer umfassenden Risikoanalyse die spezifischen Risiken bei Inanspruchnahme von Cloud-Dienstleistungen zu berücksichtigen. Diese Risikoanalyse muss differenziert für die einzelnen Datenbearbeitungen die cloud-spezifischen Risiken sowie die entsprechenden Massnahmen aufzeigen, mit denen die cloud-spezifischen Risiken ausgeschlossen oder auf ein tragbares Mass reduziert werden können. Die Beurteilung soll aufzeigen, ob für die Datenbearbeitungen die Inanspruchnahme von Cloud-Diensten umfassend, teilweise oder nicht zulässig ist.

Schriftliche Übernahme der Verantwortung Die öffentlichen Organe, die für ihre Aufgabenerfüllung Cloud-Dienstleistungen in Anspruch nehmen, tragen weiterhin vollumfänglich die Verantwortung für die Datenbearbeitung. Das öffentliche Organ (bzw. seine Leitung) ist anzuhalten, schriftlich zu bestätigen, dass es *die Risiken verstanden hat und das Restrisiko übernimmt*. Die Übernahme von Restrisiken kann allenfalls auch Auswirkungen auf die Rechnungslegung haben, was durch die Finanzkontrollen zu prüfen ist. Der Exekutive ist zu raten, die übernommenen (Rest-)Risiken regelmässig zu erfassen, da sie gegenüber Parlament und Volk letztlich die Verantwortung für den Schutz der Grundrechte der Bürgerinnen und Bürger und für das finanzielle Gebaren der Verwaltung zu tragen hat. Haben untergebene Dienststellen einen (übermässigen) Risikoappetit, *kumuliert* sich das Risiko auf Departements- und Regierungsebene.

Datenschutz-Folgenabschätzung Das öffentliche Organ muss seinerseits eine Datenschutz-Folgenabschätzung[27] durchführen. Dem Datenschutzbeauftragten sind Risikoanalyse und Massnahmenplan zur Prüfung vorzulegen (Vorabkontrolle im Sinne von § 13 IDG). Der Datenschutzbeauftragte steht den öffentlichen Organen auch bezüglich rechtlicher, organisatorischer und technischer Fragen beratend zur Seite.

Umsetzung im Kanton

Beispiele Im Kanton Basel-Stadt sind verschiedene Fragen im Zusammenhang mit Clouddiensten im Gespräch. An zwei konkreten Beispielen sollen zum Abschluss spezifische Fragen kurz angeschnitten werden. Auch andere Anbieterinnen bieten z.B. für Unterrichtszwecke vergleichbare Rahmenverträge an (z.B. die von educa.ch bzw. SWITCH mit Google ausgehandelten Rahmenverträge über die Nutzung von G Suite Enterprise for Education[28]).

Die öffentlichen Organe, die für ihre Aufgabenerfüllung Cloud-Dienstleistungen in Anspruch nehmen, tragen weiterhin vollumfänglich die Verantwortung für die Datenbearbeitung.

Microsoft Office 365 für Unterrichtszwecke Microsoft hat in einem Rahmenvertrag für Microsoft Office 365 für das Bildungswesen Schweizer Recht und Schweizer Gerichtsstand anerkannt. Der Datenschutzbeauftragte des Kantons Basel-Stadt hat, gestützt auf Vorarbeiten des Datenschutzbeauftragten des Kantons Zürich, einen Leitfaden für die datenschutzkonforme Nutzung von Microsoft Office 365 im Bildungsbereich[29] verfasst. Der Leitfaden richtet sich an Volks- und Mittelschulen des Kantons Basel-Stadt, die Microsoft Office 365 für Unterrichtszwecke nutzen wollen – nicht aber für Datenbearbeitungen durch die Schuladministration! Dafür müsste sie Microsoft 365 für die Verwaltung nutzen (siehe sogleich unten). Der Leitfaden gibt einen Überblick über die Vorgehensweise, Vorabklärungen und Massnahmen, die vor Inanspruchnahme und im Rahmen der Nutzung der Dienste umgesetzt werden müssen, um einen datenschutzkonformen Einsatz zu gewährleisten.

Microsoft 365 für die Verwaltung: Ausblick. Im Rahmenvertrag zwischen Microsoft und der Schweizerischen Informatikkonferenz (SIK) gilt für Microsoft-Onlinedienste für die Verwaltung noch immer irisches Recht und Gerichtsstand Dublin. Aus diesem Grund empfehlen die Datenschutzbehörden, die Onlinedienste *mit diesem Vertrag nicht zu nutzen*. Aber auch wenn dereinst – der Datenschutzbeauftragte von Basel-Stadt ist als Präsident von privatim, der Konferenz der schweizerischen Datenschutzbeauftragten, Teil einer Delegation, die gemeinsam mit der SIK dies zu erreichen versucht – Schweizer Recht und ein Gerichtsstand in der Schweiz gelten sollten, können diese Clouddienste *nicht einfach «für alles»* genutzt werden. Dann erst beginnt die oben dargestellte Risikoabwägung: Wenn das Cloud-Risiko bei der Bearbeitung von Sachdaten oder harmlosen Personendaten als tragbar beurteilt wird, kann das bei der Bearbeitung

von besonderen Personendaten oder Daten, die einem Berufs- oder einem besonderen Amtsgeheimnis (z.B. Steuer-, Sozialversicherungs-, Sozialhilfe oder Opferhilfegeheimnis) unterstehen, ganz anders aussehen. Auch das Risiko des Zugriffs US-amerikanischer Behörden aufgrund des CLOUD Act dürfte bei bestimmten Daten (z.B. Steuerdaten) sicher anders zu beurteilen sein als beispielsweise im Bildungsbereich bei Daten, die rein zu Unterrichtszwecken in der Cloud bearbeitet werden.

Fazit

Risikoappetit und Sparhoffnungen Der Drang in die Cloud besteht schon länger, wird aber immer stärker. Es sind auch nicht nur die grossen Projekte, die diesem Trend unterliegen. Einzelne Verwaltungsstellen (auch Private, denen der Kanton oder eine Gemeinde eine öffentliche Aufgabe übertragen haben und die deshalb zum öffentlichen Organ geworden sind) möchten gerne da und dort Clouddienste nutzen. Stark im Kommen sind etwa auch Tools für Meldeverfahren oder für Anmeldeverfahren. Von Anbieterinnen werden finanziell verführerische Einstiegsangebote unterbreitet. Bevor aber Verantwortliche die Unterschrift unter die schriftliche Bestätigung, die Risiken verstanden zu haben und das Restrisiko zu übernehmen, setzen, sollten sie sich nochmals zurücklehnen und über ihre Verantwortung nachdenken: Wollen sie diejenigen sein, denen ein paar Jahre später nach einem Datenschutzskandal vorgeworfen wird, sie hätten, geblendet von Hochglanzversprechen und der Aussicht auf Sparpotenzial, untragbare Risiken übernommen? Risiken notabene nicht für ihre Rechte, sondern für die Grundrechte der Menschen, deren Daten sie bearbeiten. Menschen, die ihre Daten dem Staat anvertraut haben, aufgrund einer gesetzlichen Pflicht anvertrauen mussten[30] oder deren Daten der Staat aufgrund einer gesetzlichen Grundlage, also ohne ihre Einwilligung und vielleicht sogar ohne ihr Wissen bearbeiten darf. Während es im Privatrecht vielleicht möglich ist, die Einwilligung der Betroffenen für eine unsichere Bearbeitung ihrer Daten einzuholen – das geht im öffentlichen Recht nicht.

1 § 3 Abs. 1 lit. c IDG; vgl. dazu PK-IDG/BS-Rudin, § 3 N 10.
2 § 6 Abs. 1 IDG; vgl. dazu PK-IDG/BS-Rudin, § 6 N 4 ff.
3 § 7 Abs. 2 IDG; vgl. dazu PK-IDG/BS-Rudin, § 7 N 57 ff.
4 Nach § 1 IDV muss nur der Auftrag an Organisationseinheiten oder Private, die nicht dem IDG unterstehen, *schriftlich* erteilt werden – zum Schutz des auftraggebenden öffentlichen Organs sollten auch Auftragserteilungen an öffentliche Organe, die dem IDG unterstehen, schriftlich erteilt werden (vgl. dazu PK-IDG/BS-Rudin, § 7 N 38).
5 § 7 Abs. 1 lit. b IDG; vgl. dazu PK-IDG/BS-Rudin, § 7 N 19 ff.
6 § 7 Abs. 1 lit. a IDG; vgl. dazu PK-IDG/BS-Rudin, § 7 N 32 ff.
7 Abrufbar über: <https://www.dsb.bs.ch/handreichungen/leitfaden-auftragsdatenbearbeitung.html>.
8 privatim-Merkblatt Cloud-spezifische Risiken und Massnahmen (v2.0 vom 17. Dezember 2019), abrufbar über: <https://www.dsb.bs.ch/handreichungen/privatim-merkblatt-cloud.html>.
9 privatim-Merkblatt (Fn. 8), Ziff. 3.1.
10 Wie erwähnt nach § 3 Abs. 1 lit. c IDG.
11 § 9 Abs. 1 oder 2 IDG; vgl. dazu PK-IDG/BS-Rudin, § 9 N 14 ff. und N 25 ff.
12 § 9 Abs. 3 IDG; vgl. dazu PK-IDG/BS-Rudin, § 9 N 51 ff.
13 § 12 IDG; vgl. dazu PK-IDG/BS-Rudin, § 12 N 2 ff.
14 § 8 IDG; vgl. dazu PK-IDG/BS-Baeriswyl, § 8 N 7 ff.
15 § 11 IDG; vgl. dazu PK-IDG/BS-Rudin, § 11 N 2 ff.
16 § 16 IDG; vgl. dazu PK-IDG/BS-Rudin, § 16 N 2 ff.
17 § 27 Abs. 1 IDG: Anspruch auf Unterlassung einer widerrechtlichen Datenbearbeitung, auf Beseitigung der Folgen einer widerrechtlichen Bearbeitung bzw. Feststellung der Widerrechtlichkeit einer Bearbeitung von Personendaten; vgl. dazu PK-IDG/BS-Husi, § 27 N 4 ff.
18 § 3 HG.
19 § 7 Abs. 1 lit. b IDG.
20 privatim-Merkblatt (Fn. 8), Ziff. 3.2.
21 Clarifying Lawful Overseas Use of Data Act (CLOUD Act), H.R. 4943, <https://www.congress.gov/bill/115th-congress/house-bill/4943>.
22 Vgl. zur Frage, wer dem U.S. CLOUD Act untersteht, das Whitepaper des US-Justizdepartements vom April 2019, insb. S. 8: <https://www.justice.gov/opa/press-release/file/1153446/download>.
23 «Verschlüsselung» meint hier, dass Informationen für Personen (oder Maschinen) ohne Zugriff auf den Schlüssel mittels kryptografischer Mittel unlesbar gemacht werden. Der Begriff der Verschlüsselung wird beispielsweise auch vom Humanforschungsgesetz verwendet, aber in einem anderen Sinn: Dort sollen Informationen durchaus lesbar bleiben, aber der Personenbezug soll (reversibel) entfernt werden. Dafür sollte der Begriff der «Pseudonymisierung» verwendet werden, um eine Verwechslung mit der kryptografischen Verschlüsselung zu vermeiden.
24 privatim-Merkblatt (Fn. 8), Ziff. 3.3.
25 Vgl. dazu Michael Herfert/Benjamin Lange/Dominik Spychalski, Verschlüsselung in der Cloud, digma 2019, S. 128 ff.
26 privatim-Merkblatt (Fn. 8), Ziff. 4.
27 Die Datenschutz-Folgenabschätzung wird nach dem europäischen Recht vorgeschrieben, ist im Grund genommen nichts anderes als die Vorbereitung der Vorlage einer Projektes zur Vorabkontrolle (jetzt schon nach 13 IDG) und sollte in der bevorstehenden Revision ins IDG aufgenommen werden.
28 Nicht aber für die kostenlose Version G Suite for Education.
29 <https://www.dsb.bs.ch/handreichungen/leitfaden-office-365-bildungsbereich.html>.
30 Anders als bei privaten Datenbearbeitern können sie, wenn sie mit der gebotenen Informationssicherheit nicht einverstanden sind, auch nicht einfach zu einer anderen Behörde wechseln: «Ich werde in Zukunft nicht mehr Sie, sondern die Steuerbehörde des Kantons Zug berücksichtigen».

Trend 3 Von unangenehmen Kunden bis zu den Gefährdern

Die grosse Mehrheit der Bürgerinnen und Bürger verhält sich im Umgang mit Verwaltungsstellen gesittet – immer mehr sehen sich aber Verwaltungsangestellte Aggressionen ausgesetzt: Sie werden grob angegangen, angeschrien, beleidigt, gar bedroht. Wie kann der Staat als Arbeitgeber seine Mitarbeiterinnen und Mitarbeiter schützen, ohne den Eindruck zu erwecken, die Bürgerinnen und Bürger alle als Störer zu betrachten?

Von überhöhtem Respekt zur Respektlosigkeit

Schweizweit Es ist bekannt, dass es schwierige Kundinnen und Kunden gibt. Auch, dass bei gewissen Leuten die Hemmschwelle sinkt, bis sie verbal aggressiv oder handfest tätlich werden. Das äussert sich häufig in grober Sprache, Anschreien, Beleidigungen, Drohungen. Die Polizei beklagt schweizweit schon seit langem, dass vermehrt Polizistinnen und Polizisten angegriffen werden. Während früher der Respekt vor Amtspersonen wohl überhöht war, kehrt die Entwicklung nun teilweise ins Gegenteil: Gewisse Mitbürgerinnen und Mitbürger verlieren Mitarbeiterinnen und Mitarbeitern der Verwaltung gegenüber jeden Respekt. Je mehr die Verwaltungsstellen ins Leben der Betroffenen ein-greifen, umso eher werden ihre Mitarbeiterinnen und Mitarbeiter zur Zielscheibe von «wutbürgerlichen» Ausbrüchen.

Telefonaufzeichnung Schon vor ein paar Jahren haben Mitarbeiterinnen und Mitarbeiter solcher Stellen (bei einer Abteilung bei der Steuerverwaltung und beim Betreibungsamt) unter telefonischen Beleidigungen bis hin zu Drohungen gelitten, die dann aber vor Gericht nicht haben bewiesen werden können. Aus diesem Grund wurde die technische Möglichkeit geschaffen, dass Telefongespräche bei diesen Stellen – nach einer Vorankündigung – aufgezeichnet werden konnten. Nach einer kurzen Frist musste anschliessend entschieden werden, ob sie zu Beweiszwecken bei einer Strafanzeige verwendet werden sollen – andernfalls wurden sie automatisch gelöscht. Der Ansagetext hat offensichtlich eine präventive Wirkung: Seit der Einführung sind – so berichtete der Regierungsrat[1]– praktisch keine Beschimpfungen und Bedrohungen mehr vorgekommen.

Beratung Der Datenschutzbeauftragte stand den beiden Verwaltungsstelle bei der Einführung dieser Aufzeichnungsmöglichkeit beratend zur Seite. Es wurden die Voraussetzungen für die Aufzeichnung festgelegt und vor allem das Verfahren nach der Aufzeichnung geregelt. Hiess es ursprünglich, die Aufzeichnung erfolge zu Schulungszwecken, so wird heute richtigerweise darauf hingewiesen, dass die Aufzeichnung aus Sicherheitsgründen erfolge. Vor der Verwendung muss amtsintern beurteilt werden, ob eine Straftat vorliegen könnte. Ausserdem kann eine interne Sensibilisierung oder Schulung erfolgen, wenn festgestellt werden sollte, dass die Mitarbeiterin oder der Mitarbeiten eine Eskalation hätte vermeiden können.

Breitere Anwendung? Inzwischen hat offenbar das respektlose oder gar strafbare Handeln gegenüber Verwaltungsmitarbeitenden stark zugenommen. Das ist auf jeden Fall aus dem Begehren oder Wunsch verschiedener Amtsstellen zu schliessen, auch eine solche Telefongesprächsaufzeichnung zu installieren, sie auszuweiten oder vermehrt Kundenschalterbereiche mit Videoanlagen zu überwachen.

Vorgehen bei Telefonaufzeichnungsanlagen

Verantwortung Die Verantwortung für die Durchführung solcher Massnahmen liegt bei der Dienststelle oder dem Departement. Betroffene Dienststellen haben aber im Vorfeld den Datenschutzbeauftragten zur Beratung beigezogen. Er verlangt zusätzliche Sachverhaltsabklärungen und eine bessere rechtliche Abstützung. Zu beachten ist, dass Art. 179bis StGB es verbietet, ein nichtöffentliches Gespräch ohne die Einwilligung der andern daran Beteiligten auf einen Tonträger aufzunehmen, und dass die Ausnahmen nach Art. 179^{quinquies} StGB nur die Aufnahme von Gesprächen mit Hilfs-, Rettungs- und Sicherheitsdiensten erlaubt sowie von Gesprächen im Geschäftsverkehr, welche Bestellungen, Aufträge, Reservationen und ähnliche Geschäftsvorfälle zum Inhalt haben.

