Datenschutzbeauftragter des Kantons Basel-Stadt

Bericht an den Grossen Rat

2013

Inhaltsübersicht

Einleitung

Themen

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

Aus dem Alltag

Fälle

Anhang

Einleitung 2013 – grosse Enthüllungen und kleine Schritte

2013 war das Jahr der NSA-Enthüllungen – geht uns das etwas an? 2013 war das zweite Jahr seit der Einführung des Öffentlichkeitsprinzips – wie offen sind die Türen der Verwaltung nun? 2013 war aber auch ein Jahr mit ganz «gewöhnlichen» Datenschutzfragen – welche Themen standen im Vordergrund?

NSA und kantonale Informationssicherheit

Überraschung? Das Jahr 2013 dürfte als das Jahr in die Geschichte eingehen, in welchem die Weltöffentlichkeit durch die Enthüllungen von Edward Snowden auf das Ausmass der weltweiten Überwachungspraktiken von Geheimdiensten aufmerksam gemacht worden ist. Konnte man überrascht sein? Seit den Untersuchungen des Europäischen Parlaments zum globalen Abhörsystem ECHELON im Jahr 2001 war die Tatsache, dass die Geheimdienste in der Kommunikation mithören, bekannt. Es wäre naiv gewesen, in Anbetracht der weiteren Entwicklungen insbesondere nach «9/11» und der rasant fortschreitenden Digitalisierungen von Wirtschaft, Gesellschaft und Verwaltung davon auszugehen, dass die Eingriffe in die Souveränitätsrechte anderer Staaten, in die Geschäftsgeheimnisse von Unternehmen und in die Persönlichkeitsrechte und Privatsphäre der einzelnen Menschen kleiner würden.

Unberührt? Kann der Kanton Basel-Stadt angesichts dieser Enthüllungen einfach weitermachen wie bisher? Kommen Cloud-Lösungen, wie sie immer wieder zur Kostenreduktion schmackhaft gemacht werden, überhaupt noch in Frage? Darf die Verantwortung für die Informationssicherheit weiterhin relativ dezentral und wenig gesteuert den Informatikabteilungen überlassen werden? Darf man weiterhin darauf vertrauen, dass schon nichts passiert? Dass das DANEBS (DAtenNEtz Basel-Stadt) sicher sei? Dass es keine stärkere Authentisierung der Berechtigten braucht? Dass eine Verschlüsselung der Kommunikation oder der Datenablage weiterhin nicht nötig ist?

Verletzlichkeit Angesichts der Entwicklungen erhält die Informationssicherheit ein ganz anderes Gewicht: Die staatliche Aufgabenerfüllung ist heute weitgehend abhängig von der Informationstechnologie. Entsprechend hoch ist die Verletzlichkeit – und nicht nur in Bezug auf staatliche Interessen, sondern auch auf private: Bei einem Grossteil der Informationen, über welche öffentliche Organe verfügen, handelt es sich um Daten, die von den Kundinnen und Kunden staatlicher Dienstleistungen dem Staat anvertraut worden sind. Der Datenschutzbeauftragte weist seit mehreren Jahren auf die Bedeutung der Informationssicherheit und den diesbezüglichen Handlungsbedarf hin.

IT-Governance 2013 erfolgte ein langerwarteter erster Schritt: Der Regierungsrat hat eine Neuregelung der IT-Governance per 1. Januar 2014 beschlossen. Damit sollen beispielsweise Steuerungsmechanismen, Aufgaben, Rollen und Verantwortlichkeiten bezüglich Erbringung und Bezug von IT-Dienstleistungen klarer geregelt werden. Wenn die Umsetzung gelingt, besteht Grund zur Hoffnung, dass die IT-Sicherheit deutlich verbessert werden kann, vorausgesetzt, dass nicht departementale Partikulärinteressen bei einzelnen Projekten die angedachte Stärkung aushebeln.

Berechtigungskonzepte Einen wichtigen Aspekt bei der Wahrnehmung der Verantwortung, die nach den §§ 6 und 7 IDG[1] beim öffentlichen Organ liegt, das Informationen zur Erfüllung seiner gesetzlichen Aufgaben bearbeitet oder bearbeiten lässt, bildet das Berechtigungskonzept. Damit wird festgelegt, wer welche Daten bearbeiten kann. Dieses Thema wird im vorliegenden Tätigkeitsbericht vertieft behandelt (Seiten 8 ff.).

Datenschutz und Öffentlichkeitsprinzip

Zwei Jahre Öffentlichkeitsprinzip Seit zwei Jahren gilt das Öffentlichkeitsprinzip – Anlass für einen vertieften Blick auf die Erfahrungen und offenen Punkte (Seiten 12 f.). Um das Bild auf der Titelseite aufzunehmen: Wie offen sind die Türen der Verwaltung? Insbesondere die Diskussionen um den BVB-Bericht der Finanzkontrolle haben gezeigt, dass die (pro-)aktive Seite der staatlichen Informationstätigkeit in ihrer Bedeutung noch unterschätzt wird. Es ist zu hoffen, dass mit der neuen Website des Kantons das Öffentlichkeitsprinzip endlich sichtbarer wird – die Ängste, das Transparenzprinzip lege die Verwaltung lahm, haben sich bislang nicht bewahrheitet.

Beratung und Kontrollen Neben den Herausforderungen im Bereich der Informationssicherheit gab es auch im Jahr 2013 das «Tagesgeschäft» – einen Einblick in den bunten Strauss der behandelten Beratungsthemen erhalten Sie auf den Seiten 20 ff. 403 Geschäfte wurden 2013 neu eröffnet (2012: 366), also 10% mehr als im Jahr zuvor. Dabei stieg auch der Anteil komplexer Beratungen (11% gegenüber 9% im Jahr 2012). Einen detaillierteren Überblick über die Zahlen des Jahres 2013 bietet die Statistik (Seiten 30 f.). Die Zahl der abgeschlossenen Datenschutz-Audits und -Assessments konnte auf 4 verdoppelt werden. Einen kurzen Überblick über die Kontrolltätigkeit erhalten Sie auf den Seiten 26 ff.

Praxiskommentar Rechtzeitig zum Jahresende erschien der Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Basel-Stadt. Sechs Autorinnen und Autoren stellen die gesetzlichen Bestimmungen dar und erläutern verständlich und klar, wie diese in der Praxis anzuwenden sind – illustriert mit reichhaltigen Beispielen aus dem Alltag. Das Feedback zeigt, dass die Praxis die Unterstützung ausserordentlich schätzt.

Zum Schluss

Dank Unsere Aufgabe, darauf hinzuwirken, dass die Rechte der Personen, über die öffentliche Organe Daten bearbeiten, geachtet werden, 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 Datenschutzfragen vertrauensvoll an uns wenden;
— allen Mitarbeiterinnen und Mitarbeitern der Verwaltung, der öffentlichrechtlichen Anstalten und der Gerichte, die mithelfen, datenschutzkonforme Lösungen zu finden und umzusetzen;
— den Kolleginnen und Kollegen der «Kleeblatt-Dienststellen» für die unkomplizierte Zusammenarbeit;
— den Präsidien und Mitgliedern des Grossen Rates, des Büros, der Datenschutz-Delegation des Büros und der Kommissionen für ihr Interesse an unserer Arbeit und ihre wertvolle Unterstützung;
— den Volontärinnen Nadine Battilana und Ella Waldmann für ihre kritische Neugier und ihre aktive Mitarbeit und
— last but not least meinem Team – Markus Brönnimann, Sandra Husi, Carmen Lindner, Daniela Waldmeier und Barbara Widmer –, das mit unverändert grossem Engagement, mit spannenden Diskussionen und konstruktiven Anregungen unsere Arbeit bereichert und vorangebracht hat.

Beat Rudin, Datenschutzbeauftragter

1 Die in den Texten erwähnten Rechtsquellen und Materialien sind in einem Verzeichnis am Schluss des Berichts detailliert aufgeführt (Seiten 38 f.).

Themen

Thema 1 Berechtigungskonzepte, oder: Wer benötigt eigentlich welche Daten wozu?

Thema 2 Erfahrungen und Pendenzen nach zwei Jahren Öffentlichkeitsprinzip

Thema 1

Berechtigungskonzepte, oder: Wer benötigt eigentlich welche Daten wozu?

Personendaten dürfen soweit bearbeitet werden, als es zur Erfüllung der Aufgabe erforderlich ist. In einem Spital, in einer grossen Dienststelle wie der Kantonspolizei, der Sozialhilfe oder der IV-Stelle ist es deshalb unzulässig, wenn alle Mitarbeitenden auf alle Daten über die Klientinnen und Klienten zugreifen können.

Ausgangslage

Überraschung Noch immer sind zahlreiche Dateneigner überrascht, wenn ihnen aufgezeigt wird, wer alles in welchem Umfang auf «ihre» Daten zugreifen kann. Ihre Verantwortung für den datenschutzkonformen Umgang mit «ihren» Daten ist den wenigsten Dateneignern bewusst – kein Wunder, denn in der Regel stehen bei Informatikprojekten die fachlichen Aspekte im Vordergrund: Sicherheitsüberlegungen werden häufig auf die lange Bank geschoben, nur am Rande oder gar nicht berücksichtigt. Das hat auch zur Folge, dass die Frage, wer zu welchem Zeitpunkt und zu welchem Zweck auf welche Information zugreifen darf, in vielen Fällen nicht oder zu spät gestellt wird.

Kosten Dabei sollten gerade Fragen zur Sicherheit, zu welchen u.a. auch eine angemessene Zugriffsteuerung gehört, und zum zuverlässigen Betrieb einer Informatiklösung bereits zu Beginn eines Projektes grundlegend geklärt sein, im Verlauf des Projektes konkretisiert werden und im «laufenden Betrieb» nur verifiziert und nötigenfalls verbessert werden. Diverse Aspekte der Sicherheit haben eine Gemeinsamkeit: Ein umfassendes «Nachrüsten» der Sicherheitsmechanismen hat meist massive Kostenfolgen oder ist gar unmöglich.

Nutzen Von allfälligen Kostenfolgen bei Informatikprojekten abgesehen: Muss man sich diese Überlegungen wirklich machen, auch bei bereits bestehenden und schon etablierten Informatiksystemen? «Es ging doch bisher auch ohne», die Nutzung dieser Informatiksysteme funktioniert weitestgehend. Wieso sollte man nun plötzlich anfangen, Zuständigkeiten in sogenannten Berechtigungskonzepten zu definieren?

Vom «warum» …

Differenzierung Je komplexer die Aufgaben der Dienststellen bzw. die unterstützenden Informatiksysteme werden und je umfangreicher und vernetzter die Daten, welche zur Erfüllung dieser Aufgaben benötigt werden, umso schwieriger lässt sich die Frage nach den Zuständigkeiten und nach der Verantwortung für die einzelnen Datenbearbeitungen beantworten. Wer benötigt welche Daten für welche Aufgabenerfüllung? Und wer trägt letztendlich die Verantwortung für die Datenbearbeitungsvorgänge innerhalb der Dienststellen? In der Regel wird die Frage nach dem «wer benötigt die Daten wozu» ganz allgemein beantwortet: Die jeweilige Dienststelle bearbeitet ausschliesslich die Informationen, für deren Bearbeitung sie eine gesetzliche Grundlage hat. Da muss doch nicht wirklich noch weiter, d.h. nach einzelnen Mitarbeiterinnen und Mitarbeitern oder Funktionen innerhalb der Organisation differenziert werden. Oder etwa doch?

Arbeitsinstrument Überlegungen dazu, wer zu welchem Zweck auf welche Daten zugreifen darf, lohnen sich durchaus, wenn daraus ein sorgfältig durchdachtes sogenanntes Berechtigungskonzept als Arbeitsinstrument resultiert: Für die Mitarbeiterinnen und Mitarbeiter hat das Berechtigungskonzept den Vorteil, dass Unklarheiten vermieden und Kompetenzen geklärt werden können. Die Frage, ob jemand auf bestimmte Daten zugreifen darf, wurde bereits im Vorfeld (nämlich bei der Ausarbeitung des Berechtigungskonzepts) geklärt. Den Verantwortlichen, d.h. den jeweiligen Vorgesetzten oder gar den Dateneignern, zeigt das Berechtigungskonzept klar auf, wer wofür zuständig ist, und erlaubt damit eine sorgfältige und zielgerichtete Kontrolle der Datenbearbeitungsvorgänge – Verantwortung kann letztendlich nur wahrgenommen werden, wenn überhaupt bekannt ist, wofür man die Verantwortung trägt.

Gesetzliche Vorgaben Dass die Frage nach der Verantwortung für das Bearbeiten von Personendaten nicht völlig aus der Luft gegriffen ist, zeigt im Übrigen ein Blick ins Gesetz: § 9 IDG hält fest, dass ein öffentliches Organ nur jene Personendaten bearbeiten darf, welche es zur Aufgabenerfüllung (im Falle besonderer Personendaten: zwingend) benötigt. Rechtmässigkeit und Verhältnismässigkeit sind hier die Stichworte, welche es zu beachten gilt. § 6 IDG wiederum hält fest, dass die Verantwortung für den Umgang mit Informationen von demjenigen öffentlichen Organ zu tragen ist, welches die Informationen zur Erfüllung seiner gesetzlichen Aufgaben bearbeitet – eine Verantwortung, welche beispielsweise auch für die Informationssicherheit übernommen werden muss (§ 8 IDG). Bei den Anforderungen an die Systeme gilt es ausserdem zu beachten, dass durch angemessene Massnahmen die Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit, Zurechenbarkeit und Nachvollziehbarkeit (§ 8 Abs. 2 IDG) gewährleistet werden müssen. Die Steuerung der Zugriffe stellt für einige dieser Schutzziele eine zentrale Massnahme dar. Die Vorgaben von § 8 IDG zur Informationssicherheit beziehen sich nicht ausschliesslich auf den Datenschutz, diese sind für jegliche Bearbeitung von Informationen einzuhalten.

Der Fachbereich muss in die Lage versetzt werden, seine Verantwortung bei der Umsetzung, dem späteren Betrieb und der Kontrolle der effektiven Berechtigungen wahrzunehmen.

Lese-Kompass Die folgenden Ausführungen zeigen, wie Verantwortlichkeiten definiert und Berechtigungskonzepte ausgearbeitet werden können: In einem ersten Schritt wird das Thema allgemein und insbesondere für Personen, die nicht tagtäglich mit IT-Fragen konfrontiert sind, vorgestellt. Weiter in die Tiefe geht in einem zweiten Schritt der Abschnitt «Detail-Überlegungen». Der Transfer der Theorie in die Praxis erfolgt schliesslich auf Seite 10 f.: Anhand eines Klinikinformationssystems soll aufgezeigt werden, welche konkreten Überlegungen bei der Ausarbeitung eines Berechtigungskonzepts anzustellen und welche Lösungs-Varianten in Erwägung zu ziehen sind.

… zum «wie»

Begriff des Berechtigungskonzepts Was ist also unter einem Berechtigungskonzept zu verstehen? Die Terminologie ist oftmals uneinheitlich, überschneidet sich und lässt regelmässig auch grosse Interpretationsspielräume: So kann beispielsweise das Berechtigungskonzept als ein Bestandteil eines Identity and Access Management (IAM) verstanden werden. Wie auch immer das Konzept genannt und wo auch immer es eingeordnet werden soll – das Berechtigungskonzept, wie es im vorliegenden Fall interpretiert werden soll, muss einen Soll-Zustand skizzieren. Enthalten sein sollen die Voraussetzungen, Grundsätze, Regeln und Prozesse für eine sichere und gesetzeskonforme Steuerung der Zugriffe auf Systeme und der damit verarbeiteten Informationen.

Abstraktion Generell muss der Fachbereich in die Lage versetzt werden, seine Verantwortung bei der Umsetzung, dem späteren Betrieb und der Kontrolle der effektiven Berechtigungen wahrzunehmen. Das bedingt unter anderem, dass eine Abstraktionsebene («Flughöhe») gefunden werden muss, welche für die Umsetzung klar genug ist und den Fachbereich vor unnötigen Details «schützt».

Verschiedene Blickwinkel Ausserdem erscheint es nicht sinnvoll, ein Berechtigungskonzept ausschliesslich aus dem «Blickwinkel» Datenschutz zu erstellen. Auch Aspekte der Finanzen (ordnungsgemässe Rechnungslegung), der öffentlichen Sicherheit oder der Sicherheit Einzelner, der freien Meinungs- und Willensbildung der öffentlichen Organe, der Behinderung der Durchführung konkreter behördlicher Massnahmen o.a. können einen Einfluss auf den «Schutzbedarf» der Informationen haben.

Pflege Neben den effektiven Zugriffsberechtigungen ist auch den Prozessen für das Zuteilen, Anpassen und Entziehen von Berechtigungen die nötige Bedeutung beizumessen. Gerade bei Systemen mit «sensitiven» Informationen erscheint es zweckmässig, in einem klar definierten Prozess regelmässig zu überprüfen, ob das Berechtigungskonzept noch korrekt ist und die zugewiesenen Zugriffsberechtigungen den aktuellen Aufgabenverteilungen immer noch entsprechen. Diese Überprüfung obliegt dem Fachbereich und muss ebenfalls nachvollziehbar, d.h. protokolliert sein.

