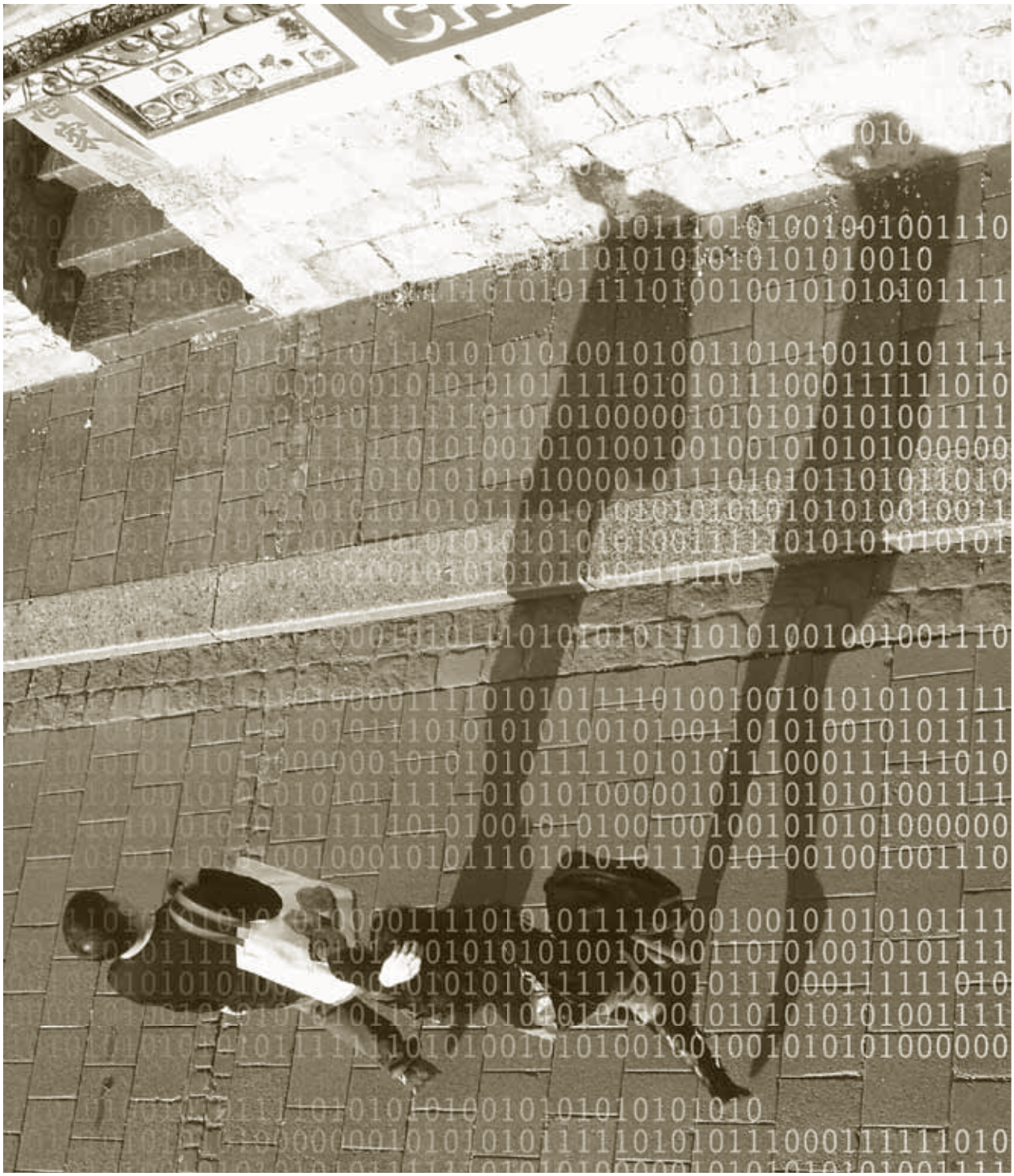
Bericht an den Grossen Rat

20
10

Tätigkeitsbericht des
Datenschutzbeauftragten
des Kantons Basel-Stadt



Der Datenschutzbeauftragte erstattet der Wahlbehörde jährlich Bericht über seine Tätigkeit, Feststellungen und Erfahrungen; der Bericht wird veröffentlicht (§ 28 lit. d DSG).

Inhaltsübersicht

Einleitung

Themen

Fälle

Anhang

Einleitung

2010 – die Datenschatten werden länger

Das zweite Jahr der «neuen» Datenschutzaufsicht stand unter dem Titel der Konsolidierung. Es ging darum, die gesetzesbedingten neuen Strukturen und Prozesse zu konsolidieren. Die Themenpalette war unverändert breit – sie reichte von «Theo dem Pfeifenraucher» bis zu den noch Ungeborenen.

Ein Blick aufs vergangene Jahr

Spannungsfeld Das Aufgabengebiet des Datenschutzbeauftragten blieb auch im Jahr 2010 unverändert spannend. Da ist einmal die technologische Entwicklung – Stichworte sind etwa die zunehmende Digitalisierung, Cloud Computing oder die Untersuchung von genetischem Material –, welche auch die öffentliche Verwaltung herausfordert. Die Schatten, die wir alle als Datenspur in der digitalisierten Welt hinterlassen, werden länger. Es sind aber auch gesellschaftliche Phänomene – wie etwa ein «Saubannerzug» in der Freien Strasse oder Hooligan-Gewalt rund um die Spiele des FCB –, die nach Reaktionen rufen. Seien es Forderungen nach einer flächendeckenden Videoüberwachung in der ganzen Stadt, die Internetfahndung, der Ruf nach einer Information «der Schule», sobald ein(e) Schüler(in) ein Delikt begangen hat, oder nach einer rigorosen Kontrolle der Sozialhilfebezüger(innen) – sie alle basieren auf verständlichen Bedürfnissen; die staatliche Reaktion muss sich aber wie alles staatliche Handeln auf eine Rechtsgrundlage stützen können und insbesondere auch verhältnismässig sein.

Aufgaben des Datenschutzbeauftragten Genau hier setzen die Aufgaben des Datenschutzbeauftragten ein: Er muss einerseits durch Beratung darauf hinwirken, dass das Datenbearbeiten der öffentlichen Organe (und der Privaten, soweit ihnen von Kanton oder Gemeinden die Erfüllung einer öffentlichen Aufgabe übertragen ist) recht- und verhältnismässig ist. Andererseits muss er die Anwendung der Bestimmungen über den Datenschutz kontrollieren.

Beratung Die Beratung nimmt den Hauptteil der Ressourcen in Anspruch. 323 neue Geschäfte wurden 2010 eröffnet (2009: 230). Initiant(inn)en waren in 71 Fällen (22%) Privatpersonen, in 13 Fällen (4%) öffentliche Organe der Gemeinden, in 12 Fällen (4%) ausserkantonale Stellen, in 11 Fällen (3%) die Medien und in 38 Fällen (12%) der Datenschutzbeauftragte selber. In den übrigen 55% der Fälle waren öffentliche Organe des Kantons (inkl. den öffentlichrechtlichen Anstalten) die Auslöser. Einen illustrativen Einblick in die Vielfalt der behandelten Fragen bieten die Rubrik «Themen» (Seiten 8 ff.) und vor allem die Rubrik «Fälle» (Seiten 26 ff.).

Kontrolle Mit den Kontrollen soll festgestellt werden, ob die datenschutzrechtlichen Bestimmungen eingehalten sind. Ein Audit kann bestätigen, dass diese Anforderung erfüllt ist, oder aufzeigen, wo Massnahmen ergriffen werden müssen, damit ein rechtskonformer Zustand hergestellt werden kann. Die Kontrolltätigkeit kam leider nicht so in Fahrt, wie wir das geplant hatten (vgl. Seiten 11 f.). Wir haben für die Zukunft die entsprechenden Konsequenzen gezogen.

Personal In personeller Hinsicht gab es nicht viele Änderungen. Frau Andrea Klüser, MLaw, beendete ihr Volontariat per Ende März 2010; ihr folgten Herr lic. iur. Björn Bastian (1. April bis 31. August 2010) und Paola Vassalli, MLaw (1. September 2010 bis 28. Februar 2011). Frau Klüser verstärkte das Team mit einem befristeten Pensum von 80% erneut (1. Oktober bis 31. Dezember 2010).

Bilanz

Wirkung Datenschutz ist Grundrechtsschutz. Es geht darum, dass bei der staatlichen Aufgabenerfüllung auch den Persönlichkeitsrechten der betroffenen Personen Rechnung getragen wird. Unsere Aufgabe ist es, darauf hinzuwirken, dass die Rechte der betroffenen Personen geachtet werden. Damit vertreten wir logischerweise eine andere Sicht auf ihre Aufgabenerfüllung und stossen manchmal auf Widerstand, wenn wir die hergebrachte Art der Aufgabenerfüllung «stören». Wenn wir aber in Zusammenarbeit mit den betroffenen öffentlichen

Organen konstruktiv Lösungen aufzeigen können, wie sie ihre Aufgaben erfüllen und gleichzeitig die Rechte der betroffenen Personen achten können, erleben wir eine grosse Bereitschaft zur Umsetzung. So wird Datenschutz zu einem Qualitätsmerkmal staatlichen Handelns. Solche Behörden legen uns später auch vielfach von sich aus kritische Fragen vor, um eine grundrechtskonforme Lösung zu finden, bevor es allenfalls zum Konflikt mit betroffenen Personen kommt.

Zwei Schwerpunkte Wir wollen in den Rubriken «Themen» und «Fälle» einige dieser Konfliktsituationen und der Lösungen darstellen. Zwei Themen greifen wir heraus und behandeln sie ausführlicher: die Überwachung am Arbeitsplatz (Seiten 14 ff.) und die Informationssicherheit (Seiten 19 ff.). Sie scheinen es wert zu sein, genauer angeschaut zu werden. Bei der Überwachung am Arbeitsplatz (Telefon- und Internet-Nutzung) gibt es zweifellos berechtigte Anliegen von Kanton und Gemeinden als Arbeitgeber; gleichzeitig müssen die Grundrechte der betroffenen Personen beachtet werden. Mit technischer Überwachung kann aber nicht mangelnde Führungskompetenz kompensiert werden. Ausserdem muss der kulturelle Aspekt mitbedacht werden: Stimmt das mit einer Überwachung vermittelte Menschenbild mit demjenigen des Personalleitbilds des Kantons überein? In Sachen Informationssicherheit stellen wir fest, dass die technologische Entwicklung hergebrachte Konzepte unterläuft. Um in dieser digitalisierten Welt, in welcher die Geschäftsprozesse zunehmend durch die Informations- und Kommunikationstechnologie durchdrungen werden und zusehends von ihr abhängig werden, noch den Überblick zu behalten, wird über kurz oder lang ein umfassendes Risikomanagement nicht zu umgehen sein. Damit Informationssicherheit zu einer Qualität der öffentlichen Verwaltung wird, ist auch eine Sicherheitsorganisation aufzubauen.

Zum Schluss

Dank Unsere Aufgabe zum Schutz der Privatheit der Bürgerinnen und Bürger, über die öffentliche Organe Daten bearbeiten, 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 mit wachem Sinn und offenen Augen durch die Welt gehen, sich bewusst sind, dass verlorene Privatheit nicht im Laden um die Ecke oder im nächsten Online-Shop ersetzt werden kann, und deshalb mit Informationen über sich und über andere sorgsam umgehen;
— allen Privaten, Mitarbeiterinnen und Mitarbeitern der Behörden von Kanton und Gemeinden, welche sich vertrauensvoll mit Datenschutzfragen an uns wenden und sich vielleicht wegen der Arbeitslast gedulden müssen, bis sie eine Antwort erhalten;
— alle Mitarbeiterinnen und Mitarbeitern der Verwaltung, der öffentlichrechtlichen Anstalten und der Gerichte, die mithelfen, datenschutzkonforme Lösungen zu finden und umzusetzen;
— den Kolleginnen und Kollegen der Ombudsstelle, der Finanzkontrolle und des Parlamentsdienstes für die unkomplizierte Zusammenarbeit;
— den Präsidien und Mitgliedern des Grossen Rates, des Büros des Grossen Rates, der Datenschutz-Delegation des Büros, der Geschäftsprüfungs- und der Justiz-, Sicherheits- und Sportkommission für ihr Interesse an unserer Arbeit und ihre wertvolle Unterstützung;
— den Volontärinnen und Volontären für ihre kritische Neugier und ihre aktive Mitarbeit
— und last but not least meinem Team – Andrea Klüser, Carmen Lindner, Sandra Stämpfli und Barbara Widmer –, das mit unverändert grossem Engagement, mit bereichernden Diskussionen und konstruktiven Vorschlägen unsere Arbeit erleichtert und vorangebracht hat

Beat Rudin, Datenschutzbeauftragter

PS. «Theo, der Pfeifenraucher» hat – logischerweise – nicht selber von unserem Einsatz für das Grundrecht auf informationelle Selbstbestimmung profitiert, wohl aber die möglichen Nachfahren, deren DNA-Profil erstellt werden sollte, um ihn zu identifizieren. Wir wurden vom Projektleiter für die Frage korrekten Datenbearbeitung dieser möglichen Nachfahren beigezogen. Auch die eingangs erwähnten noch Ungeborenen haben nicht selber profitiert. Die Spitäler weigerten sich, einer Werbefirma die Namen von Schwangeren zu kommerziellen Zwecken herauszugeben (Seite 33) – zu Recht.

Themen

Thema 1 Von A (Amtshilfe) bis Z (Zugang zu den eigenen Daten)

Thema 2 Überwachung am Arbeitsplatz – und das Menschenbild dahinter

Thema 3 Informationssicherheit – eine Qualität der öffentlichen Verwaltung?

Thema 1

Von A (Amtshilfe) bis Z (Zugang zu den eigenen Daten)

323 neue Geschäfte, 24 Autorisierungen von Online-Zugriffen – das zeigt der Blick in die Geschäftskontrolle 2010 des Datenschutzbeauftragten. Auf den folgenden Seiten zeigen wir einen kleinen Querschnitt der Datenschutzthemen, welche aktuell die staatliche Verwaltung beschäftigen. Zwei Themen – Informationssicherheit und Überwachung am Arbeitsplatz – werden separat ausführlich dargestellt.