Quantifizierung und Qualifizierung Der Datenschutzbeauftragte verlangt, dass der behauptete Sachverhalt, die starke Zunahme solcher Vorfälle, mit Zahlen untermauert wird. Es soll über eine längere Dauer eine Vorfallsliste geführt werden, in welcher die Vorfälle und die Massnahmen festgehalten und bewertet werden. Handelt es sich bei der Drohung wirklich um eine (strafrechtlich relevante) Drohung? Sind solche Drohungen häufiger geworden und/oder reagieren Mitarbeiterinnen und Mitarbeiter empfindlicher? Wie war ihre Reaktion: Haben sie deeskalierend gewirkt oder erst zur Eskalation beigetragen? Welche Massnahmen wurden ergriffen? Wurde das Verhalten der Mitarbeiterinnen und Mitarbeiter mit ihnen angeschaut und wurden Hinweise auf Deeskalationsmöglichkeiten gegeben? Haben Vorgesetzte eingegriffen und sich mit Zivilcourage mit den unangenehmen Kundinnen und Kunden auseinandergesetzt, herauszufinden versucht, was zu ihrem Wutausbruch geführt hat, und ihnen verständlich gemacht, dass Drohen nicht in Frage kommt (und auch nicht zu einer Verbesserung der Dienstleistung führt)?

Solche Überwachungsmassnahmen können spätestens dann, wenn sie verbreitet eingesetzt werden, den Eindruck eines veränderten Menschenbildes der Verwaltung vermitteln.

Bürger sind keine Störer Auch wenn das geschilderte Verfahren sicherstellen soll, dass nicht übermässig von der Aufzeichnung Gebrauch gemacht wird, gibt der Datenschutzbeauftragte zu bedenken, dass solche Überwachungsmassnahmen, die ja für die Kundinnen und Kunden zwingend transparent gemacht werden müssen[2], spätestens dann, wenn sie verbreitet eingesetzt werden, den Eindruck eines veränderten Menschenbildes der Verwaltung vermitteln können. Betrachtet die Verwaltung die Kundinnen und Kunden plötzlich generell als Störer? Das wäre ein Bild, das recht verstörend wirken würde – und heute zum Glück auch nicht zutrifft. Der Datenschutzbeauftragte regt deshalb an, eine entsprechende Rechtsgrundlage zu schaffen, wenn Telefongesprächsaufzeichnungen und Videoüberwachungen im Kundenschalterbereich verbreitet eingesetzt werden sollen – entweder durch den Regierungsrat auf Verordnungsebene, soweit ihm dazu die Kompetenz zukommt, oder durch den Gesetzgeber auf Gesetzesebene.

Weitere Geschäfte

Umgang mit Gefährdern Die Aufnahme von Telefongesprächen mit aggressiver Kundschaft – das ist natürlich nicht alles, was im Kanton Basel-Stadt im Zusammenhang mit (mehr oder weniger gefährlichen) Bedrohungen geschieht. Der Datenschutzbeauftragte war in verschiedene Geschäfte in diesem Kontext involviert. Er wurde unter anderem beigezogen im Zusammenhang:

— mit dem «Nationalen Aktionsplan zur Verhinderung und Bekämpfung von Radikalisierung und gewalttätigem Extremismus»[3],

— mit der Schaffung der interdepartemental zusammengesetzten Task-Force Radikalisierung sowie

— der Anlaufstelle Radikalisierung (und hier im Zusammenhang mit RA-PROF [Radicalisation Profiling], einer strukturierten Methode zur Einschätzung von möglichen Radikalisierungstendenzen),

— mit dem Ratschlag und Massnahmenplan 2018 Radikalisierung und Terrorismus[4] und

— mit dem Gesetzesentwurf zu einem neuen Bundesgesetz über polizeiliche Massnahmen zur Bekämpfung von Terrorismus (PMT)[5].

Projekt Kantonales Bedrohungsmanagement

Ein «altes» Thema Im letzten Jahr des Berichtszeitraumes wurde der Datenschutzbeauftragte zugezogen zu den Vorarbeiten für das Kantonale Bedrohungsmanagement (KBM). Er hatte bereits 2012 angeregt, ein Bedrohungsmanagement einzuführen[6]. Ausgangspunkt waren damals verschiedene Fälle, bei denen die Frage im Raum stand, ob eine Person, die Drohungen ausspricht, wirklich gefährlich ist oder nicht. Die daraufhin vom Justiz- und Sicherheitsdepartement beantragte Schaffung eines Bedrohungsmanagements kam aber nicht zustande. Erst etliche Jahre später wurde das Thema wieder aufgenommen. Inzwischen hat die Vernehmlassung zum Ratschlagsentwurf stattgefunden.

Herausforderungen Im Vordergrund steht für den Datenschutzbeauftragten die Formulierung von klaren Regeln, die sowohl für alle Beteiligten Rechtsicherheit bringen, und die Verhältnismässigkeit der vorgesehenen Massnahmen. Die Hauptherausforderungen sind die Umschreibung der «Gefährder», also der Personen, die im Rahmen des KBM erfasst werden sollen, und der Datenflüsse unter Behörden sowie von und/oder zu Dritten sowie die Angemessenheit der Aufbewahrungsdauer:

— Welche Personen sollen im KBM erfasst werden? Möglichst klare Kriterien sollten sicherstellen, dass solche (und nur solche) Personen erfasst werden, >

die Verwaltungsangestellte wirklich und mit einer gewissen Ernsthaftigkeit gefährden – also quasi eine Abgrenzung «nach unten» und «nach oben»: Auf der einen Seite muss die Verwaltung bloss «unangenehme» Kundinnen und Kunden hinnehmen; dafür muss sie durch Sensibilisierung und Schulung vorbereitet werden. Auf der anderen Seite sind für Straftäter und z.B. Terrorverdächtige andere Massnahmen erforderlich. Möglichst klare Kriterien sollen diese Unterscheidung ermöglichen – das ist aber zugegebenermassen nicht einfach.

Die Hauptherausforderungen sind die Umschreibung der «Gefährder», also der Personen, die im Rahmen des KBM erfasst werden sollen, und der Datenflüsse unter Behörden sowie von und/oder zu Dritten sowie die Angemessenheit der Aufbewahrungsdauer.

— Welche öffentlichen Organe (innerhalb und ausserhalb des Kantons Basel-Stadt) dürfen welche Informationen an KBM melden und dürfen oder müssen auf Anfrage von KBM Informationen über erfasste Personen bekannt geben? Welchen öffentlichen Organen darf KBM solche Informationen weitergeben? Der Kreis der Behörden soll nicht zu eng – weil sonst der Zweck nicht erreicht werden kann –, aber auch auf keinen Fall zu weit gefasst werden.

— Dürfen Dritten Informationen an KBM bekannt geben oder von ihm Informationen über erfasste Personen erhalten? Welche Dritten? Der Datenfluss von oder zu Dritten muss gerechtfertigt und streng begrenzt werden.

— Wie lange dürfen Personen im KBM erfasst bleiben? Wann müssen die Informationen gelöscht werden? Je offener der Kreis der erfassten Personen ist, umso kürzer muss die Aufbewahrungsdauer sein – und je länger die Aufbewahrungsfrist, umso besser muss sie begründet sein.

Fazit

Bedarf nach politischer Diskussion Das Bedrohungsmanagement wird sicher politisch diskutiert werden. Auch Überwachungsmassnahmen sollten politisch diskutiert werden, wenn durch ihren Einsatz der Eindruck entstehen kann, dass die Verwaltung die Bürgerinnen und Bürger grundsätzlich als Störer betrachtet. Auf der einen Seite muss der Staat als Arbeitgeber seine Verwaltungsmitarbeiterinnen und -mitarbeiter vor Angriffen schützen – auf der anderen Seite ist nicht jede Person, die mit dem, was Verwaltungsangestellte tun, nicht einverstanden ist und in einer bestimmten Situation mal laut wird, eine Gefährdung des Staats oder seiner Angestellten. Das richtige Mass macht's.

1 Antwort des Regierungsrates vom 4. März 2015 (14.5592.02) auf eine Schriftliche Anfrage.
2 § 15 IDG; vgl. dazu PK-IDG/BS-Husi, § 15 N 6 ff.
3 <https://www.ejpd.admin.ch/dam/data/ejpd/aktuell/news/2017/2017-12-04/171204-nap-d.pdf>.
4 Ratschlag und Massnahmenplan 2018 Radikalisierung und Terrorismus (18.0151.01) vom 11. April 2018.
5 Inzwischen hat der Bundesrat die Botschaft vom 22. Mai 2019 zu einem Bundesgesetz an die Bundesversammlung überwiesen: BBl 2019 4751 (<https://www.admin.ch/opc/de/federal-gazette/2019/4851.pdf>).
6 Aufgrund diverser Fragestellungen hat der Datenschutzbeauftragte 2012 festgestellt, dass der sehr allgemein gehaltene polizeiliche Auftrag zur Aufrechterhaltung der öffentlichen Sicherheit und Ordnung nicht ausreicht, und angeregt, eine hinreichende gesetzliche Grundlage für ein kantonales Bedrohungsmanagement zu schaffen; vgl. dazu TB 2012 des DSB/BS, S. 22.

Trend 4 Europäische Datenschutzreformen und das IDG

Die Europäische Union und der Europarat haben ihr Datenschutzrecht modernisiert. Was heisst das für den Kanton Basel-Stadt? Einerseits ist das baselstädtische Informations- und Datenschutzgesetz den neuen Anforderungen anzupassen, und andererseits stellt sich die Frage, ob Datenbearbeitungen durch baselstädtische öffentliche Organe aufgrund der extraterritorialen Geltung der EU-Datenschutz-Grundverordnung plötzlich dieser (zum Teil strengeren) EU-Datenschutzgesetzgebung unterstehen.

Revision des IDG

Anpassung an die internationalen Vorgaben Das IDG muss an die neuen internationalrechtlichen Anforderungen angepasst werden. Diese kommen insbesondere aus der modernisierten Europaratskonvention 108 und – im Schengen-Kontext – aus der EU-Richtlinie 2016/680.

Europarats-Konvention 108+ Der Europarat hat seine Konvention 108[1] von 1981 modernisiert und den neuen Herausforderungen angepasst. Der Bundesrat hat den Eidgenössischen Räten 2019 beantragt, die modernisierte Konvention 108 (genannt: Konvention 108+) zu ratifizieren[2]. Sobald sie ratifiziert ist, gilt sie – wie seit 1998 die Vorgängerversion – auch für die Kantone. Inzwischen haben am 19. Juni 2020 beide Räte dem Bundesbeschluss über die Genehmigung des Protokolls vom 10. Oktober 2018 zur Änderung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten zugestimmt[3]. Die Referendumsfrist läuft noch bis zum 8. Oktober 2020[4].

Richtlinie (EU) 2016/680 Mit der Schengen-Assoziierung der Schweiz im Jahre 2008 wurden die Datenschutz-Richtlinie 95/46/EG und etwas später der Rahmenbeschluss 2008/977/JI für die Schweiz verbindlich. Mit der grossen Datenschutzreform, welche die EU im Jahr 2016 abgeschlossen hat und die am 25. Mai 2018 in Kraft getreten ist, wurde die Richtlinie (EU) 2016/680[5] erlassen, die den Rahmenbeschluss ablöst. Sie ist Schengen-relevant und muss deshalb von der Schweiz innert zweier Jahre, nachdem die EU-Kommission der Schweiz dies mitteilt, im schweizerischen Recht umgesetzt werden. Diese «Notifikation» ist am 1. August 2016 erfolgt – eine Umsetzung durch den Bund und die Kantone hätte also bis 1. August 2018 erfolgen müssen.

Leitfaden der KdK Die Konferenz der Kantonsregierungen hat durch die Arbeitsgruppe Datenschutz der Begleitorganisation Schengen/Dublin (BOSD) einen Leitfaden[6] für die Umsetzung erstellen lassen und anfangs Februar 2017 den Kantonen zugestellt. Dabei zeigt sich, dass der Anpassungsbedarf in unserem Kanton – im Vergleich zu anderen Kantonen – geringer ist, u.a. weil Basel-Stadt bereits ein modernes Gesetz besitzt (und der Leitfaden etliche Formulierungen aus dem IDG als Musterformulierungen vorschlägt). Innert der Frist hat der Kanton Aargau als einziger Kanton sein Gesetz anpassen können[7]. Auch der Bund schaffte es nicht, innert Frist sein Gesetz anzupassen. Weil politisch keine Einigung zum bundesrätlichen Entwurf für eine Totalrevision zustande kam[8], hat der Bund ein «Schengen-Datenschutzgesetz»[9] erlassen und per 1. März 2019 in Kraft treten lassen, das so lange gelten soll, bis die DSG-Totalrevision in Kraft treten kann.

Entwurf Der Datenschutzbeauftragte hat einen Entwurf für eine Teilrevision des IDG am 16. Januar 2019 an den Rechtsdienst der Staatskanzlei abgeliefert. Anschliessend sollte die (vorerst interne) Vernehmlassung durchgeführt werden. Offensichtlich aufgrund zu knapper juristischer Ressourcen bei der Staatskanzlei konnte das Geschäft 2019 aber nicht weiterbearbeitet werden.

Zeitplan Mehrfach wurde der Zeitplan revidiert. Nachdem die Vernehmlassung ursprünglich im Frühjahr 2019 vorgesehen war, wurde sie auf Herbst 2019 verschoben. Dieser Zeitplan konnte aber nicht eingehalten werden. Mitte Januar 2020 kam eine erste Rückmeldung zum Entwurf. Dieser wurde u.a. in einer längeren Besprechung und mit verschiedenen Mailwechseln und Telefongesprächen mit dem zuständigen Juristen in der Staatskanzlei bereinigt. Die überarbeitete Version ging dann Ende Februar 2020 wieder zurück an die Staatskanzlei. Wie inzwischen ersichtlich, hat die Vernehmlassung auch im ersten Halbjahr 2020 nicht stattgefunden. >

Auswirkungen Die Staatskanzlei liess im Oktober 2019 beim Datenschutzbeauftragten abklären, ob die Verschiebung negative (rechtliche oder politische) Konsequenzen habe. Die Nichteinhaltung der «Schengen-First» (1. August 2018) hat unmittelbar keine Konsequenzen. Im selben Jahr – bereits im Frühjahr – hatte eine Schengen-Evaluation stattgefunden. Da konnte logischerweise noch nicht kontrolliert werden, ob die neuen Datenschutzanforderungen ein Vierteljahr später umgesetzt sein würden. Eine nächste Schengen-Evaluation wird voraussichtlich erst ca. 2022/2023 stattfinden. Da die Europarats-Konvention 108+ vom Bund noch nicht ratifiziert ist, hat auch diesbezüglich die Verspätung keine unmittelbaren Konsequenzen. Ohnehin sieht die Konvention kein Konventions-Durchsetzungsverfahren vor, das direkt rechtliche Konsequenzen nach sich zieht. Dass der Rückstand von Basel-Stadt Auswirkungen auf den Angemessenheitsbeschluss der EU-Kommission – ursprünglich vorgesehen für Mai 2020, inzwischen verschoben auf Oktober 2020 – hat, ist nicht anzunehmen. Hier wird das Hauptaugenmerk wohl eher auf das Bundesdatenschutzgesetz gelegt. Mit anderen Worten: Man kann das Geschäft weiterhin aufschieben, ohne dass deshalb direkt rechtliche Konsequenzen drohen. Politisch sieht es etwas anders aus: Für einen Kanton, der bisher in Sachen Datenschutz hoch angesehen war, erscheint die mehrfache Verschiebung eher schwierig, um nicht zu sagen: peinlich. Dass Kantone mit einem grossen «Gap» zwischen Sein und Sollen bei den Regulierungen Mühe bekunden, ihre internationalrechtlichen Verpflichtungen innert vernünftiger Zeit umzusetzen, ist allenfalls nachvollziehbar, nicht aber bei einem Kanton mit nicht allzu grossem Anpassungsbedarf.

Anwendbarkeit der DSGVO

Angemessenheitsbeschluss Am 25. Mai 2018 trat – zeitgleich mit der oben erwähnten Schengen-relevanten Richtlinie (EU) 2016/680 – die EU-Datenschutz-Grundverordnung 2016/679 (DSGVO)[10] in Kraft. Sie löste die Richtlinie 95/46/EG ab und gilt weltweit inzwischen als Datenschutzstandard. Die DSGVO ist für die Schweiz als Nicht-EU-Mitgliedsland grundsätzlich nicht verbindlich – aber auch nicht ganz unbeachtlich: Die EU-Kommission muss – wie in den Ausführungen zu den Auswirkungen der verspäteten IDG-Revision bereits erwähnt – nach Art. 45 DSGVO beschliessen, ob ein Drittland (wie die Schweiz) ein angemessenes Datenschutzniveau bietet[11]; nur dann ist eine Datenübermittlung in dieses Drittland ohne Weiteres zulässig.

Extraterritoriale Anwendbarkeit Allerdings beansprucht die DSGVO auch eine gewisse extraterritoriale Geltung. Es gibt drei Bereiche, in denen die EU-Datenschutzgesetzgebung für Behörden und Unternehmen in der Schweiz anwendbar ist:

— wenn die Behörde oder das Unternehmen über eine Niederlassung in der EU verfügt , oder

— wenn eine Behörde oder ein Unternehmen in der Schweiz Personen in der EU Waren oder Dienstleistungen anbietet[13] oder

— wenn Personen, die sich in der EU befinden, beim Besuch der Internetseite einer Behörde oder eines Unternehmens in der Schweiz mittels Analyse-Tools beobachtet werden (Verhaltenstracking)[14].

Plötzliche Hektik Nachdem die EU-Datenschutzreform auch in den Schweizer Medien schon lange thematisiert wurde, entstand bei öffentlichen Organen im Kanton Basel-Stadt plötzlich Hektik: Müssen sie jetzt auch das EU-Datenschutzrecht einhalten? Und riskieren die Verantwortlichen plötzlich Millionenbussen, wenn sie gegen EU-Datenschutzrecht verstossen?

Dass Kantone mit einem grossen «Gap» zwischen Sein und Sollen bei den Regulierungen Mühe bekunden, ihre internationalrechtlichen Verpflichtungen innert vernünftiger Zeit umzusetzen, ist allenfalls nachvollziehbar, nicht aber bei einem Kanton mit nicht allzu grossem Anpassungsbedarf.