Detail-Überlegungen

Schutzbedarfsanalyse Die treibenden Faktoren bei der Gestaltung des Berechtigungskonzepts sind zweifelsohne der Schutzbedarf, die Grösse der Datensammlung und die Anzahl der User, welche diese Informationen bearbeiten. So erscheint es für ein System, auf welches fünf User Zugriff haben, nicht notwendig, ein umfassendes Berechtigungskonzept zu erstellen. Die weiteren Massnahmen zum Schutz der Informationen müssen selbstverständlich (abhängig vom Schutzbedarf, Bedrohungen und Schwachstellen) auch in einem System mit wenigen Usern berücksichtigt werden. >

Need-to-Know-Prinzip Ein wichtiger Grundsatz bei der Steuerung der Zugriffsrechte ist die Überlegung, dass jeder Benutzer (und auch jeder Administrator etc.) nur auf jene Datenbestände zugreifen und jene Programme ausführen können soll, die er für seine Arbeit (Aufgabe) auch wirklich benötigt (das «Need-to-Know-Prinzip»).

Regeln und Ausnahmen Sinnvoll erscheint es, mittels genereller Regeln (beispielsweise mit Rollenkonzepten) die Berechtigungen zu gruppieren und die Benutzer den vordefinierten Gruppen zuzuordnen. In vielen Fällen werden so jedoch nicht alle Berechtigungen vergeben werden können. Es wird immer wieder Fälle geben, bei welchen Mitarbeitende zeitlich beschränkt (Projekte, Stellvertretung usw.) oder unbeschränkt Aufgaben übernehmen, welche mit den definierten Gruppen nicht abgebildet werden können. Hier ist es wichtig, dass das Benutzerkonzept die Mechanismen und Regeln für diese Fälle ebenfalls definiert.

Organisationsmanagement Je komplexer die Struktur einer Dienststelle oder Abteilung, umso wichtiger wird auch die Verwaltung der Organisationszugehörigkeit der Mitarbeitenden. Wird diese Information zuverlässig bearbeitet, kann sie für die Zuweisung oder Verifizierung von Berechtigungen wertvolle Dienste leisten: Sie kann für Mechanismen bei (automatisierten) Stellvertretungsregeln verwendet werden, kann die Basis darstellen für die «prozessabhängige» Zuweisung von Zugriffsrechten (Zuweisung zu einer Gruppe/Abteilung satt Einzelperson) oder kann die Kontrolle der aktuellen Berechtigungen für Linienvorgesetzte vereinfachen.

Kontrollen als flankierende Massnahmen Unter Umständen ist eine angemessene Steuerung von Zugriffsrechten schlicht nicht möglich. In der Folge kann beispielsweise eine Benutzerin massiv mehr Daten einsehen, als sie für die Erfüllung ihrer Aufgabe benötigt. Die Zugriffe der Benutzerin auf die Daten müssen in solchen Fällen zwingend protokolliert und kontrolliert werden. Eine solche Auswertung sollte mit der Hilfe von Stichproben und somit nach einem definierten Auswahlverfahren erfolgen. Die so ausgewählten Stichproben müssen in der Folge mit den durchgeführten Aufgaben der Benutzerin verglichen werden. Diese Prüfung muss durch den Fachbereich erfolgen und muss ebenfalls nachvollziehbar sein. Das Protokollieren und Auswerten muss als ergänzende Massnahme zur Steuerung der Zugriffe und nicht als Ersatz betrachtet werden.

In der Praxis

Beispiel Klinikinformationssystem Versuchen wir, die Frage des Berechtigungskonzepts am (erfundenen) Beispiel eines Klinikinformationssystems (KIS) eines Spitals mit verschiedenen Kliniken zu illustrieren. Es leuchtet unschwer ein, dass nicht alle Mitarbeitenden in einem solchen Spital zur Erfüllung ihrer Aufgaben unbeschränkt lange auf alle Daten aller Patientinnen und Patienten zugreifen können müssen.

Differenzierungsmöglichkeiten Eine Differenzierung könnte beispielsweise nach verschiedenen Kriterien erfolgen:

— nach der organisatorischen Untereinheit, also nach Klinik oder Abteilung (Chirurgie, Orthopädie, Innere Medizin, Onkologie, Gynäkologie, Zytologie-Labor usw.);

— nach der Funktion der Mitarbeitenden (ärztliches Personal, Pflegepersonal, Laborpersonal, Administrativpersonal usw.);

— nach der Phase, in welcher die Datenbearbeitung stattfindet (Patientenaufnahme, stationäre Behandlung, vielleicht auch Operation, Rechnungstellung, abgeschlossene Behandlung usw.);

— nach der Art der Daten (Administrativdaten, medizinische Daten aus dem aktuellen Behandlungskontext, Pflegeanweisungen im aktuellen Behandlungskontext, medizinische Daten aus früheren Behandlungen, Aufenthaltsdaten[1], Labordaten usw.);

— nach der Zeitdauer seit einem Eintrag.

Aufgabenerfüllung im Fokus Das Berechtigungskonzept könnte danach beispielsweise so ausgestaltet sein, dass der Mitarbeiter in der Patientenaufnahme (im stationären Bereich) auf die Administrativdaten und Aufenthaltsdaten aller Patientinnen und Patienten greifen kann, die in den letzten zehn Jahren im Spital (in allen Kliniken) stationär behandelt worden sind – nicht aber auf irgendwelche medizinischen Daten. Das ärztliche Personal der Chirurgie kann beispielsweise auf die Daten der Patientinnen und Patienten greifen, die zurzeit in der Chirurgie-Klinik liegen oder innerhalb des letzten Jahres dort gelegen haben – auf die Daten, die in der Chirurgie angefallen sind, nicht aber standardmässig auf Daten aus anderen Kliniken und nicht auf die Rechnungsdaten. Das Pflegepersonal der Inneren Medizin kann zum Beispiel auf die Pflegeanweisungen bezüglich der Patientinnen und Patienten in der Inneren Medizin im aktuellen Behandlungskontext greifen, das Laborpersonal nur auf Labordaten.

Begründung Die Festlegung der Zugriffsberechtigungen ergibt sich primär aus dem Aufgabengebiet: Daraus ergibt sich die Begründung für die Gewährung und Einschränkung von Zugriffsrechten. Welche Daten benötigt die Oberärztin der Orthopädie-Klinik, damit sie ihre Aufgabe erfüllen kann, welche der Pfleger in der Intensivstation? In einem grossen Spital sind wohl feinere Einteilungen möglich, weil auch die Organisation feiner unterteilt sein dürfte. Dass bei bestimmten Funktionen engere Zugriffsberechtigungen möglich sind als bei anderen, ist nachvollziehbar: Der Narkosearzt oder die Röntgenärztin dürften Patientinnen und Patienten aus verschiedenen Kliniken behandeln. Der Orthopäde ist wohl auf Patientinnen und Patienten aus der Orthopädie beschränkt und braucht wohl weniger Daten von früheren Aufenthalten im HNO-Bereich. Die Oberärztin der Inneren Medizin hingegen ist für die Behandlung ihrer Patientinnen und Patienten möglicherweise auf deren Daten angewiesen ist, die bei früheren Aufenthalten in anderen Kliniken eingetragen worden sind. Selbstverständlich kann nicht der Datenschutzbeauftragte abstrakt das Berechtigungskonzept erstellen – er kann es höchstens plausibilisieren, indem er die Begründungen für die gewährten Berechtigungen hinterfragt.

Jeder Benutzer soll nur auf jene Datenbestände zugreifen und jene Programme ausführen können, die er für seine Arbeit (Aufgabe) wirklich benötigt («Need-to-Know-Prinzip»).

Anpassung an die Gegebenheiten Bei der Festlegung der Berechtigungen ist auch auf die konkreten Gegebenheiten Rücksicht zu nehmen. Wenn in einem kleineren Spital Chirurgie-Patientinnen und -Patienten regelmässig auch in der Inneren Medizin liegen, weil die Bettenstation der Chirurgie-Klinik voll belegt ist, dann kann die Steuerung der Zugriffsberechtigung logischerweise nicht streng dem «Ort» folgen, wo die Patientinnen und Patienten liegen. Das Kriterium der Klinik, in welcher jemand liegt, wäre hier nicht zweckdienlich; vielmehr ist in solchen Fällen durch andere Massnahmen sicherzustellen, dass die Berechtigung zum «Übergriff» kontrolliert wird, indem beispielsweise eine Meldung an eine Stelle geht, die dann nachprüft, ob der Patient in der Inneren Medizin, auf dessen Daten die Chirurgin zugegriffen hat, wirklich ein Chirurgie-Patient ist – oder andernfalls bestimmte Massnahmen ergreift.

Spezialfall Notfallstation Speziell zu regeln sind beispielsweise auch die Zugriffe in der Notfallstation: Wenn dort die Chirurgin Dienst leistet, behandelt sie natürlich auch Patientinnen und Patienten, die anschliessend in irgendeiner Klinik des Spitals weiterbehandelt werden. Ihre Funktion «Ärztin der Notfallstation» muss ihr dann möglicherweise auch erlauben, später nochmals auf die Patientendaten zu greifen, auch wenn diese inzwischen in einer anderen Klinik liegen.

VIP-Schaltung Auch Einschränkungen sind vorzusehen: Regelmässig muss ausgeschlossen werden, dass Mitarbeitende des Spitals auf die Daten über andere Mitarbeitende des Spitals greifen können – die Tatsache, dass eine Spitalmitarbeiterin beispielsweise eine Schwangerschaftsunterbrechung hat vornehmen lassen, geht die Kolleginnen und Kollegen nichts an. Normalerweise wird dazu eine sog. «VIP-Schaltung» vorgesehen: Die Daten solcher Personen – wie eben auch von anderen exponierten Personen (VIPs) – können dann nur von speziell bezeichneten Funktionen angerufen werden, etwa von Chefärztinnen oder Chefärzten.

Umgang mit Widerständen Nicht selten stösst die Einführung eines wirksamen Berechtigungssystems auf Widerstände. «Wir können unsere Aufgabe nicht erfüllen, wenn wir nicht auf alle Daten zugreifen können», ist ein Argument, das in diesem Zusammenhang häufig zu hören ist. Hier hilft vielleicht ein taktisches Vorgehen weiter: Die Zugriffsmöglichkeiten bleiben vorderhand bestehen, aber es werden die Zugriffsprotokolle beispielsweise nach zwei Jahren ausgewertet – und wenn sich dann herausstellt, dass auf die «unverzichtbaren Daten» nie zugegriffen wurde, dann kann man die Berechtigung entweder stillschweigend einschränken (und dann wohl auch konstatieren, dass niemand das bemerkt) oder mit diesen Zahlen gegenüber den Betroffenen belegen, dass es mit der «Unverzichtbarkeit» doch nicht so weit her ist.

Verantwortung Die Erstellung eines Berechtigungskonzepts verlangt eine sorgfältige Auseinandersetzung mit den Aufgaben, die ein öffentliches Organ zu erfüllen hat, und mit den Funktionen, welche die Mitarbeitenden dabei zu erfüllen haben. Ohne ein Berechtigungskonzept kann die Spital- oder Klinikleitung die Anforderung von § 6 IDG (Verantwortung) nicht erfüllen.

—

1 Zum Beispiel: «03.03.2009-11.03.2009: Orthopädie-Klinik / 14.11.2010-27.11.2010: Innere Medizin».

Thema 2

Erfahrungen und Pendenzen nach zwei Jahren Öffentlichkeitsprinzip

Zwei Jahre Öffentlichkeitsprinzip – Zeit, ein erstes Fazit zu ziehen: Wie geht die Verwaltung mit dem angestrebten Paradigmenwechsel um? Wird die Tragweite der (pro-)aktiven Seite der Informationstätigkeit korrekt eingeschätzt? Und wie steht es mit dem Verhältnis von Öffentlichkeitsprinzip und Amtsgeheimnis, insbesondere dann, wenn vertrauliche Informationen in den Medien auftauchen?

Paradigmenwechsel

IDG Mit dem Erlass des Informations- und Datenschutzgesetzes wurde ein Paradigmenwechsel angestrebt: der Wechsel vom Geheimhaltungsprinzip mit Öffentlichkeitsvorbehalt zum Öffentlichkeitsprinzip mit Geheimhaltungsvorbehalt. Es war von Anfang an klar, dass dieser Paradigmenwechsel nicht einfach mit dem Wirksamwerden des Gesetzes eintritt. Der Wechsel muss in den Köpfen stattfinden[1]. Nach zwei Jahren rechtfertigt sich ein Blick auf die Umsetzung.

Einzelne Aspekte Dabei sollen die folgenden Aspekte betrachtet werden:

— die Unterscheidung von reaktiver und (pro-) aktiver Informationstätigkeit,

— die Entwicklung im Bereich der reaktiven Informationstätigkeit, insbesondere auch zur Sichtbarkeit des Öffentlichkeitsprinzips auf der Website des Kantons Basel-Stadt,

— die Unterschätzung der Tragweite von § 20 IDG, der (pro-)aktiven Seite des Öffentlichkeitsprinzips,

— die Einschränkungen bei der (pro-)aktiven Informationstätigkeit,

— die Erfahrungen bezüglich der Veröffentlichung des Prüfberichts der Finanzkontrolle zu den Vorkommnissen bei den Basler Verkehrs-Betrieben (BVB) und schliesslich

— das Verhältnis zwischen Öffentlichkeitsprinzip und Amtsgeheimnis, insb. beim Whistleblowing.

Reaktive und (pro-)aktive Informationstätigkeit

Zwei «Seiten» Das Öffentlichkeitsprinzip hat zwei Ausprägungen:

— Die reaktive Seite: Jede Person hat das Recht auf Zugang zu den bei einem öffentlichen Organ vorhandenen Informationen[2]. Das öffentliche Organ ist verpflichtet, den entsprechenden Zugang zu gewähren – es *reagiert* also mit seiner Informationstätigkeit auf eine Initiative «von aussen».

— Die (pro-)aktive Seite: Das öffentliche Organ informiert hierbei von Amtes wegen die Öffentlichkeit über Angelegenheiten von allgemeinem Interesse in seinem Tätigkeitsbereich[3]. Das öffentliche Organ *agiert* «von sich aus»; die Initiative zur Bekanntgabe geht vom öffentlichen Organ aus.

Reaktive Informationstätigkeit

Geringe Gesuchszahlen Die reaktive Seite des Öffentlichkeitsprinzips war relativ schnell präsent in der Verwaltung. Vor allem die Journalistinnen und Journalisten hatten mitbekommen, dass das IDG mit seinen Regeln für den Informationszugang in Kraft getreten ist, und im einen oder anderen Fall das Recht auf Zugang zu den Informationen, die bei einem öffentlichen Organ vorhanden sind, geltend gemacht. Im ersten Jahr wurden in der Statistik der kantonalen Verwaltung 48[4], im zweiten Jahr 30 schriftliche Gesuche erfasst[5]. Im Berichtsjahr wurden vom Appellationsgericht als Verwaltungsgericht zwei Rekurse behandelt; in einem Fall wurde der Rekurs teilweise gutgeheissen[6], im anderen Fall abgewiesen[7].

Ängste unberechtigt Es fand also beileibe kein Ansturm auf die Verwaltung statt, der diese lahmgelegt hätte. Die entsprechenden Ängste[8] waren unberechtigt. Deshalb könnte das Öffentlichkeitsprinzip künftig noch «öffentlicher» gemacht werden.

Sichtbarkeit Ein Blick auf die Website des Kantons zeigt, dass Basel-Stadt durchaus noch Entwicklungspotenzial bezüglich der Umsetzung des Öffentlichkeitsprinzips besitzt. Der Weg zum Informationszugang ist eher versteckt – beim Bund beispielsweise kommt man auf den Websites aller Departemente und Bundesämter mit zwei Klicks über «Dokumentation» oder «Dienstleistungen» und «Zugang zu amtlichen Dokumenten» zu den entsprechenden Informationen. Wer es bös meint, könnte dieses «Verstecken» im Kanton als Ausdruck eines Unwillens gegenüber dem Öffentlichkeitsprinzip interpretieren. Vielleicht ist es aber auch Ausdruck der erst langsam wachsenden Einsicht in die Bedeutung des Öffentlichkeitsprinzips für ein Gemeinwesen, das seinen Auftraggebern (den Stimmbürgerinnen und Stimmbürgern) und seinen Geldgebern (den Steuerzahlerinnen und Steuerzahlern) Rechenschaft ablegen will (und muss). Es ist zu hoffen, dass mit der neuen Website des Kantons das Öffentlichkeitsprinzip endlich sichtbarer wird.

Beratung im Vorfeld Der Datenschutzbeauftragte wurde in etlichen Fällen zu Rate gezogen. Es wandten sich etwa öffentliche Organe, die mit Gesuchen konfrontiert, oder gesuchstellende Personen, die von der Verwaltung abgewiesen worden waren, an ihn. Nicht selten gelangten z.B. Medienschaffende zuerst mündlich an Verwaltungsstellen und erkundigten sich nach einem abschlägigen Bericht beim Datenschutzbeauftragten nach ihren Rechten oder nach seiner Beurteilung der mitgeteilten Abweisungsgründe. So hat er im Berichtsjahr beispielsweise gegenüber der Kantonspolizei klargestellt, dass der Zugang zu «Polizeidaten» nicht a priori eingeschränkt werden kann, sondern nur unter der Voraussetzung eines überwiegenden öffentlichen Interesses[9]. Darüber hinaus könnte auch die Polizei selber an bestimmten Auswertungen ihrer Daten ein Interesse haben, um damit ihre Tätigkeit steuern zu können – und gegebenenfalls diese anonymisierten Daten im Sinne des (pro-)aktiven Öffentlichkeitsprinzips auch von sich aus publizieren.