Ein Querschnitt durch die Verwaltung

Rechte der betroffenen Personen Regelmässig kommt das Thema des Zugangs zu den eigenen Personendaten aufs Tapet. Dabei ging es beispielsweise darum, den Unterschied zum Akteneinsichtsrecht in Verwaltungsverfahren herauszuschälen und öffentliche Organe beim Entscheid über Einschränkungen zu beraten. Betroffenen Personen konnte mehrfach der Weg aufgezeigt werden, wie sie zur Auskunft über eigene Daten kommen; andererseits musste ihnen aber auch erläutert werden, dass öffentliche Organe die Auskunfterteilung oder Einsichtgewährung zum Schutz von Drittinteressen einschränken müssen. Öfters hat uns – beispielsweise im Zusammenhang mit Polizeirapporten – das Thema der Berichtigung bzw. Gegendarstellung beschäftigt. Wichtig ist auch die Unterscheidung zwischen Tatsachendarstellungen und Werturteilen. Werturteile können nicht berichtigt werden; es kann aber, wenn die betroffene Person anderer Meinung ist, eine Gegendarstellung angebracht werden. Die Unterscheidung sollte bereits bei der Erstellung von Dokumenten klar vorgenommen werden.

Private mit öffentlichen Aufgaben Das kantonale Datenschutzgesetz (und künftig auch das Informations- und Datenschutzgesetz) gilt nicht nur für das Bearbeiten von Personendaten durch öffentliche Organe von Kanton und Gemeinden. Es findet auch Anwendung auf das Datenbearbeiten durch Private, soweit diesen von Kanton oder Gemeinden die Erfüllung öffentlicher Aufgaben übertragen ist[1]. Deshalb haben sich auch private Institutionen (aus den Bereichen Wohnheim, Beobachtungsheim, Privatspital) mit ihren Datenschutzfragen an uns gewandt. Unter anderem stellte sich die Frage nach der Gewährung des Zugangs zu den eigenen Daten und eventuell der Einschränkung des Zugangs. Wir haben einem Wohnheim empfohlen, das komplette Dossier dem AKJS als auftraggebender Behörde zu übergeben, weil eine Einschränkung – mindestens auf Verlangen – per Verfügung vorgenommen werden muss. Ebenso stellte sich die Frage nach der Überbindung des Amtsgeheimnisses auf Mitarbeiter(innen) solcher Institutionen. Am besten erfolgt die Überbindung im Gesetz, das die Aufgabenübertragung regelt. Häufig ist das jedoch nicht der Fall, sondern die Überbindung erfolgt oft nur per Vereinbarung. Allerdings ist die rechtliche Wirkung umstritten: Kann eine gesetzliche Schweigepflicht über den Gesetzeswortlaut hinaus vertraglich auf weitere Personen ausgeweitet werden? Darüber würde wohl erst die Strafgerichtsbarkeit im Anwendungsfall entscheiden.

«Amtshilfe» Immer wieder werden wir von öffentlichen Organen mit der Frage konfrontiert, ob sie Informationen von sich aus einer anderen Behörde, die vielleicht daran interessiert wäre, bekannt geben dürfen. Die Bekanntgaberegeln des DSG und des IDG sind klar: Es braucht eine gesetzliche Grundlage. Wenn Gesetze ein Melderecht oder gar eine Meldepflicht statuieren, dann ist in diesem Rahmen eine Amtshilfe zulässig – aber nicht darüber hinaus. Wenn lediglich ein Auskunftsrecht oder eine Auskunftspflicht festgehalten sind, dann setzt die Datenbekanntgabe eine vorgängige Frage des Organs vor, dem die Daten bekannt gegeben werden sollen. Ausserdem können zusätzliche Anforderungen aufgestellt werden, beispielsweise wenn das Gesetz eine Auskunft nur «auf schriftliche und begründete Anfrage im Einzelfall»[2] erlaubt oder nur bestimmte öffentliche Organe ermächtigt oder verpflichtet, bestimmte Informationen zu bestimmten Zwecken weiterzugeben[3].

Personaldossiers Was gehört ins Personaldossier? Wie lange? Wer führt das vollständige Personaldossier – Linienvorgesetzte oder dezentrale Personaldienste – und wer hat Zugriff darauf? Das sind nur einige der

Fragen, die sich immer wieder im Zusammenhang mit Personaldossiers stellen. Als Grundlage für die Führung von Personaldossiers existiert soweit ersichtlich (nur) eine *Aktennotiz* des Zentralen Personaldienstes vom 23. Januar 2006, die sich erst noch auf unzutreffende Bestimmungen im Datenschutzgesetz beruft. In dieser Aktennotiz wird erläutert, dass das vollständige Personaldossier von den Dezentralen Personaldiensten geführt wird. Bei den Linienvorgesetzten dürfen bloss «Kopien von den wichtigsten Dokumenten des Personaldossiers (MAG, Arbeitsvertrag) sowie Handnotizen aufbewahrt» werden. In der gelebten Verwaltungswirklichkeit haben wir aber festgestellt, dass bei vielen Dienststellen Unklarheit oder mindestens Unsicherheit darüber herrscht, was im Führungsdossier in der Linie aufbewahrt werden muss und wer das Recht hat, darauf zuzugreifen; verbreitet herrscht Unzufriedenheit mit der Regelung und der Organisation und mit den daraus resultierenden Auswirkungen in der Führungspraxis. Diese Situation ist auch aus datenschutzrechtlicher Sicht unbefriedigend. Dass in einzelnen Dienststellen begonnen wird, separate elektronische Ablagen einzurichten, macht die Sache weder besser noch einfacher. Aus diesen Gründen haben wir beim Finanzdepartement als «Personal-Fachdepartement» angeregt, das Problem der Personalinformationen aus übergeordneter Warte umfassender anzugehen. Eine zukunftsgerichtete Lösung liegt möglicherweise künftig in einem elektronischen Personaldossier, bei welchem Inhalte, Zugriffsrechte, Anzeigedauer und Löschvorgänge massgeschneidert und datenschutzkonform ausgestaltet und so die verschiedenen Bedürfnisse und Anliegen angemessen befriedigt werden können.

Medien Regelmässig haben sich Medien mit Anfragen an den Datenschutzbeauftragten gewandt. Sie betrafen u.a. den Staatsschutz, die Videoüberwachung, die Internetfahndung, die (unzulässige) Datenbekanntgabe durch die Polizei an die BVB (betreffend eine drogenabhängige BVB-Chauffeuse) und Swiss DRG.

Informations- und Datenschutzgesetz (IDG)

Beschluss des Grossen Rates Die Justiz-, Sicherheits- und Sportkommission des Grossen Rates hat ihre Beratung zum IDG abgeschlossen und ihren Bericht[4] am 23. April 2010 den Mitgliedern des Grossen Rates zugestellt. Am 9. Juni 2010 hat der Grosse Rat die Vorlage beraten und ist dem Antrag seiner Kommission in allen Punkte gefolgt[5]. Am 24. Juli 2010 ist die Referendumsfrist[6] ungenutzt verstrichen. Über den Zeitpunkt der Wirksamkeit entscheidet der Regierungsrat[7].

Informations- und Datenschutzverordnung (IDV) Vor dem Inkrafttreten des IDG muss noch die IDV geschaffen werden. Der ins Auge gefasste Zeitplan – vorgesehen war ein Beschluss Mitte Dezember 2010 – konnte nicht eingehalten werden. Die Vorbehalte gegenüber dem vom Justiz- und Sicherheitsdepartement vorgeschlagenen Entwurf waren offenbar zu gross. Es ist nachvollziehbar, dass ein Geschäft, welches – wie die Einführung des Öffentlichkeitsprinzips – die gesamte Verwaltung erheblich betrifft, gut vorbereitet sein muss. Der Datenschutzbeauftragte hat sich deshalb auch dagegen ausgesprochen, dass Gesetz und Verordnung unmittelbar nach dem Beschluss der IDV in Kraft gesetzt werden; die Verwaltung muss den Übergang zum Öffentlichkeitsprinzip sorgfältig vorbereiten. Zusammen mit der Staatskanzlei bietet der Datenschutzbeauftragte deshalb auch für das Führungskader Schulungen im Hinblick auf den Übergang an.

Es darf nicht der Eindruck aufkommen, mit der Verordnung werde versucht, den Wechsel zum Öffentlichkeitsprinzip abzuschwächen.

Der Geist der Verfassung und des Gesetzes Dem Datenschutzbeauftragten ist es ausserordentlich wichtig, dass der Geist der Verfassung und des Informations- und Datenschutzgesetzes in der Verordnung fortlebt. Es gibt keine Anhaltspunkte dafür, dass in Basel-Stadt – anders als beim Bund und bei allen Kantonen, die das Öffentlichkeitsprinzip bereits eingeführt haben – die staatliche Aufgabenerfüllung verunmöglicht oder übermässig erschwert wird, wenn die Informationen, die bei einem öffentlichen Organ vorhanden sind, grundsätzlich zugänglich werden[8]. Dass Staatshandeln transparent(er) werden soll, ist genau der Sinn des Öffentlichkeitsprinzips. Es will «das Handeln der öffentlichen Organe transparent (…) gestalten und damit die freie Meinungsbildung und die Wahrnehmung der demokratischen Rechte (…) fördern»[9]. Es darf nicht der Eindruck aufkommen, mittels der Verordnung werde versucht, den von der Verfassung[10] vorgegebenen und im IDG umgesetzten Paradigmenwechsel vom Geheimhaltungsprinzip mit Öffentlichkeitsvorbehalt zum Öffentlichkeitsprinzip mit Geheimhaltungsvorbehalt abzuschwächen. Der Datenschutzbeauftragte, der nach dem IDG künftig sowohl für den Datenschutz als auch für die Informationsfreiheit zuständig ist, wird die Entwicklung sorgfältig verfolgen.

>

Videoüberwachung

Vorbereitung auf die neue Regelung Im Tätigkeitsbericht 2009 war Videoüberwachung eines der ausführlich behandelten Themen[11]. Die dort vorgestellte Neuregelung durch das IDG ist bekanntlich noch nicht in Kraft getreten. Wie damals angekündigt, haben wir bei allen inzwischen eingegangenen Verlängerungsgesuchen darauf hingewirkt, dass die künftig vom IDG verlangten Voraussetzungen eingehalten werden. Das hat insbesondere dazu geführt, dass die in Zukunft notwendigen Reglemente bereits erarbeitet worden sind, so dass mit dem Inkrafttreten des IDG kein grosser Umstellungsaufwand entsteht.

Die «grosse Innenstadtüberwachung» Mit der Verabschiedung des IDG wurde auch die gesetzliche Grundlage geschaffen für die «grosse Innenstadtüberwachung». Im Berichtsjahr liefen dafür die notwendigen Vorbereitungsarbeiten. Vom Justiz- und Sicherheitsdepartement muss ein Reglement erarbeitet und erlassen werden, in welchem die Einsatzmodalitäten geregelt sind. Der Reglementsentwurf ist dem Datenschutzbeauftragten zur Vorabkontrolle vorzulegen. Dieser entscheidet aber – um möglichen Missverständnissen vorzubeugen – nicht darüber, ob die «grosse Innenstadtüberwachung» kommt oder nicht. Er kann nur Empfehlungen dazu abgeben. Der Entscheid über das «ob» liegt beim Vorsteher JSD und – im Rahmen der notwendigen finanzrechtlichen Schritte – bei Regierungsrat und Grossem Rat. Diese Instanzen müssen entscheiden, wie weit die Überwachung im Kanton gehen soll und wie weit die Freiheiten der Bürger(innen) eingeschränkt werden sollen. Dabei darf die offene Frage der Wirksamkeit von Videoüberwachung nicht ausser Acht gelassen werden: Kann sie die erwünschte Wirkung erreichen und können unerwünschte Nebenwirkungen vermieden werden?

Evaluation Die Geltungsdauer des Reglements eines Videoüberwachungssystems ist auf maximal vier Jahre zu begrenzen; vor einer allfälligen Verlängerung ist die Wirksamkeit der Videoüberwachung zu evaluieren[12]. Bei einer Evaluation geht es also darum, der Unsicherheit über die Wirkung von Videoüberwachung Rechnung zu tragen. Konnte der mit der Installation verfolgte Zweck erreicht werden? Hat eventuell bloss eine Verlagerung stattgefunden, haben also die Kameras die unerwünschten «Phänomene» einfach nur an nicht überwachte Orte verdrängt? Oder hat Videoüberwachung gar zu einer Verschlechterung der Sicherheitslage geführt, wenn etwa aufgrund der «technischen Präsenz» die physische Präsenz von Sicherheitskräften reduziert wird? Im Idealfall kann so die Situation vor der Einrichtung der Videoüberwachung mit der Situation während des Betriebs der Videoüberwachung verglichen werden. Bei bereits seit Jahren bestehenden Anlagen wird es schwierig sein, an Daten zur Situation «vorher» heranzukommen; hier beschränkt sich die Evaluation auf die Wirksamkeit an sich: Wenn der Zweck (z.B. Abhalten von Angriffen auf das Schalterpersonal) nicht erreicht wird, muss die Einrichtung ganz generell überdacht werden. Bei neuen Anlagen hingegen sind unbedingt Daten zur Situation «vorher» zu erheben, damit auch unerwünschte Nebenwirkungen wie z.B. die oben erwähnten Verdrängungseffekte erkannt werden können. Bei grossen Anlagen – wie etwa bei der geplanten sehr weitläufigen Innenstadtüberwachung durch die Kantonspolizei – reicht es sicher nicht aus, ein paar Zahlen erheben zu lassen. Solche Projekte müssen unseres Erachtens zwingend durch unabhängige Forschung begleitet werden, wie sie die Sicherheitsdirektion der Stadt Luzern bezüglich der Videoüberwachung im öffentlichen Raum (u.a. um den Bahnhof Luzern) bei einem Forscher der Universität Basel (Department of Business and Economics) in Auftrag gegeben hat.