Merkblatt des Datenschutzbeauftragten Der Datenschutzbeauftragte hat daraufhin ein Merkblatt zur Anwendbarkeit der EU-Datenschutzgesetzgebung auf baselstädtische Behörden verfasst und auf seiner Website veröffentlicht[15]. Nur ausnahmsweise dürfte die DSGVO zur Anwendung gelangen, wie die auf derselben Seite veröffentlichten Anwendungsbeispiele zeigen:

— Eine Gefahr besteht vor allem, wenn Internetseiten Tracking betreiben (z.B. mittels Google Analytics, Cookies); allerdings ist festzuhalten, dass der Datenschutzbeauftragte des Kantons Basel-Stadt schon vor geraumer Zeit darauf aufmerksam gemacht hat, dass es für einen (über die IP-Adresse identifizierenden) Einsatz von Tracking- oder Profiling-Tools (z.B. Google Analytics) durch öffentliche Organe im Kanton Basel-Stadt schon nach schweizerischem Recht keine gesetzliche Grundlage gibt.

— Nur allein, dass sich Eintrittskarten für staatliche oder staatlich subventionierte Museen über das Internet beziehen lassen, bringt noch keine Geltung der DSGVO. Anders, wenn eine solche Dienstleistung (gezielt) Personen, die sich in der EU befinden, ange-

boten wird: Hier kommt es auf die Ausgestaltung der jeweiligen Website an. Wenn zum Beispiel das Kunstmuseum Basel auf seiner Website[16] die Ticket-Preise auch in Euro angibt, eine Anfahrtsbeschreibung aus Deutschland enthält und beim Online-Kauf das Land des Käufers angegeben werden muss, sind dies einige Indizien dafür, dass sich das Angebot auch an Personen richtet, die sich in der EU aufhalten.

— Dass Amtsstellen eine Niederlassung im EU-Ausland betreiben, dürfte kaum der Fall sein – möglich ist dies hingegen eher bei (wie es im EU-Recht heisst) «Einrichtungen und sonstigen Stellen», also beispielsweise bei Privaten, die über kantonale oder kommunale Leistungsaufträge verfügen und insoweit zu einem öffentlichen Organ werden (wie z.B. Listenspitäler). Solche Stellen sollten daher prüfen, ob sie über entsprechende Niederlassungen im grenznahen Ausland verfügen. Falls ja, würden diese Niederlassungen der EU-Datenschutzgesetzgebung unterstehen (und zwar auch, wenn die Personendaten nicht im EU-Ausland, sondern im «Mutterhaus» in der Schweiz bearbeitet werden).

— Wenn ein öffentliches Organ eine Auftragsdatenbearbeiterin im EU-Ausland beizieht, untersteht zwar diese dem EU-Datenschutzrecht[17], das auftraggebende öffentliche Organ aber ebenso wenig wie wenn es Bewerbungsunterlagen von Personen aus EU-Mitgliedstaaten entgegennimmt.

— Bewirbt die Universität einen Summer Course in International Relations spezifisch an Universitäten in Deutschland und Österreich, dann stellt dies ein Anbieten von Waren/Dienstleistungen gezielt an Personen dar, die sich in der EU befinden. Bietet sie aber Studierenden einen Masterlehrgang online an, bei dem genügende Deutsch- und Englischkenntnisse und ein Bachelor-Abschluss – gleichermassen für Studierende aus der Schweiz, aus EU-Staaten oder Drittstaaten – Voraussetzung sind und bei dem die Studiengebühren in Schweizer Franken zu bezahlen sind, dann richtet sich das Angebot nicht gezielt an Studierende aus der EU.

Fazit

Reformbedarf auf Bundesebene Europa hat einen Schritt in die Zukunft getan – ohne dass deshalb alle Datenschutzprobleme gelöst wären. Die Schweiz tut sich auf Bundesebene (immer noch) schwer damit, diesen Schritt ebenfalls zu tun. Nötig wäre er, denn erstens hat der Bundesrat aufgrund einer Evaluation des DSG festgestellt, dass der Datenschutz gestärkt werden müsse. Zweitens verlangen internationale Verpflichtungen eine Anpassung des Schweizer Datenschutzrechts an die neuen Anforderungen, einerseits an jene aus der Europarats-Konvention 108+, die von der Schweiz ratifiziert werden soll, andererseits aus der Richtlinie (EU) 2016/680, die für die Schweiz aufgrund der Schengen-Assoziierung gilt. Drittens wird die EU-Kommission das Schweizer Datenschutzniveau ohne Anpassungen das DSG kaum mehr als angemessen beurteilen, womit die Datenübermittlung aus EU-Staaten in die Schweiz nicht mehr ohne Weiteres zulässig wäre.

Reformbedarf auf Kantonsebene Auf kantonaler Ebene muss das IDG aus den gleichen Gründen an die neuen Anforderungen angepasst werden.

1 Übereinkommen (des Europarates) zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, abgeschlossen in Strassburg am 28. Januar 1981, SR 0.235.1. Für die Schweiz ist die ER-Konv 108 am 1. Februar 1998 in Kraft getreten.
2 Botschaft vom 6. Dezember 2019 zur Genehmigung des Protokolls vom 10. Oktober 2018 zur Änderung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, BBl 2020 565.
3 Geschäft 19.068: Nationalrat: AB 2020 N 1183 (143 Ja gegen 6 Nein bei 49 Enthaltungen); Ständerat: AB 2020 S 629 (einstimmig bei 2 Enthaltungen).
4 BBl 2020 5725.
5 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. L 119, 4.5.2016, S. 89–131.
6 Leitfaden der Konferenz der Kantonsregierungen: EU-Datenschutzreform/Modernisierung der Europarats-Konvention 108: Anpassungsbedarf bei den kantonalen (Informations- und) Datenschutzgesetzen, Bern, 2. Februar 2017, Link auf der Seite: <https://www.dsb.bs.ch/datenschutz/privatim-und-kdk-leitfaden.html> (Kurz-URL des PDF-Files: <https://bit.ly/2k5iHGz>).
7 Vgl. dazu Beat Rudin, Datenschutzreform in der Schweiz, digma 2018, S. 194 ff., insb. S. 198 ff. Im Kanton Bern hat der Regierungsrat per 1. September 2018 eine Dringlichkeitsverordnung beschlossen; damit kann die Zeit bis zur Revision des Datenschutzgesetzes überbrückt werden. Seither haben auch die Kantone St. Gallen, Appenzell Innerrhoden und Zürich ihre (Informations- und) Datenschutzgesetze nachgeführt (Stand 1. Juli 2020).
8 A.a.O., insb. S.196 f.
9 Bundesgesetz vom 28. September 2018 über den Datenschutz im Rahmen der Anwendung des Schengen-Besitzstands in Strafsachen (Schengen-Datenschutzgesetz, SDSG), SR 235.3.
10 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. L 119, 4.5.2016, S. 1-88.
11 Das tut – vice versa – auch die Schweiz: Nach Art. 13 Abs. 1 E-DSG dürfen Personendaten ins Ausland bekannt gegeben werden, wenn der Bundesrat festgestellt hat, dass die Gesetzgebung des betreffenden Staates oder das internationale Organ einen angemessenen Schutz gewährleistet.
12 Art. 3 Abs. 1 DSGVO.
13 Art. 3 Abs. 2 lit. a DSGVO.
14 Art. 3 Abs. 2 lit. b DSGVO.
15 Link auf der Seite <https://www.dsb.bs.ch/handreichungen/merkblatt-eu-datenschutzrecht.html>.
16 <https://kunstmuseumbasel.ch/>.
17 Vgl. dazu auch TB 2017-2019 des DSB/BS, S.12 ff. im Zusammenhang mit Cloud Computing.

Jahresrückblick

2017–2019:
Kurzer Blick auf die wichtigsten Geschäfte

Statistik

Jahresrückblick

2017–2019: Kurzer Blick auf die wichtigsten Geschäfte

Die gesetzliche Aufgabe des Datenschutzbeauftragten besteht vor allem in der Beratung und Kontrolle der öffentlichen Organe, die dem Informations- und Datenschutzgesetz unterstehen. Was waren die wichtigsten Beratungs- und Kontroll-Geschäfte? Warum ist die Vorabkontrolle ein Sorgenkind? Wie steht es um die Verantwortung und IT-Governance? Was tat der Datenschutzbeauftragte im Zusammenhang mit Pilotversuchen? Und was sagt die Statistik über Geschäftsfälle und personelle Ressourcen?

Beratungstätigkeit

Querschnittsthema Die Beratungstätigkeit, die über drei Viertel der Ressourcen des Datenschutzbeauftragten bindet, hat auch in den vergangenen drei Jahren die gesamte Breite der Staatsverwaltung erfasst. Ausgewählte Bereiche sind vorne im Kapitel «Trends» (S. 8 ff.), einzelne Fragestellungen hinten im Kapitel «Fälle» (S. 38 ff.) dargestellt. Nur exemplarisch seien hier weitere Themen erwähnt:

— *Stellungnahmen in Rechtsetzungsverfahren* sowohl auf kantonaler wie auch (zum Teil im Rahmen von privatim, der Konferenz der schweizerischen Datenschutzbeauftragten) auf Bundesebene, so u.a. zu den Entwürfen zu einem Adressdienstegesetz, zu einem Bundesgesetz über anerkannte elektronische Identifizierungsdienste (E-ID-Gesetz), zu Änderungen des AHV-Gesetzes (systematische Verwendung der AHV-Nummer als Personenidentifikator durch Behörden), des DNA-Profil-Gesetzes, des Transplantationsgesetzes, zum Staatsvertrag beider Basel über die Universitätsspital Nordwest AG, zu interkantonalen Regelungen zur Harmonisierung der Polizeitechnik und -informatik bzw. über den Datenaustausch zum Betrieb von Lage- und Analysesystemen im Bereich der seriellen Kriminalität («PICAR»[1]) und zu mehreren Schengen-Weiterentwicklungen u.a.m.

— *Vorabkontrollen bei Vorhaben*, die aufgrund der Art der Bearbeitung oder der zu bearbeitenden Daten geeignet ist, besondere Risiken für die Rechte und Freiheit der betroffenen Personen mit sich zu bringen (dazu auch unten S. 31), so etwa in unterschiedlichen Phasen beim Kundenportal der IWB, bei der Fallführungssoftware citysoftnet (Ablösung Tutoris bei der Sozialhilfe), im Projekt eSteuern, zum Berechtigungskonzept bei der Geschäftsverwaltungssoftware der Gemeinde Riehen usw.

— *Vorabkontrollen* bei Einrichtung, Ausweitung oder Verlängerung von *Videoüberwachungen*, so u.a. bei Museen, in den Betriebsräumlichkeiten der Zentralen Informatikdienste (ZID), bei der Berufsfeuerwehr, beim Gesundheitsdepartement, im Universitätsspital oder am Strafgericht.

— Stellungnahmen im Zusammenhang mit dem *Recht auf Zugang zu den eigenen Personendaten und mit dem allgemeinen Informationszugangsrecht* (Öffentlichkeitsprinzip), zum Beispiel bezüglich der Kommunikation zu Untersuchungsberichten über Fälle von Verletzungen der sexuellen Integrität, im Zusammenhang mit Mitarbeitendenbefragungen und diversen Anfragen von Medienschaffenden.

— Beratungen im Zusammenhang mit Meldungen von Datenschutzverletzungen (noch nicht gestützt auf die neu zu schaffende Meldepflicht[2], sondern auf den Grundsatz von Treu und Glauben).

— Abklärungen im Zusammenhang mit konkreten Vorfällen, so etwa beim Online-Bussenschalter, bei welchem ein Journalist Tausende von Datensätzen mit Personendaten von Ordnungsbussen-Empfängerinnen und -Empfängern herunterladen konnte.

Onlinezugriffs-Gesuche Im Rahmen der Beratungstätigkeit nimmt auch die Vorabkontrolle von Onlinezugriffs-Gesuchen einen breiten Raum ein. Was im Bund und in vielen Kantonen unter E-Government-Aspekten erst diskutiert wird, besteht in Basel-Stadt seit langem: Im Datenmarkt werden den öffentlichen Organen Personen- und Sachdaten, die von mehr als einem öffentlichen Organ zur Erfüllung seiner gesetzlichen Aufgaben benötigt werden, tagesaktuell auf einer zentralen Plattform zur Verfügung gestellt[3]. Nun darf sich ein anderes öffentliches Organ natürlich nicht einfach bei einem Datenbestand eines anderen öffentlichen Organs «bedienen»: Datenbezüge im Abrufverfahren (zum Beispiel durch einen Onlinezugriff oder via Webservice) bedürfen einer generellen Autorisierung durch die Dateneignerin[4]. Die Autorisierungen sind dem Datenschutzbeauftragten zur

Vorabkontrolle vorzulegen[5]. Für die Abwicklung dieser Gesuche betreiben die Zentralen Informatikdienste (ZID) ein Onlinesystem (AWS, «Autorisierungs-Workflow-System»). Der Datenschutzbeauftragte hat die (positiven) Beurteilungen der Dateneignerinnen zu überprüfen, bevor die Zugriffsmöglichkeit freigeschaltet wird. Diese Vorabkontrolle ist recht aufwändig, da in den Gesuchen oft die Rechtsgrundlagen nicht vollständig oder nicht korrekt angegeben werden. Dadurch dauert die Gesuchsabwicklung öfters übermässig lang. Das Verfahren könnte spürbar beschleunigt werden, wenn erstens die Rechtsdienste der gesuchsstellenden öffentlichen Organe in die Gesuchsbegründung einbezogen würden und zweitens die Information über die im Datenmarkt verfügbaren Informationen verbessert werden könnte.

Wenn der Zugriff nicht wirksam eingeschränkt werden kann, muss wenigstens eine Möglichkeit bestehen, die getätigten Zugriffe nachträglich stichprobenweise zu kontrollieren.

Unverhältnismässigkeit bei Onlinezugriffen Die Zugriffsberechtigung kann durch Filter und Masken eingeschränkt werden. Wenn ein öffentliches Organ zur Erfüllung seiner gesetzlichen Aufgabe nur die Daten von über 65-jährigen Personen benötigt, kann mit einem *Filter* (Alter > 65 Jahre) der Zugriff auf die entsprechenden Personen begrenzt werden. Wenn von Personen nur Namen, Geburtsdatum und Meldeadresse benötigt werden, dann kann mit einer *Maske* dafür gesorgt werden, dass auch nur genau diese Attribute (und nicht noch die Steuerdaten, die Information, dass jemand Krankenkassen-Prämienverbilligung bezieht usw.) angezeigt werden. Falls aber das für die Zugriffssteuerung nötige Attribut (zum Beispiel: «ist Klient der Bewährungshilfe») im Datenmarkt gar nicht vorhanden ist, dann hat das datenbeziehende öffentliche Organ unter Umständen Zugriff auf Daten von zu vielen Personen. In einem solchen Fall müsste die Einräumung der Onlinezugriffsmöglichkeit als unverhältnismässig beurteilt und von der Dateneignerin verweigert werden. Als Beispiel: Eine Amtsstelle soll vor der Bewährungsentlassung von Strafgefangenen mit deren näherem Umfeld (Partnerinnen und Partnern, Verwandten und Arbeitgeberinnen) Kontakt aufnehmen können. Das betrifft jährlich rund 100 Personen. Weil eine Begrenzung durch einen Filter nicht möglich ist, kann die Amtsstelle auf Daten von rund 940'000 Personen zugreifen: auf Daten der in Basel-Stadt angemeldeten natürlichen Personen, der hier ansässigen juristischen Personen und der «Zugehörigen» (Grenzgängerinnen und Grenzgänger, ausserkantonal wohnhafte Grundeigentümerinnen und Grundeigentümer usw.).

Logfile-Kontrollen Wenn der Zugriff nicht wirksam eingeschränkt werden kann, muss wenigstens eine Möglichkeit bestehen, die getätigten Zugriffe nachträglich stichprobenweise zu kontrollieren. Der Datenschutzbeauftragte verlangt seit längerem, dass eine Logfile-Kontrollmöglichkeit programmiert wird. Er wird beginnen, in seinen Stellungnahmen den Dateneignerinnen, die ja für die Rechtmässigkeit und Verhältnismässigkeit der Datenbekanntgabe die Verantwortung tragen, zu empfehlen, die Autorisierungen zum Beispiel auf ein Jahr zu befristen, solange die Logfile-Kontrolle nicht möglich ist. Entweder wird der Druck, dass diese Programmierung endlich erfolgt, grösser – oder es zeigt sich vielleicht sogar im Laufe dieses Jahres, dass die Aufgabenerfüllung auch ohne die Daten oder mit weniger Daten möglich ist.