Beratung nach Verfügungserlass Ist einer gesuchstellenden Person vom ersuchten öffentlichen Organ bereits mitgeteilt worden, dass es in Betracht ziehe, ihr Gesuch ganz oder teilweise abzuweisen[10], dann kann sie den Erlass einer Verfügung verlangen und gegen diese bei der nächsthöheren Instanz und letztlich beim Appellationsgericht rekurrieren[11]. In dieser Phase klärt der Datenschutzbeauftragte die gesuchstellende Person nur noch über ihre Rechte auf. Von den Rekursinstanzen kann er aber als Fachorgan zur Stellungnahme eingeladen werden.

Vermittlung Bevor das öffentliche Organ eine Verfügung erlässt, kann der Datenschutzbeauftragte hingegen noch beraten und zwischen gesuchstellender Person und öffentlichem Organ zu vermitteln versuchen. Voraussetzung ist allerdings die Bereitschaft beider Seiten, sich auf eine Vermittlung einzulassen; ein Vermittlungsversuch ist zwecklos, wenn die eine Seite markiert, dass sie keinesfalls gewillt ist, von ihrer Position abzurücken[12]. Im Unterschied etwa zum Bund kennt der Kanton Basel-Stadt kein spezifisches Schlichtungsverfahren[13]; dort ist es dem öffentlichen Organ nicht freigestellt, sich auf das Verfahren einzulassen.

Während die reaktive Informationstätigkeit «in den Köpfen angekommen» ist, wird die Tragweite des § 20 IDG, der die (pro-)aktive Informationstätigkeit regelt, eher unterschätzt.

(Pro-)aktive Informationstätigkeit

Unterschätzt Während die reaktive Informationstätigkeit «in den Köpfen angekommen» ist, wird die Tragweite des § 20 IDG, der die (pro-)aktive Informationstätigkeit regelt, eher unterschätzt[14]. Inwieweit der mit dem IDG angestrebte Paradigmenwechsel – vom Geheimhaltungsprinzip mit Öffentlichkeitsvorbehalt zum Öffentlichkeitsprinzip mit Geheimhaltungsvorbehalt – schon stattgefunden hat, misst sich vor allem an der (pro-)aktiven Informationstätigkeit.

Von allgemeinem Interesse Voraussetzung für dieses Bekanntgeben von Informationen ist, dass es sich um eine «Angelegenheit von allgemeinem Interesse» handelt[15]. Das IDG versucht, diesem unbestimmten Rechtsbegriff mehr Konturen einzuhauchen. Das gelingt aber mit der Formulierung «Informationen, die Belange von öffentlichem Interesse betreffen und für die Meinungsbildung und zur Wahrung der demokratischen Rechte der Bevölkerung von Bedeutung sind» nur sehr begrenzt. Von allgemeinem Interesse sind – nach dem IDG-Ratschlag[16] – «Beschlüsse, wichtige >

Geschäfte, bedeutende Entscheide und Massnahmen, Ziele, Lagebeurteilungen, Planungen usw.». Ob eine Information von allgemeinem Interesse ist, muss das öffentliche Organ *im konkreten Fall* beurteilen. Dabei können nach dem Praxiskommentar zum IDG[17] die folgenden Aspekte berücksichtigt werden:

— die (demokratische) Funktion des öffentlichen Organs;

— die Wichtigkeit einer Information für die sachgerechte Meinungsbildung der Öffentlichkeit, insbesondere der Stimmberechtigten im Hinblick auf ihre demokratische Teilhabe;

— die politische Brisanz eines Geschäftes: Entscheide von Behörden in Angelegenheiten, die politisch sehr umstritten waren;

— die Bedeutung oder Tragweite eines Geschäftes für den Kanton oder eine Gemeinde, für eine Sachpolitik oder die Betroffenen;

— die Notwendigkeit, Falschmeldungen zu berichtigen;

— das (u.U. medial verstärkte) Interesse der Öffentlichkeit an einer Information.

Ob eine Information von allgemeinem Interesse ist, muss das öffentliche Organ im konkreten Fall beurteilen.

Entscheid Der Entscheid darüber, ob eine (pro-)aktive Informationstätigkeit angezeigt ist, obliegt primär dem öffentlichen Organ selber. Dabei sind in der kantonalen Verwaltung die Regeln zu beachten, die der Regierungsrat dazu zu erlassen hat[18]. Selbstverständlich können hierarchisch übergeordnete öffentliche Organe im Rahmen ihrer Weisungsbefugnis die Veröffentlichung anordnen oder selber vornehmen.

Einschränkungen bei der (pro-)aktiven Informationstätigkeit

Unterschiedliche Regelung Bezüglich der Einschränkungen besteht der einschneidendste Unterschied zwischen der reaktiven Informationstätigkeit nach § 25 IDG und der (pro-)aktiven nach § 20 IDG in der Anwendbarkeit von § 30 IDG: Dieser Paragraf, der verlangt, dass alle Personendaten ausnahmslos anonymisiert werden, gilt nur für den *Zugang* zu Informationen, nicht für die Bekanntgabe von Personendaten. Die reaktive Informationstätigkeit, das allgemeine Informationszugangsrecht, ist unter dem Titel «Zugang zu Informationen» in § 25 IDG im Kapitel «V. Informationszugangsrecht und andere Rechtsansprüche» geregelt und fällt damit unter die Anonymisierungspflicht. Die (pro-)aktive Informationstätigkeit ist hingegen in § 20 IDG im Kapitel «IV. Bekanntgabe von Informationen» geregelt, stellt deshalb nicht eine Zugangsgewährung, sondern eine *Bekanntgabe* dar und fällt damit nicht unter die *generelle Anonymisierungspflicht* beim Zugang zu Informationen nach § 30 IDG[19].

Einschränkungen Trotzdem untersteht auch die (pro-)aktive Informationstätigkeit Einschränkungen: Nach § 29 IDG hat das öffentliche Organ die *Bekanntgabe* von (wie auch den Zugang zu) Informationen im Einzelfall ganz oder teilweise zu verweigern oder aufzuschieben, wenn eine besondere gesetzliche Geheimhaltungspflicht oder ein überwiegendes öffentliches oder privates Interesse entgegensteht.

Gesetz Einer (pro-)aktiven Informationstätigkeit stehen also erstens *besondere gesetzliche Geheimhaltungspflichten* entgegen[20]. Zu den besonderen gesetzlichen Geheimhaltungsbestimmungen gehören insbesondere die besonderen Amtsgeheimnisse wie das Steuergeheimnis, das Stimmgeheimnis, das Sozialversicherungsgeheimnis usw., und die Berufsgeheimnisse wie das ärztliche Berufsgeheimnis oder das Anwaltsgeheimnis. Nicht dazu gehört das allgemeine Amtsgeheimnis nach dem Personalgesetz (PG), das im Gegenteil durch das IDG konkretisiert wird: Wenn Informationen nach den Vorschriften des IDG bekannt gegeben oder zugänglich gemacht werden dürfen, kann die Bekanntgabe oder Zugangsgewährung keine Verletzung des allgemeinen Amtsgeheimnisses nach § 19 PG darstellen, wie weiter unten noch genauer dargestellt wird. Eine Bekanntgabe von Informationen, die besonderen gesetzlichen Geheimhaltungspflichten unterstehen, ist auch nach § 20 IDG nur zulässig, wenn vorgängig eine Entbindung vom entsprechenden Geheimnis erfolgt.

Überwiegende Geheimhaltungsinteressen Einer (pro-)aktiven Informationstätigkeit stehen weiter *überwiegende öffentliche oder private Interessen* entgegen[21]. Wenn ein öffentliches oder privates Interesse i.S.v. § 29 Abs. 2 oder 3 IDG entgegensteht, hat das öffentliche Organ eine *Interessenabwägung im konkreten Fall* vorzunehmen: Es hat abzuwägen zwischen dem allgemeinen Interesse der Öffentlichkeit, i.S.v. § 20 Abs. 2 IDG informiert zu werden, und dem entgegenstehenden öffentlichen oder privaten Geheimhaltungsinteresse. Ein überwiegendes (öffentliches oder privates) Geheimhaltungsinteresse führt nicht automatisch dazu, dass überhaupt nicht informiert werden darf. Die Datenbekanntgabe ist ganz oder teilweise einzuschränken – soweit eben die Geheimhaltungspflicht oder das überwiegende Geheimhaltungsinteresse reicht.

Private Geheimhaltungsinteressen Auch wenn die generelle Anonymisierungspflicht nach § 30 IDG nicht besteht, kann die Anonymisierung das geeignete Mittel und erforderlich sein, um überwiegende private Geheimhaltungsinteressen zu schützen. Besteht beispielsweise nach der Beurteilung des verantwortlichen öffentlichen Organs ein überwiegendes allgemeines Interesse an Untersuchungsberichten zu besonderen Vorkommnissen, so ist trotzdem zu prüfen, ob alle Informationen und insbesondere alle Namen bekannt gegeben werden oder inwieweit im konkreten Fall ein überwiegendes privates Interesse dem entgegensteht. Ein überwiegendes privates Interesse wird nach § 23 IDV auf jeden Fall bei besonderen Personendaten[22] vermutet. Allerdings geniessen Mitarbeitende der öffentlichen Verwaltung, die in Erfüllung einer öffentlichen Aufgabe gehandelt haben, insbesondere solche in höheren Führungspositionen, den Schutz der Privatsphäre nicht im gleichen Umfang wie «private» Dritte. Sie müssen sich die in Ausübung ihrer öffentlichen Funktion vertretenen Ansichten und Positionen anrechnen lassen, weshalb sie in diesem Zusammenhang nicht den Schutz ihrer Privatsphäre geltend machen können[23].

Anonymisierung Zur Frage, wie eine Anonymisierung bei Dokumenten wirksam vorgenommen werden kann, hat der Datenschutzbeauftragte ein Merkblatt veröffentlicht[24].

Der BVB-Prüfbericht der Finanzkontrolle

Konkreter Anwendungsfall Kurz vor Jahresende hat die späte Publikation des Prüfberichtes der Finanzkontrolle zu den Vorkommnissen bei den Basler Verkehrs-Betrieben (BVB) hohe Wellen geworfen. Ab Mittwoch, 11. Dezember 2013, war der Vorsteher des Bau- und Verkehrsdepartements (BVD) gewillt, den Bericht zu publizieren. Die Finanzkontrolle berief sich aber vehement darauf, dass das Finanz- und Verwaltungskontrollgesetz eine Publikation strikt untersage, was der BVD-Vorsteher in verschiedenen am Donnerstag, 12. Dezember 2013, erteilten und am Freitag, 13. Dezember 2013, in den Medien publizierten Interviews wiedergab. Auf die Fehlinterpretation der Geheimhaltungsbestimmung wies erst der Datenschutzbeauftragte am Donnerstagabend hin, als er vom Leiter der Finanzkontrolle angerufen wurde.

Ein überwiegendes (öffentliches oder privates) Geheimhaltungsinteresse führt nicht automatisch dazu, dass überhaupt nicht informiert werden darf.

Nur kein Zugang nach § 25 IDG Das Finanz- und Verwaltungskontrollgesetz (FVKG) hält fest: «Die Berichte der Finanzkontrolle und die ihnen zugrunde liegenden Materialien sind nicht öffentlich zugänglich im Sinne von § 25 Abs. 1 des Informations- und Datenschutzgesetzes»[25]. Der Ausschluss betrifft damit eben nur den Zugang nach § 25 IDG, also die Zugangsgewährung auf Gesuch hin. Der Auftraggeber der Spezialprüfung (das BVD) oder der Regierungsrat – nicht jedoch die Finanzkontrolle oder die geprüfte Stelle – können aber gestützt auf § 20 IDG unter der Voraussetzung, dass es sich nach ihrer Beurteilung um eine «Angelegenheit von allgemeinem Interesse» handelt, die (pro-)aktive Veröffentlichung anordnen. Dabei kann sich das allgemeine Interesse auch in einer Häufung von Zugangsgesuchen manifestieren[26].

Anonymisierung Der Hinweis stiess beim BVD auf offene Ohren. Das allgemeine Interesse war in diesem Fall zweifellos gegeben. Am Freitag, 13. Dezember 2013, hat das BVD den Bericht samt zahlreichen Beilagen öffentlich zugänglich gemacht. Zwischen dem Entscheid über die Publikation am Freitagmorgen und dem Aufschalten am Freitag gegen Abend mussten die fast 150 Textseiten daraufhin überprüft werden, ob zum Schutz privater Interessen Textstellen abzudecken sind. Nachdem sich die Anonymisierungen in einer ersten Version als überwindbar herausgestellt haben, wurde durch das BVD am gleichen Abend noch eine wirksam anonymisierte Fassung aufgeschaltet. >

Präjudiz? Dass in diesem Fall ein Prüfbericht der Finanzkontrolle (pro-)aktiv veröffentlicht worden ist, heisst nicht, dass dies künftig bei allen Berichten der Finanzkontrolle so ist. Auch in Zukunft wird jeweils sorgfältig zu prüfen sein, ob es sich bei einem Bericht tatsächlich um eine «Angelegenheit von allgemeinem Interesse» handelt.

Öffentlichkeitsprinzip und Amtsgeheimnis

Konkretisierung Inwieweit steht das Amtsgeheimnis der Informationstätigkeit öffentlicher Organe entgegen? «Soweit nach dem IDG eine Information zugänglich ist, kann die dadurch erlaubte Zugangsgewährung logischerweise ebenso wenig eine Verletzung des (allgemeinen) Amtsgeheimnisses sein wie das Bekanntgeben von Informationen, zu dem ein Sachgesetz verpflichtet oder ermächtigt. In diesem Sinne konkretisieren die Bestimmungen des IDG das (allgemeine) Amtsgeheimnis»[27]. Wird damit das Amtsgeheimnis aufgehoben?

Es liegt nicht im Belieben einzelner Mitarbeitenden, Dritte mit Informationen zu bedienen.

Zuspiel an Medien Die Tatsache, dass offenbar mindestens zwei Medienredaktionen über den BVB-Bericht der Finanzkontrolle verfügt haben, bevor dieser vom BVD zugänglich gemacht wurde, oder dass (im Februar 2014) die Basler Zeitung über Informationen zum «Schwedenreisli» (oder scheinbar zum «Schwedenreisli»[28]) verfügt hat, legt die Vermutung nahe, dass Mitarbeitende der Verwaltung bestimmten Medien Informationen zugespielt haben. Lässt sich das mit dem Öffentlichkeitsprinzip rechtfertigen?

Zuständigkeit Das IDG weist die Aufgabe der (pro-)aktiven und der reaktiven Informationstätigkeit jedem *öffentlichen Organ* zu[29] – nicht jeder einzelnen Mitarbeiterin oder jedem einzelnen Mitarbeiter[30]. Für den Entscheid, welche Informationen auf Gesuch hin zugänglich gemacht oder (pro-)aktiv bekannt gegeben werden sollen, ist die Leitung eines öffentlichen Organs zuständig. Selbstverständlich kann sie die Erfüllung dieser Aufgabe an bestimmte untergeordnete Stellen oder Personen delegieren. Generell bleiben somit gerade für die Medienarbeit die Kommunikationsbeauftragten zuständig, es liegt nicht im Belieben einzelner Mitarbeitenden, Dritte mit Informationen zu bedienen. Handelt es sich bei den Informationen um solche, die dem Amtsgeheimnis unterstehen, dann ist die Bekanntgabe oder das Zugänglichmachen durch nicht dafür zuständige Personen eine Verletzung des Amtsgeheimnisses.

Meldung von Missständen Was aber, wenn Mitarbeitende der Meinung sind, es bestünden in der Verwaltung gravierende Missstände, die nicht behoben werden? Müssen sie sich dann einfach ducken und schweigen – oder dürfen sie damit an die Öffentlichkeit gehen, beispielsweise die Informationen einer Zeitungs- oder Fernsehredaktion zuspielen? Sicher nicht einfach gestützt auf das Öffentlichkeitsprinzip. Der Kanton Basel-Stadt hat im Jahr 2013 für die Meldung von Missständen eine Whistleblowing-Regelung getroffen[31]: «[1]Mitarbeitende sind berechtigt, der kantonalen Ombudsstelle Missstände zu melden. (…) [3]Zulässige Meldungen verstossen nicht gegen die Verschwiegenheitspflicht gemäss § 19 Personalgesetz und stellen keine Amtsgeheimnisverletzung im Sinne von Art. 320 Strafgesetzbuch dar. [4]Mitarbeitende dürfen aufgrund von zulässigen Meldungen im Anstellungsverhältnis nicht benachteiligt werden»[32]. Ein Missstand liegt vor, wenn gegen rechtliche Bestimmungen verstossen wird[33]. Zulässig sind nur Meldungen, die in gutem Glauben erfolgen[34], d.h. wenn die oder der Meldung erstattende Mitarbeitende aus objektiver Sicht davon ausgehen darf, dass tatsächlich ein Missstand vorliegt und die Meldung nicht der Erlangung persönlicher Vorteile dienen soll[35].