Führt Videoüberwachung gar zu einer Verschlechterung der Sicherheitslage, weil aufgrund der «technischen Präsenz» die physische Präsenz von Sicherheitskräften reduziert wird?

Rund 900 Kameras weniger Die Zahl der nach § 6a DSG autorisierten Kameras hat im Vergleich zum Vorjahr um rund 900 abgenommen. Trotzdem erfassen nicht weniger, sondern mehr Kameras den öffentlichen Raum im Kanton. Die Auflösung dieses scheinbaren Widerspruchs: Durch das Personenbeförderungsgesetz des Bundes[13] werden die konzessionierten Transportunternehmen dem Datenschutzgesetz des Bundes und der Aufsicht durch den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten unterstellt. Damit werden die Kameras der Basler Verkehrsbetriebe BVB nicht mehr mitgezählt, weil sie nicht mehr der kantonalen Datenschutzgesetzgebung unterliegen – aber logischerweise ist keine Kamera weniger im Einsatz.

Kritik an der Bundesregelung privatim, die Vereinigung der schweizerischen Datenschutzbeauftragten, hat diese Regelung des Bundes kritisiert. Auch wenn die Unterstellung unter das DSG-Bund nach der Meinung des Bundesamtes für Justiz[14] nicht verfassungswidrig sei, weil der Bund im Bereich von Bundesmonopolen frei legiferieren dürfe, ist die Regelung weder notwendig noch sachgerecht: Der Bund darf aufgrund der Sachkompetenz materielle Datenschutzregeln aufstellen. Alles, was er datenschutzrechtlich harmonisieren will, könnte er auf diesem Weg regeln, ohne das DSG-Bund auf kantonale und städtische Transportunternehmen anwendbar zu erklären. Ihre Unterstellung lässt ausserdem verschiedene Fragen offen bzw. schafft neue Probleme:

> Die Kameras der BVB werden nicht mehr mitgezählt, aber logischerweise ist keine Kamera weniger im Einsatz.

— Abgrenzung der Bundeszuständigkeit: Gilt das DSG-Bund abschliessend nur für den eigentlichen Verkehrsbetrieb (z.B. Videoüberwachung in Trams, Bussen und bei Depots) oder auch dort, wo nicht nur der konzessionierte Betrieb betroffen ist? Mit anderen Worten: Welches Recht ist anwendbar, falls vielleicht in Zukunft Videoüberwachung die Allmend aufnehmen, also z.B. an Haltestellen wie etwa am Barfüsserplatz oder am Claraplatz auch oder sogar vorwiegend Nicht-Fahrgäste erfassen wird? (Notabene: für die Überwachungskamera der Polizei gleich nebendran würde kantonales Recht gelten und der kantonale Datenschutzbeauftragte zuständig sein …)
— Verfahrensrecht, Rechtsweg: Welches Verfahrensrecht gilt, wenn eine private Person von den BVB den Erlass einer Feststellungsverfügung (etwa bezüglich des Betriebs einer Videoüberwachungsanlage im Tram) verlangt: das OG oder das Bundesverwaltungsverfahrensgesetz? Welchen Rechtsmittelweg müsste eine betroffene Person beschreiten, wenn sie sich gegen eine solche Verfügung wehren wollte: denjenigen ans kantonale Verwaltungsgericht oder den ans Bundesverwaltungsgericht?
— Öffentlichkeitsprinzip: Gilt für die BVB das Bundes-Öffentlichkeitsgesetz? Gilt das kantonale IDG – aber ohne den Datenschutzteil? Oder gilt das Öffentlichkeitsprinzip der Kantonsverfassung für die BVB einfach nicht, weil der Bund das DSG-Bund anstelle des kantonalen IDG anwendbar erklärt hat?
— Personalrecht: Welches Personalrecht gilt für das BVB-Personal? Wir nehmen an, dass es nicht zu Bundespersonal wird und dass deshalb weiterhin das kantonale Personalrecht (oder das in den kantonalen Gesetzen oder interkantonalen Vereinbarungen anwendbar erklärte Personalrecht) Anwendung findet. Gilt das auch für das Datenschutzrecht in diesem Teil – also gilt in Personalfragen weiterhin das DSG bzw. das IDG?
— Aufsicht: Überall, wo das DSG-Bund anwendbar ist, ist auch der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte für die Aufsicht zuständig. Es ist nicht davon auszugehen, dass die BVB, wenn sie sich mit Fragen an den EDÖB wenden, die gleiche Beratung erhalten wie bisher im Kanton. Das gilt auch für Fahrgäste der BVB, die sich an die Datenschutzaufsicht wenden wollen. Und schliesslich wird auch die Datenschutzkontrolle durch den EDÖB, der ohnehin bereits an Ressourcenmangel leidet, kaum verstärkt werden, wenn alle kantonalen und städtischen Transportunternehmen auch noch bei ihm angesiedelt sind …

Das Thema bleibt pendent privatim, die Vereinigung der schweizerischen Datenschutzbeauftragten, hat beim Bundesamt für Justiz die entsprechenden Fragen deponiert und hofft auf befriedigende Antworten.

Datenschutz-Audit

Abschluss der Pilot-Audits Die zwei Pilotversuche des Datenschutz-Audits konnten erfolgreich zu Ende geführt werden. Mit Unterstützung der Fachstelle für Informatik und Organisation und des Datenschutzbeauftragten konnten von den geprüften Stellen die notwendigen Regelungen erlassen, die erforderlichen Dokumente erstellt und eine Schulung des Kaderpersonals durchgeführt werden.

Feststellungen beim ersten «scharfen» Audit Es hat sich allerdings beim ersten «scharfen» Datenschutz-Audit herausgestellt, dass die Anforderungen für eine erfolgreiche Durchführung – Kenntnis über die eigenen Geschäftsprozesse und über die eingesetzte Informatik – in der Verwaltungsrealität offenbar hoch, vielleicht sogar zu hoch angesetzt sind. Wir mussten feststellen,
— dass interne Regelungen, wie sie zur Umsetzung des Datenschutzes und der Informationssicherheit unerlässlich sind, fehlen;
— dass im Bereich der Informationssicherheit die Verteilung der Verantwortlichkeit zwischen den datenbearbeitenden öffentlichen Organen als Leistungsempfängern und der übergeordneten oder externen Informatikorganisation als Leistungserbringer nicht überall klar ist;
>

— dass wichtige Dokumente wie beispielsweise ein Sicherheitskonzept oder ein Rollen-/Berechtigungskonzept fehlen;
— dass die Leitungsebene die Arbeiten, die für die Vorbereitung des Audits notwendig sind, weitgehend den Mitarbeiter(inne)n «an der Front» zu überlassen scheint, und
— dass schliesslich Unterstützung durch die Fachleute von der Fachstelle für Informatik und Organisation, wie sie zur Vorbereitung mehrfach angeboten wurden, nicht in Anspruch genommen wurde.

Abbruch Bis der Audit vor Ort vorgenommen werden konnte, verging statt der vorgesehenen vier Monate über ein halbes Jahr. Als beim Audit-Teil «IT» auch dann noch die verlangten Dokumente nicht vorgelegt werden konnten, wurde der Audit (im Januar 2010) abgebrochen. Zu den im Teil «Recht» vorgelegten Unterlagen konnte der verantwortlichen Juristin ein vorläufiges positives Feedback gegeben werden. Die Defizite wurden gemeinsam mit dem Generalsekretär des entsprechenden Departements eruiert und Vorschläge für eine erfolgreiche Durchführung des Audits im Jahr 2011 erarbeitet (vgl. ausserdem die Ausführungen zur Informationssicherheit Seiten 19 ff.).

Nutzen Obwohl im Vorbereitungsgespräch mit der Amtsstellenleitung auf den Nutzen des Audits für sie hingewiesen wurde, scheint diese Botschaft in der Führungsebene nicht wirklich angekommen zu sein. Die Leitung trägt – in rechtlicher wie in technischer Hinsicht – die Verantwortung für das grundrechtskonforme Datenbearbeiten der Amtsstelle. Ein Audit kann bestätigen, dass diese Anforderung erfüllt ist, oder aufzeigen, wo Massnahmen ergriffen werden müssen, damit ein rechtskonformer Zustand hergestellt werden kann. Er ist in diesem Sinne eine Unterstützung für die Amtsleitung.

Schengen

Schengen-Kontrolle Abgestimmt mit anderen Kantonen (u.a. Basel-Landschaft, Bern, Zug) liess der Datenschutzbeauftragte 2009/2010 die Zugriffsberechtigungen der kantonalen Stellen auf das Schengener Informationssystem (SIS) durch eine externe Revisionsgesellschaft kontrollieren. Im Grossen und Ganzen konnte festgestellt werden, dass die baselstädtischen Behörden korrekt mit dem neuen Instrument umgehen. Einzig im Bereich der Verwaltung der Berechtigungen mussten geringfügige Verbesserungen verlangt werden. So wurde eine jährliche Kontrolle der Zugriffsberechtigungen etabliert und insbesondere bei der Alarmzentrale in Erinnerung gerufen, dass das Zugriffsprotokoll beim Bundesamt für Polizei (fedpol) systembedingt nur den Namen des abrufenden Benutzers registriert – also denjenigen des Mitarbeiters in der Einsatzzentrale –, während die/der Polizist(in) auf Patrouille, die/der via Funk die Abfrage tatsächlich auslöst, nicht verzeichnet wird. Die übrigen Verbesserungsvorschläge betrafen allesamt Fragestellungen, welche in die Kompetenz des Bundes fallen.

Ein Audit kann bestätigen, dass ein Datenbearbeiten grundrechtskonform ist, oder aufzeigen, welche Massnahmen ergriffen werden müssen.

Autorisierungen von Online-Zugriffen

24 Autorisierungen Wenn ein öffentliches Organ einem anderen öffentlichen Organ einen Online-Zugriff auf seine Datenbestände einräumt, muss nach Datenschutzgesetz[15] ein Autorisierungsverfahren durchlaufen werden. Im Jahr 2010 wurden 24 Autorisierungen erteilt. Ein Teil dieser «Bewilligungen» betraf bloss Ergänzungen oder Änderungen bereits existierender Autorisierungen, indem etwa der Zugriff auf neue Attribute («Datenfelder») nötig wurde.

Vernetzung

Informationsaustausch kantonsintern Ein regelmässiger Informationsaustausch zu Datenschutzfragen fand mit der Staatskanzlei, der Geschäftsleitung des Justiz- und Sicherheitsdepartements, den Zentralen Informatikdiensten, dem Rechtsdienst des Universitätsspitals und mit dem kantonalen Staatsschutzkontrollorgan statt. Der Datenschutzbeauftragte ist vertreten in der Fachkommission für Informationslogistik (FKIL), in der Fachkommission für Informationssicherheit (FKIS) und erhält regelmässig die Informationen aus der Informatik-Konferenz (IK). Keinen Zugang hatte er zu CONSUL. Er wurde regelmässig aus dem Justiz- und Sicherheitsdepartement, dem Finanzdepartement, dem Präsidialdepartement und zunehmend aus dem Erziehungsdepartement zu Vernehmlassungen zu Erlassen, die für den Datenschutz erheblich sind, eingeladen[16], ebenso vom Grundbuch- und Vermessungsamt.

Interkantonale Zusammenarbeit Das Datenschutzgesetz verpflichtet ausdrücklich zur Kooperation mit den Organen der anderen Kantone, des Bundes und des Auslandes, welche dieselben Aufgaben erfüllen[17]. Der Datenschutzbeauftragte nutzt diese Zusammenarbeit intensiv, um auch von den Aktivitäten und der Kompetenz anderer Kantone zu profitieren. Besondere Berührungspunkte ergeben sich bezüglich der Universitätskinderklinik (UKBB), der Rheinhäfen beider Basel und der grenzüberschreitenden Sportanlagen mit der Datenschutzbeauftragten des Kantons Basel-Landschaft sowie bezüglich der Fachhochschule Nordwestschweiz mit den Datenschutzbeauftragten der anderen Trägerkantone (Aargau, Basel-Landschaft und Solothurn). Eine intensive Zusammenarbeit besteht auch mit dem Datenschutzbeauftragten des Kantons Zürich, u.a. im Zusammenhang mit dem Datenschutz-Audit; mangels eines eigenen Informatikrevisors wurde für die Kontrolltätigkeit die entsprechende Dienstleistung im Kanton Zürich eingekauft. Der grösste Teil der interkantonalen Zusammenarbeit findet aber im Rahmen von privatim, der Vereinigung der schweizerischen Datenschutzbeauftragten, statt. In diesem Rahmen wurde u.a. Themen behandelt im Zusammenhang mit Vernehmlassungen des Bundes zum Polizeiaufgabengesetz und zum Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs, zur unabhängigen Datenschutzaufsicht im Staatsschutz sowie zu Grundbuchdaten im Internet. Ausserdem wurden die Datenschutzfragen im Zusammenhang mit der neuen Spitalfinanzierung und SwissDRG bearbeitet – sie werden im Laufe des Jahres 2011 aktuell werden.

Zusammenarbeit mit dem EDÖB Die kantonalen Datenschutzbeauftragten und der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) haben unterschiedliche Zuständigkeitsbereiche: Für das Datenbearbeiten durch Private und durch Bundesorgane ist der EDÖB zuständig; für das Datenbearbeiten durch kantonale und kommunale öffentliche Organe sind es die kantonalen Datenschutzbeauftragten. Berührungspunkte ergeben sich logischerweise dort, wo Bundes- und Kantonsbehörden zusammenarbeiten, etwa im Zusammenhang mit Schengen oder im Bereich des Staatsschutzes. Die Zusammenarbeit mit dem EDÖB ergibt sich aus der Pflicht zur Koordination bei der Kontrolle des Schengener Informationssystems (SIS). Die seit 2009 bestehende Koordinationsgruppe der schweizerischen Datenschutzbeauftragten tagt deshalb ein- bis zweimal jährlich. Eine in allen Kantonen gleichzeitig durchgeführte und mit dem Bund koordinierte Kontrolle des SIS fand noch nicht statt.