Pilotversuche

Übersicht § 9a IDG erlaubt es, unter engen Voraussetzungen und zeitlich befristet im Rahmen von Pilotversuchen besondere Personendaten zu bearbeiten, ohne dass die nach § 9 Abs. 2 IDG erforderliche formellgesetzliche Grundlage besteht[6]. In den Jahren 2017–2019 liefen zwei Pilotversuche: der eHealth-Modellversuch Basel und der Pilotversuch Erweiterte Gefährderansprache. Beide Pilotversuche wurden 2019 beendet.

eHealth-Modellversuch Basel Bei diesem Modellversuch ging es darum, eine Stammgemeinschaft im Sinne des Bundesgesetzes zum elektronischen Patientendossier (EPDG)[7] aufzubauen und die Machbarkeit einer funktionsfähigen und datenschutzkonformen Umsetzung der bundesrechtlichen Vorgaben zu beweisen. Nach umfangreichen Vorbereitungen konnte im August 2018 mit der Eröffnung der ersten elektronischen Patientendossiers begonnen werden. Der Datenschutzbeauftragte hat den Modellversuch begleitet und stand dem myEPD-Datenschutz- und Datensicherheits-Board beratend zur Verfügung. Nachdem der Trägerverein eHealth Nordwestschweiz im Frühjahr 2019 beschlossen hat, sich mit der axsana/

>

XAD zu einer Gemeinschaft zusammenzuschliessen, wurde der dreijährige Modellversuch Mitte 2019 abgeschlossen. Beim Abschlussprozess wurde der Datenschutzbeauftragte vom verantwortlichen Gesundheitsdepartement aktiv beigezogen. Den myEPD-Dossierinhaberinnen und -inhabern wurde angeboten, die in ihrem Dossier enthaltenen Dokumente herunterzuladen. Eine Überführung in die neue Stammgemeinschaft war aus technischen Gründen nicht möglich.

Pilotversuch Erweiterte Gefährderansprache Mit diesem Pilotversuch sollte gestützt auf eine am 1. Januar 2016 in Kraft getretene Verordnung über die Meldung von gefährdenden Personen im Rahmen eines Pilotversuchs («Erweiterte Gefährderansprache») aufgezeigt werden, ob durch die Erweiterung des Kreises der zu meldenden gefährdenden Personen an die Beratungsstelle mehr solche Personen angesprochen und zur Teilnahme an geeigneten Massnahmen motiviert werden können, als wenn nur, wie damals im Polizeigesetz vorgesehen, Gefährderinnen und Gefährder angesprochen werden, gegenüber denen eine Wegweisung ausgesprochen worden ist. Im Jahr 2017 – der Regierungsrat hatte Ende 2016 die Geltung der Pilotversuchsverordnung verlängert – wurde der Datenschutzbeauftragte beigezogen zur Vorbereitung der Revision des Polizeigesetzes, mit welcher die erweiterte Gefährderansprache ins Gesetz überführt werden soll. Mit Beschluss vom 13. Februar 2019 hat der Grosse Rat die §§ 37a–37g PolG revidiert. Mit dem Inkrafttreten dieser Bestimmungen per 1. Januar 2020 konnte der Pilotversuch in den Regelbetrieb überführt werden.

Kontrolltätigkeit

Übersicht Nach § 44 lit. a IDG kontrolliert der Datenschutzbeauftragte nach einem autonom aufzustellenden Prüfprogramm die Anwendung der Bestimmungen über den Umgang mit Informationen. Die Prüfungen konzentrieren sich im Bereich des gewählten Prüfumfangs auf rechtliche und Informationssicherheitsaspekte. Bei allen Prüfungen haben die geprüften Stellen offen und transparent mitgewirkt. Die Feststellungen und Empfehlungen wurden mit ihnen besprochen. Die Audits vermögen der geprüften Stelle keinen vollständigen Nachweis über ihre Datenschutz-Compliance zu geben. Die Berichte, welche die oder der Datenschutzbeauftragte im Rahmen der Kontrolltätigkeit erstellt, und die ihnen zugrunde liegenden Materialien sind nicht öffentlich zugänglich im Sinne von § 25 Abs. 1 IDG[8]. Hier wird im Sinne der Transparenz kurz auf die wichtigsten Feststellungen (i.d.R. hohe und mittlere Priorität) hingewiesen.

Kontrolltätigkeit 2017

Abgeschlossene Prüfungen Der Datenschutzbeauftragte hat 2017 vier Datenschutzprüfungen abgeschlossen. Kontrolliert wurden Bereiche bei den Volksschulen (Sekundarstufe), bei der Steuerverwaltung, beim Universitätsspital sowie bei den Basler Verkehrs-Betrieben.

Volksschulen Bei dieser Prüfung wurden Aspekte des Datenschutzes und der Informationssicherheit in zwei Schulhäusern der Sekundarschule unter die Lupe genommen. Geprüft wurden jeweils die Verantwortlichkeiten und konzeptionellen Vorgaben, der generelle Umgang mit Informationen, der Zugang zu den eigenen Personendaten und das Löschen und Vernichten von Personendaten. Die wichtigsten Feststellungen betrafen die Festlegung von Verantwortlichkeiten, die Ermittlung des Schutzbedarfs und das Risikomanagement, Vorgaben zur Umsetzung des Zugangs zu den eigenen Personendaten und zum Umgang mit privaten IT-Mitteln sowie Weisungen/Konzepte betreffend Aufbewahrung, Archivierung und Vernichtung von Informationen.

Beim Abschlussprozess des nach drei Jahren abgebrochenen eHealth-Modellversuchs Basel wurde der Datenschutzbeauftragte vom verantwortlichen Gesundheitsdepartement aktiv beigezogen.

Steuerverwaltung Bei der Steuerverwaltung wurde eine Prüfung mit dem Fokus auf Verantwortlichkeiten und konzeptionelle Vorgaben, Berechtigungen, den Prozess Akteneinsicht (inkl. Zugang zu den eigenen Personendaten) und das Löschen und Vernichten von Personendaten durchgeführt. Die wichtigsten Feststellungen betrafen Grundlagen für ein Informationssicherheits-Managementsystem (ISMS), die Überwachung von IT-Leistungen, Schutzbedarf und Risikomanagement, Berechtigungen sowie die Archivierung und Vernichtung von Daten.

Universitätsspital Dieselben Prüfpunkte wurden auch im Rahmen des Audits beim USB untersucht. Hier zeigte sich ein Spannungsfeld zwischen den Interessen des Datenschutzes und der Patientensicherheit, das auch spitalintern intensiv diskutiert wird. Die wichtigsten Feststellungen betrafen die Verantwortung für die Informationssicherheit, den Erlass und die

Durchsetzung von Weisungen, Richtlinien und Abläufen, das Informationssicherheits-Managementsystem (ISMS) und das Risikomanagement, Differenzierungen im Berechtigungssystem sowie die Archivierung und Vernichtung von Daten.

BVB Die Prüfung bei den Basler Verkehrs-Betrieben war eine Prüfung aus besonderem Anlass. Ein Medienbericht hatte suggeriert, eine auf forensische Untersuchungen spezialisierte Firma hätte im Auftrag des BVB-Verwaltungsratspräsidenten E-Mail- und/oder Telefon-Daten ausgewertet. Deshalb hatte der Datenschutzbeauftragte eine Untersuchung im Sinne von § 45 IDG eingeleitet. Er hat untersucht, ob die BVB aus datenschutzrechtlicher Sicht die Durchführung einer Administrativuntersuchung an eine externe Firma auslagern durften und ob dabei sichergestellt war, dass die externe Firma die Informationen nur so bearbeitet, wie das die BVB auch tun dürften[9]. Die Untersuchung hat keinerlei Anhaltspunkte für den durch die Medienberichte entstandenen Verdacht ergeben, dass von den BVB im Zusammenhang mit der Administrativuntersuchung wegen des Verdachts auf unkorrekten Umgang mit vertraulichen Informationen E-Mail- und/oder Telefondaten ausgewertet oder der externen Firma ausgehändigt worden sind. Für die künftige Vertragsgestaltung hat der Datenschutzbeauftragte kleinere Verbesserungen vorgeschlagen. Über das Resultat der Abklärungen wurde auch die Geschäftsprüfungskommission des Grossen Rates informiert.

Kontrolltätigkeit 2018

Abgeschlossene Prüfungen Wie bereits im Jahresbericht 2018 des Regierungsrates erwähnt[10], konnten wegen der Vakanz beim IT-Personal nur wenige Audits durchgeführt werden[11]. Der Datenschutzbeauftragte hat 2018 zwei Datenschutzprüfungen abgeschlossen[12]. Kontrolliert wurden die Nutzung des Schengener Informationssystems (SIS) durch die Staatsanwaltschaft und die Nutzung des Visa-Informationssystems (VIS) durch das Migrationsamt.

SIS-Prüfung Staatsanwaltschaft Bei der Staatsanwaltschaft Basel-Stadt wurde die Nutzung des Schengener Informationssystems (SIS)[13] und der nationalen polizeilichen Informationssysteme (RIPOL usw.) einem Audit unterzogen. Der Fokus der Prüfung lag auf der Einhaltung der rechtlichen Vorgaben bei der SIS-Nutzung einschliesslich der generellen Kenntnis datenschutzrechtlicher Vorgaben und Rahmenbedingungen für die Nutzung der nationalen polizeilichen Informationssysteme. Geprüft wurden zudem anhand von Logdateien des fedpol stichprobenweise die Berechtigungen konkreter Datenbankabfragen. Die Feststellungen betrafen automatische Abfragen im SIS, die periodisch zu wiederholende Information der Mitarbeitenden zur SIS-Nutzung sowie die Möglichkeit, strengere kantonale Vorgaben einzuführen bezüglich des Einsatzes der Zugangskarte zum Single Sign On-Portal (des Bundes) und bezüglich der Passwörter.

Im Rahmen des Audits beim Universitätsspital Basel zeigte sich ein Spannungsfeld zwischen den Interessen des Datenschutzes und der Patientensicherheit, das auch spitalintern intensiv diskutiert wird.

VIS-Prüfung Migrationsamt Beim Migrationsamt wurde die Nutzung des Visa-Informationssystems (VIS)[14] durch die Mitarbeiterinnen und Mitarbeiter des Migrationsamtes geprüft. Schwergewichtig wurden die Abfragen geprüft – auch hier stichprobenmässig aufgrund von Logdateien des Staatssekretariats für Migration (SEM). Nach der Beurteilung des Datenschutzbeauftragten haben die kontrollierten Mitarbeiterinnen und Mitarbeiter das System ihren gesetzlichen Aufgaben entsprechend genutzt, weshalb sich eine Feststellung erübrigt hat.

Kontrolltätigkeit 2019

Abgeschlossene Prüfungen Im Jahr 2019 hat der Datenschutzbeauftragte vier Datenschutzprüfungen abgeschlossen, obwohl die Vakanz im IT-Bereich immer noch bestand. Jeweils mit externer Unterstützung wurden ein Bereich im Grundbuch- und Vermessungsamt sowie drei Bereiche in der Verwaltung der Gemeinde Riehen kontrolliert.

Grundbuch- und Vermessungsamt Im GVA wurde die Grundbuchapplikation «Capitastra» einem Audit unterzogen. Geprüft wurden die Einhaltung der gesetzlichen und regulatorischen Vorgaben bezüglich des Auskunftsportals, das Benutzer- und Berechtigungskonzept und die Auswertung nach auffälligen Abfragen. Die einzige Feststellung mit hoher Priorität betraf die Terminierung von Benutzerkonten. Sie soll innert nützlicher Frist in Zusammenarbeit mit den Kundinnen und Kunden des GVA durch entsprechende Massnahmen verbessert werden. Fünf weitere Feststellungen (rechtliche Vorgaben bezüglich der Rollenprofile, Schwachstellen bezüglich der Administration von Benutzerkonten, Konfiguration der Passworteinstellungen, punktuelle inadäquate Zugriffsberechtigungen, Auswertung der Protokolldateien nach Auffälligkeiten) waren von mittlerer Priorität. >

Riehen: Bereich Personal Bei diesem Audit wurden drei Geschäftsprozesse (Stellenausschreibung bis Abschluss des Bewerbungsverfahrens, Anstellung und bestehendes Arbeitsverhältnis bis zur Beendigung, abweichende Prozessschritte im Schulumfeld) und vier IT-Prozesse (Berechtigungskonzept, Benutzer-/Berechtigungsadministrationsprozess und Passworteinstellungen, kritische Berechtigungen, wesentliche elektronische Schnittstellen) geprüft. Unter rechtlichen Aspekten wurden einzig zwei Feststellungen von mittlerer Priorität (zu Auftragsdatenbearbeitungen sowie Aufbewahrung und Löschung) getroffen. Bezüglich der IT-Sicherheitsaspekte betraf die einzige Feststellung mit hoher Priorität Schwachstellen im Benutzeradministrationsprozess. Zwei weitere Feststellungen (Schwachstellen im Berechtigungsadministrationsprozess, Überwachung von externen Dienstleistern) waren von mittlerer Priorität.

Eine engere Zusammenarbeit besteht auch über die Kantonsgrenzen hinweg, insbesondere mit den Datenschutzbehörden der Kantone Basel-Landschaft, Zürich, Bern, Aargau und Zug.

Riehen: Bereich Sozialhilfe Bei diesem Audit wurden drei Geschäftsprozesse (Fallaufnahme: vom Erstkontakt bis zur Dossiereröffnung, Fallführung: von der Anspruchsprüfung bis zur Leistungsauszahlung, Fallabschluss: Aufbewahrung und Archivierung der Dossiers) und fünf IT-Prozesse (Berechtigungskonzept, Benutzer-/Berechtigungsadministrationsprozess und Passworteinstellungen, kritische Berechtigungen, Datensicherung/Datenwiederherstellung und Notfallplanung, wesentliche elektronische Schnittstellen) geprüft. Unter rechtlichen Aspekten wurden drei Feststellungen von mittlerer Priorität (zu Auftragsdatenbearbeitungen, Aufbewahrung/Löschung, Online-Zugriffen) getroffen. Bezüglich der IT-Sicherheitsaspekte betraf die einzige Feststellung von hoher Priorität wiederum Schwachstellen im Benutzeradministrationsprozess; zwei weitere Feststellungen (zu inadäquat eingeschränkten Benutzerkonten und obsoleten Berechtigungen sowie zu Schwachstellen bei der Datensicherung, der Datenwiederherstellung und Notfallplanung) waren bloss von mittlerer Priorität.

Riehen: Verstärkte Massnahmen Schulen Beim dritten Audit in der Verwaltung der Einwohnergemeinde Riehen wurden ein Geschäftsprozess (Erkennung des Unterstützungsbedarfs bis zur Genehmigung, Fortsetzung oder Ablehnung von verstärkten Massnahmen) und drei IT-Prozesse (Berechtigungskonzept, Benutzer-/Berechtigungsadministrationsprozess, ausgewählte kritische Berechtigungen, welche die erwähnten Geschäftsprozesse unterstützen) geprüft. Hier wurden einzig Feststellungen von mittlerer Priorität getroffen: drei in rechtlicher Hinsicht (Dokumentenversand per E-Mail, Dossieraufbewahrung, Umsetzung des Aufbewahrungs- und Löschkonzeptes) und eine bezüglich IT-Sicherheitsaspekten (Schwachstelle beim Berechtigungskonzept und bei der Administration ausgewählter Benutzerkonten).

Zusammenarbeit

privatim Die Zusammenarbeit unter Datenschutzbehörden hilft Ressourcen sparen. Der Datenschutzbeauftragte fungiert seit Juni 2016 als Präsident von privatim, der Konferenz der schweizerischen Datenschutzbeauftragten. Die Mitglieder des Datenschutz-Teams wirken aufgabenspezifisch mit in den verschiedenen Arbeitsgruppen von privatim (Sicherheit, Gesundheit, Digitale Verwaltung, ICT). Eine engere Zusammenarbeit besteht auch über die Kantonsgrenzen hinweg, insbesondere mit den Datenschutzbehörden der Kantone Basel-Landschaft, Zürich, Bern, Aargau und Zug.

Schengen Die zuständige Juristin hat in der Koordinationsgruppe Schengen der Datenschutzbeauftragten von Bund und Kantonen und in der Arbeitsgruppe Datenschutz der Begleitorganisation Schengen/Dublin der Konferenz der Kantonsregierungen mitgewirkt und u.a. die Schengen-Evaluation (SchEval) 2018 der Schweiz vorzubereiten mitgeholfen. Es war vorgesehen, dass die Expertinnen und Experten aus den Schengen-Staaten dabei neben Bundesstellen auch Polizei- und Datenschutzbehörden der Kantone Luzern und Basel-Stadt inspizieren. Aus Zeitgründen wurde auf die Inspektion in Basel-Stadt verzichtet. Die Juristin hat hingegen 2019 als Expertin an der Schengen-Evaluation von Polen teilgenommen.

International Der Datenschutzbeauftragte pflegt auch den Erfahrungsaustausch mit ausländischen Datenschutzbehörden. Einerseits stellen sich ab und zu Fragen über die Landesgrenze hinweg: Hier besteht eine gute Zusammenarbeit mit dem Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg. Auch mit anderen deutschen

Landesbeauftragten ergeben sich immer wieder Gelegenheiten zum Erfahrungsaustausch. Ausserdem hat der Datenschutzbeauftragte in allen drei Jahren an der International Conference of Data Protection and Privacy Commissioners (ICDPPC)[15] in Hongkong, Brüssel/Belgien und Tirana/Albanien teilgenommen.

Informationszugangsgesuche

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 für die Jahre 2017–2019 finden sich – über die gesamte Verwaltung zusammengefasst – im Statistikteil dieses Tätigkeitsberichts (S. 34). Nach Departement aufgeschlüsselt hat sie der Regierungsrat jeweils in seinem Jahresbericht veröffentlicht[16].

Mässiger Anstieg – «Einbruch» – stabil In den Berichtsjahren zeigt sich eine gewisse «Unruhe» bei den Informationszugangsgesuchen – und zwar in einer Art Zweijahresrhythmus. In der Vergangenheit gingen relativ wenig Gesuche ein (2014: 18 / 2015: 19). 2016 stieg die Zahl auf 33 (+74%) und war 2017 mit 37 Gesuchen nur leicht höher (+12%). 2018 erfolgte wieder ein «Einbruch» auf 23 Gesuche (-38%) – und diese Zahl blieb 2019 mit 24 Gesuchen wiederum stabil (+4%). Eine Interpretation der Entwicklung ist schwierig. 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.