Whistleblowing-Regelung Nach dieser Regelung muss sich also eine Person, die einen Missstand melden will, an dessen Beseitigung die Allgemeinheit als solche ein Interesse hat, an die *Ombudsstelle* wenden. Nicht erlaubt ist es, direkt an die *Öffentlichkeit* zu gelangen. Ob die oder der Mitarbeitende nach der Meldung an die Ombudsstelle die Öffentlichkeit informieren darf, hängt vom Tätigwerden der Ombudsstelle ab: «Ist die Meldung über einen Missstand an die kantonale Ombudsstelle erfolgt und ist eine Frist von zehn Arbeitstagen ohne Reaktion seitens der kantonalen Ombudsstelle abgelaufen, können Mitarbeitende an die Öffentlichkeit gelangen, sofern ihre Meldung im guten Glaube und im öffentlichen Interesse erfolgt.

Mit der Whistleblowing-Verordnung wird die Möglichkeit geschaffen, auf die Beseitigung von Missständen hinzuwirken, wenn Hinweise verwaltungsintern scheinbar ungehört verhallen.

Leitet die kantonale Ombudsstelle hingegen ein Verfahren ein oder findet sie keine Anzeichen für das Vorliegen des gemeldeten Missstandes, ist die Information der Öffentlichkeit unzulässig»[36]. Mit dieser Regelung ermöglicht der Kanton Basel-Stadt den Mitarbeitenden, auf die Beseitigung von Missständen hinzuwirken, wenn ihre Hinweise verwaltungsintern scheinbar ungehört verhallen. Gleichzeitig wird aber auch klar, dass es nicht angeht, Informationen über (vermeintliche oder tatsächliche) Missstände den Medien zuzuspielen, wenn die Voraussetzungen der Whistleblowing-Verordnung nicht erfüllt sind. Ein solches Zuspielen ist unzulässig und kann eine strafbare Verletzung des Amtsgeheimnisses darstellen.

—

1 TB 2011, 19.
2 § 25 IDG.
3 § 20 Abs. 1 IDG.
4 TB 2012, 6 f., 30.
5 TB 2013, 26.
6 Urteil des Appellationsgerichts des Kantons Basel-Stadt als Verwaltungsgericht vom 1. März 2013 (VD.2012.153) gegen einen Entscheid des Erziehungsdepartements vom 10. Juli 2012 betreffend Verweigerung der Einsichtnahme in die Traktandenliste zur Sitzung der Kommission für Jugendfragen vom 14. Juni 2012.
7 Urteil des Appellationsgerichts des Kantons Basel-Stadt als Verwaltungsgericht vom 19. Juni 2013 (VD.2012.179) gegen eine Verfügung des Finanzdepartements vom 3. August 2012 betreffend Gesuch um Zugang zu Informationen betreffend Basler Kantonalbank.
8 Vgl. TB 2011, 19 f.
9 Im Sinne von § 29 Abs. 2 IDG.
10 § 33 Abs. 2 IDG, vgl. dazu PK-IDG/BS-Waldmeier 2014, § 33 N 2 ff.
11 § 33 Abs. 4 IDG; vgl. dazu PK-IDG/BS-Waldmeier 2014, § 33 N 9 ff.
12 So PK-IDG/BS-Schilling 2014, § 44 N 26.
13 Art. 13 BGÖ. Vgl. dazu Ratschlag 08.0637.01 (IDG-Ratschlag), 50 und 52 (zu § 34 E-IDG), und Bericht 08.0637.02 (IDG-Bericht der JSSK), 21 f.
14 Abgesehen von der (pro)aktiven Veröffentlichung der Regierungsratsbeschlüsse seit dem Inkrafttreten des IDG.
15 § 20 Abs. 1 und 2 IDG; vgl. dazu PK-IDG/BS-Rudin 2014, § 20 N 34 ff.
16 IDG-Ratschlag, 36.
17 PK-IDG/BS-Rudin 2014, § 20 N 36 ff., jeweils mit Beispielen.
18 Vgl. dazu den gestützt auf § 20 Abs. 4 IDG erlassenen Leitfaden Öffentlichkeitsarbeit.
19 PK-IDG/BS-Rudin 2014, § 20 N 8 f., § 30 N 2 und N 45.
20 Vgl. dazu PK-IDG/BS-Rudin 2014, § 29 N 11 ff.
21 Vgl. dazu PK-IDG/BS-Rudin 2014, § 29 N 18 ff. und N 39 ff.
22 § 3 Abs. 4 IDG; vgl. dazu PK-IDG/BS-Rudin 2014, § 3 N 33 ff.
23 Weitere Details in PK-IDG/BS-Rudin 2014, § 29 N 44 ff.
24 <http://www.dsb.bs.ch/dms/dsb/download/DSB-BS_Merkblatt_Anonymisierung_-technisch-/DSB-BS_Merkblatt–Anonymisierung_%28technisch%29.pdf>.
25 § 16 Abs. 5 FVKG.
26 PK-IDG/BS-Rudin 2014, § 20 N 10.
27 PK-IDG/BS-Rudin 2014, § 29 N 17.
28 Es handelte sich bei der Liste der Teilnehmerinnen und Teilnehmer aufgrund der aufgeführten Namen offensichtlich nicht um Angaben zur entsprechenden Studienreise nach Stockholm.
29 § 20 Abs. 1 bzw. § 25 Abs. 1 i.V.m. §§ 32 ff. IDG.
30 Vgl. dazu auch den Leitfaden Öffentlichkeitsarbeit, insb. 5.
31 § 19a PG; Whistleblowing-Verordnung.
32 § 19a Abs. 1 Satz 1, Abs. 3 und 4 PG.
33 § 2 Abs. 1 Whistleblowing-Verordnung.
34 § 19a Abs. 1 Satz 2 PG.
35 § 2 Abs. 2 Whistleblowing-Verordnung.
36 § 4 Abs. 1 und 2 Whistleblowing-Verordnung.

Aus dem Alltag

Einblicke in die Beratungstätigkeit

Einblicke in die Kontrolltätigkeit

Statistik

Aus dem Alltag

Einblicke in die Beratungstätigkeit

Der Datenschutzbeauftragte wird laufend mit neuen und herausfordernden Fragen konfrontiert. Der Einblick in die Beratungstätigkeit bietet Ihnen einen Eindruck davon: Von der Frage, ob Handnotizen vom Zugangsrecht zu den eigenen Personendaten ausgenommen sind, über die Bekanntgabe von Abschiedsbriefen an Versicherungen bis hin zu Vernehmlassungsantworten und der intensiven Zusammenarbeit mit anderen Datenschutzbeauftragten – der Aufgabenstrauss des Datenschutzbeauftragten ist bunt.

Keine Sonderbehandlung für sog. Handnotizen

Unter Handnotizen versteht man kurze, meist – aber nicht zwingend – handschriftlich verfasste Aufzeichnungen, die dem Verfasser als Gedächtnisstütze dienen sollen. Als solche enthalten sie regelmässig Personendaten. Der Datenschutzbeauftragte musste feststellen, dass in der Verwaltung nicht selten die Auffassung vertreten wird, dass solche Handnotizen nicht unter den Anspruch auf Zugang zu den eigenen Personendaten (§ 26 IDG) fallen, da sie ein persönliches Arbeitsinstrument darstellen würden. Diese Ansicht ist jedoch nicht zutreffend. Überwiegende private oder öffentliche Interessen sowie besondere gesetzliche Geheimhaltungspflichten stellen die einzigen Einschränkungsgründe für den Zugang zu den eigenen Personendaten dar (§ 29 IDG); «persönliche» Arbeitsinstrumente zählen nicht zu den Einschränkungsgründen nach § 29 IDG. In der Vernehmlassungsvorlage zum IDG war – angelehnt an die Regelung im früheren Datenschutzgesetz des Kantons Basel-Landschaft – noch eine entsprechende Ausnahme vom Geltungsbereich vorgesehen («wenn eine Person Informationen bearbeitet, um ausschliesslich für sich selbst über ein persönliches Arbeitsmittel zu verfügen»). Sie wurde vom Regierungsrat wieder gestrichen, nachdem in der Vernehmlassung die Befürchtung geäussert wurde, sie führe zu einer «doppelten Buchhaltung»[1]. Das Argument, dass die Verfasserin oder der Verfasser der Handnotiz ein privates Interesse daran habe, seine bzw. ihre Handnotizen unter Verschluss zu halten, weil beispielsweise Wertungen darin enthalten seien, ist aus datenschutzrechtlicher Sicht nicht haltbar: Auch Werturteile können so formuliert werden, dass sie nicht beleidigend oder verletzend sind; sind die Werturteile in angebrachtem Tonfall formuliert, so kann kaum geltend gemacht werden, Notizen, die grundsätzlich zur «amtlichen» Aufgabenerfüllung erstellt wurden, unterstünden nicht dem datenschutzrechtlichen Zugangsrecht[2].

Datenschutzkonzepte der Listenspitäler

Aufgrund der Leistungsvereinbarungen des Kantons mit den «Listenspitälern»[3] sind diese jeweils verpflichtet, ein Datenschutzkonzept zu erarbeiten. Die Ausgestaltung der Datenschutzkonzepte kann ganz unterschiedlich ausfallen: Der Haupttext kann auf der konzeptuellen Ebene verbleiben und durch Detailregelungen für jeden Bereich gesondert in Merkblättern konkretisiert werden, oder bereits selbst konkrete Handlungsanweisungen für die jeweiligen Situationen enthalten. Einige dieser Datenschutzkonzepte wurden dem Datenschutzbeauftragten bereits vorgelegt und konnten in der Diskussion mit den verantwortlichen Stellen inhaltlich verbessert werden.

Fussgängerzählgerät

Zu Beginn des Jahres 2013 wurden vom Bau- und Verkehrsdepartement an verschiedenen Stellen der Basler Innenstadt graue Kästchen montiert, welche die vorbeigehenden Fussgängerinnen und Fussgänger zählen, um einen Überblick über ihr Mobilitätsverhalten zu erhalten. Bei einer Vor-Ort-Vorführung wurde dem Datenschutzbeauftragten erklärt, dass das Gerät die vorbeigehenden Wärmequellen zählt, welche sich um mindestens +/-1°C von der Umgebungstemperatur unterscheiden. Dabei spiele es keine Rolle, ob die Wärme von einem grossen Hund, einem Menschen oder einer anderen Wärmequelle stammt. Zwei dicht nebeneinander gehende Personen werden damit als eine Wärmequelle erfasst und folglich als ein Fussgänger bzw. eine Fussgängerin gezählt. Jede Nacht werden die Zähldaten (Anzahl erfasste Wärmequellen pro Zeiteinheit) sodann an eine zentrale Stelle gesendet, um dort ausgewertet zu werden. Da das Gerät keine Wärmebild- oder sonstigen Aufnahmen macht, welche Rückschlüsse auf bestimmte Personen zulassen würden, fällt die Registrierung dieser Daten nicht unter den Anwendungsbereich des IDG. Alarmistische Medienberichte («Überwachung der Fussgänger») konnten nicht bestätigt werden.

Auswertung von Telefonverbindungsdaten

Auch im vergangenen Jahr wurde der Datenschutzbeauftragte angefragt, den ZID Aufträge für die Detailauswertung von Telefonverbindungsdaten zu erteilen. Allerdings kamen die Anfragen dieses Jahr vorwiegend von Personen, die einen eigenen Anschluss besitzen und eine Übersicht über ihre Kostenzusammensetzung wollten. Eine solche Auswertung ist unproblematisch, soweit der Anschluss ausschliesslich auf die anfragende Person lautet und sie die Daten tatsächlich für ihren eigenen Bedarf möchte. Da nicht mit Sicherheit ausgeschlossen werden kann, dass nicht doch der Arbeitgeber Druck auf die betroffene Person ausübt, ist die ersuchende Person in jedem Fall auf das ihr zustehende Recht auf Anonymisierung der privaten Telefonnummern hinzuweisen und über den gewöhnlichen Ablauf[4] einer solchen Detailauswertung zu informieren.

Die Abwägung, ob sich eine Ärztin über die Autonomie ihrer Patientin, die den Täter nicht anzeigen will, hinwegsetzen soll oder nicht, bleibt der jeweiligen Fachperson überlassen.

Aushändigung eines Abschiedsbriefes an eine Versicherung?

Dass Versicherungen an die Kantonspolizei gelangen und von dieser einen spezifischen Rapport (oder sogar eine ganze Sammlung von Rapporten) herausverlangen, um ihre Leistungspflicht zu beurteilen, ist nichts Neues[5]. Die Kantonspolizei fragt in diesen Fällen üblicherweise nach, wozu denn die Rapporte konkret benötigt würden bzw. welche Fragen sich für die Versicherung stellen würden – und gibt dann gestützt auf die Ausführungen der Versicherung nur diejenigen Informationen bekannt, die beispielsweise zur Berechnung der Leistungspflicht tatsächlich geeignet und erforderlich sind (Stichwort: Verhältnismässigkeit). So weit so gut. Neu war im Jahr 2013 jedoch, dass sogar Abschiedsbriefe von Personen, die einen Selbstmordversuch unternommen hatten, von den Versicherungen «benötigt» wurden. Die sachlich und neutral abgefassten Polizei-Rapporte schienen den Versicherungen nicht zu genügen, vielmehr wollten die Versicherungen sogar Kenntnis von den Beweggründen der verstorbenen oder allenfalls nur verletzten Personen nehmen. Dass im Falle eines erfolglosen Selbstmordversuchs die betroffene Person selbst zu ihren Beweggründen hätte gefragt werden können oder dass der Polizeirapport allenfalls genügend und insbesondere sachliche Informationen geliefert hätte, wurde von den Versicherungen nicht in Erwägung gezogen. Der Datenschutzbeauftragte unterstützte die Kantonspolizei auch bei der Beurteilung dieser Problematik darin, mittels konkreter Fragen von der jeweiligen Versicherung in Erfahrung zu bringen, wofür welche Informationen benötigt würden, und so eine verhältnismässige Bekanntgabe von Personendaten zu ermöglichen.

Schulung «Häusliche Gewalt»

Die Koordinationsstelle «Halt Gewalt» lud den Datenschutzbeauftragten dazu ein, anlässlich eines Round Table-Gesprächs zum Thema Informationsaustausch in Fällen häuslicher Gewalt zu referieren und gemeinsam mit den Vertreterinnen und Vertretern von Opferhilfe, Frauenhaus, Männerbüro, Triangel, Frauenklinik, Migrationsamt und Staatsanwaltschaft (um nur einige zu nennen) Fragen der Zusammenarbeit zu diskutieren. Dabei kristallisierte sich heraus, dass es den diversen Stellen in der Regel nicht an den gesetzlichen Grundlagen mangelt, um in Fällen häuslicher Gewalt Informationen mit anderen Stellen austauschen zu dürfen. Vielmehr stellt sich jeweils die Frage, ob von dieser Möglichkeit auch Gebrauch gemacht und ein allenfalls über lange Zeit hinweg aufgebautes Vertrauensverhältnis zwischen Ärztin, Betreuer oder Sozialarbeiterin und Opfer unter Umständen schwer belastet werden soll – und wenn ja, in welchem Umfang die Informationen weitergegeben werden sollen. Eine Antwort, die für jeden Sachverhalt gilt, kann es auf diese Fragen nicht geben: Die Abwägung, ob sich eine Ärztin über die Autonomie ihrer Patientin, die den Täter nicht anzeigen will, hinwegsetzen oder ob ein Sozialarbeiter das Vertrauensverhältnis zu seinem Schützling belasten möchte und vom Melde- bzw. Anzeigerecht Gebrauch machen möchte, bleibt letztlich immer den jeweiligen Fachpersonen überlassen. Die langjährige Erfahrung der verschiedenen Institutionen im Umgang mit von Häuslicher Gewalt betroffenen Personen dürfte beim Entscheid, ob eine Anzeige gemacht werden soll oder nicht, eine wertvolle Stütze sein – ebenso wie der Austausch untereinander und mit dem Datenschutzbeauftragten.

Mein Körper gehört mir!

Das Projekt «Mein Körper gehört mir!» ist ein interaktives Ausstellungsprojekt der Stiftung Kinderschutz Schweiz zur Prävention von sexueller Gewalt gegen Kinder im Primarschulalter. In Gruppenarbeiten sollen die Kinder für die Problematik sexueller Gewalt sensibilisiert werden, womit natürlich auch damit zu rechnen ist, dass Kinder Spontanaussagen zu erlebten sexuellen Übergriffen machen. Der Datenschutzbeauftragte wurde vom Kinder- und Jugenddienst (KJD) angefragt, wie mit derartigen Äusserungen umgegangen werden sollte. Es ging darum, ein Verfahren zu >

finden, welches den Bedürfnissen der Kinder gerecht wird, die verantwortlichen Betreuungspersonen in ihrem (sozial-)pädagogischen Auftrag unterstützt und gleichzeitig die datenschutzrechtlichen Vorgaben bezüglich der Bekanntgabe von besonderen Personendaten berücksichtigt. Gemeinsam mit dem KJD wurde schliesslich folgender Ablauf festgelegt: Macht ein Kind eine Spontanaussage, so füllt die Moderatorin bzw. der Moderator ein entsprechendes Protokoll aus und leitet dieses an die für das Projekt zuständige Fachperson beim KJD weiter. Nach einer ersten Triage kontaktiert diese Fachperson die Klassenlehrperson, mit der die Situation besprochen wird: Allenfalls gab es bereits Hinweise, welche aber nicht richtig «eingeordnet» werden konnten. Sollte sich unmittelbarer Handlungsbedarf herauskristallisieren, so werden die notwendigen Schritte von der Fachperson eingeleitet. Sehen Klassenlehrperson und Fachperson (vorerst) keinen Handlungsbedarf, so wird eine anonymisierte Version des Protokolls an den Schulpsychologischen Dienst und an Triangel weitergeleitet. Allenfalls sehen diese Stellen aufgrund ihres grossen Erfahrungsschatzes Interventionsbedarf und können dann wiederum mit dem KJD Kontakt aufnehmen. Dieses Vorgehen berücksichtigt sowohl das Wohl der betroffenen Kinder wie auch die Vorgaben des Datenschutzrechts.