Mitarbeit in interkantonalen und internationalen Gremien Der Datenschutzbeauftragte und seine Mitarbeiterinnen arbeiten aktiv in verschiedenen Gremien mit. Beat Rudin ist Mitglied des Büros von privatim, der Vereinigung der schweizerischen Datenschutzbeauftragten. Ausserdem war er im Berichtsjahr Mitglied der Expertenkommission eHealth des Eidgenössischen Departements des Innern und vertrat privatim in der Arbeitsgruppe «Diagnoseregister» des Bundesamtes für Gesundheit. Schliesslich war er Mitglied des Kernteams der Task Force «Informed Consent für Biobanken», die gemeinsam von der Schweizerischen Akademie der Medizinischen Wissenschaften, der Stiftung biobank-suisse und den Datenschutzbeauftragten der Kantone Zürich und Basel-Stadt getragen wurde. Aufgrund dieser intensiven Auseinandersetzung mit Gesundheitsthemen übernimmt er ab Ende des Jahres auch die Leitung der Arbeitsgruppe Gesundheit (AGX) von privatim, in welcher schon länger Carmen Lindner mitwirkt. Sandra Stämpfli ist Mitglied der Arbeitsgruppe Innere Sicherheit (AGIS) von privatim und vertritt die Kantone im Datenschutzaufsichtsorgan für Schengen (Joint Supervisory Authority, JSA). Barbara Widmer arbeitet in der Arbeitsgruppe Informations- und Kommunikationstechnologie (AG ICT) mit und vertritt privatim im eHealth Suisse-Teilprojekt «Standards und Architektur».

—

1 § 2 Abs. 5 Satz 4 DSG, künftig § 3 Abs. 1 lit. c IDG.
2 z.B. Art. 33 Abs. 1 ATSG.
3 Nach § 15 Abs. 4 Aufenthaltsgesetz sind beispielsweise die Industriellen Werke Basel und andere registerführende Stellen verpflichtet, die Daten, die sind, auf Anfrage der Einwohnerkontrollbehörde unentgeltlich zur Verfügung zu stellen – als nicht von sich aus, sondern nur auf Anfrage, und nicht irgendwelche Daten, sondern nur jene, die zur Bestimmung und Nachführung der Wohnungsnummer einer Person erforderlich sind.
4 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).
5 Grossratsbeschluss Nr. 10/23/5G vom 09.06.2010.
6 Kantonsblatt vom 12. Juni 2010, 914 ff., 919.
7 § 55 IDG.
8 § 25 IDG.
9 § 1 Abs. 2 lit. a IDG.
10 § 75 KV.
11 TB 2009, 17 ff.
12 § 18 Abs. 3 IDG.
13 Art. 54 Abs. 1 und 3 PBG.
14 Stellungnahme vom 8. Dezember 2010.
15 § 10 Abs. 2 DSG; keine Entsprechung im IDG.
16 § 28 lit. c DSG, künftig § 44 lit. f IDG (ausgeweitet auf Erlasse, die für den Umgang mit Informationen oder den Datenschutz erheblich sind).
17 § 28 lit. i DSG, künftig § 48 IDG.

Thema 2

Überwachung am Arbeitsplatz – und das Menschenbild dahinter

Erfahrungsgemäss gibt es immer wieder einzelne Mitarbeiter(innen), welche am Arbeitsplatz nicht bloss ihre Arbeit erledigen. Sie verursachen dem Arbeitgeber unnötige Kosten, vergeuden die Arbeitszeit oder begehen im schlimmsten Fall gar Straftaten. Zweifellos haben Kanton oder Gemeinden als Arbeitgeber ein Interesse, dies zu verhindern. Doch wie weit dürfen sie dabei gehen?

Zwei Anwendungsbereiche

Aktuelle Fälle 2010 Gleich mehrfach tauchten im Jahr 2010 Fragestellungen im Zusammenhang mit der Überwachung am Arbeitsplatz auf. Einerseits ging es um die Auswertung von Telefonranddaten, andererseits um Internetmonitoring.

Auswertung von Telefonranddaten

Fragestellung Hat eine Mitarbeiterin/ein Mitarbeiter zu häufig telefoniert – vor allem: private Telefongespräche vom Arbeitsplatz aus geführt und damit dem Arbeitgeber Kosten verursacht, die nicht mit der Aufgabenerfüllung zusammenhängen?

Rechtsgrundlage Die vom Regierungsrat am 19. Oktober 2010 genehmigte Richtlinie des Zentralen Personaldienstes betreffend Gebrauch von Telefonen und Mobiltelefonen (Telefonrichtlinie) erlaubt die Auswertung von Telefonranddaten (Telefonnummern, Zeiterfassung, Gebühren), wenn der Verdacht besteht, dass eine Mitarbeiterin/ein Mitarbeiter das Telefon missbräuchlich verwendet hat (Ziff. 3 der Telefonrichtlinie). Diese Rechtsgrundlage – Richtlinie des ZPD, nicht Gesetz oder Verordnung – vermag einen Eingriff ins Grundrecht auf informationelle Selbstbestimmung[1] allerdings nicht zu rechtfertigen. Wenn ausgehende Privatgespräche, die bezüglich ihrer Destination oder ihrer (voraussichtlichen!) Dauer über ein vernachlässigbares Mass nicht hinausgehen, erlaubt und auch nicht kostenpflichtig sind (Ziff. 5.1 der Telefonrichtlinie), dann kann von den Mitarbeiter(inne)n auch nicht verlangt werden, dass ihre Gesprächspartner offen gelegt werden.

Früheres Vorgehen Bereits mit dem früheren Datenschutzbeauftragten war abgesprochen, dass die Zentralen Informatikdienste (ZID) Gesuche von Amtsstellen, die eine Detailauswertung bestimmter Telefonanschlüsse bestellen, dem Datenschutzbeauftragten zur Stellungnahme unterbreiten. Dieses Prozedere wurde beibehalten, aber verfeinert mit dem Zweck, die Rechte der betroffenen Mitarbeiter(innen) zu gewährleisten. Wenn ein Gesuch einer Amtsstelle eingeht oder von den ZID dem Datenschutzbeauftragten überwiesen wird, wird zuerst die Begründung überprüft. Als Grund werden in der Regel überdurchschnittlich hohe Gesprächsgebühren angeführt. Als überdurchschnittlich werden gemeinhin monatliche Rechnungsbeträge von über CHF 50.00 angenommen. Nach der positivern Stellungnahme des Datenschutzbeauftragten haben die ZID früher die Auszüge erstellt und der Amtsstelle – in der Regel in elektronischer Form – zugestellt. Damit wurden aber die Zielnummern von Privatgesprächen einer oder mehreren Personen in dieser Amtsstelle bekannt gegeben, obwohl dies zur Abklärung der übermässigen Nutzung nicht erforderlich ist.

Vorgehen Neu wird wie folgt vorgegangen: Die Amtsstellenleitung «bestellt» beim Datenschutzbeauftragten die Detailsauswertung für einen bestimmten Telefonanschluss in ihrem Verantwortungsbereich und begründet das Begehren.

— Der Datenschutzbeauftragte prüft die Begründung (i.d.R. überdurchschnittlich hohe Gesprächsgebühren) und holt bei den ZID den Detailauszug ein.
— Der Datenschutzbeauftragte erstellt aus den Rohdaten drei Listen (chronologisch, nach Gebührenhöhe und nach angerufenen Nummern geordnet).
— Er stellt die drei Listen auf Papier der betroffenen Person zu mit der Aufforderung, die privat abgerufenen Nummern (nur die Nummern, nicht Zeitpunkt, Dauer und Gebühren) abzudecken und die entsprechend behandelte Liste innert einer Woche einer vorgesetzten Stelle zukommen zu lassen.

— Eine Kopie des Schreibens (aber logischerweise ohne die Beilagen) geht an die bezeichnete vorgesetzte Stelle.
— Die betroffene Person deckt bei den Privatgesprächen die angerufene Telefonnummer ab und reicht die Listen an die bezeichnete vorgesetzte Stelle weiter.

Resultat Auf diese Weise kann anschliessend die personalrechtliche Frage der übermässigen Telefonnutzung gemeinsam mit der betroffenen Person behandelt werden. Wo zugegebenermassen Privatgespräche geführt werden, bleiben die verursachten Kosten ersichtlich, während die Gesprächspartner wiederum geheim bleiben. Übermässiges privates Telefonieren kann so erkannt werden, ohne dass das Grundrecht auf informationelle Selbstbestimmung verletzt wird.

Internet-Überwachung

Die Versuchungen des Internets Offenbar können auch immer wieder einzelne Mitarbeiter(innen) den Versuchungen des Internets nicht widerstehen und nutzen es übermässig oder greifen auf unerlaubte und unerwünschte Inhalte zu. 2010 tauchten deshalb auch mehrere Fälle zum Thema Internetüberwachung auf. Dabei standen zwei verschiedene «Auslösemomente» am Anfang: ein Generalverdacht oder ein Individualverdacht.

Individual- oder Generalverdacht Es kommt vor, dass gegen eine(n) Mitarbeiter(in) konkrete Verdachtsmomente bestehen, sei es bezüglich des Inhalts (Pornografie, Rassismus u.ä.), sei es bezüglich des Umfangs der Nutzung. Eine andere Dimension liegt vor, wenn generell gegenüber allen Mitarbeiter(inne)n oder gegenüber bestimmten Gruppen von Mitarbeiter(inne)n der Verdacht besteht, Arbeitszeit mit Surfen im Internet zu vertrödeln («die Buchhaltung arbeitet höchstens 70%»). Hier geht es in der Regel um den Umfang der Internetnutzung, weniger um verbotene oder verpönte Inhalte.

Umfang oder Inhalt Die Internetnutzung kann in verschiedener Hinsicht unerwünscht sein: Es kann sich einerseits um übermässige Nutzung handeln, wenn beispielsweise ein(e) Mitarbeiter(in) stundenlang im Internet surft; möglicherweise handelt es sich sogar um eine suchtähnliche Nutzung des Internets (z.B. bei sozialen Rollenspielen u.ä.). Andererseits kann auch der Inhalt zum Problem werden, etwa wenn Websites mit verbotenem oder verpöntem Inhalt aufgerufen werden.

Strafbare oder verpönte Inhalte Bezüglich des Inhalts ist nochmals zu unterscheiden: Es gibt Inhalte, deren Konsum und/oder Weiterverbreitung vom Strafgesetzbuch unter Strafe gestellt werden, beispielsweise sog. harte Pornografie (insb. Kinderpornografie), Rassismus o.ä. Werden solche Straftatbestände erfüllt, kommt die Strafverfolgung zum Zug. Andere Inhalte sind wohl nicht verboten, aber ebenfalls unerwünscht, beispielsweise Sexseiten unterhalb der Strafbarkeitsgrenze; sie werden hier als «verpönt» bezeichnet. Gegen die Verletzung entsprechender Verbotsnormen greifen nur personalrechtliche Massnahmen.

Beweismittel Wie können solche Verstösse bewiesen werden? Beim «Ausgang» vom Kantonsnetzwerk ins Internet fallen sog. Log-Daten an. Sie zeigen, von welcher IP-Adresse (eine Adresse, welche – vergleichbar mit einer Telefonnummer – jeder Station im Netzwerk zugewiesen wird) aus und von welcher Benutzerin/welchem Benutzer welche Inhalte im Internet aufgerufen wurden. Diese Log-Daten werden über eine bestimmte Zeitdauer aufbewahrt und können nach verschiedenen Kriterien ausgewertet werden. Es können bestimmte IP-Adressen oder Benutzerkennungen herausgefiltert werden, aber auch bestimmte Inhalte (wobei der Beweiswert, solange die Benutzeridentifikation nicht stärker wird, beschränkt ist).

Offenbar können einzelne Mitarbeiter(innen) den Versuchungen des Internets nicht widerstehen und greifen auf verbotene oder verpönte Inhalte zu.

Auswertung bezüglich des Inhalts Die Auswertung ist jedoch nicht trivial. Erstens fallen Unmengen von Daten an, pro Monat etwa 5 Gigabyte. Es wird nämlich jedes einzelne Element, aus welchem eine Website aufgebaut ist, erfasst. Das können gut und gerne 20 bis 50 Einträge sein, wenn eine einzige Website aufgerufen wird. Zweitens ist die Interpretation nicht einfach: Dass eine bestimmte Adresse auftaucht, heisst noch lange nicht, dass ein(e) Mitarbeiter(in) diese Seite auch selber aufgerufen hat. Ein Aufruf der Website www.bazonline.ch generiert u.a. diverse Aufrufe auf Werbeservern und auf Facebook. Für Irritationen hat im Jahr 2010 etwa die Erkenntnis geführt, dass sich von einem Monat zum nächsten die Anzahl Facebook-Aufrufe um den Faktor 7.3 vervielfacht hat – ohne dass die Datenmenge sich relevant verändert hätte. Die Zahlen vorher und die Zahlen nachher blieben jeweils stabil. Dass sich die (wohl kaum dienstlich

>

begründete) Facebook-Nutzung explosionsartig vermehrte, führte zu einer gewissen Alarmstimmung … Fehlalarm! Des Rätsels Lösung: Es war der Zeitpunkt, an welchem die Basler Zeitung anfing, aktiv Facebook zu nutzen und auf der Website www.bazonline.ch Facebook-Links einfügte. Die 7.3-fache Vervielfachung der Facebook-Einträge in den Log-Daten konnte also ohne einen einzigen zusätzlichen Facebook-Aufruf durch eine Mitarbeiterin/einen Mitarbeiter entstehen.