Erledigung Der Anteil der ganz oder teilweise gutgeheissenen Gesuche fiel zu Beginn der Dreijahresberichtsperiode, im Jahr 2017, auf 46% (2016: 58%), stieg dann aber wieder an (2018: 61% / 2019: 67%). Der Anteil der ganz abgewiesenen Gesuche war anfangs noch hoch (2017: 43% / 2018: 39%), fiel dann aber im dritten Jahr deutlich (2019: 17%). Am Jahresende noch nicht rechtskräftig entschieden war 2017 über rund jedes neunte Gesuch (11%), 2018 über keines und 2019 wieder über jedes sechste (17%). Ob die höhere Gutheissungs- und tiefere Abweisungsquote an der besseren Qualität der Gesuche lag oder an der höheren Bereitschaft der Verwaltung, allfällige Geheimhaltungsinteressen als weniger gewichtig zu bewerten, kann ohne Kenntnis der Ablehnungsgründe nicht beurteilt werden.

Es war vorgesehen, dass die Expertinnen und Experten aus den Schengen-Staaten 2018 neben Bundesstellen auch Polizei- und Datenschutzbehörden der Kantone Luzern und Basel-Stadt inspizieren. Aus Zeitgründen wurde auf die Inspektion in Basel-Stadt verzichtet.

Wegfall der früher absoluten Anonymisierungspflicht Seit dem 4. Januar 2018 ist die früher absolute Anonymisierungspflicht nach § 30 Abs. 2 IDG aufgehoben und – wie im Bundesöffentlichkeitsgesetz (BGÖ) durch eine Pflicht zur Abwägung ersetzt: Ist der Zugang zu den bei einem öffentlichen Organ vorhandenen Personendaten (also nach § 25 Abs. 1 IDG[17]) nicht schon nach § 29 IDG wegen einer entgegenstehenden besonderen gesetzlichen Geheimhaltungspflicht[18] oder einem überwiegenden öffentlichen[19] oder privaten Geheimhaltungsinteresse[20] ganz oder teilweise zu verweigern, dann sind die Personendaten vor der Zugangsgewährung zu anonymisieren[21]. Ist eine Anonymisierung nicht bzw. nicht vollständig[22] möglich, so darf das öffentliche Organ Zugang zu nicht anonymisierten Personendaten gewähren, wenn

— (neu) ein überwiegendes öffentliches Interesse am Zugang zu diesen Personendaten besteht oder

— (wie zuvor schon) die Voraussetzungen für die Bekanntgabe von Personendaten nach §§ 20 ff. IDG erfüllt sind.

Neu: Abwägungspflicht Wie zuvor sind Personendaten vor der Zugangsgewährung grundsätzlich zu anonymisieren. Nur wenn dies *nicht möglich* ist (weil zum Beispiel öffentlich bekannt ist, um welche betroffenen Personen es sich in einem bestimmten Kontext handelt), darf *ausnahmsweise* zu Personendaten Zugang gewährt werden, wenn ein öffentliches (nicht

>

bloss ein privates) Interesse an diesem Zugang überwiegt. Ohne ein solches gegenüber den entgegenstehenden Geheimhaltungsinteressen überwiegendes öffentliches Zugangsinteresse darf kein Zugang zu nicht anonymisierten Personendaten gewährt werden.

Beispiel Wie diese Abwägung umzusetzen ist, kann an einem (erfundenen!) Beispiel illustriert werden: Eine Medienschaffende möchte Zugang zum Bericht einer Administrativuntersuchung zu in der Öffentlichkeit schon thematisierten Vorgängen bei einem öffentlichen Organ. Wer dessen Leiter ist, dem eine ungenügende Kontrolle vorgeworfen wird, ist allgemein bekannt. Deshalb ist eine Anonymisierung in Bezug auf den Amtsleiter nicht möglich. Wenn es nun um die Aufarbeitung der Vorgänge geht, dann kann im konkreten Fall – Abwägungen sind immer im konkreten Fall vorzunehmen – das öffentliche Zugangsinteresse gegenüber dem Geheimhaltungsinteresse des Amtsleiters überwiegen. Im gleichen Fall vermag jedoch das öffentliche Zugangsinteresse gegebenenfalls das Geheimhaltungsinteresse weiterer im Bericht erwähnter, hierarchisch tiefer stehender Mitarbeiterinnen oder Mitarbeitern nicht zu überwiegen; bezüglich ihrer Person kann deshalb auf eine Anonymisierung (zum Beispiel durch Einschwärzungen) nicht verzichtet werden.

Auswirkungen auf die Gesuchserledigung? Zur Frage, ob diese Gesetzesänderung in Bezug auf die Gesuchserledigung schon Auswirkung gezeitigt hat, lässt sich den erfassten Daten nicht entnehmen.

Die Geschäftslast steigt seit Jahren unaufhörlich. Über die letzten sechs Jahre ist ein Anstieg um 29.3% zu verzeichnen.

Statistik zu den Geschäften des Datenschutzbeauftragten

Verweis Die Zahlen für die Jahr 2017–2019 finden sich im Statistikteil dieses Tätigkeitsberichts (S. 34 f.).

Drei Jahre (mit Vorjahresvergleich) Die Zahl der neu eröffneten Geschäfte hat sich um 2017 um 1% (451; Vorjahr 2016: 447), 2018 um 5% (472) und 2019 um fast 10% (517) erhöht. Bei den Beratungsgeschäften ist der Anteil komplexer Geschäfte im Langzeitvergleich äusserst stabil (2016: 14% / 2017: 15% / 2018: 13% / 2019: 13%). Von den nicht-komplexen Beratungsgeschäften wurden in den ersten beiden Jahren ein etwa gleich grosser Anteil innert 14 Tagen abgeschlossen (Vorjahr 2016: 53% / 2017: 52% / 2018: 55%). Im letzten Jahr konnte dann ein deutlich geringerer Anteil innert dieser Zeit abgeschlossen werden (2019: 40%). Ebenfalls konnten im letzten Jahr wieder weniger Schulungen von öffentlichen Organen durchgeführt werden (Vorjahr 2016: 7 / 2017: 9 / 2018: 9 / 2019: 5).

Involvierte Stellen im langjährigen Vergleich Interessant sind die Veränderungen bei den Stellen, die in die vom Datenschutzbeauftragten bearbeiteten Geschäften involviert waren[23]. In den meisten Fällen verändern sich die Zahlen wenig. Zugenommen hat der Anteil der Fälle,

— in denen der Datenschutzbeauftragte selber aktiv geworden ist (etwa bei Vorhaben, die ihm zur Vorabkontrolle hätten vorgelegt werden müssen, aber nicht vorgelegt wurden, oder wenn er von sich aus Abklärungen startet),

— in denen andere Datenschutzbehörden (inkl. privatim, die Konferenz der schweizerischen Datenschutzbeauftragten) involviert waren, was zum Beispiel auf die verstärkte interkantonale Zusammenarbeit in Datenschutzsachen zurückzuführen ist, und

— in denen Privatpersonen involviert waren, was darauf schliessen lässt, dass die Sensibilisierung für Datenschutzfragen bei den Privaten – meistens den von einer behördlichen Datenbearbeitung betroffenen Personen – zugenommen hat.

Geschäftslast im langjährigen Vergleich Die Geschäftslast steigt seit Jahren unaufhörlich. Über die letzten sechs (abgeschlossenen) Jahre ist ein Anstieg um 29.3%[24] zu verzeichnen.

Headcount Auf der anderen Seite stieg der Headcount (bewilligte Stellen) in den letzten sechs Jahren um 0.4[25]. Die Erhöhung mit dem Budget 2017 hatte zwei Gründe:

— Einerseits wurden 30 Jurist(inn)en-Stellenprozente in 50 Sekretariats-Stellenprozente umgewandelt. Diese Umwandlung war aufgrund der unterschiedlichen Lohnklassenzuteilung *budgetneutral*, d.h. es hat nichts am Aufwand geändert, aber logischerweise am Headcount (+0.2).

— Andererseits wurde 2017 aus einer Jurist(inn)enstelle eine Informatiker(innen)-Stelle geschaffen, weil der Bedarf an IT-Beratungs- und IT-Audit-Kompetenz deutlich zunahm. Da sich auf dem Markt – wie sich auch in den Kantonen Basel-Landschaft und Zürich gezeigt hatte – im IT-Bereich keine geeigneten Kandidat(inn)en zu 60% finden liessen, wurde das Pensum mit Genehmigung durch das Ratsbüro (und

dann natürlich mit der Budgetgenehmigung durch den Grossen Rat) von 60% auf 80% erhöht (+0.2).

Die Zunahme beim Headcount um 0.4 (davon aufwandrelevant: 0.2) über den gesamten Zeitraum von sechs Jahren entspricht somit einer Steigerung um +8.7% (aufwandrelevant: +4.3%). Zu den personellen Ressourcen des Datenschutzbeauftragten vgl. unten S. 32 f.

Falls ein Projekt nicht rechtzeitig zur Vorabkontrolle vorgelegt wird und nicht von sich aus alle datenschutzrelevanten Anforderungen berücksichtigt, besteht die Gefahr, dass ein beschafftes System nicht datenschutzkonform nutzbar ist oder dass nachträglich Änderungen angebracht werden müssen, was in der Regel zu Mehrkosten führt.

Sorgenkind Vorabkontrolle

Unregelmässig Projekte kommen – trotz entsprechender Sensibilisierung – nicht durchgehend zur Vorabkontrolle. Nach dem Projektmanagement Basel-Stadt (PM.BS) wäre es klar, dass und in welchem Zeitpunkt Projekte vorgelegt werden müssten.

Plicht zur Vorabkontrolle Ein Vorhaben ist dem Datenschutzbeauftragten zur Vorabkontrolle vorzulegen, wenn eine Bearbeitung von Personendaten aufgrund der Art der Bearbeitung oder der zu bearbeitenden Daten geeignet ist, besondere Risiken für die Rechte und Freiheit der betroffenen Personen mit sich zu bringen[27]. Wann solche Risiken vorliegen, konkretisiert die Informations- und Datenschutzverordnung[28]. Leider werden nicht alle vorabkontrollpflichtigen Vorhaben rechtzeitig vorgelegt. Die Fachstelle Informationssicherheit hat bei IT-Projekten, die ihr vorgelegt wurden, jeweils auf die Pflicht zur Vorabkontrolle hingewiesen. Dass ein Vorhaben vor dem Beschaffungsentscheid vorzulegen ist, hat durchaus seine Berechtigung: Dann kann dafür gesorgt werden, dass bereits im Pflichtenheft die datenschutzrelevanten Anforderungen gestellt sind. Falls ein Projekt nicht rechtzeitig vorgelegt wird und nicht von sich aus alle datenschutzrelevanten Anforderungen berücksichtigt, besteht die Gefahr, dass ein beschafftes System nicht datenschutzkonform nutzbar ist oder dass nachträglich Änderungen angebracht werden müssen, was in der Regel zu Mehrkosten führt.

Fehlende Unterlagen Ein Problem stellt nicht nur dar, wenn ein Vorhaben nicht rechtzeitig vorgelegt wird. Ebenso oft sind die Unterlagen nicht vorhanden, die der Datenschutzbeauftragte für seine Beurteilung braucht. Für die Durchführung einer Vorabkontrolle werden – so legt es die IDV[29] fest – die folgenden Dokumente benötigt:

— eine Beschreibung des Vorhabens (d.h. eine vollständige Projekt-/Systembeschreibung),

— die Beschreibung der Rechtslage (d.h. eine Rechtsgrundlagenanalyse) und

— eine Übersicht über die Massnahmen zur Verhinderung von Persönlichkeitsverletzungen (d.h. eine Schutzbedarfsanalyse, ggf. eine Risikoanalyse, eine Darstellung der rechtlichen, technischen und/oder organisatorischen Massnahmen, die geplant sind, um die Risiken auszuschliessen oder auf ein tragbares Mass zu reduzieren).

Wenn diese Unterlagen nicht vorhanden sind, dann kann eben keine Vorabkontrolle stattfinden, sondern der Datenschutzbeauftragte berät höchstens projektbegleitend[30].

Verantwortung und IT-Governance

(Gesamt-)Verantwortung Ansprechpartner des Datenschutzbeauftragten ist das im Sinne von § 6 IDG verantwortliche öffentliche Organ, in der Regel die Dateneignerin[31]. Nicht immer ist jedoch klar, wer für eine Datenbearbeitung verantwortlich ist[32]. Bei (Software-)Projekten ist darauf hinzuweisen, dass möglichst bald auch die Stelle involviert wird, die nach Projektabschluss verantwortlich ist. Grössere Unsicherheit besteht bei grösseren Anwendungen, bei denen viele öffentliche Organe beteiligt sind. Handelt es sich wie beim Datenmarkt um Datenpools im Sinne von § 1a IDV, dann ist das verantwortliche Organ in der Rechtsgrundlage nach § 1b IDV festzulegen[33]. Handelt es sich aber nicht um einen Datenpool, sondern um Basisleistungen wie etwa das E-Mail-System MailBS, das Ablagesystem FileBS oder das ERP-System SAP, dann sind die Datenpool-Bestimmungen der IDV nicht direkt anwendbar. Trotzdem braucht es eine Stelle, welche die Gesamtverantwortung[34] übernimmt. Einerseits muss die Gesamt-Risikobeurteilung vorgenommen und das Gesamtrisiko verantwortet werden, zum andern muss auch sichergestellt sein, dass die Teilverantwortungen zugewiesen und ihre Wahrnehmung überwacht und die Verantwortung für die nicht anderen öffentlichen Organen zugewiesenen Bereiche übernommen wird. Diese Gesamtverantwortung ist bei verschiedenen Anwendungen nicht klar zugewiesen. Sie dürfte faktisch entweder bei der Konferenz für Organisation und Informatik (KOI) oder beim obersten Führungsgremium, dem Regierungsrat, liegen. >

IT-Governance Damit ist ein wichtiges Element der IT-Governance angesprochen. Die IT-Governance wurde im Berichtszeitraum insofern gestärkt, als durch die Schaffung einer «Regierungsrats-Delegation Informatik» der Einbezug des Regierungsrates erfolgt ist, was zuvor leider zu wenig der Fall war[35]. Allerdings scheint – soweit man das aus einer Aussensicht feststellen kann – die Umsetzung der IT-Governance nicht reibungslos zu klappen. Für Aussenstehende ist manchmal schwierig zu erkennen, welches Gremium wofür verantwortlich ist und ob die Gremien in ihrer konkreten Zusammensetzung wirklich primär die gesamtkantonale Sicht wahrnehmen. Auch die auf Departementsstufe notwendigen Ressourcen scheinen nicht überall vorhanden zu sein, was sich etwa ausdrückt, wenn sich ein departementaler Informationssicherheitsbeauftragter (ISBD) gegenüber dem Datenschutzbeauftragten ausserstande erklären, die Schutzbedarfs- oder Risikoanalysen durchzuführen oder zu begleiten. In departementsübergreifenden Projekten werden dann auch die Rechtsdienste zum Teil selten oder spät beigezogen, etwa wenn es im Zusammenhang mit Auftragsdatenbearbeitungen durch externe Stellen um die vertragliche Absicherung geht. Erschwerend kommt hinzu, dass beispielsweise bei der Verwendung von Cloud-Technologien die Anbieterinnen oft im (nicht-deutschsprachigen) Ausland sitzen.

Für Aussenstehende ist manchmal schwierig zu erkennen, welches Gremium wofür verantwortlich ist und ob die Gremien in ihrer konkreten Zusammensetzung wirklich primär die gesamtkantonale Sicht wahrnehmen.

Hoffnung auf die Überarbeitung der IT-Governance Die Überarbeitung der IT-Governance ist in Angriff genommen. Als sichtbares Zeichen erfolgte die Integration der Fachstelle Informatiksicherheit und Organisation (ISO) in die Zentralen Informatikdienste (ZID). Der Datenschutzbeauftragte hofft, dass die längerfristige Lösung wieder berücksichtigt, dass die Rollen von der Leistungsbezügerin, welche die Anforderungen definieren muss, und der Leistungserbringerin, welche die Anforderungen zu erfüllen hat, auf verschiedene Organe verteilt sein sollten. Ausserdem müssen, wenn gewisse Leistungen weiterhin dezentral erbracht werden sollen, in den Departementen auch genügend personelle Ressourcen zur Verfügung gestellt werden.

Hoffnung auf den Abschluss von Kernprojekten Weiter sollten auch verschiedene Projekte vorangetrieben und abgeschlossen werden, damit die Informationssicherheit verbessert und e-Government-Lösungen vorangetrieben werden können. Seit Jahren besteht der Bedarf nach einem Identity and Access Management (IAM). Und für die Sicherheit in der E-Mail-Kommunikation wird es dringend, eine Verschlüsselungslösung zu bieten. Dass einzelne Dienststellen sich individuell um Verschlüsselung kümmern müssen, ist keine langfristig taugliche Lösung.

Personelle Ressourcen des Datenschutzbeauftragten

Vakanz Rund zwei Jahre lang konnte die eine 80%-IT-Stelle nicht besetzt werden, da der entsprechende Markt – zu den Konditionen, die der Kanton bieten kann – stark ausgetrocknet ist. Erst seit Oktober 2019 ist das Team nun vollzählig. Das mit dieser zweiten IT-Stelle erworbene Audit-Knowhow soll dazu genutzt werden, die gesetzliche Kontrollaufgabe umfassender wahrzunehmen.