Das Einwohneramt verfügt derzeit über keine gesetzliche Grundlage, welche eine Datenbekanntgabe zu Forschungs- oder Umfragezwecken erlauben würde.

Zugang zu PCs und Mail-Accounts verstorbener Mitarbeitender

Verstirbt eine Mitarbeiterin oder ein Mitarbeiter unerwartet, so stellt sich für die Vorgesetzten die Frage, wie mit dem E-Mail-Account der oder des Mitarbeitenden zu verfahren ist. Im Jahr 2013 wurde der Datenschutzbeauftragte mit dieser Fragestellung (und ähnlichen) kontaktiert. Kommt die vorgesetzte Stelle zum Schluss, dass der Zugriff auf den E-Mail-Account für die Aufgabenerfüllung des Amtes notwendig sei, und können im Account vermutete Informationen nicht bei bereits bekannten Kontakten eingeholt werden, so gilt es verschiedene Punkte zu beachten: Der Zugriff auf den Account sollte nur unter Wahrung des Vier-Augen-Prinzips vonstatten gehen. Alternativ bietet es sich auch an, eine neutrale externe Stelle mit der Sichtung der E-Mails nach bestimmten Kriterien zu beauftragen. E-Mails, die einen privat anmutenden Betreff aufweisen, dürfen nicht geöffnet werden. Bei Unsicherheiten kann die Absenderin oder der Absender kontaktiert und nach allenfalls geschäftlichen Anliegen gefragt werden. Die gesichtete und gesicherte Geschäftskorrespondenz ist auszudrucken – der E-Mail-Account muss danach gelöscht werden und darf nicht «zur weiteren Benutzung» aktiviert bleiben. Der Datenschutzbeauftragte steht für Fragen und die Ausarbeitung von spezifischen Vorgehensweisen zur Verfügung. Er hat auch angeregt, die erforderlichen Prozesse zu definieren, damit möglichst rasch nach dem Ableben und ohne Einblick in den E-Mail-Account eine Abwesenheitsmeldung aufgeschaltet werden kann, damit nicht weitere E-Mails eingehen und wie eben beschrieben behandelt werden müssen.

Alle Jahre wieder: Adressbekanntgaben für Studien

Auch im Jahr 2013 wurde der Datenschutzbeauftragte mit der Frage konfrontiert, ob das Einwohneramt Adressdaten Forschungsinstitutionen bekanntgeben darf. Die Forschungsinstitutionen verwenden dann die Adressdaten, um potentielle Forschungs- oder Umfrageteilnehmerinnen oder teilnehmer zu kontaktieren. Das Problem ist bekannt[6]: Die Bekanntgabe der Adressdaten durch die Einwohnerkontrolle an die Forschungsinstitutionen stellt eine personenbezogene Bekanntgabe von Personendaten im Sinne von § 21 IDG dar; erst in der zweiten Phase, der Auswertung der Fragebögen oder Messresultate, handelt es sich um ein Bearbeiten zu einem nicht personenbezogenen Zweck. Das Einwohneramt verfügt derzeit über keine gesetzliche Grundlage, welche eine Datenbekanntgabe zu Forschungs- oder Umfragezwecken erlauben würde. Auch die teilweise in anderen Kantonen praktizierte Subsumtion dieser Datenbekanntgaben unter den Anwendungsbereich der Bestimmungen über die Datenbekanntgabe zu nichtpersonenbezogenen Zwecken (analog § 22 IDG), ist aus rechtstaatlicher Sicht nicht haltbar[7]. Bereits im Jahr 2012 hat der Datenschutzbeauftragte daher eine Ergänzung des Aufenthaltsgesetzes um eine entsprechende Norm vorgeschlagen – die Regelung soll mit dem neuen Statistikgesetz eingeführt werden[8]. In Anbetracht dessen, dass der Vorschlag derzeit pendent ist, interveniert der Datenschutzbeauftragte auf Zusehen hin nicht gegen die Bekanntgabe von Adressdaten durch das Einwohneramt für die Kontaktaufnahme für Umfragen oder Forschungsprojekte. Sollte die Bestimmung jedoch keinen Eingang in das

Aufenthaltsgesetz finden, so würde es dem Einwohneramt an den gesetzlichen Grundlagen für eine Bekanntgabe fehlen – der Datenschutzbeauftragte müsste dann die Datenbekanntgaben untersagen (§ 47 IDG).

Mit dem Verzicht auf eine Regelung im UKBB-Vertrag wurde die Chance verpasst, den von Datenbearbeitungen im UKBB betroffenen Personen die erforderliche Rechtssicherheit zu gewähren.

Adressbekanntgaben zum Zweiten

Die Thematik der Adressbekanntgaben wurde im Jahr 2013 erweitert: Wie sollen Personen, die für Präventionsprogramme und -massnahmen[9] gewonnen werden sollen, kontaktiert werden? Die bereits vorgeschlagene Ergänzung des Aufenthaltsgesetzes sieht die Datenbekanntgabe lediglich für Studienzwecke (bzw. zur Kontaktaufnahme mit potentiellen Studienteilnehmer[inne]n) vor. Der Datenschutzbeauftragte hat dem Regierungsrat einen Vorschlag zur Ergänzung des bereits vorgeschlagenen § 30a Aufenthaltsgesetz vorgelegt, der in der Folge in die laufende Beratung des Geschäftes in der grossrätlichen Justiz, Sicherheits- und Sportkommission eingebracht wurde[10].

Videoüberwachung

Wie in den vergangenen Jahren beschäftigten zahlreiche Fragestellungen rund um die Videoüberwachung den Datenschutzbeauftragten auch im aktuellen Berichtsjahr. Acht Vorabkontrollen wurden initiiert, zudem wurden unter anderem Fragen zur Zuständigkeit des kantonalen Datenschutzbeauftragten im Falle privater Videoüberwachung[11], zur Verwendung von Werbevideos (beispielsweise der Einwohnerkontrolle oder des Stadtmarketings), zur Zulässigkeit von Baufortschrittskameras oder des Einsatzes von sog. Quadrocoptern diskutiert. Auch der Umstand, dass Polizistinnen und Polizisten bei ihren Einsätzen immer häufiger von Passantinnen oder Passanten bzw. betroffenen Personen mit dem Smartphone gefilmt werden und die Aufzeichnungen im Web landen, wurde ausgiebig diskutiert.

Follow-up Regelung der Internetnutzungs-Überwachung

Der in den vergangenen Jahren mit Vertretern des Zentralen Personaldienstes (ZPD), der Fachstelle Informatik und Organisation (FIO) und der Zentralen Informatikdienste (ZID) erarbeitete Entwurf einer Verordnung zur Überwachung der Nutzung der Internet- und E-Mail-Dienste (IÜV) wurde 2013 in die interne Vernehmlassung geschickt. Die daraufhin eingegangen Inputs und geführten Gespräche haben dazu geführt, dass der Entwurf zurückgenommen wurde. Die Thematik soll nun im grösseren Zusammenhang mit der vom Datenschutzbeauftragten bereits in der Vergangenheit monierten ungenügenden bzw. teilweise unklaren Regelung der Nutzung von Informatikmitteln geregelt werden

Follow-up UKBB-Staatsvertrag

Der Datenschutzbeauftragte hat, wie auch die Aufsichtsstelle Datenschutz des Kantons Basel-Landschaft, im Jahr 2012 zur Revision des Vertrags vom 16. Februar 1988 zwischen den Kantonen Basel-Stadt und Basel-Landschaft über das Universitäts-Kinderspital beider Basel Stellung genommen[12]. Der im Rahmen der Vernehmlassung gemachte Vorschlag, den Vertragsentwurf um einen § 23a mit dem Wortlaut «Für den Umgang mit Informationen gilt das Informations- und Datenschutzrecht des Sitzkantons» wurde vom Regierungsrat nicht übernommen[13]. Mit dem Verzicht auf eine klare Regelung im Vertrag wurde die Chance verpasst, den von Datenbearbeitungen im UKBB betroffenen Personen die erforderliche Rechtssicherheit zu gewähren: Streng genommen ist das UKBB bei der Behandlung von Kindern aus dem Kanton Basel-Stadt ein baselstädtisches öffentliches Organ – bei Kindern aus dem Kanton Basel-Landschaft aber ein basellandschaftliches, weil der Landkanton die öffentliche Aufgabe «stationäre Gesundheitsversorgung von Kindern» dem UKBB übertragen hat. Eltern könnten nun geltend machen, eine datenschutzrechtliche Streitfrage müsste nach dem Baselbieter IDG entschieden und nach dem Baselbieter Verfahrensrecht den Baselbieter Rechtsmittelinstanzen vorgelegt werden. Mit der Regelung des anwendbaren Datenschutzrechts im Staatsvertrag hätten solche Situationen vermieden werden können. Auf Intervention des Datenschutzbeauftragten hat die Gesundheits- und Sozialkommission des Grossen Rates diese Frage thematisiert und in ihrem Bericht explizit festgehalten: «Die Kommission erachtet die Regelung der Fragen des Datenschutzes als äusserst wichtig, um Unklarheiten bei allfälligen gerichtlichen Verfahren zu verhindern. Da neu der Sitz des UKBB >

einzig im Kanton Basel-Stadt ist, macht es am meisten Sinn, dass das Datenschutzrecht des Sitzkantons – also das Gesetz über die Information und den Datenschutz des Kantons Basel-Stadt – gültig ist, soweit nicht übergeordnetes Recht zur Anwendung gelangt»[14].

Vernehmlassungen

Dem Datenschutzbeauftragten wurden im Jahr 2013 18 Vernehmlassungen zur Stellungnahme vorgelegt. Besondere Erwähnung sollen im Folgenden die Vernehmlassung zum Krebsregistrierungs-Gesetz des Bundes und zum neuen Kinder- und Jugendgesetz sowie die Vernehmlassungen zu den Schengen-Weiterentwicklungen finden:

Da nur wenige kantonale Krebsregister über die notwendigen Rechtsgrundlagen verfügen, befürwortet der Datenschutzbeauftragte die Schaffung einer bundesweiten Rechtsgrundlage.

Vorentwurf für ein Krebsregistrierungsgesetz des Bundes

Im vergangenen Jahr hat der Datenschutzbeauftragte zum Vorentwurf für ein Bundesgesetz über die Registrierung von Krebserkrankungen Stellung genommen. Bei der Registrierung von Krebserkrankungen fallen sehr sensitive Personendaten an, für deren Bearbeitung aus datenschutzrechtlicher Sicht eine hinreichend bestimmte und demokratisch legitimierte Gesetzesgrundlage erforderlich ist. Da nur wenige kantonale Krebsregister über eine solche Rechtsgrundlage verfügen und auch die Regelung im Kanton Basel-Stadt[15] den rechtstaatlichen Anforderungen nicht genügt, befürwortet der Datenschutzbeauftragte die Schaffung einer bundesweiten Rechtsgrundlage. Der im Vorentwurf vorgesehene Zweck – die vollständige Erfassung aller Krebsfälle in der Schweiz – kann jedoch mit der dafür vorgesehenen Meldepflicht mit Widerspruchsrecht nicht erreicht werden, zumal nach der vorgeschlagenen Lösung die Daten derjenigen Personen, die widersprochen haben, via Datenabgleich mit der Todesursachenstatistik des Bundesamtes für Statistik wieder in den Gesamtdatensatz einfliessen sollen. Deshalb hat der Datenschutzbeauftrage vorgeschlagen, bei der Erhebung des Minimaldatensatzes auf das Widerspruchsrecht gänzlich zu verzichten, sofern es sich dabei wirklich um den minimal notwendigen Datensatz handelt und mit dem neuen Gesetz eine hinreichend bestimmte Rechtsgrundlage geschaffen wird. Als weiterer Kritikpunkt erscheint es dem Datenschutzbeauftragten unzweckmässig, wie in der Vorlage vorgesehen die AHVN13 als Personenidentifikator zu verwenden. Er hat stattdessen vorgeschlagen die ePatientendossiernummer als Identifikationsmerkmal einzusetzen. Nach den neusten Informationen möchte der Bundesrat jedoch aufgrund der besseren Akzeptanz am Konstrukt der Meldepflicht mit Widerspruchslösung festhalten. Ebenso bleibt es voraussichtlich bei der AHVN13 als eindeutigem Identifikator.

Kinder- und Jugendgesetz

Das Gesetz über die Jugendhilfe, welches noch aus dem Jahr 1984 stammte, bedarf dringend einer Anpassung an den weitreichenden gesellschaftlichen Wandel der vergangenen dreissig Jahre. Der Entwurf zum Kinder- und Jugendgesetz (KJG) wurde im Rahmen der kantonalen Vernehmlassung auch dem Datenschutzbeauftragten vorgelegt. Dieser hielt in seiner Stellungnahme fest, dass dem Gesetzesentwurf die aus rechtstaatlicher Sicht erforderliche Normdichte fehlt, um als genügende gesetzliche Grundlage für die mit der Kinder- und Jugendarbeit bzw. –hilfe einhergehenden Eingriffe in die Persönlichkeitsrechte der Betroffenen zu dienen. Aus diesem Grund hatte der Datenschutzbeauftragte dringend empfohlen, die Aufgabennormen dahingehend zu konkretisieren, dass für die involvierten Stellen klar ist, wer welche Aufgaben zu erfüllen hat. Ausserdem sollten die Verantwortlichkeiten bereits im KJG festgelegt oder allenfalls auf Verordnungsstufe konkretisiert werden. Schliesslich schlug der Datenschutzbeauftragte vor, die Regelung zur Datenbearbeitung den zu konkretisierenden Aufgabennormen anzupassen und die Schweigepflichtsregelung dem gesamtlegislativen Kontext von § 19 PG sowie § 4 Abs. 3 E-Staatsbeitragsgesetz[16] anzupassen.

Schengen-Weiterentwicklungen

Der Datenschutzbeauftragte konnte dieses Jahr zu sieben Schengen-Weiterentwicklungen Stellung nehmen. Sechs Weiterentwicklungen boten wenig Brisanz – die Weiterentwicklung des Dublin-Besitzstands war jedoch aus rechtstaatlicher Sicht umso problematischer[17]: In Eurodac verzeichnete Fingerabdrücke sollen neu auch für Strafermittlungen genutzt werden können. Diese Zweckänderung bzw. -erweiterung ist aus rechtstaatlicher Sicht ausgesprochen fragwürdig: Werden Fingerabdrücke im Rahmen eines Asylverfahrens abgenommen und in Eurodac eingespiesen, so stellt ein Abgleich der Fingerabdrücke im Strafverfolgungskontext eine Zweckänderung dar. Auch wenn diese Zweckänderung in einer Verordnung und damit in einer Rechtsgrundlage von genügender Normstufe[18] vorgesehen ist, so ist der Eingriff in die Persönlichkeitsrechte der betroffenen Personen gravierend und

nach der vom Datenschutzbeauftragten vertretenen Auffassung auch aus rechtstaatlichen Überlegungen nicht verantwortbar.

Das Medieninteresse an Datenschutzfragen hat im Berichtsjahr deutlich zugenommen.

Medienanfragen

Das Medieninteresse an Datenschutzfragen hat im Berichtsjahr deutlich zugenommen: 27 mal wurde der Datenschutzbeauftragte von Zeitungen und Radiostationen um Stellungnahmen zu unterschiedlichsten Themen gebeten: Vom Smart Metering der IWB über das «intransparente Ausspionieren von Arbeitssuchenden durch das RAV», von der Jugendbefragung 2013 über die Verwendung von Google Maps bei den GPS-Fussfesseln bis hin zur Frage, ob Sponsoringverträge der Universität Basel nach dem Öffentlichkeitsprinzip zugänglich sein sollten – die Medien und die Öffentlichkeit haben Datenschutz- und Informationsrechtliche Themen im Jahr 2013 deutlich intensiver aufgegriffen und verfolgt.

Schulungen

Auch in diesem Jahr war das Bedürfnis nach bereichsspezifischen informations- und datenschutzrechtlichen Schulungen gross: So führte der Datenschutzbeauftragte beispielsweise eine spezifische Schulung für die Staatsanwaltschaft Basel-Stadt durch und informierte auch die Mitarbeitenden der Kantonspolizei auf dem Kannenfeldposten über aktuelle Fragestellungen. Anlässlich des Round Table «Häusliche Gewalt» führte der Datenschutzbeauftragte eine Schulung zum Thema Informationsaustausch durch[19]. Die Schulung «Das IDG kurz erklärt» konnte zweimal durchgeführt werden, und auch das Modul «Datenschutz, Amtsgeheimnis und Archivierung», welches Teil des Lehrplans der KV-Lehre in der öffentlichen Verwaltung ist, durfte wurde wieder angeboten. Zum Ende des Jahres hin wurden schliesslich gemeinsam mit der Koordinationsstelle IDG Schulungen zur Führung des in § 24 IDG vorgesehenen Verzeichnisses über die Verfahren, bei denen Personendaten bearbeitet werden, durchgeführt.