Auswertung bezüglich des Umfangs Erst recht schwierig wird die Interpretation bezüglich des Umfangs der Internetnutzung. Wenn ein(e) Mitarbeiterin jetzt die BaZ-Website aufruft und dann erst eine Stunde später die nächste Website – hat sie/er dann eine Stunde lang Zeitung gelesen? Wohl kaum. Wenn es ein sehr langes Bundesgerichtsurteil auf der Website www.bger.ch war, dann dauerte die Lektüre vielleicht schon so lange. Umgekehrt: Wenn die Log-Daten zeigen, dass ein(e) Mitarbeiter(in) den ganzen Nachmittag über im Rhythmus weniger Minuten Inhalte einer bestimmten Website aufgerufen hat? Auch das sagt noch nichts über das tatsächliche Verhalten aus. Wenn eine Website einen Live-Ticker eingerichtet hat oder ein(e) Mitarbeiter(in) einen RSS-Service nutzt, dann aktualisiert sich die Seite unablässig, solange sie offen ist – auch wenn die Mitarbeiterin/der Mitarbeiter selber gar nicht auf die Seite schaut, an einem Word-Dokument schreibt oder eine Besprechung durchführt … Mit andern Worten: Eine maschinelle Auswertung bezüglich des zeitlichen Umfangs der Internetnutzung ist kaum aussagekräftig.

Rechtliche Beurteilung

Bestehende Regelung Die Auswertung von Log-Daten stellt – wenn sie personenbezogen erfolgt – ein Bearbeiten von Personendaten dar. Anders als beim Blick auf Telefonnummern wird bei der Internet-Überwachung der Inhalt der Kommunikation offen gelegt. Sie ist damit eine Einschränkung des Grundrechts auf Datenschutz[2], muss deshalb auf einer gesetzlichen Grundlage basieren und verhältnismässig sein[3]. Grundsätzlich kann der Kanton als Arbeitgeber regeln, ob und inwieweit den Mitarbeiter(inne)n das Internet am Arbeitsplatz zur Verfügung gestellt wird und wie sie es nutzen dürfen. Wenn er die private Nutzung nicht ausnahmslos ausschliesst, wird er auch regeln dürfen, wie er die Einhaltung der Regeln überwacht und durchsetzt. Greift er dabei in Grundrechte ein, dann muss die entsprechende gesetzliche Grundlage vorhanden und hinreichend bestimmt sein. Aktuell regelt einzig eine Weisung der Informatik-Konferenz von 2003/2004 die Nutzung des Internets und die allfällige Auswertung der Log-Daten. Sie ist bezüglich der Zulässigkeit der Auswertung eindeutig – sie lässt, ausser im Falle des Verdachts auf strafrechtlich verbotene Handlungen, einzig die prospektive Auswertung nach vorgängiger Ankündigung zu –, wurde aber offensichtlich in der Vergangenheit sehr extensiv ausgelegt. Die ZID verwiesen deshalb mehrere Antragsteller im Jahr 2010 an den Datenschutzbeauftragten mit der Bitte, die rechtliche Zulässigkeit abzuklären. Ein Amtsstellenleiter etwa wollte die Log-Daten eines Mitarbeiters für die letzten eineinhalb Jahre auswerten, um ihm zu beweisen, wie viele Stunden er nichtdienstlich im Internet verbracht und deshalb nachzuholen habe. Aus einem anderen Departement kam das Begehren, im gesamten Departement regelmässig bis auf Stufe Abteilung (z.T. mit bloss einigen wenigen Mitarbeiter[inne]n) eine Auswertung zu erstellen, um nachweisen zu können, dass in bestimmten Abteilungen nicht mehr als 70% gearbeitet werde.

Eine maschinelle Auswertung bezüglich des zeitlichen Umfangs der Internetnutzung ist kaum aussagekräftig.

Neue Regelung Die verschiedenen Bedürfnisse haben den Datenschutzbeauftragten veranlasst, die Frage der Regelung von Internetnutzung und Überwachung genereller auf die Traktandenliste zu setzen. Eine Arbeitsgruppe mit Vertretern des Zentralen Personaldienstes (ZPD), der Fachstelle Informatik und Organisation (FIO) und dem Datenschutzbeauftragten bereitet eine belastbare Rechtsgrundlage für die Nutzung von E-Mail und Internet und die entsprechende Überwachung vor.

Mögliches Regelungskonzept

Klare Regelung und nicht-personenbezogene Systemüberwachung Dabei könnte das Konzept für den «Regelbetrieb» wie folgt aussehen:

— Es wird möglichst klar geregelt, wie Internet und E-Mail genutzt werden dürfen. Insbesondere stellt sich die Frage, ob die private Nutzung – wie bisher – überhaupt und gegebenenfalls mit welchen Einschränkungen zugelassen werden soll oder nicht. Ein komplettes Verbot der privaten Nutzung erscheint unseres Erachtens allerdings als unrealistisch, unverhältnismässig

und im Vergleich zu anderen öffentlichen und privaten Arbeitgebern unattraktiv.

— Wenn Einschränkungen vorgesehen werden sollen, ist möglichst klar zu regeln, welche Nutzungen verboten oder verpönt sein sollen. Während der Verweis auf die strafrechtlich verbotenen Inhalte relativ einfach anzubringen ist, wird es schwierig sein, das verpönte Verhalten so verbindlich und verständlich zu umschreiben, dass im Falle eines Verstosses dagegen auch Sanktionen rechtlich hieb- und stichfest begründet werden können. Ausserdem dürfte die früher übliche mengenmässige Beschränkung aufgrund der Bandbreitenproblematik angesichts der laufenden Entwicklungen zunehmend unerheblich sein.

— In einer Systemüberwachung wird nicht-personenbezogen die Internetnutzung überwacht. Dabei können etwa eine «Rangliste» der aufgerufenen Websites oder gezielt Auswertungen nach bestimmten Websites (z.B. Facebook) erstellt werden. Ein Gremium (eine «Monitoringstelle»), in welchem wohl das Personalwesen, die Führungsebene – beispielsweise über eine Vertretung der Generalsekretärenkonferenz – und eventuell auch die Kommunikation vertreten sein sollten, beobachtet das Geschehen und schlägt nötigenfalls Massnahmen vor; es könnte z.B. vorschlagen, den Zugang zu bestimmten Seiten (z.B. Facebook) ganz oder vorübergehend sperren zu lassen, falls die Zugriffe darauf ein unerwünschtes Mass erreichen und andere Massnahmen (z.B. die Erinnerung an die Nutzungsregeln) keine Besserung gebracht haben.

— Bei der Systemüberwachung können beispielsweise mit einer Blacklist – eine extern gepflegte Liste von Websites, deren Inhalte bekanntermassen verboten (oder verpönt) sind – Zugriffe auf unerlaubte Inhalte erkannt werden.

— Eine Systemüberwachung ist nicht-personenbezogen, wenn auch in der kleinsten Auswertungseinheit der Schluss auf eine Person nicht mehr möglich ist. Es dürfte angebracht sein, hier eine Faustregel zu beachten, die seit Jahren im Bereich der Statistik gilt: In der kleinsten ausgewiesenen Organisationseinheit müssen mindestens die Daten von 20 Personen verarbeitet sein (bei besonderen Personendaten: von mindestens 50 Personen).

Eskalation bei Missbrauchsverdacht Für die zweite Phase, bei konkreten Verdachtsmomenten, könnte das Konzept wie folgt aussehen:

— Falls ein Verdacht auf die Begehung strafbarer Handlungen (z.B. harte Pornografie, Rassismus, Betrug, Bestechlichkeit, Amtsgeheimnisverletzung u.ä.) besteht, ist der Fall unverzüglich der Staatsanwaltschaft zu übergeben – unabhängig davon, ob der Verdacht aufgrund der nicht-personenbezogenen Systemüberwachung zustande gekommen ist oder ob er durch Beobachtungen von Vorgesetzten oder Kolleg(inn)en entstanden ist (vgl. dazu auch Seite 37). Die Staatsanwaltschaft kann aufgrund ihrer gesetzlichen Grundlage, der schweizerischen Strafprozessordnung, auch retrospektiv die Internetnutzung auswerten, also beispielsweise bei den ZID Log-Daten beschlagnahmen und forensisch durchsuchen lassen.

Falls ein Verdacht auf die Begehung strafbarer Handlungen besteht, ist der Fall unverzüglich der Staatsanwaltschaft zu übergeben.

— Falls der Verdacht bloss auf personalrechtliche, nicht strafrechtlich zu ahndende Verstösse (z.B. Zugriff auf verpönte Inhalte) durch eine unbekannte «Täterschaft» geht, ist eine retrospektive, d.h. rückwärts gewandte Auswertung der Log-Daten nicht zulässig (allenfalls mit einer Ausnahme: siehe unten). Hingegen kann, nachdem die Nutzer(innen) nochmals auf die geltenden Nutzungsregeln hingewiesen worden sind, die Durchführung von personenbezogenen Auswertungen angekündigt werden. Anschliessend können während einer zu bestimmenden Dauer (z.B. während eines Monats) stichprobenweise (z.B. an vier oder fünf Tagen) Auswertungen vorgenommen werden. Falls wiederum Zugriffe auf verpönte Inhalte festgestellt werden, kann nun die fehlbare Person eruiert werden. Das «Resultat» ist in einem noch festzulegenden Verfahren der entsprechenden Amtsleitung zukommen zu lassen, damit diese die angemessenen personalrechtlichen Massnahmen treffen kann.

— Richtet sich der Verdacht – z.B. aufgrund von Beobachtungen durch Vorgesetzte oder Kolleg(inn)en – gegen eine bestimmte Person (oder gegen bestimmte Einzelpersonen), dann sind die Massnahmen nur ihr (bzw. ihnen) gegenüber anzudrohen und durchzuführen. Die Auswertung kann in solchen Fällen nicht nur den Inhalt, sondern auch den (zeitlichen) Umfang der Internetnutzung zum Gegenstand haben.

>

— In schweren Fällen, etwa wenn bereits personalrechtliche Massnahmen ergriffen werden mussten (z.B. ein Verweis oder eine Bewährungsfrist), kann die Auswertung auch für eine längere Zeitdauer (mindestens für die gesamte Dauer der Bewährungsfrist, allenfalls auch länger, falls ein Rückfall nicht unwahrscheinlich erscheint) und nicht bloss stichprobenweise durchgeführt werden. Auch hier ist das «Resultat», der Untersuchungsbericht, in einem noch festzulegenden Verfahren der entsprechenden Amtsleitung zukommen zu lassen, damit diese die notwendigen weiteren personalrechtlichen Massnahmen treffen kann.
— Eine Ausnahme vom Verbot der rückwirkenden Auswertung unterhalb der Strafbarkeitsgrenze könnte im Zusammenhang mit der E-Mail-Nutzung allenfalls ausdrücklich vorgesehen werden, weil Mobbing strafrechtlich nicht erfasst ist.
— Für die Anordnung und Durchführung der Untersuchung sollte ein Gremium eingesetzt werden, in welchem wohl Recht und Personalrecht (z.B. aus dem ZPD) vertreten sein müssen; der Datenschutzbeauftragte könnte hier beratend involviert sein. Es ist davon auszugehen, dass dieses Gremium für die konkrete Durchführung Leute mit Spezialwissen beiziehen kann oder muss.

> Mit technischer Überwachung können Mankos in der Personalführung nicht kompensiert werden.

Ausblick

Rechtsstaatlich korrekt Mit einer solchen Regelung, die mindestens auf Verordnungsstufe erlassen werden sollte, können die Internetnutzung und ihre Überwachung auf eine rechtsstaatlich korrekte Weise normiert werden. In den Fällen, in welchen ein(e) Mitarbeiter(in) konkret des Verstosses gegen Regeln verdächtigt wird, bietet sie den nötigen Spielraum für die notwendigen Massnahmen.

Keine Kompensation für Führungsschwäche Trotzdem: Es werden damit nicht alle Probleme gelöst – vor allem nicht jene, die in einen Generalverdacht münden. Mit technischer Überwachung können Mankos in der Personalführung nicht kompensiert werden. Wenn Mitarbeiter(innen) nicht arbeiten und die Vorgesetzten dies nicht an der abgelieferten Arbeitsleistung feststellen, dann liegt das Problem weniger auf der Mitarbeiter- als viel mehr auf der Führungsebene.

Vertrauens- oder Misstrauenskultur? Ausserdem muss bei einer Regelung der kulturelle Aspekt im Auge behalten werden. Aus arbeitspsychologischer Sicht ist es klar, dass Menschen ihre innere Motivation und ihr eigenverantwortliches Handeln aufgeben, wenn technische Überwachung ein grundsätzliches Misstrauen vermittelt (Gudela Grote[4]). Das Personalleitbild des Kantons baut auf einem anderen Menschenbild auf! Stichworte sind etwa Vertrauen sowie Mitverantwortung und Mündigkeit der Mitarbeiter(innen). Deshalb ist es dringend notwendig, das Element der Überwachung nicht leichtfertig einzusetzen.

Kurz & bündig (Management Summary)

Regelung und nicht personenbezogene Systemüberwachung Internetmonitoring braucht eine verlässliche Rechtsgrundlage. Es müssen klare Regelungen für die Nutzung aufgestellt werden. Im Normalbetrieb darf nur eine nicht personenbezogene Systemüberwachung stattfinden. Eine «Monitoringstelle» behält die Entwicklung im Auge und beantragt allenfalls notwendige rechtliche, organisatorische oder technische Massnahmen.

Personenbezogene Auswertung von Log-Daten Bestehen aus diesem Monitoring oder aus Beobachtungen durch Vorgesetzte oder Kolleg(inn)en Hinweise für einen Missbrauch, kann eine personenbezogene Auswertung angekündigt werden; ab diesem Zeitpunkt darf stichprobenweise personenbezogen ausgewertet werden. Den Auftrag dazu soll ein dafür fest eingesetztes Gremium erteilen. Ausser im Fall von Cybermobbing darf aber bloss prospektiv, d.h. ab der Ankündigung, personenbezogenen ausgewertet werden. Besteht der Verdacht, dass strafbare Handlungen erfolgt sind, dann ist der Fall unverzüglich der Staatsanwaltschaft zu übergeben, welche aufgrund ihrer strafprozessualen Kompetenzen Log-Daten auch retrospektiv auswerten darf.