Folgen der Ressourcenknappheit Die Ressourcenknappheit hat dazu geführt, dass nicht mehr alle gesetzlichen Aufgaben mit der nötigen Tiefe und innert angemessener Frist erfüllt werden können. Wie anhand dieses Dreijahres-Tätigkeitsberichts festgestellt werden kann, wurde beispielsweise der Berichtspflicht nur mündlich gegenüber der Geschäftsprüfungskommission (anlässlich der jährlichen Hearings bei der GPK) nachgekommen, aber kein schriftlicher Tätigkeitsbericht veröffentlicht. Auch gelang es, wie aus den oben ausgewiesenen Indikatoren ersichtlich ist, nicht mehr, die Hälfte aller nicht-komplexen Beratungsgeschäfte innert 14 Tagen abzuschliessen. Der Datenschutzbeauftragte entschuldigt sich bei allen Stellen, die länger warten mussten, und hofft auf deren Verständnis.

Dringender Bedarf Auf der anderen Seite werden die Aufgaben – nicht nur gemessen an der Geschäftszahl – immer gewichtiger. Die Digitalisierungsprojekte nehmen sehr stark zu. Der Drang der Verwaltung in die «Cloud» ist extrem stark[36], einerseits weil Cloud-Lösungen Kosteneinsparungen versprechen, andererseits weil gewisse IT-Anbieter ankündigen, dass ihre beim Kanton genutzten Lösungen künftig nur noch als Cloud-Lösungen verfügbar sein sollen. Der Gang in die Cloud bringt immer einen Kontrollverlust mit sich. Die Thematisierung der Risiken nicht nur für die Aufgabenerfüllung, sondern auch für die Rechte der Bürgerinnen und Bürger im Rahmen der Vorabkontrolle ist sehr aufwändig. Dieser Teil der Beratungsaufgabe

beansprucht nicht nur IT-, sondern verstärkt auch juristisches Knowhow: In der Regel können die Risiken nicht allein durch Kryptografie und andere technische Schutzmassnahmen vermieden werden, sondern es braucht rechtliche Absicherungen. Ausserdem ist die Frage, welche behördlichen Daten – vor allem dort, wo es um besondere Personendaten (i.S.v. § 3 Abs. 4 IDG) oder Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterstehen – dem verbleibenden Restrisiko in der Cloud ausgesetzt werden dürfen, rechtlicher Natur. Aus diesen Gründen wird beantragt, mit dem Budget 2021 den Headcount aufzustocken. Schon vor einem Jahr wurde der Aufstockungsbedarf gegenüber der Datenschutz-Delegation des Büros des Grossen Rates thematisiert, aber schliesslich auf einen Antrag für das Budget 2020 verzichtet, weil der Datenschutzbeauftragte nochmals versuchen wollte, die steigende Aufgabenlast mit den bestehenden Ressourcen zu meistern. Aufgrund der erneuten Zunahme der Geschäfte (2019: +9.5%) sieht sich der Datenschutzbeauftragte ausserstande, dies ohne Ressourcenerhöhung zu schaffen. Mit einer Stelle würde der Headcount um den gleichen Faktor angehoben, wie die Geschäftszahl gewachsen ist. Aber es geht ja nicht nur um einen Ausgleich dieses Wachstums: Es soll ja auch die gesetzliche Kontrollaufgaben endlich besser wahrgenommen werden können.

1 Plateforme d'Information du CICOP pour l'Analyse et le Renseignement; CICOP: Concept Intercantonal de Coordination Opérationelle et Préventive (Polizeikonkordat der Westschweizer und des Tessiner Polizeikorps).
2 Sog. Data breach notification; diese Meldepflicht wird mit der IDG-Revision eingeführt werden müssen.
3 § 2 DMV.
4 § 5 Abs. 2 DMV.
5 § 5 Abs. 3 DMV.
6 Vgl. dazu die Ausführungen in: TB 2016 des DSB/BS, S. 41, sowie PK-IDG/BS-Husi, § 9a N 6 ff.
7 Siehe die Ausführungen dazu in: TB 2016 des DSB/BS, S. 42.
8 § 45 Abs. 3 IDG; vgl. dazu PK-IDG/BS-Schilling, § 45 N 15.
9 § 7 Abs. 1 lit. b IDG; vgl. dazu PK-IDG/BS-Rudin, § 7 N 4 ff.
10 Jahresbericht 2018 (des Regierungsrates), 3.10.4 Datenschutzbeauftragter, S. 268.
11 Der frühere IT-Revisionsleiter, Markus Brönnimann, wurde per 1. April 2018 zum neuen Datenschutzbeauftragten des Kantons Basel-Landschaft gewählt. Die zusätzlich bewilligte Stelle eines IT-Auditors/einer IT-Auditorin konnte erst auf Herbst 2019 besetzt werden.
12 Die im Jahresbericht 2018 (des Regierungsrates) angegebene Zahl 3 musste auf 2 reduziert werden, da die Prüfung beim Grundbuch- und Vermessungsamt (aufgrund einer anderen Abschlusspraxis beim zur Unterstützung beigezogenen externen Unternehmen) tatsächlich erst im Jahr 2019 abgeschlossen werden konnte.
13 Nach Art. 55 N-SIS-Verordnung.
14 Nach Art. 37 VISV.
15 Künftig: Global Privacy Assembly (GPA).
16 Jahresbericht 2017 (des Regierungsrates), Staatskanzlei, Informationszugangsgesuche nach Departement, S. 153; Jahresbericht 2018 (des Regierungsrates), 3.2.3 Staatskanzlei, Öffentlichkeitsprinzip, S. 56; Jahresbericht 2019 (des Regierungsrates), 3.2.3 Staatskanzlei, Öffentlichkeitsprinzip, S. 60.
17 Die Regelung von § 30 IDG gilt nur bei der reaktiven Informationstätigkeit (also bei einem Informationszugangsgesuch nach § 25 IDG), nicht bei der (pro-)aktiven Informationstätigkeit nach § 20 IDG, die nicht im Kapitel «Informationszugangsrecht …», sondern im Kapitel «Bekanntgabe von Informationen» geregelt ist. Im Unterschied dazu gelten die Einschränkungen nach § 29 IDG für «die Bekanntgabe von oder den Zugang zu Informationen»; vgl. dazu PK-IDG/BS-Rudin, § 30 N 2.
18 § 29 Abs. 1 IDG; vgl. dazu PK-IDG/BS-Rudin, § 29 N 11 ff.
19 § 29 Abs. 1 und 2 IDG; vgl. dazu PK-IDG/BS-Rudin, § 29 N 18 ff.
20 § 29 Abs. 1 und 3 IDG; vgl. dazu PK-IDG/BS-Rudin, § 29 N 39 ff.
21 § 30 Abs. 1 IDG in der Fassung des Grossratsbeschlusses vom 8. November 2017; vgl. dazu Ratschlag 17.0998 zu einer Änderung des Gesetzes über die Information und den Datenschutz vom 9. Juni 2010 (Informations- und Datenschutzgesetz, IDG).
22 Die Formulierung «nicht vollständig möglich» ist überflüssig, denn entweder sind die Personendaten anonymisiert (d.h. der Personenbezug ist effektiv entfernt) oder eben nicht.
23 Grafik E im Statistikteil (S. 35).
24 2014: 400 neu eröffnete Geschäfte / 2019: 517.
25 2015: 4.6, nämlich 100% Leitung, 280% Jurist(inn)en, 80% Informatiker(innen) / 2020: 5.0, nämlich 100% Leitung, 190% Jurist(inn)en, 160% Informatiker(innen), 50% Sekretariat.
26 Siehe sogleich: Die Umwandlung von 0.3 Jurist(inn)en-Stellen in 0.5 Sekretariatsstelle erhöhte logischerweise zwar den Headcount, war aber budgetneutral.
27 § 13 IDG; vgl. dazu PK-IDG/BS-Rudin, § 13 N 2 ff.
28 § 2 IDV.
29 § 4 IDV.
30 Nicht zu verwechseln mit der Projektbegleitung, die von der Pflicht zur Durchführung einer Vorabkontrolle befreit (§ 2 Abs. 2 IDV): Eine solche Projektbegleitung setzt einen (beratenden) Einsitz in der Projektorganisation voraus, was aber aus Ressourcengründen nur sehr selten sinnvoll ist.
31 Vgl. dazu: Die «schwierige» Dateneignerin, in: TB 2015 des DSB/BS, S. 13 ff.
32 Vgl. dazu schon TB 2014 des DSB/BS, S. 16 f.
33 Für den Datenmarkt: § 3 Abs. 1 DMV.
34 Vgl. dazu TB 2015 des DSB/BS, S. 15 f.
35 Zum entsprechenden Manko vgl. TB 2014 des DSB/BS, S. 16.
36 Vgl. dazu ausführlicher vorne S. 11 ff.

Statistische Auswertungen 2017–2019 (mit Vorjahresvergleich)

A Geschäfte

	2019		2018		2017		2016	
	Anzahl	%	Anzahl	%	Anzahl	%	Anzahl	%
Anzahl eröffnete Geschäfte	517		472		451		447	
prozentuale Veränderung gegenüber Vorjahr		10		5		1		9

B Indikatoren gemäss Budget

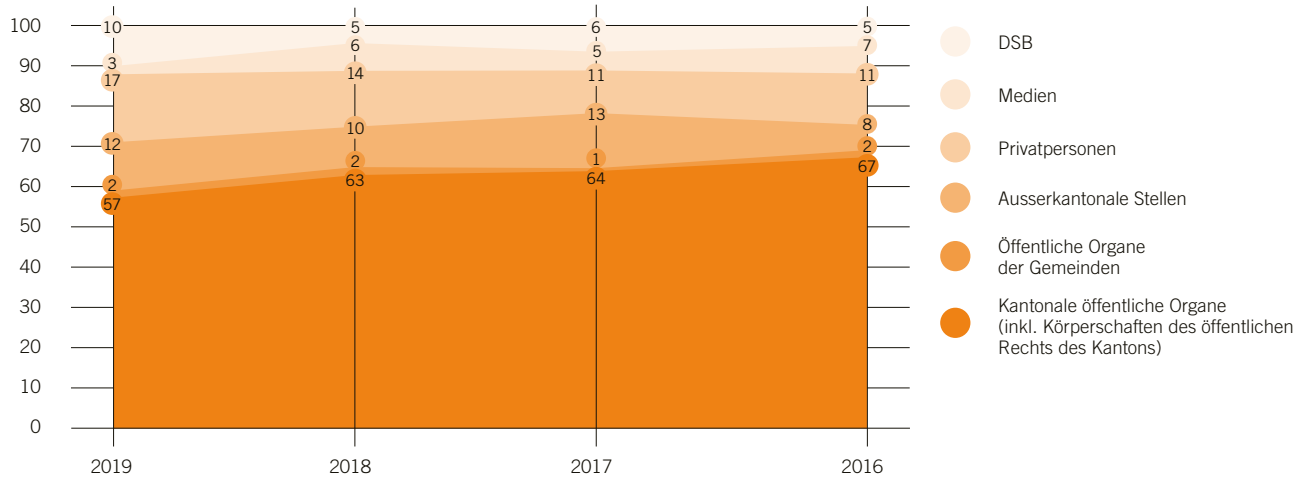
	2019		2018		2017		2016	
	Anzahl	%	Anzahl	%	Anzahl	%	Anzahl	%
Anteil komplexer Beratungen								
prozentualer Anteil an allen Beratungen		13		13		15		14
Innert 14 Tagen abgeschlossene nicht-komplexe Beratungen								
prozentualer Anteil an allen nicht-komplexen Beratungen		40		55		52		53
Durchgeführte Audits								
Anzahl durchgeführte Audits	4		2		4		1	
Durchgeführte Schulungen für öffentliche Organe								
Anzahl durchgeführte Schulungen	5		9		9		7	

C Öffentlichkeitsprinzip

	2019		2018		2017		2016	
	Anzahl	%	Anzahl	%	Anzahl	%	Anzahl	%
Eingereichte Gesuche nach § 25 IDG								
Anzahl eingereichte Gesuche	24		23		37		33	
prozentuale Veränderung gegenüber Vorjahr		4		-38		12		74
Behandlung der Gesuche nach § 25 IDG								
Anzahl gutgeheissener Gesuche	16	67	12	52	15	41	17	52
Anzahl teilweise gutgeheissener Gesuche	0	0	2	9	2	5	2	6
Anzahl ganz abgewiesener Gesuche	4	17	9	39	16	43	13	39
Anzahl noch nicht rechtskräftig entschiedener Gesuche	4	17	0	0	4	11	1	3

Öffentlichkeitsprinzip ab 2012
Zahlen erfasst durch die Staatskanzlei aufgrund der Meldungen der Departemente (§ 31 IDV).
Zahlen aufgeschlüsselt nach Departementen (nicht enthalten sind jeweils die Zahlen zur Staatsanwaltschaft):
Jahresbericht 2017 (des Regierungsrates), Staatskanzlei, Informationszugangsgesuche nach Departementen im Jahre 2017, S. 153
Jahresbericht 2018 (des Regierungsrates), Staatskanzlei, Informationszugangsgesuche nach Departementen im Jahre 2018, S. 56
Jahresbericht 2019 (des Regierungsrates), Staatskanzlei, Informationszugangsgesuche nach Departementen im Jahre 2019, S. 60

D Initianten: Veranlasser der Geschäfte (A) in %



E In die Geschäfte (A) involvierte Stellen in %

«Involviert» sind die Stellen oder Personen, die ein Geschäft initiiert haben (D), und die Stellen, um deren Datenbearbeiten es geht. Beschwert sich eine Privatperson über eine Dienststelle eines Departements, so ist die Privatperson die Initiantin (D); unter E erscheint das Geschäft zusätzlich beim entsprechenden Departement.

Die Fälle dienen der Sensibilisierung der öffentlichen Organe, die vergleichbare Fragen zu beantworten haben. Sie knüpfen zwar an Fällen an, die der Datenschutzbeauftragte behandelt hat, sind aber «abgespeckt», aus mehreren Fällen kombiniert und/oder um zusätzliche Sachverhaltselemente angereichert worden. Sie haben sich also nicht genau so ereignet.

Fälle

Fall 1 Ein Blick auf den Baufortschritt dank Webcam

Der Kanton oder eine Gemeinde hat ein grosses Bauprojekt. Ein neues Gebäude entsteht. Spannend zu sehen, wie der Bau Fortschritte macht, ohne dass, wer daran interessiert ist, sich durch Nässe, Kälte oder Hitze zur Baustelle begeben muss. Eine Webcam ermöglicht's. Was ist vorzukehren, damit nicht die Rechte von Bauarbeitern, Passantinnen oder Nachbarn verletzt werden?

Der (zugegebenermassen sehr eifersüchtige) Ehemann der Bauführerin verfolgt von zu Hause aus, wie sich der Polier auffällig lange mit seiner Frau unterhält. Der Aufpasser, der schaut, dass alles mit rechten Dingen zugeht, merkt sich die Autonummern der im Parkverbot neben der Baustelle parkierten Autos und meldet sie regelmässig der Polizei. Der Chef der Baufirma notiert sich fein säuberlich, wie lange seine Mitarbeiterinnen und Mitarbeiter Pausen machen oder hinter dem Baustellencontainer rauchen. Eine um die Volksgesundheit besorgte Frau fotografiert jeweils, wenn sich – trotz epidemiologischem Distanzgebot – zwei Personen auf der Baustelle zu nahe kommen. Und der Nachbar fotografiert ab seinem Bildschirm die Wildpinkler und will die Fotos am Gartenhag aufhängen…

Überwachung dank der behördlichen Aufzeichnung und Übertragung der Bilder ins Internet – ist das zulässig?

Bilder mit einer Webcam aufnehmen ist ein Datenbearbeiten[1], die Bilder veröffentlichen ein Datenbekanntgeben[2]. Wenn die gefilmten Personen identifizierbar sind, handelt es sich um Personendaten[3]. Personendaten erheben darf ein öffentliches Organ, wenn eine gesetzliche Bestimmung dazu verpflichtet oder ermächtigt (unmittelbare gesetzliche Grundlage), oder dies zur Erfüllung einer gesetzlichen Aufgabe erforderlich ist (mittelbare gesetzliche Grundlage)[4]. Bekanntgeben darf ein öffentliches Organ die Bilder unter den gleichen Voraussetzungen oder, zusätzlich, im Einzelfall mit ausdrücklicher Einwilligung der betroffenen Person[5] – wenn die Personendaten vorher überhaupt zu Recht erhoben worden sind. Eine Videoüberwachung, bei der Personen erkennbar sind, darf nur unter den Voraussetzungen von §§ 17 und 18 IDG zum Schutz von Personen und Sachen vor strafbaren Handlungen erfolgen. Aber selbst wenn diese Datenerhebung zulässig ist: Für die *Bekanntgabe* der Personendaten ist weder eine (unmittelbare oder mittelbare) gesetzliche Grundlage ersichtlich noch wird die ausdrückliche Einwilligung aller Betroffenen vorliegen.

Also bleibt nur ein Verzicht auf das Bekanntgeben – oder ein Bekanntgeben, aber nicht von Personendaten. Wenn nicht auf die Dokumentation des Baufortschritts verzichtet werden soll, dann muss vermieden werden, dass auf den Bildern Personen bestimmt oder bestimmbar sind:

— Wenn die Kamera so weit weg ist und/oder die Auflösung der Kamera so gering ist, dass eine beobachtende Person ohne Spezialwissen auf dem veröffentlichten Bild nicht erkennen kann, um wen es sich bei den aufgenommenen Personen handelt, enthalten die Bilder keine Personendaten mehr.

— Dasselbe lässt sich erreichen, wenn Bereiche, in denen Personen erkennbar wären (z.B. ein Baustellencontainer im Vordergrund) abgedeckt oder verpixelt werden.

Der Persönlichkeitsschutz gebührt aber nicht nur Personen auf der Baustelle. Auch Nachbarn müssen geschützt werden. Sie müssen es sich nicht gefallen lassen, dass dank einer Webcam herausgefunden werden kann, ob sie zuhause sind oder nicht. Auch hier hilft eine Abdeckung oder Verpixelung.