Zusammenarbeit

Kantonsinterne und übergreifende Zusammenarbeit stellte auch im Jahr 2013 ein wesentliches Element der Tätigkeit des Datenschutzbeauftragten dar. So engagierte sich der Datenschutzbeauftragte nicht nur im privatim-Büro und innerhalb der privatim-Arbeitsgruppen Gesundheit, Schule und ICT, sondern war auch in den Arbeitsgruppen eHealth Standards & Architektur und eGRIS des Bundes vertreten. Auf kantonaler Ebene konnte der Datenschutzbeauftragte sein Fachwissen in der Basler Expertengruppe «Datenschutz im Gesundheitswesen» einbringen. Weiterhin intensiv beschäftigt hat den Datenschutzbeauftragten auch die Revision des Datenschutzrechts auf EU-Ebene[20] und die Kontrolle der Umsetzung des Schengen-Besitzstandes (SCH-Eval) in der Schweiz, welche im Jahr 2014 durchgeführt wird und detailliert vorbereitet werden muss[21]. Die Interessen der Kantone in der Datenschutz-Arbeitsgruppe der Konferenz der Kantone, in der SCH-Eval-Vorbereitungsgruppe und in der Schengen Coordination Group (SCG), welche die Joint Supervisory Authority of Schengen (JSA) abgelöst hat, werden ebenfalls vom Datenschutzbeauftragten des Kantons Basel-Stadt vertreten. Damit ist auch sichergestellt, dass die laufenden Entwicklungen im Bereich des Datenschutzes in der EU konzentriert und zeitnah beurteilt werden können.

—

1 Ratschlag 08.0637.01 (IDG-Ratschlag), 19.
2 Ratschlag 08.0637.01 (IDG-Ratschlag), 42 f.
3 TB 2012, 21 f.
4 TB 2010, 14 f.
5 TB 2010, Fall 5, 30.
6 TB 2011, 11 f.
7 Ausführlich dazu PK-IDG/BS-Husi 2014, § 30a AufenthG N 3 ff.
8 TB 2012, 24. Vgl. Ratschlag 13.0634.01 (Statistikgesetz), 30 f. und inzwischen auch Bericht 13.0634.02 (Statistikgesetz), 3 und 11 ff.
9 Auslöser für die Diskussion war die Debatte um das Mammografie Screening Programm, siehe dazu <http://www.klbb.ch/de/mammografie_screening_programm_kanton_basel_stadt/> (zuletzt besucht am 15.04.2014).
10 Vgl. Bericht 13.0634.02 (Statistikgesetz), 3 und 11 ff.
11 Dazu TB 2013, Fall 3, 36.
12 TB 2012, 25.
13 Siehe dazu die wenig überzeugende Begründung im Ratschlag zur Revision des Staatsvertrages zwischen den Kantonen Basel-Stadt und Basel-Landschaft über das Universitäts-Kinderspital beider Basel (Kinderspitalvertrag) vom 16. Februar 1998, 12.0626.01, 6.
14 Bericht 12.0626.02 der Gesundheits- und Sozialkommission vom 10. April 2013 zum Ratschlag Revision des Staatsvertrages zwischen den Kantonen Basel-Stadt und Basel-Landschaft über das Universitäts-Kinderspital beider Basel (Kinderspitalvertrag) vom 16. Februar 1998, 7.
15 § 56 Abs. 1 lit. c GesG.
16 Geschäftsnummer 11.1792, abrufbar unter <http://www.grosserrat.bs.ch/de/geschaefte-dokumente/datenbank?such_kategorie=1&content_detail=200105724> (zuletzt besucht am 15.04.2014).
17 Ausführlich dazu Sandra Husi, Die Propheten in der Wüste haben Recht!, digma 2013, 160 ff.
18 Je schwerer der Eingriff in die Grundrechte, umso höhere Anforderungen sind an die den Eingriff vorsehenden Rechtsgrundlagen zu stellen; SGK-BV-Schweizer 2008, Art. 36, N 12 ff.
19 Siehe vorne 21.
20 TB 2012, 26 f.
21 Siehe dazu sogleich 28 f.

Aus dem Alltag

Einblicke in die Kontrolltätigkeit

Der Datenschutzbeauftragte – so sieht es § 44 lit. a IDG vor – kontrolliert nach einem autonom aufzustellenden Prüfprogramm die Anwendung der Bestimmungen über den Umgang mit Informationen. Im Jahr 2013 wurden vier Datenschutz-Audits bzw. –Assessments abgeschlossen und bereits weitere begonnen. Ausserdem wurde eine Schengen-Kontrolle durchgeführt und das Follow-up zur Schengen-Kontrolle des Jahres 2010/2011 abgeschlossen. Die Zusammenarbeit mit dem Staatsschutzkontrollorgan funktioniert weiterhin einwandfrei.

Übersicht

Im Jahr 2013 wurden vier Datenschutz-Audits bzw. -Assessments abgeschlossen – doppelt so viele wie im Jahr zuvor:

- Datenschutz-Audit bei der Sozialhilfe Basel-Stadt,
- Datenschutz-Assessment im Bereich der IKT-Basisleistungen (MailBS, FileBS),
- Schengen-Kontrolle bei der Jugendanwaltschaft und
- Schengen-Kontrolle beim Migrationsamt.

Begonnen wurden zwei Kontrollen:

- Datenschutz-Audit bei der IV-Stelle Basel-Stadt und
- Datenschutz-Assessment im Bereich der Passwort-Qualität.

Schliesslich wurden bei der Staatsanwaltschaft und bei der Kantonspolizei die Follow-Ups zu den Schengen-Kontrollen der Jahre 2010/2011 durchgeführt.

Datenschutz-Audit bei der IV-Stelle Basel-Stadt

Der Datenschutzbeauftragte hat im Berichtsjahr bei der IV-Stelle ein Audit begonnen. Im Zentrum des Audits stehen die Zugriffe auf die sensitiven und umfassenden Informationen innerhalb der Fachanwendung OSIV, welche zur Erfüllung ihrer gesetzlichen Aufgabe bearbeitet werden. Diese Anwendung wird in sieben Kantonen eingesetzt. Der Datenschutzbeauftragte arbeitet diesbezüglich mit den Datenschutzbeauftragten dieser Kantone zusammen.

Datenschutz-Audit bei der Sozialhilfe Basel-Stadt

Das Datenschutz-Audit bei der Sozialhilfe wurde im Jahr 2013 abgeschlossen. Bei der Sozialhilfe wird das Thema Datenschutz aktiv bearbeitet, sie ist sich der diesbezüglichen Problematik, welche sich aus ihren Aufgaben ergibt, bewusst und hat bereits diverse Massnahmen umgesetzt. Innerhalb des vom Datenschutzbeauftragten definierten Umfangs der Prüfung wurde unter anderem folgender Handlungsbedarf festgestellt:

— Es gibt Optimierungsbedarf bei der angemessenen Definition und Zuteilung der Verantwortlichkeit. Insbesondere bei den Informatik-Leistungserbringern innerhalb und ausserhalb der Sozialhilfe Basel-Stadt erscheint die Definition und Zuteilung als noch nicht optimal. In diesem Bereich sollte aus Sicht des Datenschutzes der klaren Zuweisung von Verantwortlichkeiten und dem Austausch von Informationen zur Steuerung (Überwachung) der Informatikleistungen die angemessene Beachtung geschenkt werden.

— Bezüglich der eingesetzten Fachanwendung Tutoris sind im Bereich des Datenschutzes und der Informationssicherheit Mängel bei der Vergabe von angemessenen Berechtigungen sowie beim fehlenden Löschen (Vernichten) von Informationen festgestellt worden.

Alle Feststellungen und entsprechenden Empfehlungen wurden von der Sozialhilfe akzeptiert, die entsprechenden Massnahmen sollen umgesetzt werden.

Assessment im Bereich der IKT-Basisleistungen

Im Bereich der beiden IKT-Basisleistungen MailBS und FileBS hat der Datenschutzbeauftragte festgestellt, dass es Unklarheiten bezüglich des angemessenen Einsatzes dieser beiden Services gibt. Insbesondere fehlen klare Angaben zum gewährleisteten Schutzniveau. Auch sind keine angemessenen Weisungen oder Anleitungen zum sicheren Umgang mit den beiden IKT-Basisleistungen für die Benutzer bekannt. Die geprüften Weisungen erscheinen nicht mehr auf dem neuesten Stand und decken ausschliesslich einen Teilaspekt ab. Die Abteilung Informatiksteuerung und Organisation (ISO, ehemals Fachstelle für Informatik und Organisation, FIO) arbeitet auf der Basis des sich in Erarbeitung befindlichen, ganzheitlichen Information Security Management Systems (ISMS.BS) zu Handen der Konferenz für Organisation und Informatik (KOI, ehemals Informatik-Konferenz, IK) angemessene Massnahmen zur Behebung dieser Mängel aus.

Assessment im Bereich der Passwort-Qualität

Der Datenschutzbeauftragte hat unterstützt durch einen externen Spezialisten die Passwort-Qualität beim Active Directory (AD) untersucht. Dieses System wird von allen Benutzerinnen und Benutzern der Verwaltung genutzt (im Minimum zur Anmeldung am PC und beispielsweise bei FileBS/MailBS/Kalender). Es ist davon auszugehen, dass die Feststellungen bezüglich der Passwort-Qualität auf andere Systeme übertragbar sind. Bei der Prüfung musste festgestellt werden, dass Mängel bestehen: Viele der Passwörter konnten innert kürzester Zeit «erraten» werden. Der simulierte Angriff wurde «offline» gemacht, was bedeutet, dass der Schutzmechanismus des AD, welcher nach ein paar falschen Versuchen den Zugang einer Benutzerin oder eines Benutzers vorübergehend sperrt, für den Test umgangen wurde. Dennoch zeigte sich Handlungsbedarf bei der Passwort-Policy (Vorgabe und Umsetzung), der Sensibilisierung von Mitarbeitenden, bei den Prozessen der Benutzerverwaltung (Identity- und Access-Management [IAM]) sowie bei der Verantwortlichkeit (Dateneigner). Abgeschlossen wird dieses Assessment erst im Jahr 2014.

Staatsschutz

Der Datenschutzbeauftragte hat entsprechend dem vereinbarten modus operandi[1] die an ihn herangetragenen Anfragen an das Staatsschutzkontrollorgan weitergeleitet.

Die durchgeführten Prozessprüfungen haben ergeben, dass Datenbearbeitungen in N-SIS für die jeweilige Aufgabenerfüllung grundsätzlich verhältnismässig und zweckmässig erfolgen.

SIS-Kontrollen

Noch im Herbst 2012 startete der Datenschutzbeauftragte seine SIS-Kontrollen bei der Jugendanwaltschaft und beim Migrationsamt. Geprüft werden sollte, ob die beiden Stellen das Schengener Informationssystem entsprechend den europarechtlichen und nationalen Vorgaben nutzten. Das «Kick-off-meeting» fand am 19. Dezember 2012 statt, die Kontrollen selbst wurden im Januar und Februar 2013 durchgeführt. Dabei wurden die Logfiles der während einer Woche von der Jugendanwaltschaft und dem Migrationsamt getätigten N-SIS[2]-Abfragen ausgewertet und auf Auffälligkeiten hin geprüft: Fanden Abfragen zu ungewöhnlichen Uhrzeiten statt? Fanden viele Anfragen innert kürzester Zeit statt? Wurden – zumindest von aussen betrachtet – ungewöhnliche Namenskombinationen usw. abgefragt? Die jeweiligen Mitarbeiterinnen und Mitarbeiter wurden in Gesprächen zu ihren Logfile-Auszügen befragt und hatten die Möglichkeit, ihren Umgang mit dem SIS zu präsentieren. Folgende Punkte konnten festgehalten werden:

— Die Datenbearbeitung in N-SIS durch die Jugendanwaltschaft und das Migrationsamt erfolgt im Rahmen der gesetzlichen Grundlagen. Abfragen und Ausschreibungen in N-SIS sowie dem vorgelagerten schweizerischen Fahndungssystem RIPOL[3] erfolgen zum Zweck der jeweiligen Aufgabenerfüllung. Die durchgeführten Prozessprüfungen haben ergeben, dass Datenbearbeitungen in N-SIS für die jeweilige Aufgabenerfüllung geeignet und erforderlich sind und damit grundsätzlich verhältnismässig und zweckmässig erfolgen.

— Der Prozess zur Definition und zur Verwaltung der N-SIS Zugriffsrechte erscheint insgesamt angemessen, um sicherzustellen, dass das Berechtigungskonzept wirksam angewendet und umgesetzt wird. >

— Aufgrund der Analyse der Logfiles wurden je vier Benutzerinnen bzw. Benutzer der Jugendanwaltschaft und des Migrationsamts zu den getätigten N-SIS-Abfragen persönlich befragt. Bis auf eine unrechtmässige Abfrage zu privaten Zwecken (es handelte sich bei den erfragten Daten jedoch lediglich um Informationen zum eigenen Auto), erfolgten alle Abfragen zur jeweiligen Aufgabenerfüllung und konnten ohne Weiteres begründet werden. Im Rahmen der Prüfung wurde aber festgestellt, dass sich die Mitarbeiterinnen und Mitarbeiter kaum bewusst sind, dass Abfragen im SSO[4]-Portal des Bundes (insbesondere RIPOL) im Hintergrund automatisch eine N-SIS-Abfrage auslösen. N-SIS-Abfragen werden kaum je bewusst vorgenommen. Der Datenschutzbeauftragte hat daher vorgeschlagen, im Rahmen des Eintritts neuer Mitarbeitender sowie wiederkehrend alle zwei Jahre eine N-SIS-Schulung durchzuführen.

Die SIS-Kontrolle bei der Jugendanwaltschaft und beim Migrationsamt kann damit als ausgesprochen positiv und zufriedenstellend beurteilt werden.

Expertinnen und Experten aus anderen Schengen-Staaten sowie der EU werden prüfen, ob die Schweiz die Schengener Vorschriften korrekt anwendet.

Ebenfalls durchgeführt wurden Follow-Ups zu den im Jahr 2010/2011 durchgeführten SIS-Kontrollen bei der Kantonspolizei und der Staatsanwaltschaft: Damals wurde zum einen festgestellt, dass interne (und insbesondere aktuelle) Listen der SIS-Nutzerinnen und -Nutzer und der entsprechenden Zugriffsberechtigten fehlten und dass für Schulungen mit dem SIS das «Original-SIS» genutzt wurde (das Schulungs-Tool, so die Begründung, sei wenig praxistauglich, eine Verbesserung des Lehrmittels obliegt jedoch fedpol). Die Listen der SIS-Nutzerinnen und -Nutzer werden von den IT-Verantwortlichen nun jährlich auf ihre Aktualität hin überprüft und auch den jeweiligen Abteilungsleiterinnen bzw. -leitern zur Gegenprüfung vorgelegt. Nichts verändert hat sich jedoch beim Schulungstool – im Gegenteil: Mittlerweile funktioniert nicht einmal mehr der Link auf das Schulungstool. Die Schulungsverantwortlichen der Kantonspolizei sind sich der Problematik jedoch bewusst und weisen zu Beginn der Schulungen nicht nur darauf hin, dass mit «scharfen» Daten gearbeitet werde, sondern informieren die Zuhörerinnen und Zuhörer auch über ihre datenschutzrechtliche Verantwortung und machen darauf aufmerksam, dass der Datenschutzbeauftragte im Rahmen der SIS-Kontrollen durchaus auch sie zu einer Datenbearbeitung befragen könnte. Der Datenschutzbeauftragte wird das Thema Schulungstool einmal mehr in der Schengen-Koordinationsgruppe der schweizerischen Datenschutzbeauftragten aufgreifen.

Die Schengen-Koordinationsgruppe der schweizerischen Datenschutzbeauftragten hat sich im Jahr 2013 einmal zu einer Sitzung getroffen, aber auch in diesem Jahr keine koordinierte Kontrolle durchgeführt[5].

Schengen-Kontrolle der EU in der Schweiz

Die Schweiz wird im Jahr 2014 zum zweiten Mal das Schengen-Evaluierungsverfahren durchlaufen. Expertinnen und Experten aus anderen Schengen-Staaten sowie der EU werden prüfen, ob die Schweiz die Schengener Vorschriften korrekt anwendet. Untersucht werden insbesondere die Bereiche Datenschutz, Aussengrenzschutz (Flughäfen), Schengener Informationssystem, polizeiliche Zusammenarbeit und Visa. Die Schengen-Evaluierung findet in drei Etappen statt. In einer ersten Phase verschaffen sich die Expertinnen und Experten einen Überblick über die Umsetzung und Anwendung der Schengen-Vorschriften in der Schweiz. Neben einer Präsentation der Schweiz und ihrer Rechtslandschaft soll den Expertinnen und Experten dieser Überblick anhand eines 200 Fragen fassenden Katalogs ermöglicht werden. In einer zweiten Phase werden vier Evaluierungsbesuche in der Schweiz sowie ein Evaluierungsbesuch bei zwei Schweizer Vertretungen im Ausland durchgeführt. Die Besuche sind den Bereichen Polizeizusammenarbeit, Datenschutz, Visumsausstellung, Aussengrenzen sowie Schengener Informationssystem gewidmet. Die Expertenteams zeigen dabei allfällige Mängel auf und können Empfehlungen und Verbesserungsvorschläge erarbeiten. Dazu verfassen sie Evaluierungsberichte, die erneut in der Ratsarbeitsgruppe «SCH-Eval» besprochen und gutgeheissen werden. Die Schweiz wird

in einer dritten Phase in der Ratsarbeitsgruppe über allfällige Massnahmen, die sie aufgrund der Empfehlungen getroffen hat, Bericht erstatten. Die Evaluierung wird mit der Annahme von Schlussfolgerungen durch den Rat der EU auf Ministerebene formell abgeschlossen[6]. Der Datenschutzbeauftragte vertritt die Interessen der kantonalen Datenschutzbeauftragten in der Arbeitsgruppe, welche die Kontrollen organisiert. Primär galt es im Jahr 2013, die Antworten der kantonalen Datenschutzbeauftragten zu sammeln und zu konsolidieren, und schliesslich den gesamten Antwortenkatalog akribisch zu redigieren. Nachdem das von der Arbeitsgruppe vorgeschlagene Prüfprogramm von der EU weitestgehend genehmigt wurde, können nun zu Beginn des Jahres 2014 die einzelnen Besuche bei den kantonalen Datenschutzbeauftragten vorbereitet werden.