Auch eine Frage der «Unternehmens-Kultur» Es muss darauf geachtet werden, dass mit einer Überwachung, die wegen einigen wenigen schwarzen Schafen eingerichtet wird, nicht ein Menschenbild vermittelt wird, das dem Personalleitbild des Kantons diametral widerspricht.
—

1 Art. 13 Abs. 2 BV, § 11 lit. j KV.
2 Recht auf informationelle Selbstbestimmung nach Art. 13 Abs. 2 BV und § 11 lit. j KV.
3 Art. 36 Abs. 1 und 2 BV, § 13 Abs. 1 und 2 KV, §§ 5 und 6 DSG, § 9 IDG.
4 Gudela Grote, Totale Überwachung oder blindes Vertrauen? Vom Menschenbild, das sich hinter der technischen Kontrolle am Arbeitsplatz verbirgt, digma 2004, 102-105.

Thema 3 Informationssicherheit – eine Qualität der öffentlichen Verwaltung?

Die Verwaltungsprozesse werden zunehmend von Informatik durchdrungen. Staatliche Aufgabenerfüllung wird deshalb auch immer stärker von Informatik abhängig. Die damit einhergehenden Risiken müssen beherrscht werden. In diesem Bereich besteht Handlungsbedarf – nicht weil eklatante Lücken nachgewiesen wurden, sondern weil kaum bekannt ist, welche Risiken überhaupt bestehen.

Ausgangslage

Angriff auf die Informatik des EDA Im Oktober 2009 war die Informatik des Eidgenössischen Departements für auswärtige Angelegenheiten (EDA) Ziel einer massiven Attacke. Was genau die Angreifer, die offensichtlich sehr professionell vorgegangen sind, angerichtet haben, ist nicht offiziell bekannt. Die damals ergriffenen Sofortmassnahmen – die gesamte Verbindung zum Internet wurde vorübergehend vollständig unterbrochen – sowie die seither erfolgten erheblichen Bemühungen zur Verbesserung der Informationssicherheit lassen darauf schliessen, dass der Angriff alles andere als harmlos gewesen ist.

Geschichten aus einer anderen Welt? Könnte das auch in Basel geschehen? Vielleicht lockt der Bund als Angriffsziel mehr – aber es geht bei der Informationssicherheit nicht nur um die Abwehr von Angriffen, sondern generell um das zuverlässige Funktionieren einer Verwaltung und den wirksamen Schutz der Informationen, welche sie bearbeitet.

ICT als Chance Die Informations- und Kommunikationstechnologie (ICT) wird zu Recht als Chance (auch) für die Verwaltung angesehen. Die stetige Weiterentwicklung der Informationssysteme und die zunehmende Verschmelzung der betriebsinternen Netze mit dem Internet ermöglichen es auch den öffentlichen Organen, ihre Leistungen näher an ihre Anspruchsgruppen – Bürger(innen), Unternehmen und andere öffentliche Organe – zu bringen und an deren Bedürfnisse anzupassen. Die Leistungen können effizienter und für die Anspruchsgruppen transparenter erbracht werden. Diese Entwicklung wird auch bereits in der vom Regierungsrat 2007 beschlossenen Informatikstrategie des Kantons Basel-Stadt untermauert. Eine Folge dieser Entwicklung sind unter anderem das kantonale Projekt Bewilligungsplattform und das Impulsprogramm sowie auf Stufe Bund etwa die «IKT-Plattform für den sicheren Datenaustausch (sedex)» im Bereich e-Government.

Durchdringung der Verwaltungsprozesse Die fachlichen Prozesse werden so weit von ICT-Dienstleistungen durchdrungen und unterstützt, dass diese integraler Bestandteil der Leistungserbringung geworden sind. Die Informatik hat einen direkten Einfluss auf die Qualität und Zuverlässigkeit der Leistungserbringung und steuert im Idealfall einen wesentlichen Beitrag zur Ereichung der strategischen und betrieblichen Ziele bei.

ICT aber auch als Risiko Der boomende Einsatz der Informations- und Kommunikationstechnologie hat aber nicht nur eine Sonnen-, sondern auch eine Schattenseite. Die Abhängigkeit von der Informatik hat nicht nur in der Privatwirtschaft, sondern auch in der Verwaltung dramatisch zugenommen. Damit entstehen neue Risiken, die es zu beherrschen gilt. Voraussetzung dafür ist eine Gesamtsicht, welche die Durchdringung der Verwaltungsprozesse durch die ICT aufzeigt und dadurch ermöglicht, die Risiken und Chancen zu erkennen und zu bewerten. In der Privatwirtschaft haben sich dazu Frameworks (IT-Governance-Regelwerke wie CoBIT u.ä.) etabliert. International anerkannte Standards widerspiegeln den Stand der Technik (z.B. der BSI-Grundschutz nach dem (deutschen) Bundesamt für Sicherheit in der Informationstechnik, die Standards des British Standards Institution oder der International Standard Organization ISO).

>

Schadenspotenzial Die Informatik ist angreifbar. Die Schäden, die mit Attacken wie etwa gegen das EDA angerichtet werden können, sind enorm. Es können etwa Systeme oder Anwendungen ausfallen. Während des Ausfalls ist die Leistungserbringung gestört oder unmöglich, was bei Anwendungen, die auf eine hohe Verfügbarkeit angewiesen sind (z.B. Alarm- und Führungssysteme im Blaulichtbereich, Steuerungssysteme im Versorgungsbereich, Datenmarkt, Bewilligungsplattform) erhebliche Negativauswirkungen haben kann. Eine andere Gefahr liegt darin, dass Daten aus Systemen zugänglich und/oder manipulierbar werden. Das ist bei Anwendungen, die auf eine hohe Vertraulichkeit (z.B. im Gesundheits-, Steuer- oder Strafverfolgungsbereich) oder auf hohe Integrität (z.B. bei Registern, etwa im Zivilstandsbereich oder beim Grundbuch) angewiesen sind, gravierend. Dabei können nicht nur Informationen über die staatliche Aufgabenerfüllung («staatliche Daten») offen gelegt oder verändert werden, sondern auch Informationen über Private (Privatpersonen und Unternehmen), welche ihre Informationen einem öffentlichen Organ – unfreiwillig aufgrund einer gesetzlichen Verpflichtung oder freiwillig beispielsweise im Rahmen eines Gesuchsverfahrens – anvertraut haben, zugänglich und manipulierbar werden.

Von «aussen» und von «innen» Attacken können nicht nur von «aussen» kommen, sondern auch von «innen». Mitarbeiter(innen) seien das grösste Risiko, heisst es immer wieder in verkürzter Weise. Das mag stimmen, wenn man nicht bloss die absichtliche, sondern auch die unbeabsichtigte Schädigung in Betracht zieht. Auf jeden Fall zeigt dies, dass Abwehrstrategien, die ausschliesslich auf einer Trennung von «innen» und «aussen» basieren, der heutigen Bedrohungslage nicht mehr gerecht werden.

Ausgehebelt Ausserdem wird diese Vorstellung – «innen» die «Guten», «aussen» die «Bösen» – je länger desto mehr überholt und ausgehebelt durch die technologische Entwicklung: Längst ist auch das baselstädtische Netzwerk (DAtenNEtz Basel-Stadt DANEBS) nicht mehr bloss ein statisches Netz mit lauter fix eingerichteten Stationen, an denen immer die selben Mitarbeiter(innen) mit zentral verwalteten Programmen arbeiten. Der Zugriff von Externen für die Entwicklung und Wartung von Systemen, die Nutzung von Anwendungen ausserhalb der kantonalen Informatik (Bundesanwendungen, Invalidenversicherung, eVoting) und die Zulassung von mobilen Geräten (der Zugriff über Mobiltelefone, Notebooks und andere mobile Geräte auf E-Mails und Daten) lassen die Idee eines wirksamen Perimeterschutzes an der herkömmlichen Netzgrenze verblassen. Entwicklungen wie «bring your own device» (die Bearbeitung von geschäftlichen Daten auf irgendwelchen, dienstlichen wie privaten Geräten, z.B. beim Home Office, bei Telework), in der Privatwirtschaft längst angewandt, machen auch vor den Amtstüren nicht Halt. Sie werden die Herausforderungen für die Informationssicherheit noch zusätzlich steigern.

Informationssicherheit und Datenschutz

Zusammenhang Was kümmert den Datenschutzbeauftragten die Informationssicherheit? Je mehr ICT die staatliche Aufgabenerfüllung durchdringt, umso stärker sind die Auswirkungen der Informationssicherheit, insbesondere der fehlenden oder ungenügenden Informationssicherheit. Nicht ohne Grund waren die ersten gesetzlichen Bestimmungen, welche zur Informationssicherheit verpflichteten, diejenigen der Datenschutzgesetze[1]. Das Informations- und Datenschutzgesetz verdeutlicht diese Bedeutung in seinem § 8 (siehe Kästchen auf der gegenüberliegender Seite). Die Begründung ist logisch: Es droht eine Verletzung des Datenschutzes, wenn Personendaten Dritten unrechtmässig zur Kenntnis gelangen, unrichtig oder unvollständig oder bei Bedarf nicht verfügbar sind.

Abwehrstrategien, die ausschliesslich auf einer Trennung von innen und aussen basieren, werden der heutigen Bedrohungslage nicht mehr gerecht.

Verantwortlichkeit Wer für die Gewährleistung der Informationssicherheit verantwortlich ist, ist klar: Die Verantwortung für den Umgang mit Informationen trägt dasjenige öffentliche Organ, das die Informationen zur Erfüllung seiner gesetzlichen Aufgaben bearbeitet oder bearbeiten lässt[2] (siehe Kästchen auf der gegenüberliegenden Seite). Mit anderen Worten: Auch wenn ein öffentliches Organ die IT-Leistungen bei einem Dritten (Leistungserbringer, z.B. die Zentralen Informatikdienste ZID, aber auch externe IT-Anbieter) bezieht, bleibt es für den Umgang vollumfänglich verantwortlich; es muss deshalb als Leistungsbezüger dafür sorgen, dass der Leistungserbringer seinen Teil zur Gewährleistung der Informationssicherheit beiträgt. Nicht zu vergessen ist, dass die Verantwortlichen auch befähigt werden müssen, ihre Verantwortung wahrzunehmen.

Aktivitäten des Datenschutzbeauftragten

Festlegung des Schutzbedarfs Bereits im Jahr 2009 hat der Datenschutzbeauftragte festgestellt, dass eine der Grundbedingungen für die Gewährleistung der Informationssicherheit nicht gegeben ist: Der Leistungserbringer kann nicht ermessen, welche Sicherheit er erbringen muss, wenn er nicht weiss, welcher Schutzbedarf besteht. Dabei ist es Sache des Leistungsbezügers (die Amtsstelle, welche eine Informatikleistung z.B. bei den ZID bezieht), den Schutzbedarf zu bestimmen und vom Leistungserbringer die entsprechende Sicherheitsleistung zu fordern. Nur der Leistungsbezüger weiss, welche Informationen (z.B. besondere Personendaten) bearbeitet werden und wie hoch der Schutzbedarf aus Sicht des Persönlichkeitsschutzes der betroffenen Personen (insb. bezüglich Vertraulichkeit und Integrität) und aus dem Blickwinkel der Aufgabenerfüllung (insb. bezüglich Verfügbarkeit und Integrität, aber auch bezüglich Vertraulichkeit, wenn es um den Schutz öffentlicher Interessen geht) ist. Im Jahr 2010 wurde ein Bewertungstool gemeinsam mit der Fachstelle Informatik und Organisation (FIO) entwickelt und in konkreten Anwendungsfällen auf seine Umsetzbarkeit in der Praxis getestet. Seither steht das Tool der Verwaltung zur Verfügung.

Datenschutz-Audit Die Informationssicherheit wird auch beim Datenschutz-Audit unter die Lupe genommen (siehe dazu die Ausführungen auf den Seiten 11 f.). Ausserdem ist Informationssicherheit immer auch das Thema der regelmässigen Zusammenarbeit mit den ZID und der FIO.

Aufbau des fachlichen Know-hows Es hat sich gezeigt, dass es notwendig ist, beim Datenschutzbeauftragten auch das entsprechende fachliche Know-how aufzubauen. Mit dem Budget 2011 haben wir deshalb eine zusätzliche Stelle beantragt, welche schwergewichtig der Stärkung in diesem Bereich dienen soll.

Informationssicherheit im Kanton

Fehlende Grundlagen Wie steht es mit der Informationssicherheit in der Verwaltung des Kantons Basel-Stadt? Diese Frage lässt sich zurzeit nicht zuverlässig beantworten. Im Rahmen unserer Kontroll- und Beratungstätigkeit mussten wir feststellen, dass, um dies beurteilen zu können, weitgehend die Grundlagen fehlen. Daraus kann nicht abgeleitet werden, die Informationssicherheit sei nicht gegeben – aber eben auch nicht das Gegenteil.

Feststellungen Unsere Feststellungen im Einzelnen:

— Eine Einsicht in die Wichtigkeit der Informationssicherheit ist durchaus gegeben, jedoch fehlt es oft am Erkennen der diesen zugrunde liegenden Gefährdungen und Bedrohungen und dementsprechend an den notwendigen Gegenmassnahmen.

— Nicht selten fehlt aber schon der Überblick über die eingesetzte Informatik (wo laufen welche Anwendungen, woher kommen welche Informationen bzw. wohin gehen sie, wer hat Zugriff auf welche Informationen, wo werden Informatikleistungen von Dritten bezogen?) – das Wissen ist zwar bei den einzelnen Spezialisten vorhanden, aber nicht in einer Form visualisiert, dass sich die Leitungsebene mühelos einen Überblick verschaffen kann.

— Damit mangelt es häufig ebenso an der Übersicht, welche Geschäftsprozesse von welchen IT-Leistungen abhängig sind, weshalb auch die entsprechenden Risiken kaum bekannt sind.

— Den mit der Informationssicherheit betrauten Mitarbeiter(innen) kommen diesbezüglich kaum Kompetenzen zu; ausserdem vermissen sie klare Vorgaben.

>

Informations- und Datenschutzgesetz

Verantwortung

§ 6. Die Verantwortung für den Umgang mit Informationen trägt dasjenige öffentliche Organ, das die Informationen zur Erfüllung seiner gesetzlichen Aufgaben bearbeitet.
2 Bearbeiten mehrere öffentliche Organe einen gemeinsamen Informationsbestand, regeln sie die Verantwortung.