Zur Reduktion des Überwachungscharakters tragen auch weitere Massnahmen bei, etwa der Verzicht auf eine permanente Aufnahme und Veröffentlichung (z.B. nur ein Bild pro Minute) oder die zeitliche Begrenzung der Aufnahmen (z.B. nur von 8 bis 20 Uhr).

Ergebnis

Mit einer Webcam kann der Baufortschritt eines Bauwerks für eine interessierte Öffentlichkeit dokumentiert werden. Dabei muss aber verhindert werden, dass auf den Bildern Personen (z.B. Bauarbeiter, Passantinnen, Nachbarn) erkennbar sind – sei es durch eine entsprechende Wahl des Kamerastandorts und/oder der Bildauflösung, sei es durch Abdecken oder Verpixeln.

1 § 3 Abs. 5 IDG; vgl. dazu PK-IDG/BS-Rudin, § 3 N 48 ff.
2 § 3 Abs. 6 IDG; vgl. dazu PK-IDG/BS-Rudin, § 3 N 56 f.
3 § 3 Abs. 3 IDG; vgl. dazu PK-IDG/BS-Rudin, § 3 N 10 ff.
4 § 9 Abs. 1 lit. a bzw. b IDG; vgl. dazu PK-IDG/BS-Rudin, § 9 N 14 ff.
5 § 21 Abs. 1 lit. a bis c IDG; vgl. dazu PK-IDG/BS-Rudin, § 21 N 3 ff.

Fall 2 Befragung als Auftragsdatenbearbeitung und eigene Forschung mit den Daten

Ein öffentliches Organ des Kantons lässt eine Befragung in seinem Auftrag durch eine Universität oder Fachhochschule durchführen. Die Auftragsnehmerin soll anschliessend mit den anonymisierten Daten auch forschen dürfen. Weil sie damit auch eigene Interessen verfolgen kann, dürfte sie dem kantonalen Amt beim Preis für die Durchführung der Befragung etwas entgegenkommen. Ist das datenschutzrechtlich problemlos?

Ein öffentliches Organ lässt eine Befragung durch eine Universität oder Fachhochschule durchführen. Datenschutzrechtlich stellt dies eine Auftragsdatenbearbeitung dar. Informationen (insbesondere Personendaten) durch eine Dritte oder einen Dritten bearbeiten zu lassen, ist zulässig, wenn keine vertragliche oder gesetzliche Geheimhaltungspflicht entgegensteht[1]. Das auftraggebende öffentliche Organ bleibt verantwortlich[2] und muss durch Vereinbarung sicherstellen, dass die Auftragnehmerin die Daten nur so bearbeitet, wie es selbst das tun dürfte[3].

Forschungseinrichtungen wie die Universität oder die Fachhochschule dürfen forschen[4]. Ein öffentliches Organ darf anderen öffentlichen Organen Personendaten zur Bearbeitung für einen nicht personenbezogenen Zweck, namentlich eben für Forschung, bekannt geben, sofern dies nicht durch eine besondere Geheimhaltungsbestimmung ausgeschlossen ist[5]. Die Empfängerin oder der Empfänger hat sich zu verpflichten, die Personendaten zu anonymisieren oder zu pseudonymisieren, sobald es der Bearbeitungszweck zulässt, und die Auswertungen nur so bekannt zu geben, dass keine Rückschlüsse auf betroffene Personen möglich sind[6]. Kann die Forschung von Anfang an mit anonymisierten Daten erfolgen[7], dann müssen die Daten von Anfang an anonymisiert sein, dürfen also schon nur in anonymisierter Form bekannt gegeben werden[8].

Bei der Auftragsdatenbearbeitung bearbeitet die Auftragsnehmerin im Auftrag des öffentlichen Organs, zu dessen Aufgabenerfüllung, Personendaten. Wenn die Auftragsdatenbearbeiterin die Daten anschliessend in anonymisierter Form zu Forschungszwecken, also zu einem eigenen Zweck, weiterbearbeiten darf, muss jemand die Anonymisierung übernehmen. Dafür verantwortlich ist das öffentliche Organ, das «seine» Daten für Forschungszwecke zur Verfügung stellt. Kann es nun die Resultate der Auftragsdatenbearbeitung zurückbekommen und darauf vertrauen, dass die Universität oder Fachhochschule als Auftragsdatenbearbeiterin die Daten anonymisiert und dann ausschliesslich in anonymisierter Form weiterbearbeitet?

Der Datenschutzbeauftragte empfiehlt dringend ein anderes Vorgehen, bei dem *Auftragsdatenbearbeitung und Datenbekanntgabe zu Forschungszwecken strikt getrennt* (und damit die Verantwortlichkeiten klar zugeteilt) sind:

— Das auftraggebende öffentliche Organ nimmt die Resultate der Auftragsdatenbearbeitung zurück, kontrolliert sie und schliesst damit die Auftragsdatenbearbeitung ab.

— Dann vernichtet die Auftragsdatenbearbeiterin alle Daten, die zur Auftragsdatenbearbeitung bearbeitet worden sind, kontrolliert und bestätigt dem auftraggebenden öffentlichen Organ den Vollzug.

— Anschliessend anonymisiert das öffentliche Organ die Daten, die es zu Forschungszwecken zur Verfügung stellen will, kontrolliert, ob der Personenbezug effektiv entfernt ist, und übermittelt die anonymisierten Daten der Forschungseinrichtung.

Ergebnis

Der Datenschutzbeauftragte empfiehlt, Auftragsdatenbearbeitung und Zurverfügungstellen von Daten zu Forschungszwecken strikt zu trennen. Nach der Auftragsdatenbearbeitung werden die Daten an das auftraggebende öffentliche Organ (zurück-)geliefert und die Personendaten bei der Auftragsdatenbearbeiterin kontrolliert gelöscht. Anschliessend anonymisiert das öffentliche Organ die Daten und händigt diese nach einer Kontrolle an die Forschungseinrichtung aus, die damit nun forschen kann, ohne in den Verdacht zu kommen, vielleicht ein Hintertürchen offen gelassen zu haben, um doch nicht-anonymisierte Daten zur Verfügung zu haben.

1 § 7 Abs. 1 lit. a IDG.
2 § 7 Abs. 2 IDG.
3 § 7 Abs. 1 lit. b IDG.
4 Art. 26 Abs. 1 HFKG (für die Fachhochschulen) und § 2 Universitätsvertrag (für die Universität Basel).
5 § 22 Abs. 1 IDG.
6 § 22 Abs. 2 lit. a und b IDG; vgl. dazu PK-IDG/BS-Husi, § 22 N 22 ff. und PK-IDG/BS-Rudin, §§ 14 N 10 ff.
7 Etwa weil sie nicht mit Personendaten aus anderen Quellen kombiniert werden müssen.
8 PK-IDG/BS-Rudin, § 10 N 19 (mit Verweis auf Ratschlag IDG, 26, zu § 10 Abs. 1 des IDG-Entwurfs).

Fall 3 Forschungsstudie – aus wissenschaftlichem Interesse oder in behördlichem Auftrag?

Ein Institut der Universität führt eine wissenschaftliche Studie durch und befragt dazu ein paar tausend Personen. Tut es das einfach aus ureigenem wissenschaftlichem Interesse oder im Auftrag eines öffentlichen Organs? Und hat die Antwort auf diese Frage Auswirkungen auf das anwendbare Datenschutzrecht und die datenschutzrechtliche Verantwortung?

Ein Institut der Universität Basel führt eine wissenschaftliche Studie durch. Nicht einfach eine rein wissenschaftliche Studie, sondern eine, deren Resultate für staatliche Aktivitäten, beispielsweise für die Gesundheits- oder Alterspolitik, sehr relevant sind. Das Forschungsinstitut will dazu ein paar tausend Personen anschreiben und sie zur Teilnahme an der Studie einladen. Es wendet sich an den Datenschutzbeauftragten. Dieser soll es unterstützen, damit die Studie datenschutzkonform abläuft.

Welches Datenschutzrecht gilt in diesem Fall? Und ist der Datenschutzbeauftragte des Kantons Basel-Stadt überhaupt zuständig?

Stellt sich die Institutsleiterin die Forschungsfrage *aus eigenem Antrieb*, dann gilt für das Uni-Institut das IDG des Kantons Basel-Stadt[1] und ist der Datenschutzbeauftragte des Kantons Basel-Stadt für die Beratung und Aufsicht zuständig.

Was gilt aber, wenn das Uni-Institut *im Auftrag einer Behörde des Kantons Basel-Stadt* oder einer seiner Gemeinden forscht? Wenn beispielsweise eine kantonale Dienststelle ein Unterstützungsprogramm evaluieren lassen will und genau vorgibt, wie das zu geschehen hat? Dann bearbeitet das Uni-Institut die Informationen im Auftrag dieses Organs[2]. Da für das auftraggebende baselstädtische öffentliche Organ auch das IDG des Kantons Basel-Stadt gilt, bleiben die Regeln und die Aufsichtszuständigkeit unverändert. Das öffentliche Organ bleibt verantwortlich für die durch das Uni-Institut in seinem Auftrag durchgeführte Datenbearbeitung[3].

Was gilt, wenn das Uni-Institut *im Auftrag eines öffentlichen Organs eines anderen Kantons* forscht? Wenn beispielsweise ein Amt des Kantons Basel-Landschaft herausfinden will, welche Bedürfnisse die Baselbieter Seniorinnen und Senioren in Bezug auf die ambulanten und stationären Pflegeangebote haben, genau vorgibt, wie das zu geschehen hat, und mit der Durchführung der Studie das Uni-Institut beauftragt, dann wird die Tätigkeit des Uni-Instituts zu einer Auftragsdatenbearbeitung nach dem basellandschaftlichen Informations- und Datenschutzgesetz[4]. Die Baselbieter Dienststelle trägt für die Datenbearbeitung die Geamtverantwortung[5], und es ist diesbezüglich der Baselbieter Datenschutzbeauftragte zuständig[6].

Und wenn ein Bundesorgan das Institut zu einem Forschungsvorhaben beizieht[7]? Dann hat das grundsätzlich dieselbe Folge: Das Datenbearbeiten des Basler Uni-Instituts ist eine Auftragsdatenbearbeitung nach dem Bundesdatenschutzgesetz[8], und diesbezüglich ist der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte zuständig.

Deshalb ist es unerlässlich, dass rechtzeitig die Rollen geklärt werden: Gibt es ein auftraggebendes öffentliches Organ? Oder ist ein öffentliches Organ einfach sehr interessiert an den Resultaten eines Forschungsprojektes, welches das Uni-Institut in eigener Verantwortung aus wissenschaftlichem Interesse an der Forschungsfrage durchführt?

Ergebnis

Forscht ein Institut der Universität Basel aus (eigenem) wissenschaftlichem Interesse, dann gilt für das entsprechende Datenbearbeiten das IDG des Kantons Basel-Stadt; das Uni-Institut trägt die volle Verantwortung für die Datenbearbeitung. Wenn das Uni-Institut aber im Auftrag einer staatlichen Behörde forscht, dann wird sein Datenbearbeiten zu einer Auftragsdatenbearbeitung, für die das auftraggebende öffentliche Organ weiterhin die Verantwortung trägt. Entsprechend gilt das jeweilige (Informations- und) Datenschutzgesetz und ist für die Aufsicht die entsprechende Datenschutzaufsichtsbehörde zuständig. Es ist unerlässlich, dass die entsprechenden Rollen wegen der unterschiedlichen Verantwortung rechtzeitig geklärt werden.

1 § 43 Universitätsvertrag: «Soweit dieser Vertrag und die zu erlassenden Vollziehungsvorschriften keine Regelung enthalten, findet subsidiär und sinngemäss das Recht des Sitzkantons Anwendung». Damit kommt das IDG des Kantons Basel-Stadt zur Anwendung. Gleichermassen für Swiss TPH: § 30 Swiss TPH-Vertrag, wobei dort die Anknüpfung am Sitz dazu führt, dass sich ab dem Bezug des neuen Sitzes in Allschwil die Aufsichtszuständigkeit in den Landkanton verschiebt.
2 § 7 IDG.
3 § 7 Abs. 2 IDG.
4 § 7 IDG/BL.
5 § 7 Abs. 2 IDG/BL.
6 § 41 IDG/BL.
7 Doch Achtung: Bundesorgane können nach Art. 16 FIFG auch «Forschung initiieren», weil sie die Resultate dieser Forschung zur Erfüllung ihrer Aufgaben benötigen (sog. Ressortforschung). Wenn ein Bundesamt dann im Sinne von Art. 16 Abs. 2 lit. f FIFG einen Forschungsauftrag erteilt («Auftragsforschung»), dann ist es datenschutzrechtlich nicht mehr das verantwortliche öffentliche Organ, sondern das Uni-Institut wird es.
8 Art. 10a DSBG/Bund.

Fall 4 Lieferung von Grundbuchdaten an das Bundesamt für Statistik

Wenn ein öffentliches Organ Personendaten an ein anderes öffentliches Organ bekannt geben soll, dann braucht es dazu eine gesetzliche Grundlage. Ohne eine solche ist es nicht zulässig, Personendaten zu übermitteln. Darf ein Grundbuchamt, wenn die Aufbereitung von Daten für das Bundesamt für Statistik aufwändig wäre, einfach den gesamten Grundbuchdatensatz liefern? Nein, findet das Grundbuch- und Vermessungsamt Basel-Stadt – und der Datenschutzbeauftragte unterstützt es in dieser Ansicht.

Das Bundesamt für Statistik (BFS) hat vielfältige Aufgaben. Wenn die (Bundes-)Politik stärker datenbasiert erfolgen soll, braucht sie Daten. Diese bereitzustellen, ist im Bund die Aufgabe des BFS. Dabei stammen die Daten zu einem grossen Teil aus den Kantonen.

Damit ein öffentliches Organ des Kantons dem BFS Daten liefern darf, braucht es eine gesetzliche Grundlage[1]. Für die Datenlieferungen an das BFS findet sich diese in der Statistikerhebungsverordnung des Bundes. Auf fast 160 Seiten listet der Anhang dieser Verordnung auf, wer dem BFS zu welchem Zweck welche Daten bekannt geben muss.

Wenn eine Rechtsgrundlage keine Lieferung von Personendaten vorsieht, dann ist es auch nicht zulässig, Personendaten zu liefern. Dann muss das öffentliche Organ die Daten so aufbereiten, dass die verlangten Daten geliefert werden können, aber eben keine Personendaten mehr sind. Auch wenn diese Aufbereitung einen gewissen Aufwand erfordert, ist es nicht zulässig, einfach «alle Personendaten» zu liefern und darauf zu vertrauen, dass das BFS dann schon nur die nötigen Daten (ohne Personenbezug) daraus bezieht.

Das Grundbuch- und Vermessungsamt Basel-Stadt (GVA) hat bei der Erhebung von Grundbuchdaten im Zusammenhang mit dem Eidgenössischen Gebäude- und Wohnungsregister sowie dem schweizerischen Immobilienpreisindex genauer hingeschaut und die bundesrechtlichen Grundlagen geprüft. Dabei ist es zum Schluss gekommen, dass mindestens bei Eigentümerinnen und Eigentümern, die natürliche Personen sind, keine Personendaten zu liefern sind.

Der Datenschutzbeauftragte hat das GVA in dieser Auslegung bestätigt[2]. Auch eine Auslegung von § 22 IDG führt zum gleichen Resultat: § 22 IDG[3] erlaubt, dass Personendaten zu einem nicht personenbezogenen Zweck (z.B. eben für die Statistik) bekannt gegeben werden dürfen, wenn der Bearbeitungszweck dies erfordert. Dann muss sich die Empfängerin verpflichten, die Daten zu anonymisieren oder zu pseudonymisieren, sobald es der Bearbeitungszweck zulässt. Der Regierungsrat hat aber schon im IDG-Ratschlag[4] festgehalten: Wenn der Bearbeitungszweck keine Bekanntgabe von Personendaten erfordert, dann dürfen auch keine Personendaten geliefert werden. Dann muss also das bekanntgebende öffentliche Organ dafür sorgen, dass die Daten vor der Lieferung anonymisiert oder pseudonymisiert werden. Offenbar wird das von etlichen anderen Grundbuchämtern aber nicht so gemacht, sondern diese liefern einfach gerade «alle» Daten an eine vom BFS beauftragte private Firma; das BFS bedient sich dann bei diesem Datenbestand.

Aufgrund dieser Sachlage hat das GVA einen Filter entwickeln lassen. Durch dessen Einsatz lässt sich erreichen, dass das BFS lediglich jene Grundbuchdaten erhält, die es zur Erfüllung seiner gesetzlichen Aufgabe auch tatsächlich benötigt. Soweit es sich dabei um Personendaten handelt, die natürliche Personen betreffen, hat das GVA diese vor der Lieferung zudem anonymisiert. Der Datenschutzbeauftragte begrüsst dieses Vorgehen – dieses qualifiziert sich nicht nur als gesetz-, sondern auch als verhältnismässig.

Ergebnis

Wenn ein öffentliches Organ einer anderen Amtsstelle zu einem nicht personenbezogenen Zweck (wie Statistik, Planung) Daten liefern muss oder soll, dann muss es – ohne eine abweichende gesetzliche Grundlage, die zur Lieferung von Personendaten ermächtigt oder verpflichtet – die Daten vorher anonymisieren oder pseudonymisieren. Eine Lieferung von Personendaten wäre nicht gesetz- und verhältnismässig.