—

1 Dazu TB 2011, 13 f.
2 Mit N-SIS wird der nationale Teil des Schengener Informationssystems bezeichnet.
3 RIPOL ist das automatisierte Fahndungssystem des Bundes. Der Name stammt aus der französischen Sprache und ist die Abkürzung für Recherches informatisées de police. Das Fahndungssystem RIPOL umfasst Datenbanken für Personenfahndungen, Fahrzeugfahndungen, Sachfahndungen und ungeklärte Straftaten.
4 Das SSO-Portal (Single Sign On-Portal) EJPD bildet die zentrale Sicherheitsarchitektur und infrastruktur des EJPD und erlaubt es auch kantonalen Behörden, auf die Applikationen des Bundes zuzugreifen.
5 Siehe dazu schon TB 2011, 14.
6 Siehe dazu auch die Medienmitteilung des Bundesamtes für Justiz unter <https://www.bfm.admin.ch/content/ejpd/de/home/dokumentation/mi/2013/ref_2013-12-10.html> (zuletzt besucht am 15.04.2014).

Aus dem Alltag

Statistische Auswertungen 2013 (mit Vorjahresvergleichen)

A Geschäfte

	2013		2012		2011		2010	
	Anzahl	%	Anzahl	%	Anzahl	%	Anzahl	%
Anzahl eröffnete Geschäfte	403		366		341		323	
prozentuale Veränderung gegenüber Vorjahr		10		7		6		40[1]

[1]Vorjahr erst ab 1. Mai 2009 erfasst.

B Indikatoren gemäss Budget

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

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

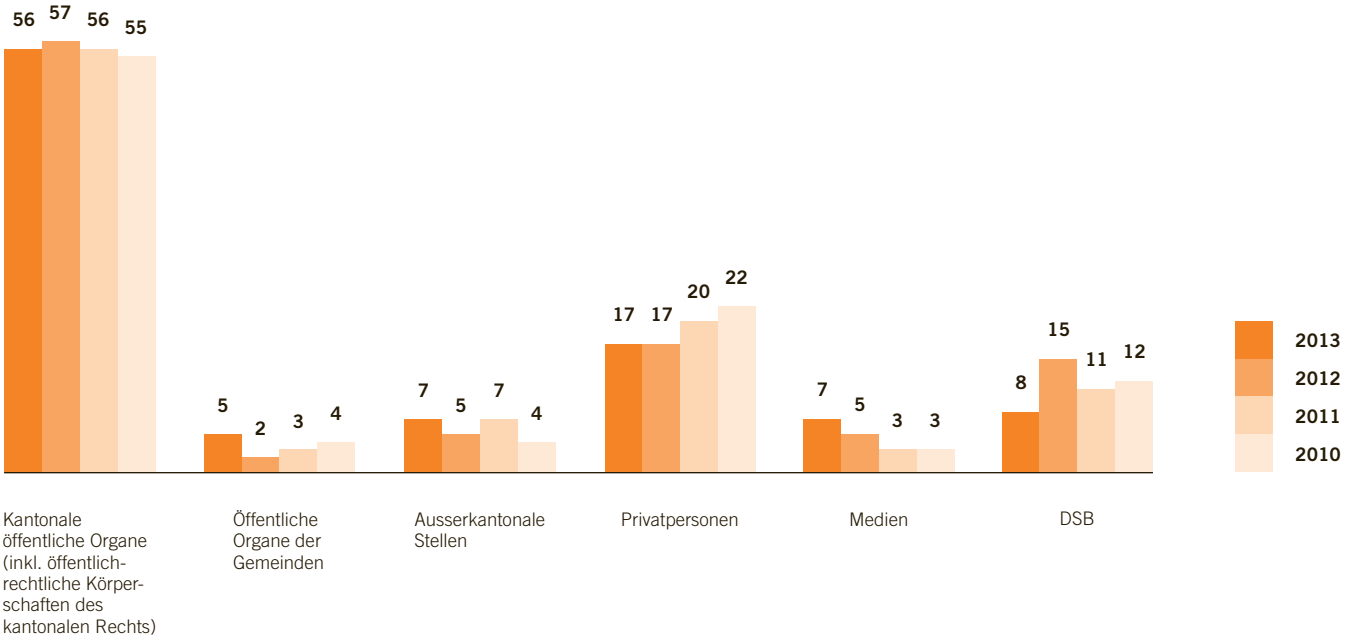
Indikatoren erfasst ab 2011.

C Öffentlichkeitsprinzip

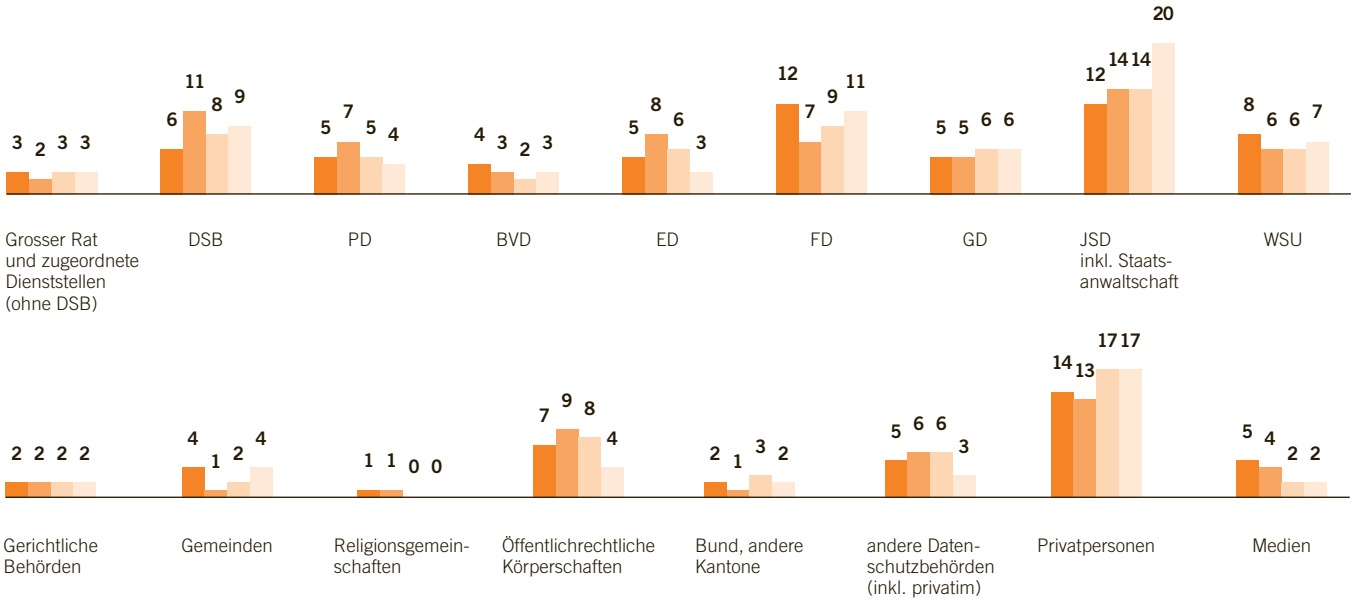
	2013		2012	
	Anzahl	%	Anzahl	%
Eingereichte Gesuche nach § 25 IDG				
Anzahl eingereichte Gesuche	30		48	
Behandlung der Gesuche nach § 25 IDG				
Anzahl gutgeheissener Gesuche		37		60
Anteil teilweise gutgeheissener Gesuche		17		17
Anteil ganz abgewiesener Gesuche		37		13
Anteil noch nicht rechtskräftig entschiedener Gesuche		10		10

Öffentlichkeitsprinzip ab 2012.
Zahlen erfasst durch die Staatskanzlei aufgrund der Meldungen der Departemente (§ 31 IDV).
Zahlen aufgeschlüsselt nach Departementen: 180. Verwaltungsbericht des Regierungsrates (noch nicht publiziert), Vorabdruck, Ziff. 4.2.1, Präsidialdepartement, Staatskanzlei, Öffentlichkeitsprinzip, S. 155.

D Initianten: Veranlasser der Geschäfte (A) in %



E In die Geschäfte (A) involvierte Stellen in %



Fälle

Fall 1 Leistungstest der Nordwestschweizer Schulen und Öffentlichkeitsprinzip

Fall 2 Fotos von Mitarbeiterinnen und Mitarbeitern im Internet?

Fall 3 Videoüberwachung durch Private

Fall 4 Videoüberwachung durch Private auf öffentlichem Grund

Fall 1 Leistungstest der Nordwestschweizer Schulen und Öffentlichkeitsprinzip

Lehrpersonen und ihre Verbände befürchten, dass die Resultate der Leistungstests der vier Nordwestschweizer Kantone für Schulrankings verwendet werden. Kann mit der Veröffentlichungsbestimmung im Schulgesetz ausgeschlossen werden, dass die Resultate bei grossen Schulen mit einer grossen Anzahl betroffener Lehrpersonen gestützt auf das Öffentlichkeitsprinzip zugänglich werden?

Die Nordwestschweizer Kantone Aargau, Basel-Landschaft, Basel-Stadt und Solothurn haben vereinbart, in bestimmten Fächern gemeinsame Leistungstests zu Beginn der 3. Klasse (Check P3), zu Beginn der 6. Klasse (Check P6), Mitte der 2. Klasse der Sekundarstufe I (Check S2) und am Ende der 3. Klasse der Sekundarstufe I (Check S3) durchzuführen[1]. Es stellt sich die Frage, ob verhindert werden kann, dass die Resultate dieser Tests für ein Schulhaus-Ranking verwendet werden.

Das baselstädtische Schulgesetz bestimmt dazu in § 57c Abs. 6: «Gegenüber der Öffentlichkeit dürfen die Ergebnisse nur in anonymisierter Form, ohne Nennung von Schulen, Klassen oder Schülerinnen und Schülern, als statistische Auswertung des Gesamtergebnisses bekannt gemacht werden.» Das tönt auf den ersten Blick klar. Trotzdem ist zu prüfen, ob nicht doch ein Schulranking möglich wird.

Zwei Einschränkungen sind datenschutzrechtlich motiviert:

— Klarerweise dürfen die Ergebnisse der Leistungstests nicht in der Form von Resultaten einzelner *Schülerinnen und Schüler* mit deren Namen veröffentlicht werden. Hier überwiegt das private Interesse gegenüber irgendwelchen Informationszugangsinteressen. In Bezug auf das allgemeine Informationszugangsrecht – in Form des reaktiven Öffentlichkeitsprinzips nach § 25 IDG – legt auch § 30 IDG unzweideutig fest, dass die Personendaten vor der Zugangsgewährung anonymisiert werden müssen.

— Ebenso müssen Personendaten über die *Lehrpersonen* anonymisiert werden. Als solche erscheinen die Resultate nach Klassen; sie sagen auch etwas über die entsprechenden Lehrpersonen aus: der Klassendurchschnitt in Mathematik über die Mathelehrerin, in Deutsch über den Deutschlehrer. Auch dafür schreibt § 30 IDG die Anonymisierung vor.

Ob der Durchschnitt einer ganzen Schule, also etwa aller 3. Klassen der Sekundarstufe I in Deutsch, noch ein Personendatum darstellt, kommt auf die Grösse der Schule und die Anzahl der entsprechenden Lehrpersonen an. Wenn in einer kleinen Schule alle drei 3. Klassen der Sekundarstufe I vom gleichen Deutschlehrer unterrichtet werden, dann sagt auch der Schuldurchschnitt etwas über diesen Deutschlehrer aus – damit stellt auch diese Informationen ein Personendatum dar. Wenn aber beispielsweise in einer grossen Schule die 3. Klassen der Sekundarstufe I von zehn verschiedenen Mathelehrerinnen und lehrern unterrichtet werden, dann sagt der Schuldurchschnitt nichts mehr über eine einzelne Lehrperson aus – der Durchschnitt stellt kein Personendatum mehr dar.

Falls in einem solchen Fall – also bei einer grossen Schule mit einer grossen Anzahl von betroffenen Lehrpersonen – jemand gestützt auf § 25 IDG (das allgemeine Informationszugangsrecht) Zugang zu den Schulresultaten verlangt, dann können keine Datenschutzgründe gegen die Zugangsgewährung ins Feld geführt werden. Es ist nicht auszuschliessen, dass dann letztlich ein richterliches Urteil abwägen müsste zwischen dem verfassungsrechtlich verankerten Öffentlichkeitsprinzip (§ 75 Abs. 2 KV) und dem Geheimhaltungsinteresse auf Stufe Schule – also dem Anliegen, aus schulpolitischen Gründen kein Schulranking zuzulassen. Das Resultat dieser Abwägung kann nicht mit Sicherheit vorausgesagt werden.

Ergebnis

Aus Gründen des Persönlichkeitsschutzes dürfen die Resultate der Leistungstests nicht auf einzelne Schülerinnen und Schüler oder auf einzelne Klassen (und damit Lehrpersonen) bezogen zugänglich gemacht werden. Das Schulgesetz erlaubt die Publikation auch nur ohne Nennung der Schule. Ob in einer allfälligen richterlichen Abwägung das Interesse, Schulrankings zu verhindern, bei grossen Schulen mit einer grossen Anzahl betroffener Lehrpersonen gegenüber dem verfassungsrechtlich verankerten Öffentlichkeitsprinzip überwiegen würde, kann nicht garantiert werden.

1 § 57c SchulG; § 39 Abs. 1 SLV.

Fall 2 Fotos von Mitarbeiterinnen und Mitarbeitern im Internet?

Weil es sich dadurch eine erhöhte Kundenfreundlichkeit erhofft, möchte ein öffentliches Organ Fotos seiner Mitarbeiterinnen und Mitarbeiter im Internet veröffentlichen. Eine betroffene Mitarbeiterin stösst sich daran und möchte deshalb wissen, ob sie sich wehren kann.

Anhand eines Portraitfotos können Mitarbeiterinnen und Mitarbeiter persönlich identifiziert werden. Portraitfotos sind damit Personendaten i.S.v. § 3 Abs. 3 IDG. Sollen Portraitfotos z.B. im Internet veröffentlicht werden, so sind die Voraussetzungen des IDG zu erfüllen: Die Bekanntgabe von Personendaten ist nach § 21 IDG zulässig, wenn dafür eine gesetzliche Grundlage besteht (sog. unmittelbare gesetzliche Grundlage) oder die Bekanntgabe im Internet zur Erfüllung der gesetzlichen Aufgabe erforderlich ist (sog mittelbare gesetzliche Grundlage).

Als mögliche gesetzliche Grundlage für die Publikation der Fotos von Mitarbeiterinnen und Mitarbeitern im Internet kommt § 20 Abs. 3 IDG in Frage: Danach stellt das öffentliche Organ Informationen über seinen Aufbau, seine Zuständigkeiten und über Ansprechpersonen zur Verfügung.

Sind alle Mitarbeiterinnen und Mitarbeiter «Ansprechpersonen» und fallen ihre Fotos unter «Informationen über Ansprechpersonen»?

Ansprechpersonen sind primär diejenigen, die von Bürgerinnen und Bürgern ganz direkt angesprochen werden können sollen. Von den Ansprechpersonen dürfen diejenigen Angaben veröffentlicht werden, die erforderlich sind, damit sie angesprochen werden können, also Vorname und Name, Angaben zur Funktion und Zuständigkeit, die Geschäftsadresse sowie Angaben zur dienstlichen Erreichbarkeit wie geschäftliche Telefonnummer(n) und E-Mail-Adresse sowie allenfalls Angaben zur Anwesenheit bei Teilzeitbeschäftigten.

Weitere Angaben wie private Adresse, private Kontaktinformationen oder eben auch Fotos sind in aller Regel für die Zweckerreichung nicht erforderlich und dürfen deshalb (ohne oder gar gegen den Willen der betroffenen Personen) nicht einfach gestützt auf § 20 Abs. 3 IDG veröffentlicht werden[1]. Eine Publikation kann höchstens durch eine ausdrückliche und freiwillig erteilte Einwilligung der betroffenen Personen gerechtfertigt werden. Allerdings darf im Arbeitsverhältnis die Einwilligung nicht vorschnell angenommen werden. Häufig fühlen sich Arbeitnehmerinnen oder Arbeitnehmer nämlich in einer Zwangssituation. Gruppendruck oder explizit oder implizit geäusserte Erwartungen von Vorgesetzten können dazu führen, dass die Einwilligung nicht als freiwillig erteilt erscheint. Die Einwilligung ist im Übrigen jederzeit frei widerrufbar[2].