Bearbeiten im Auftrag

§ 7. Das öffentliche Organ kann das Bearbeiten von Informationen Dritten übertragen (...).
2 Es bleibt für den Umgang mit Informationen nach diesem Gesetz verantwortlich.

Informationssicherheit

§ 8. Das öffentliche Organ schützt Informationen durch angemessene organisatorische und technische Massnahmen.
2 Die Massnahmen richten sich nach den folgenden Schutzzielen:
a) Informationen dürfen nicht unrechtmässig zur Kenntnis gelangen (Vertraulichkeit);
b) Informationen müssen richtig und vollständig sein (Integrität);
c) Informationen müssen bei Bedarf vorhanden sein (Verfügbarkeit);
d) Informationsbearbeitungen müssen einer Person zugerechnet werden können (Zurechenbarkeit);
e) Veränderungen von Informationen müssen erkennbar und nachvollziehbar sein (Nachvollziehbarkeit).
3 Die zu treffenden Massnahmen richten sich nach der Art der Information, nach Art und Zweck der Verwendung und nach dem jeweiligen Stand der Technik.
4 Der Regierungsrat regelt das Nähere für die kantonale Verwaltung, der Gemeinderat für die kommunale Verwaltung.»

— Eine Risikobeurteilung findet, insb. im Rahmen von Informatikprojekten, teilweise statt. Ein umfassendes Risikomanagement (auch ausserhalb des IT-Sicherheitsbereichs) fehlt aber. Allerdings kann ein solches seine Funktion auch nur dann vollumfänglich erfüllen, wenn es sich in eine Verwaltungs- und IT-Governance eingebettet findet; eine solche ist im Kanton Basel-Stadt zurzeit jedoch nicht oder nur teilweise vorhanden.
— Ein Penetrationstest (durch externe Spezialisten kontrolliert durchgeführter Angriff auf die Ressourcen innerhalb des DANEBS) hat 2007 die Gefahr der Verletzlichkeit gezeigt. Die festgestellten Mängel, die einzelne Systeme betreffen, sind von den verantwortlichen Techniker umgehend behoben worden. Die generellen Probleme, für welche in der bestehenden Informatikorganisation die Verantwortlichkeiten und Zuständigkeiten nicht klar geregelt sind, konnten nur teilweise und unvollständig behoben werden.
— Die Informatikkonferenz (IK) hat 2009 beschlossen, dass Projekte nach dem «Leitfaden zur Abwicklung und Prüfung von Informatikprojekten im Kanton Basel-Stadt» (eine vom Projektmanagement-Tool HERMES des Bundes abgeleitete Projektführungsmethode) abzuwickeln seien. Wir stellen fest, dass diesem Beschluss offensichtlich nicht verwaltungsweit nachgelebt wird.

Ein umfassendes Risikomanagement fehlt; es müsste in eine Verwaltungs- und IT-Governance eingebettet sein.

— Das Projekt Identity and Access Management (IAM), bei welchem es um den Schutz von Ressourcen und eine eindeutige Identifikation geht, ist im Gange. Es wird eine deutliche Verbesserung der Verwaltung von Benutzer(inne)n und den entsprechenden Rechten bringen.
— Besondere Personendaten können im Kanton Basel-Stadt per E-Mail nur bei einigen wenigen Einzellösungen verschlüsselt übermittelt werden. In verschiedenen anderen Kantonen und im Bund stehen verschlüsselte E-Mail-Dienste generell zur Verfügung. Die frühere Begründung, das DANEBS sei sicher, lässt sich nach den oben wiedergegebenen Erkenntnissen nicht mehr halten. In Basel-Stadt muss deshalb darauf hingewiesen werden, dass die Übermittlung von besonderen Personendaten per E-Mail generell unzulässig ist.

Schlussfolgerungen

Generell Was schliessen wir aus den Feststellungen?
— Wir gehen davon aus, dass die Verwaltung über kurz oder lang um ein umfassendes Risikomanagement (insb. IT-Risikomanagement) nicht herumkommen wird. Die angestossenen Massnahmen zur Schaffung eines solchen Managements sind voranzutreiben. Dabei sind die Verantwortlichkeiten auf Stufe Regierungsrat, Departement und Amtsstellen klar festzulegen. Ein umfassendes Risikomanagement wird um ein Internes Kontrollsystem IKS, wie es in Unternehmen der Privatwirtschaft nicht wegzudenken ist, nicht herumkommen.
— Die Bemühungen betreffend die Informationssicherheit sind zu verstärken. Insbesondere wird es unerlässlich sein, eine Sicherheitsorganisation aufzubauen. Dabei sind bestimmte Funktionen unverzichtbar: Sicherheitsbeauftragte (ob dezentral oder zentral als Chief Security Officer CSO) und ein Gremium, welches die Risikopolitik verbindlich festlegt (welche Risiken sollen zwingend durch Sicherheitsmassnahmen ausgeschaltet werden, welche Risiken können mit welchen Massnahmen verkleinert werden und welches Restrisiko wird bewusst übernommen?).
— Diese Funktionen haben klare Verantwortlichkeiten und Kompetenzen zu erhalten. Ausserdem sind Unvereinbarkeiten mit anderen Funktionen festzulegen.

Für die Aktivitäten des Datenschutzbeauftragten
Für unsere Tätigkeit schliessen wir daraus:
— Das Thema Informationssicherheit muss auf dem Radarschirm bleiben und verstärkt bearbeitet werden.
— In personeller Hinsicht hat der Grosse Rat mit dem Budget 2011 beim Datenschutzbeauftragten eine zusätzliche Stelle bewilligt, die mit einer Informatikerin/einem Informatiker besetzt werden soll. Dadurch kann auch das Thema Informationssicherheit mit der nötigen Professionalität angegangen werden.
— Die Anforderungen des Datenschutz-Audits sollen im Informatik-Teil vorläufig den individuellen Voraussetzungen bei den Amtsstellen angepasst werden, indem nicht zwingend das fertige Paket von erforderlichen Dokumenten vorausgesetzt wird, sondern gegebenenfalls deren Erstellung erst unterstützt wird.
— Im Rahmen von Vorabkontrollen werden wir darauf hinwirken, dass die notwendigen Dokumentationen künftig vorweg erstellt werden, damit sie bei der Inbetriebnahme vorhanden sind.
— Wir unterstützen die Bemühungen zum Aufbau einer Sicherheitsorganisation und einer umfassenden Risikomanagements aktiv.

— Es soll in Zusammenarbeit mit Verwaltungsstellen geprüft werden, wie das Bewusstsein für die Wichtigkeit der Informationssicherheit («Awareness») bis auf die Stufe der Mitarbeiter(innen) gestärkt werden kann.

Bestimmte Funktionen sind unverzichtbar: Sicherheitsbeauftragte und ein Gremium, welches die Risikopolitik verbindlich festlegt.

Kurz & bündig (Management Summary)

Neue Risiken Die Verwaltungsprozesse werden zunehmend von Informations- und Kommunikationstechnologie durchdrungen. Damit drohen der staatlichen Aufgabenerfüllung neue Risiken – und ebenso den Privatpersonen und Unternehmen, über welche die Verwaltung Daten bearbeitet.

Verantwortung Das Informations- und Datenschutzgesetz legt die Verantwortung für die Informationssicherheit eindeutig fest: Sie liegt nicht bei der IT, sondern klar beim öffentlichen Organ, welches Informationen bearbeitet oder bearbeiten lässt – also bei den Amtsstellen und Departementen. Die technologische Entwicklung hebelt Abwehrstrategien, die ausschliesslich auf einer Trennung von «innen» und «aussen» basieren, aus. Wie es um die Informationssicherheit im Kanton Basel-Stadt steht, kann zurzeit nicht zuverlässig beurteilt werden, da die Beurteilungsgrundlagen weitgehend fehlen.

Risikomanagement und Sicherheitsorganisation Wir gehen davon aus, dass für die Verwaltung über kurz oder lang ein umfassendes Risikomanagement aufgebaut werden muss, das in eine Verwaltungs- und IT-Governance eingebettet ist. Unerlässlich wird auch der Aufbau einer Sicherheitsorganisation mit klaren Verantwortlichkeiten und Kompetenzen sein.

—

1 (z.B. § 17 Abs. 1 DSG)
2 (§ 6 Abs. 1 und § 7 Abs. 1 und 2 IDG, siehe Kästchen; ebenso schon § 7 Abs. 1 DSG)

Fälle

Fall 1 Die Prüfungsnoten im Internet

Rasch und «transparent»: Wer an der Universität eine Prüfung absolviert, konnte bei bestimmten Instituten die Note im Internet nachschauen – auf einer Liste mit Namen und Noten. Das konnten natürlich auch alle anderen, und dies auch noch lange Zeit später. Ebenso waren Namen und Adresslisten der Teilnehmer(innen) an Seminaren für jedermann/jedefrau sichtbar. Ist das zulässig?

Per Zufall stellte ein ehemaliger Studierender der Universität fest, dass auf den Seiten seines Instituts noch immer Prüfungsergebnisse einer längst vergangenen Prüfungssession sowie Teilnehmerlisten von Seminaren einsehbar waren. Er wandte sich an die Ombudsstelle der Universität mit der Bitte, sich dieser Sache anzunehmen. Der Datenschutzbeauftragte beurteilte den Stand der Dinge in der Folge gemeinsam mit der Ombudsstelle.

Werden Prüfungsergebnisse publiziert, so stellt dies eine Datenbekanntgabe dar, welche einer gesetzlichen Grundlage bedarf (§ 10 DSG). Der «Bildungsauftrag» der Universität genügt in diesem Falle nicht als Grundlage für eine solche Publikation. Mangels anderer gesetzlicher Grundlagen ist eine Publikation von Prüfungsergebnissen daher aus datenschutzrechtlicher Sicht unzulässig.

Sollte eine gesetzliche Grundlage für die Publikation der Ergebnisse geschaffen werden, so müsste die Bekanntgabe immer noch verhältnismässig sein. Es dürfte also kein milderes Mittel geben, welches zum gleichen Ziel führen würde. Hier stellt sich die Frage, ob das bereits bestehende System «MOnA» (My Online Account) nicht sinnvoller/konsequenter genutzt werden könnte. Bei diesem System können sich die Studierenden in ihr persönliches Konto einloggen und sehen dort ihre Noten – sie sehen nur *ihre* Noten und auch nur sie können diese sehen. Einzelne Fakultäten (z.B. die Wirtschaftswissenschaftliche Fakultät) veröffentlichen Prüfungsergebnisse schon heute ausschliesslich über MOnA. Aus der Sicht des Datenschutzbeauftragten besteht kein Gewinn, wenn die Resultate auf MOnA und auch noch als Liste im Internet veröffentlicht werden sollen. Wer sich eine Liste im Internet anschaut, kann sich auch bei MOnA einloggen.

Sollte die Universität der Ansicht sein, dass die Publikation von Notenlisten im Internet – parallel zu MOnA – unverzichtbar sei, so müssen die Ergebnisse zumindest pseudonymisiert werden. Pseudonymisiert heisst, dass anstelle des Namens ein «Schlüssel» verwendet wird, in der Regel eine Nummer. Auch dieses System wird bereits an einzelnen Instituten angewandt: Dabei erhält jede(r) Student(in) mit jeder Prüfung eine spezifische Nummer, welche dann – anstelle der immer gleich bleibenden Matrikelnummer – auf den Listen mit den Prüfungsresultaten erscheint. Wenn pro Prüfung eine andere Nummer vergeben wird, kann eine Drittperson auch nicht durch Kombination zurückverfolgen, wer welche Noten erzielt hatte. Ausserdem müssen Notenlisten nicht «ewig» öffentlich einsehbar bleiben. Im Sinne des Verhältnismässigkeitsgrundsatzes ist die Publikation zeitlich zu beschränken.

Ähnliches gilt auch für die Veröffentlichung von Listen mit Seminarteilnehmer(inne)n. Derzeit besteht keine gesetzliche Grundlage, welche die Publikation solcher Listen (üblicherweise Name, Adresse, Telefonnummer, E-Mail und bearbeitetes Thema) rechtfertigen würde. Auch erscheint eine Publikation im Internet unverhältnismässig, würde es doch ausreichen, den Teilnehmer(inne)n eine solche Liste per E-Mail zuzusenden oder ausgedruckt auszuhändigen. Möchte eine Seminarleitung die Listen gleichwohl rund um die Uhr und für die Teilnehmenden überall auf der Welt zugänglich machen, so bietet sich die Ablage auf einer passwortgeschützten Seite der Universität bzw. des Instituts an. Und auch dort gilt: Die Informationen müssen nicht über ein Semester hinaus online abrufbar bleiben. In der Regel können Unterlagen später bei den Instituten bezogen werden.

Die Universität nahm diesen Vorfall und die vom Datenschutzbeauftragten vorgelegten Denkanstösse zum Anlass, die (studentische wie auch fakultäre) Internetnutzung zu überdenken und aussagekräftigere Regelungen auszuarbeiten.

Ergebnis

Prüfungsergebnisse und Listen von Seminarteilnehmer(inne)n stellen Personendaten dar. Sollen diese im Internet veröffentlicht werden, bedarf es einer gesetzlichen Grundlage. Abgesehen davon ist es nicht erforderlich und deshalb unverhältnismässig, anderen als den betroffenen Personen die Noten namentlich zugänglich zu machen. Die Listen dürfen zudem nicht im Internet «vergessen» werden, sondern müssen spätestens nach Ablauf eines Semesters gelöscht werden.

Fall 2 Vorgangslisten im Einbürgerungsverfahren

Um zu beurteilen, ob die Bewerber(innen) die Einbürgerungsvoraussetzungen erfüllen, müssen Einbürgerungsbehörden «die notwendigen Erhebungen» durchführen. Verwaltungsbehörden sind verpflichtet, ihnen die verlangten Auskünfte zu erteilen. Wie steht es mit den Vorgangslisten der Staatsanwaltschaft? Dürfen diese Listen in allen Gesuchsfällen vollumfänglich, ungeachtet sachlicher oder zeitlicher Kriterien, an die Einbürgerungsbehörden übermittelt werden?