1 § 21 Abs. 1 und (bei besonderen Personendaten) Abs. 2 IDG; vgl. dazu PK-IDG/BS-Rudin, § 21 N 3 ff. und 34 ff.
2 Das BFS sieht das anders und leitet – u.E. unzutreffenderweise – aus diversen Gesetzes- bzw. Verordnungsbestimmungen ab, dass eine Lieferung von umfassenden Grundbuchdaten inkl. Personendaten zulässig ist.
3 Vgl. dazu PK-IDG/BS-Rudin, § 22 N 6 und § 10 N 19.
4 Ratschlag 08.0637.01, S. 26; PK-IDG/BS-Rudin, § 10 N 19.

Fall 5 Drohnen – nur ein neues Mittel zur Erfüllung der gesetzlichen Aufgaben?

Es wäre so praktisch: Statt sich physisch irgendwo hin bewegen zu müssen, einfach aus der Luft beobachten. Mit Drohnen kann man live beobachten, fotografieren und filmen. Doch dürfen öffentliche Organe einfach Drohnen verwenden? Abgesehen von den luftverkehrsrechtlichen Vorschriften des BAZL[1]: Welche Rechtsgrundlagen braucht die Verwaltung für den Drohneneinsatz?

Beispiele aus anderen Kantonen gibt es schon etliche: Die Baupolizei in der Luzerner Gemeinde Horw will zum Beispiel mittels Drohnen feststellen, ob illegale Bauten erstellt worden sind[2]. Viele Polizeien und Rettungsdienste überlegen sich, ob Drohnen ihre Einsätze unterstützen könnten. Argumentiert wird, dass die öffentlichen Organe ja nur mit einem neuen technischen Mittel das tun, was sie schon lange tun dürften – etwa Verstösse gegen das Baurecht feststellen oder eine Demonstration beobachten. Mindestens im erstgenannten Fall hat das Kantonsgericht Luzern mangels Vorliegen einer gesetzlichen Grundlage einen Riegel geschoben[3].

Der Datenschutzbeauftragte hat sich mehrfach zum Drohneneinsatz geäussert. Einerseits sind Aufnahmen aus so grosser Höhe, dass auf den Bildern keine Personen bestimmbar sind, aus datenschutzrechtlicher Sicht wenig problematisch; wenn dann allerdings die Polizei Personen, die auf Bildern sichtbar sind, «am Boden» kontrolliert und so ihre Identität feststellt, werden die Personen bestimmt und die Aufnahmen nachträglich zu Personendaten[4]. Andererseits dürfte bei Katastropheneinsätzen der Rettung (Grossbrand, Hauseinsturz o.ä.) wohl eine (mindestens mittelbare) gesetzliche Grundlage dafür zu finden sein, dass nach verletzten Personen gesucht werden darf.

Darf aber die Kantonspolizei gestützt auf § 58 PolG zum Beispiel bei Demonstrationen Drohnen einsetzen? Die Bestimmung ist technologieneutral formuliert: «Die Kantonspolizei kann aus Gründen der Beweissicherung Teilnehmerinnen oder Teilnehmer einer öffentlichen Veranstaltung aufnehmen, sofern die konkrete Gefahr besteht, dass Straftaten begangen werden». Doch konnte der Gesetzgeber vor bald einem Vierteljahrhundert auch nur ahnen, welche Mittel künftig zur Verfügung stehen könnten? Zudem erscheint der (potenzielle) Eingriff in die Persönlichkeitsrechte der Betroffenen schwerwiegender als bei den bisher verwendeten technischen Mitteln. Die Drohne ist nicht einfach eine lineare Weiterentwicklung der Aufnahmegeräte. Sie erlaubt – im Vergleich zu anderen Überwachungsmassnahmen – einen speziellen, ihr eigenen Blick auf das Geschehen. Im Unterschied zur Polizistin mit der Kamera in der Hand kann die Drohne fast uneingeschränkt und äusserst mobil Aufnahmen aus verschiedenen Distanzen und Blickwinkeln machen, ohne dass dies für die Betroffenen notwendigerweise ersichtlich ist. Ausserdem ist für die Betroffenen schwierig abzuschätzen, was die Drohne genau macht und wer die Verantwortung für den Einsatz trägt – anders als bei der stationären Videoüberwachung, wo mit einer Beschilderung auf die Überwachung hingewiesen werden muss.

Bei Demonstrationen steht nicht nur die informationelle Selbstbestimmung auf dem Spiel, sondern auch die Versammlungsfreiheit. Schon im Ratschlag zum Polizeigesetz wurde festgestellt, dass mit § 58 PolG «eine politisch heikle Materie» geregelt wird. Darum wird der Zweck auf die Beweissicherung im Hinblick auf ein Verzeigungs- oder Strafverfahren beschränkt. Zudem sei «der Zeitpunkt für Beginn und Ende sowie die Zielrichtung von solchen Massnahmen […] so zu wählen, dass sich die Aufnahmen mit hoher Wahrscheinlichkeit auf strafrechtlich relevantes Verhalten konzentrieren».

Ergebnis

Unseres Erachtens stellt § 58 PolG keine hinreichende gesetzliche Grundlage für den Drohneneinsatz dar. Für den recht- und verhältnismässigen Einsatz müssten neben den legitimen Einsatzzwecken auch Fragen der Transparenz, der Auskunftsrechte der Betroffenen, der Berechtigungen zum Zugriff auf die aufgezeichneten Daten, die Aufbewahrung usw. geregelt werden. Deshalb empfiehlt der Datenschutzbeauftragte die Schaffung einer Rechtsgrundlage. Die politisch-mediale Dimension eines Drohneneinsatzes ohne vorgängige gesellschaftliche und parlamentarische Diskussion sollte nicht unterschätzt werden.

1 Vgl. dazu: <https://www.bazl.admin.ch/bazl/de/home/gutzuwissen/drohnen-und-flugmodelle/allgemeine-fragen-zu-drohnen.html>.
2 Das Bau- und Gewerbeinspektorat Basel-Stadt hat auf eine Medienanfrage hin am 20. Februar 2017 bestätigt, zur Überwachung von Bauten und Anlagen mit Bezug auf deren Sicherheit und Einhaltung der Baugesetzgebung keine Drohnen einzusetzen.
3 Vgl. Urteil 7H 17 49 des Kantonsgerichts Luzern vom 18. April 2018, <https://datenschutz.lu.ch/-/media/Datenschutz/Dokumente/Urteil_Kantonsgericht_Luzern_7H_17_49_18042018.pdf?la=de-CH>.
4 Die Tatsache, dass die bearbeiteten Daten Personendaten werden, führt dazu, dass für das Bearbeiten die Regeln des Informations- und Datenschutzgesetzes eingehalten werden müssen.

Fall 6 Nicht für alle Ewigkeit – aber wer sagt, für wie lange?

Das Bearbeiten von Personendaten muss verhältnismässig sein. Das zeitliche Element der Verhältnismässigkeit verlangt, dass Personendaten nicht länger aufbewahrt werden, als dies zur Aufgabenerfüllung erforderlich ist. Häufig wird der Datenschutzbeauftragte gefragt, wie lange dies sei. Er kann den öffentlichen Organen die Entscheidung aber nicht abnehmen.

Ein öffentliches Organ bearbeitet Personendaten, um seine gesetzliche Aufgabe zu erfüllen. Dafür gilt das Informations- und Datenschutzgesetz (IDG). Und dieses schreibt in § 16 vor: «Nicht mehr benötigte Personendaten, die von der gemäss Archivgesetz zuständigen Stelle als nicht archivwürdig beurteilt werden, sind vom öffentlichen Organ zu vernichten.»[1]

Was heisst das? Es gibt eine erste Phase, die des «Benötigens». Personendaten werden vom öffentlichen Organ verwendet, um dessen gesetzliche Aufgabe zu erfüllen. Werden sie nicht mehr benötigt, dann werden die Daten vom zuständigen Archiv (bei der Kantonsverwaltung also vom Staatsarchiv), archiviert, wenn es die Daten im Sinne des Archivgesetzes (ArchivG) als archivwürdig beurteilt hat[2]. Die öffentlichen Organe sind verpflichtet, die Unterlagen, die sie zur Erfüllung der Aufgaben nicht mehr benötigen, auszusondern und periodisch dem Archiv zur Übernahme anzubieten[3]. Nicht archivwürdige Daten sind nach dem Ende des «Benötigens» zu vernichten.

Was heisst aber «nicht mehr benötigt»? Wie lange sind Personendaten aufzubewahren? Mit dieser Frage wird der Datenschutzbeauftragte häufig konfrontiert. Einfach ist die Frage zu beantworten, wenn eine spezialgesetzliche Aufbewahrungsfrist besteht[4]. Ist dies nicht der Fall, dann hat das *öffentliche Organ grundsätzlich selber* zu bestimmen, wann es die Personendaten nicht mehr für die Erfüllung seiner Aufgaben benötigt. Es kann am besten abschätzen, wie lange es einen Informationsbestand regelmässig[5] benötigt, um seine gesetzliche Aufgabe erfüllen zu können. Dabei gilt es zwei Aspekte zu beachten:

— Da nach § 12 Abs. 3 ArchivG Personendaten, die vom öffentlichen Organ nach § 18 DSG (korrekterweise: nach § 16 IDG) dem zuständigen Archiv angeboten und von diesem übernommen worden sind, dem abliefernden öffentlichen Organ nicht mehr zur Verfügung stehen (Rückkoppelungsverbot), ist bei der Bestimmung des Zeitpunkts, ab welchem das öffentliche Organ die Personendaten nicht mehr benötigt, auch die Dauer zu berücksichtigen, während der Daten *zu Beweis- und Sicherungszwecken* (zum Beispiel als Beweismittel, um allfällige Schadenersatzansprüche abzuwehren) aufbewahrt werden müssen.

— § 21 der Registratur- und Archivierungsverordnung (RAV) legt fest, dass die öffentlichen Organe die Personendaten dem Staatsarchiv in der Regel spätestens zehn Jahre nach Abschluss der Unterlagen[6] anzubieten haben.

— Die Frist kann bei Unterlagen, die nicht als archivwürdig bewertet worden sind, auch sehr kurz sein. Bewerbungsunterlagen von nicht berücksichtigten Stellenbewerberinnen und -bewerbern sind beispielsweise nach wenigen Monaten zu vernichten, ausser die Betroffenen bitten um die weitere Aufbewahrung, weil die Bewerbung bei einer nächsten Vakanz wieder einbezogen werden soll.

Die jüngeren Datenschutzrechtsreformen gewichten die zeitliche Komponente des Verhältnismässigkeitsprinzip zunehmend höher. Es ist deshalb wichtig, den Aufbewahrungsfristen (zum Beispiel im Rahmen des Records Managements) mehr Aufmerksamkeit zu schenken als bisher.

Ergebnis

Personendaten dürfen nur so lange bearbeitet werden, als es zur Erfüllung der gesetzlichen Aufgabe notwendig ist. Anschliessend sind sie zu archivieren, wenn das zuständige Archiv sie als archivwürdig bewertet hat, beziehungsweise durch das öffentliche Organ zu vernichten. Wie lange die Daten zur Aufgabenerfüllung benötigt werden, hat grundsätzlich das öffentliche Organ festzulegen, wenn nicht spezialrechtliche Aufbewahrungsfristen bestehen. Dabei ist auch die Dauer zu berücksichtigen, während der Daten zu Beweis- und Sicherungszwecken aufbewahrt werden müssen.

1 Vgl. dazu PK-IDG/BS-Rudin, § 16 N 2 ff.
2 § 5 Abs. 1 lit. a ArchivG; § 23 RAV.
3 Anbietungspflicht nach § 7 ArchivG.
4 Zum Beispiel § 29 Abs. 2 GesG oder § 45 SoHaV (und Anhang II).
5 Andere Gesetze sprechen (oder sprachen) von «nicht mehr ständig» (so Art. 21 Abs. 1 DSG/Bund) oder «voraussichtlich nicht mehr regelmässig» benötigen (so § 15 Abs. 1 des Baselbieter Datenschutzgesetzes vor dem Inkrafttreten des IDG/BL).
6 Nach § 10 Abs. 3 ArchivG gilt als Abschluss der Unterlagen das Jahr, in welchem die Unterlagen durch Vervollständigung oder den letzten organischen Zuwachs abgeschlossen wurden.

Anhang

Verzeichnis der zitierten Gesetze, Materialien, Literatur und Abkürzungen

Kanton Basel-Stadt:
Rechtsgrundlagen, Materialien

Rechtsgrundlagen

ArchivG Gesetz vom 11. September 1996 über das Archivwesen (Archivgesetz), SG 153.600.

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

GesG Gesundheitsgesetz vom 21. September 2011 (GesG), SG 300.100.

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

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.

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

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

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

Swiss TPH-Vertrag Vertrag vom 10. November 2015 zwischen den Kantonen Basel-Landschaft und Basel-Stadt über die gemeinsame Trägerschaft des Schweizerischen Tropen- und Public Health-Instituts (Swiss TPH-Vertrag), SG 447.650.

Universitätsvertrag Vertrag vom 27. Juni 2006 zwischen den Kantonen Basel-Landschaft und Basel-Stadt über die gemeinsame Trägerschaft der Universität Basel, SG 442.400.

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.

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).

Kanton Basel-Landschaft
Rechtsgrundlagen

Rechtsgrundlagen

IDG/BL Gesetz (des Kantons Basel-Landschaft) vom 10. Februar 2011 über die Information und den Datenschutz (Informations- und Datenschutzgesetz, IDG), SGS 162.

Bund:
Rechtsgrundlagen, Materialien

Rechtsgrundlagen

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.

FIFG Bundesgesetz vom 14. Dezember 2012 über die Förderung der Forschung und der Innovation (FIFG), SR 420.1.

HFKG Bundesgesetz vom 30. September 2011 über die Förderung der Hochschulen und die Koordination im schweizerischen Hochschulbereich (Hochschulförderungs- und -koordinationsgesetz, HFKG), SR 414.20.

SDSG Bundesgesetz vom 28. September 2018 über den Datenschutz im Rahmen der Anwendung des Schengen-Besitzstands in Strafsachen (Schengen-Datenschutzgesetz, SDSG), SR 235.3.

Statistikerhebungsverordnung Verordnung vom 30. Juni 1993 über die Durchführung von statistischen Erhebungen des Bundes (Statistikerhebungsverordnung), SR 431.012.1.

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

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

VTS Verordnung vom 19. Juni 1995 über die technischen Anforderungen an Strassenfahrzeuge (VTS), SR 741.41.

Materialien

E-DSG Entwurf (vom 15. September 2017) zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl 2017 7193.

PMT Bundesgesetz über polizeiliche Massnahmen zur Bekämpfung von Terrorismus (PMT) (Botschaft und Entwurf: BBl 2019 4751)

Europarat, Europäische Union: Rechtsgrundlagen

Rechtsgrundlagen

DSGVO (oder: Verordnung [EU] 2016/679) 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 L 119, 4.5.2016, S. 1-88.

Europarats-Konvention 108 Übereinkommen (des Europarates) zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, abgeschlossen in Strassburg am 28. Januar 1981, SR 0.235.1 (für die Schweiz in Kraft getreten am 1. Februar 1998).

Europarats-Konvention 108+ Übereinkommen (des Europarates) zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten in der Fassung des Protokolls vom 10. Oktober 2018 zur Änderung des Übereinkommens.

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 L 119, 4.5.2016, S. 89–131.

Richtlinie 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 vom 23.11.1995, S. 31 ff.

Tätigkeitsberichte

TB (Jahr) des DSB/BS Tätigkeitsbericht (Jahr) des Datenschutzbeauftragten des Kantons Basel-Stadt, abrufbar unter: <https://www.dsb.bs.ch/ueber-uns/taetigkeitsberichte.html>.

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.

Abkürzungen

BAZL Bundesamt für Zivilluftfahrt
BBl Bundesblatt
BFS Bundesamt für Statistik
KBM Kantonales Bedrohungsmanagement
RA-PROF Radicalisation Profiling
SG Systematische Gesetzessammlung (des Kantons Basel-Stadt)
SGS Systematische Gesetzessammlung (des Kantons Basel-Landschaft)
SIK Schweizerische Informatikkonferenz
SR Systematische Rechtssammlung (des Bundes)

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

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

Team
per 31.12.2019:
Eva Maria Bader (Sekretariat) (ab 1.4.2017)
Pascal Lachenmeier, Dr. iur., Advokat (ab 1.10.2019)
Sukhwant Singh, Master in IT Business Engineering (ab 1.10.2019)
Thomas Sterchi, Wirtschaftsinformatiker HF (ab 1.7.2018)
Ines Weihrauch, lic. iur., Advokatin (seit 1.5.2019)
Barbara Widmer, Dr. iur., LL.M., CIA

früher im Berichtszeitraum:
Rüdiger Bachmann (1.9.2017–30.4.2018)
Markus Brönnimann, CISA (bis 31.3.2018)
Katja Gysin, Fürsprecherin (bis 30.9.2019)
Nicole Kuster, Dr. iur., Advokatin (1.6.2017–31.5.2019)
Sarah Salzmann, MLaw (Weiteranstellung nach Volontariat: 1.1.2017–31.3.2017)

Volontärinnen/Volontäre:
Simone Mäder, MLaw (1.1.2017–30.6.2017)
Meltem Aslan, MLaw (1.7.2017–31.12.2017)
Larissa Meyer, MLaw (1.1.2018–30.6.2018)
Cäcilia Dürdoth, MLaw (1.7.2018–31.12.2018)
Lucas Maciejewski, MLaw (1.1.2019–30.6.2019)
Tobias Schwaller, MLaw (1.7.2019–31.12.2019)

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

Bezug
Datenschutzbeauftragter des Kantons Basel-Stadt
Henric Petri-Strasse 15
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