Anders sieht es bei Inhaberinnen und Inhabern politischer Ämtern (Mitglieder der Legislative und der Exekutive) aus: Hier ist die Wiedergabe von Porträtaufnahmen gerechtfertigt. Auch bei Leitungspersonen der Verwaltung mag ein gewisses öffentliches Interesse an der Veröffentlichung eines Fotos bestehen; trotzdem ist eine Publikation ohne die (mindestens konkludente) Einwilligung der betroffenen Leitungsperson nicht zulässig.

Ergebnis

Fotos von Mitarbeiterinnen und Mitarbeitern dürfen im Internet nicht allein gestützt auf die Pflicht der öffentlichen Organe, Informationen über ihren Aufbau, ihre Zuständigkeiten und über Ansprechpersonen zur Verfügung zu stellen (§ 20 Abs. 3 IDG), publiziert werden – ausser bei politischen Ämtern und allenfalls Leitungspersonen der Verwaltung wäre die Publikation (ohne oder gar gegen den Willen der betroffenen Personen) unverhältnismässig. Allenfalls ist eine Publikation gestützt auf eine ausdrücklich und freiwillig erteilte Einwilligung der betroffenen Personen zulässig. Allerdings darf im Arbeitsverhältnis die Einwilligung nicht vorschnell angenommen werden.

1 PK-IDG/BS-Rudin 2014, § 20 N 48.

2 Es ist zu empfehlen, im Einwilligungsformular von den Mitarbeitenden bestätigen zu lassen, dass sie der Publikation freiwillig, ohne Druck und in Kenntnis, dass die Einwilligung freiwillig ist und jederzeit ohne Konsequenzen widerrufen werden kann, zustimmen.

Fall 3 Videoüberwachung durch Private

Immer wieder wenden sich Bürgerinnen und Bürger an den Datenschutzbeauftragten, weil sie sich an Videoüberwachungssystemen stören, die durch Privatpersonen betrieben werden. Wenn Privatpersonen Personendaten bearbeiten, ist das Bundesdatenschutzgesetz anwendbar. Gegen eine unzulässige Videoüberwachung können sich betroffene Personen nur auf dem Weg der Zivilklage zu Wehr setzen.

Der Mieter A. wendet sich an den Datenschutzbeauftragten, weil er sich darüber aufregt, dass die Vermieterin B. im Treppenhaus beim Lifteingang eine Videokamera installiert hat, die alle Personen aufnimmt, welche den Lift betreten oder ihn verlassen.

Sobald die Personen auf den Aufnahmen erkennbar sind, handelt es sich um ein Bearbeiten von Personendaten durch eine Privatperson. Auf dieses Datenbearbeiten ist nicht das kantonale Informations- und Datenschutzgesetz anwendbar, sondern das Bundesdatenschutzgesetz[1]. Dementsprechend ist auch nicht der kantonale Datenschutzbeauftragte zuständig, sondern der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB)[2].

Videoaufnahmen verletzen die Persönlichkeitsrechte der aufgenommenen Person – widerrechtlich ist das (nur) dann nicht, wenn ein Gesetz, ein überwiegendes privates oder öffentliches Interesse oder die Einwilligung der aufgenommenen Personen die Aufnahme rechtfertigt[3].

Im Kanton Basel-Stadt existiert kein Gesetz, das eine private Videoüberwachung rechtfertigt. Auch wird es in aller Regel unmöglich sein, von allen betroffenen Personen vorgängig eine Einwilligung einzuholen. Somit bleibt zur Rechtfertigung einzig ein überwiegendes Interesse. Reiner «Gwunder», wer sich irgendwo bewegt, vermag gegenüber den Persönlichkeitsschutzinteressen der aufgenommenen Personen regelmässig nicht zu überwiegen – anders als etwa Sicherheitsinteressen. Allerdings genügt ein diffuses «allgemeines Sicherheitsinteresse» nicht. Es muss ein konkretes Sicherheitsinteresse vorliegen, etwa aufgrund der konkreten Gegebenheiten (z.B. bei Bancomaten im Eingangsbereich einer Bank).

Auch wenn eine Videoüberwachung gerechtfertigt werden kann, muss ihr Einsatz verhältnismässig sein[4]. Das ist er nur, wenn mit weniger in die Persönlichkeitsrechte eingreifenden Mitteln (z.B. mit besserer Beleuchtung, zusätzlichen Verriegelungen, Verstärkungen der Eingangstüren, Installation eines Alarmsystems) der angestrebte Zweck – mehr Sicherheit – nicht erreicht werden kann. Ausserdem muss sich der Aufnahmebereich auf das zur Zweckerreichung Notwendige beschränken und müssen die konkreten Modalitäten des Betriebs (z.B. Live-Übermittlung und Auswertung der Aufnahmen oder blosse Aufzeichnung, regelmässige Auswertung der Aufzeichnungen oder bloss bei bestimmten Vorkommnissen, Begrenzung der Personen, die auf die Aufnahmen zugreifen können, Löschung der Aufzeichnungen usw.) angemessen sein.

Die Durchsetzung geschieht auf privatrechtlichem Weg, also über eine Klage beim Zivilgericht[5] – mit entsprechendem Kostenrisiko. Der Datenschutzbeauftragte empfiehlt, vorher das Gespräch mit der Betreiberin zu suchen.

Personen, die sich wegen privater Videoüberwachung an ihn wenden, berät der Datenschutzbeauftragte über ihre Rechte und stellt ihnen den Link zu den Merkblättern des EDÖB[6] zu. Für weitere Informationen muss er sie dann an den EDÖB verweisen.

Ergebnis

Wenn Privatpersonen eine Videoüberwachungsanlage betreiben, gilt das Bundesdatenschutzgesetz. Zur Rechtfertigung des Einsatzes von Videoüberwachung braucht es ein überwiegendes privates oder öffentliches Interesse (z.B. Sicherheitsinteresse). Die Videoüberwachung muss aber auch verhältnismässig sein; zuerst sind deshalb Massnahmen zu ergreifen, die weniger stark in die Persönlichkeitsrechte der betroffenen Personen eingreifen.

1 Art. 2 Abs. 1 lit. a DSG/Bund.
2 <http://www.edoeb.admin.ch>, (letztmals kontrolliert: 7. April 2014), Telefon 058 462 43 95 (Montag bis Freitag, jeweils 10:00 bis 12:00).
3 Art. 13 Abs. 1 DSG/Bund.
4 Art. 4 Abs. 2 DSG/Bund.
5 Vgl. nun auch die Antwort des Regierungsrates auf die Interpellation Nr. 5 von André Auderset betreffend «Nichthandeln der Behörden bei illegalen Videoüberwachungen» (Schreiben 14.5049.02 des Regierungsrates vom 25. Februar 2014), Ziffer 2.
6 <http://www.edoeb.admin.ch> (letztmals kontrolliert: 7. April 2014), unter Datenschutz | Technologien | Videoüberwachung.

Fall 4 Videoüberwachung durch Private auf öffentlichem Grund

Wenn Private mit ihrer Videoüberwachung nicht bloss im privaten Raum, sondern auf öffentlichem Grund filmen, stellen sich zusätzliche Fragen: Dürfen Private mit ihrer Videoüberwachung Personen im öffentlichen Raum erfassen? Darf der Kanton die Videoüberwachung auf öffentlichem Grund durch Private gesetzlich regeln?

Herr G. beschwert sich beim Datenschutzbeauftragten darüber, dass der Hauseigentümer H. an der Fassade seines Hauses eine Videokamera montiert hat, die alle Passantinnen und Passanten aufnimmt, die auf dem Trottoir vor dem Haus vorbeigehen.

Auch[1] in diesem Fall handelt es sich, sofern auf den Aufnahmen die Personen erkennbar sind, um ein Bearbeiten von Personendaten durch Privatpersonen, worauf das Bundesdatenschutzgesetz anwendbar ist. Und auch hier ist es notwendig, dass die Widerrechtlichkeit der Persönlichkeitsverletzung, die durch die Überwachung erfolgt, durch einen Rechtfertigungsgrund beseitigt wird. Das wiederum wird auch hier nicht durch die Einwilligung aller betroffenen Personen geschehen können. Ein privates oder öffentliches Interesse wird in aller Regel nicht gegenüber dem Persönlichkeitsschutzinteresse aller Passantinnen und Passanten überwiegen, die sich ja auf öffentlichem Grund bewegen. Damit wird somit eine Überwachung, die den öffentlichen Raum miterfasst, nicht gerechtfertigt werden können. Und ebenso wenig existiert im Kanton Basel-Stadt ein Gesetz, das Privaten Videoüberwachung auf öffentlichem Grund erlaubt. Der für das Datenbearbeiten durch Privatpersonen zuständige Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) schreibt denn auch in seinem Merkblatt «Videoüberwachung des öffentlichen Raums durch Privatpersonen»[2], es sei «grundsätzlich nicht zulässig, dass Privatpersonen Videoüberwachungsanlagen auf öffentlichem Grund betreiben»[3].

Der EDÖB empfiehlt Privatpersonen, welche öffentlichen Grund aus Sicherheitsgründen überwachen möchten, sich mit dem hierfür zuständigen Gemeinwesen (Gemeinde, Polizei, allenfalls kantonale Stellen) in Verbindung zu setzen und mit diesem zu vereinbaren, die notwendigen Videoüberwachungsmassnahmen selbst durchzuführen[4]. Im Kanton Basel-Stadt kann man nicht einfach mit der Polizei eine Videoüberwachung «vereinbaren». Es ist auch kaum denkbar, dass die Kantonspolizei eine private Videoüberwachung in eine ihr (d.h. der Polizei) erlaubte Videoüberwachung[5] uminterpretiert, die sie an den privaten Betreiber «ausgelagert» hat; sie müsste dann im Übrigen die gesamte Verantwortung «übernehmen» (bzw. sie bliebe bei ihr als «Auftraggeberin»[6]).

Es bliebe dem Kanton die Möglichkeit, eine rechtliche Regelung über private Videoüberwachung zu erlassen. Er könnte per Gesetz eine Bewilligungspflicht für privat betriebene Überwachung des öffentlichen Raums einführen. Auf welche Kompetenz er sich dazu stützen könnte, ist kritisch zu hinterfragen. Die Videoüberwachung ist ja nicht typischerweise eine «Nutzung des öffentlichen Raums», wie sie vom NöRG erfasst wird. Auch wenn der Kanton die Videoüberwachung des öffentlichen Raums durch Private bewilligungspflichtig erklären würde, bliebe das bewilligte Videoüberwachen ein Datenbearbeiten durch Private, worauf das Bundesdatenschutzgesetz anwendbar und wofür der EDÖB zuständig bliebe. Die Zuständigkeit für die Erteilung von Videoüberwachungsbewilligungen müsste wohl bei den für den Vollzug des NöRG zuständigen Stellen angesiedelt werden. Ob eine solche gesetzliche Regelung geschaffen werden soll, ist politisch zu beantworten. Der Regierungsrat sieht zurzeit keine Notwendigkeit dafür[7].

Ergebnis

Die Videoüberwachung des öffentlichen Raums durch Private dürfte in aller Regel unzulässig sein. Ob eine Bewilligungspflicht für solche Videoüberwachungsanlagen eingeführt werden soll, ist politisch zu beantworten. In jedem Fall blieben das Bundesdatenschutzgesetz anwendbar und die Aufsicht beim EDÖB.

1 Vgl. dazu TB 2013, Fall 3, 36.
2 <http://www.edoeb.admin.ch/datenschutz/00625/00729/00738/index.html?lang=de> (letztmals kontrolliert: 7. April 2014).
3 Vgl. nun auch die Antwort des Regierungsrates auf die Interpellation Nr. 5 von André Auderset betreffend «Nichthandeln der Behörden bei illegalen Videoüberwachungen» (Schreiben 14.5049.02 des Regierungsrates vom 25. Februar 2014), Ziffer 1.
4 <http://www.edoeb.admin.ch/datenschutz/00625/00729/00738/index.html?lang=de> (letztmals kontrolliert: 7. April 2014).
5 Durch §§ 17 f. IDG.
6 § 7 Abs. 2 IDG; vgl. dazu PK-IDG/BS-Rudin 2014, § 7 N 57 ff.
7 Interpellationsantwort des Regierungsrates (Fn. 3), Ziffer 5.

Anhang

Verzeichnis der zitierten Gesetze, Materialien und Literatur

Rechtsgrundlagen des Kantons Basel-Stadt

Aufenthaltsgesetz Aufenthaltsgesetz vom 16. September 1998, SG 122.200.
IDG Gesetz vom 9. Juni 2010 über die Information und den Datenschutz (Informations- und Datenschutzgesetz, IDG), SG 153.260.
IDV Verordnung vom 5. August 2011 über die Information und den Datenschutz (Informations- und Datenschutzverordnung, IDV), SG 153.270.
FVKG Finanz- und Verwaltungskontrollgesetz vom 17. September 2003 (FVKG), SG 610.200.
GesG Gesundheitsgesetz vom 21. September 2011, SG 300.100.
NöRG Gesetz vom 16. Oktober 2013 über die Nutzung des öffentlichen Raumes (NöRG), SG 724.100.
PG Personalgesetz vom 17. November 1999, SG 162.100.
SchulG Schulgesetz vom 4. April 1929, SG 410.100.
SLV Verordnung vom 11. September 2012 über die Beurteilung und die Schullaufbahnentscheide der Schülerinnen und Schüler der Volksschule und der weiterführenden Schulen (Schullaufbahnverordung, SLV), SG 410.700.
UKBB-Vertrag Vertrag vom 16.02.1998 zwischen den Kantonen Basel-Stadt und Basel-Landschaft über das Universitäts-Kinderspital beider Basel (Kinderspitalvertrag), SG 331.300.
Whistleblowing-Verordnung Verordnung vom 24. September 2013 über die Meldung von Missständen (Whistleblowing-Verordnung), SG 162.600.

Bundesrecht

BGÖ Bundesgesetz vom 17. Dezember 2004 über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz, BGÖ), SR 152.3.
DSG Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG), SR 235.1.

Materialien

Bericht 13.0634.02 Bericht 13.0634.02 der Justiz, Sicherheits- und Sportkommission vom 20. März 2014 zum Ratschlag zu einem kantonalen Gesetz über die öffentliche Statistik (StatG) und Motion Brigitta Gerber betreffend Schaffung eines Statistikgesetzes (P105252).
Bericht 12.0626.02 Bericht 12.0626.02 der Gesundheits- und Sozialkommission vom 10. April 2013 zum Ratschlag Revision des Staatsvertrages zwischen den Kantonen Basel-Stadt und Basel-Landschaft über das Universitäts-Kinderspital beider Basel (Kinderspitalvertrag) vom 16. Februar 1998.
Bericht 08.0637.02 Bericht 08.0637.02 der Justiz-, Sicherheits- und Sportkommission vom 14. April 2010 zum Ratschlag 08.0637.01 betreffend Gesetz über die Information und den Datenschutz (Informations- und Datenschutzgesetz).
Leitfaden Öffentlichkeitsarbeit Leitfaden zur Öffentlichkeitsarbeit von Regierungsrat und kantonaler Verwaltung, September 2011, herausgegeben von der Staatskanzlei des Kantons Basel-Stadt, Kommunikation.
Ratschlag 13.0634.01 Ratschlag 13.0634.01 vom 11. Juni 2013 zu einem kantonalen Gesetz über die öffentliche Statistik (StatG) und Motion Brigitta Gerber betreffend Schaffung eines Statistikgesetzes (P105252).
Ratschlag 12.0626.01 Ratschlag zur Revision des Staatsvertrages zwischen den Kantonen Basel-Stadt und Basel-Landschaft über das Universitäts-Kinderspital beider Basel (Kinderspitalvertrag) vom 16. Februar 1998 (12.0626.01).
Ratschlag 11.1792.01 Ratschlag vom 6. Februar 2013 zu einem neuen Staatsbeitragsgesetz (11.1792.01)
Ratschlag 08.0637.01 Ratschlag 08.0637.01 vom 10. Februar 2009 betreffend Gesetz über die Information und den Datenschutz (Informations- und Datenschutzgesetz).
TB 2012 Tätigkeitsbericht des Datenschutzbeauftragten des Kantons Basel-Stadt, 2012, abrufbar unter <http://www.bs.ch/publikationen/datenschutz/taetigkeitsbericht-datenschutzbeauftragten-jahr-2012.html>.
TB 2011 Tätigkeitsbericht des Datenschutzbeauftragten des Kantons Basel-Stadt, 2011, abrufbar unter <http://www.bs.ch/publikationen/datenschutz/taetigkeitsbericht-datenschutzbeauftragten-jahr-2011.html>.

Literatur

PK-IDG/BS-Autor(in) 2014 Beat Rudin/Bruno Baeriswyl (Hrsg.), Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Basel-Stadt, Basel/Genf/Zürich 2014.
SGK-BV-Autor(in) 2008 Bernhard Ehrenzeller/Philippe Mastronardi/Rainer J. Schweizer/Klaus Vallender (Hrsg.), Die Schweizerische Bundesverfassung, (St. Galler) Kommentar, 2. Auflage, Zürich/St. Gallen 2008.

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

Datenschutzbeauftragter
Beat Rudin, Dr. iur., Advokat

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

Volontärin:
Nadine Battilana, MLaw
(1.10.2012 - 30.6.2013)
Ella Waldmann, MLaw
(1.7.2013 - 31.12.2013)

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

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

Gestaltung
Andrea Gruber,
Visuelle Gestaltung, Basel

Druck
Gremper AG