Die Staatsanwaltschaft führt sogenannte Vorgangslisten. Diese sind im Grunde genommen nichts anderes als ein auf eine bestimmte Person bezogener Auszug aus der Geschäftskontrolle. Enthalten sind darin Angaben darüber, gegen wen wann ein strafrechtliches Ermittlungsverfahren wegen Verbrechen, Vergehen oder Übertretungen eingeleitet wurde, sowie ob, wann und wie dieses erledigt worden ist. Die Vorgangslisten umfassen somit auch Angaben über Verfahrenserledigungen, die nicht im schweizerischen Strafregister eingetragen worden sind (Verfahrenseinstellungen, Verfahrensabtretungen und nichteintragungspflichtige Urteile). Bei den auf den Vorgangslisten ausgewiesenen Vorgängen handelt es sich mindestens teilweise um besonders schützenswerte Personendaten (DSG) bzw. künftig um besondere Personendaten (IDG). Ausserdem geben sie nicht nur erhärtete und gesicherte Informationen wie Urteile wieder, sondern enthalten beispielsweise auch blosse Verdachtsmeldungen, die keine Weiterungen zur Folge hatten, und Informationen aus Strafverfahren, die nicht eröffnet oder eingestellt wurden. Insbesondere finden sich auf den Listen auch Angaben zu Verfahren, in denen die beschuldigte Person noch gar keine Kenntnis davon hat, dass gegen sie ein Strafverfahren geführt wird.

Das Bearbeiten derart sensitiver Daten bedarf einer qualifizierten Rechtsgrundlage in einem Gesetz im formellen Sinn. Besondere Personendaten dürfen bearbeitet werden, «wenn ein Gesetz dazu ausdrücklich ermächtigt oder verpflichtet» (sog. unmittelbare gesetzliche Grundlage) «oder es für eine in einem Gesetz klar umschriebene Aufgabe zwingend notwendig ist» (sog. mittelbare gesetzliche Grundlage)[1]. Ausserdem muss jedes Bearbeiten von Personendaten verhältnismässig sein[2]. Das gilt auch für das Bekanntgeben von Personendaten; zusätzlich kann eine Bekanntgabe aber im Einzelfall durch die ausdrückliche (und freiwillige) Einwilligung der betroffenen Person gerechtfertigt werden[3]. Allerdings schliesst die explizite Beschränkung auf den Einzelfall eine Standardbekanntgabe aus; zudem kann eine Einwilligung nicht als freiwillig angesehen werden, wenn ohne sie das Einbürgerungsverfahren nicht durchgeführt wird.

Eine unmittelbare gesetzliche Grundlage, welche zur generellen Übermittlung der Vorgangslisten der Staatsanwaltschaft an die Einbürgerungsbehörden von Kanton und Gemeinden ausdrücklich ermächtigt oder verpflichtet, fehlt. Somit bleibt im Moment einzig die Möglichkeit der Rechtfertigung in Form einer mittelbaren gesetzlichen Grundlage: Die nicht-einzelfallbezogene Übermittlung und Verwendung der Vorgangslisten ist zulässig, wenn sie für eine in einem Gesetz klar umschriebene Aufgabe zwingend notwendig ist. Notwendig ist eine solche Übermittlung und Verwendung, wenn es kein milderes Mittel gibt, mit welchem die gesetzliche Aufgabe erfüllt werden kann, wenn also die gesetzliche Aufgabe ohne die besonderen Personendaten, mit weniger solchen Personendaten oder mit weniger sensitiven Personendaten nicht erfüllt werden kann. Mit der Formulierung, dass die Datenbekanntgabe und -bearbeitung zwingend notwendig sein muss, hat der Gesetzgeber bewusst einen strengen Massstab vorgegeben.

Nach dem Bürgerrechtsgesetz haben die Einbürgerungsbehörden «die notwendigen Erhebungen» durchzuführen, um beurteilen zu können, ob die Bewerber(innen) die Einbürgerungsvoraussetzungen[4] erfüllen. Daraus ergibt sich nach unserer Beurteilung, dass diese Bestimmung des Bürgerrechtsgesetzes keine gesetzliche Grundlage «für alles» abzugeben vermag, sondern nur für das zur Aufgabenerfüllung zwingend Erforderliche. Die vollumfängliche Übermittlung der Vorgangslisten in allen Gesuchsfällen, ungeachtet sachlicher oder zeitlicher Kriterien, erscheint uns unverhältnismässig und steht damit im Widerspruch zu den datenschutzgesetzlichen Vorgaben.

Ergebnis

Eine vollumfängliche Übermittlung der Vorgangslisten in allen Gesuchsfällen, ungeachtet sachlicher oder zeitlicher Kriterien, ist unverhältnismässig und steht damit im Widerspruch zu den datenschutzgesetzlichen Vorgaben. Allenfalls kann mittels eines Kriterienkatalogs versucht werden zu beurteilen, in welchen Fällen und in welcher Form der Beizug von Vorgangslisten allenfalls verhältnismässig sein könnte.

1 § 6 DSG bzw. künftig § 9 Abs. 2 IDG.
2 § 5 Abs. 2 DSG bzw. § 9 Abs. 3 IDG.
3 So künftig § 21 Abs. 1 lit. c und – für besondere Personendaten – Abs. 2 lit. c IDG.
4 Nach § 13 Abs. 2 BüRG: guter Leumund, Vertrautheit mit allgemeinen Lebensgewohnheiten und wichtigen öffentlichen Institutionen in Gemeinde, Kanton und Bund, Bejahung der schweizerischen Demokratie, Respektierung der geltenden Rechtsordnung, Erfüllung der privaten und öffentlichrechtlichen Verpflichtungen.

Fall 3 Die Warnung vor dem Gift im Paprika

Bei einer Lebensmittelkontrolle wird in einer Produktgruppe ein Anteil giftiger Substanzen über dem Grenzwert festgestellt. Die Chargen und auch die bereits ausgelieferten Mengen des Produkts werden zurückgerufen, doch ist nicht auszuschliessen, dass bereits Teile der belasteten Produktgruppe an Konsumenten abgegeben worden sind. Muss die Bevölkerung darüber informiert/davor gewarnt werden?

In der Bevölkerung besteht in einem solchen Fall nicht nur ein Bedürfnis, über das Ergebnis der Untersuchung informiert zu werden, sondern auch zu erfahren, wo die beanstandeten Proben verkauft wurden und von welchem Hersteller sie stammen. Diesem Bedürfnis stehen die wirtschaftlichen Interessen der Hersteller und Verkäufer gegenüber. Sowohl dem Hersteller als auch dem Verkäufer kann nämlich im Einzelfall unter Umständen gar kein Fehlverhalten vorgeworfen werden, beide tragen aber bei einer namentlichen Publikation potentiell einen hohen Imageschaden davon. Es muss also abgewogen werden zwischen dem Informationsbedürfnis der Bevölkerung und den wirtschaftlichen Interessen der Hersteller und Verkäufer.

Das Lebensmittelrecht ist auf Bundesebene geregelt, der Vollzug aber obliegt den Kantonen. Für das Bearbeiten von Personendaten durch die mit dem Vollzug betrauten kantonalen öffentlichen Organe gilt das jeweilige kantonale Datenschutzrecht. Sollen Daten bekannt gegeben werden, braucht es eine gesetzliche Grundlage[1], die in aller Regel im anwendbaren Fachrecht – hier also in der Lebensmittelgesetzgebung des Bundes – zu suchen ist. Auf der anderen Seite kann das Fachrecht aber auch einschränkende Regeln enthalten, also besondere Geheimhaltungspflichten, welche die Bekanntgabe einschränken.

Tatsächlich auferlegt das Lebensmittelgesetz des Bundes denjenigen Personen, die mit dem Gesetzesvollzug betraut sind, eine Schweigepflicht[2]. Die mit der Kontrolle betrauten Personen haben folglich nicht das Recht, bei Fragen aus der Bevölkerung oder der Presse die Namen der Hersteller oder der Verkäufer von beanstandeten Produkten zu nennen. Hingegen besteht eine Informationspflicht seitens der Vollzugsbehörden, wenn gesundheitsgefährdende Lebensmittel an eine unbestimmte Anzahl von Konsumenten abgegeben wurden[3]. Hier ist die Bevölkerung im Sinne einer Warnung zu informieren.

Im konkret zu beurteilenden Fall – es ging um die Feststellung krebserregender Stoffe (Mykotoxine) in Paprika – bestand das Problem darin, dass gar nicht bekannt war, ob überhaupt gesundheitsgefährdende Lebensmittel an Konsumenten abgegeben wurden; es bestand nur die Befürchtung. Dies spricht jedoch gerade nicht für eine gross angelegte Warnung der Bevölkerung. Zudem ist nicht klar, wie konkret die Gesundheitsgefährdung sein muss, um eine Warnung durch die Vollzugsorgane auslösen zu können. Handelt es sich beispielsweise um einen Schadstoff, welcher erst bei chronischem Verzehr zu Gesundheitsgefährdungen führt, müsste man wohl von einer Warnung absehen, da im Verhältnis zum Informationsinteresse der Bevölkerung, der Imageschaden für die Hersteller und Verkäufer überdurchschnittlich hoch wäre. Handelt es sich jedoch um einen Stoff, welcher schon beim ersten Verzehr zu erheblichen Gesundheitsschäden führt, dann ist eine Warnung sicher zu rechtfertigen, ja sogar geboten.

Ergebnis

Die Information der Bevölkerung vor gesundheitsgefährdenden Stoffen in Lebensmitteln ist im Lebensmittelgesetz des Bundes verankert. Die Tatsache, dass für die Vollzugsorgane grundsätzlich eine Schweigepflicht besteht und wenn möglich vor einer Warnung der Bevölkerung die Hersteller, Importeure, Verteiler oder Verkäufer sowie die Konsumentenorganisationen anzuhören sind, deutet darauf hin, dass nicht schon bei jeder potentiell ungesunden Belastung der Lebensmittel gewarnt werden muss, sondern dass nur Gesundheitsgefährdungen von einiger Intensität und auch nur, wenn entsprechende Produkte an Konsument(inn)en abgegeben wurden, eine Warnung auszulösen vermögen.

1 § 5 i.V.m. § 11 DSG für die Bekanntgabe an Private, künftig § 21 IDG.
2 Art. 42 LMG.
3 Art. 43 Abs. 1 LMG.

Fall 4 Der Pöstler mit dem offenen Zahlungsbefehl

Ist es aus datenschutzrechtlicher Sicht zulässig, wenn das Betreibungsamt die Zustellung von Betreibungsurkunden an die Post delegiert und diese daraufhin die Betreibungsurkunden oder auch Vorladungen zur Abholung der Betreibungsurkunden beim Betreibungsamt offen, d.h. ohne Couvert zustellt, so dass der Postbote vom Inhalt des Schreibens Kenntnis erhält?

Die Zustellung von Zahlungsbefehlen ist im Bundesgesetz über Schuldbetreibung und Konkurs (SchKG) geregelt: «Die Zustellung geschieht durch den Betreibungsbeamten, einen Angestellten des Amtes oder durch die Post»[1]. Das Gesetz favorisiert keine dieser Zustellungsarten, folglich ist es den Betreibungsämtern freigestellt, nach welcher Variante sie vorgehen möchten.

Im Kanton Basel-Stadt ist es langjährige und gängige Praxis, dass die ersten Zustellungsversuche von der Post vorgenommen werden. Da der Postbote auf jeweils zwei Ausführungen des Zahlungsbefehls bescheinigen muss, an wen und wann er zugestellt hat[2], muss er diese offen übergeben. Der Postbote kann demnach also Kenntnis nehmen vom Inhalt der durch ihn zugestellten Zahlungsbefehle. Da er jedoch dem Amtsgeheimnis untersteht[3], muss er sämtliche während des Dienstes zur Kenntnis genommenen, nicht für die Öffentlichkeit bestimmten Fakten vertraulich behandeln. Widerhandlungen gegen das Amtsgeheimnis können strafrechtlich verfolgt werden[4]. Zusätzlich unterstehen die Postbeamten dem Postgeheimnis[5], welches die ungerechtfertigte Weitergabe von Angaben, die im Rahmen von Postdienstleistungen zur Kenntnis genommen wurden, mit Strafe bedroht. Diese Verpflichtungen wirken jeweils auch über das Ende des Anstellungsverhältnisses hinaus. Aus datenschutzrechtlicher Sicht kann deshalb nichts dagegen eingewendet werden, wenn das Betreibungsamt die Post die Betreibungsurkunden offen zustellen lässt.

Bleibt die Frage, wie es bei der offenen Zustellung von Vorladungen aussieht. Bei den Vorladungen handelt es sich um Zettel in grell-pinker Farbe, welche dem allfälligen Schuldner in den Briefkasten geworfen werden und ihn zur Abholung des Zahlungsbefehls beim Betreibungsamt auffordern. Für den Fall, dass der Zahlungsbefehl nicht abgeholt wird, wird mit einer Publikation im Amtsblatt gedroht. Aus datenschutzrechtlicher Sicht ist das Einwerfen der offenen Vorladung in den Briefkasten des Schuldners zulässig. Die Vorladung dient der gesetzlichen Aufgabe des Betreibungsamtes, nämlich der Durchführung des Betreibungsverfahrens. Die Tatsache, dass die Vorladung ohne Couvert überbracht wird, rechtfertigt sich dadurch, dass die Farbe dem allfälligen Schuldner auffallen soll. Zudem soll dieser nachher nicht behaupten können, er habe die Vorladung übersehen, weil er den Umschlag nicht geöffnet habe. Es besteht natürlich die Möglichkeit, dass eine im selben Haushalt lebende Person beim Leeren des Briefkastens Kenntnis vom Inhalt des Zettels erhält; ist doch der Briefkasten eine Art Angebot des Schuldners, ihm auf diesem Weg eine Nachricht zukommen zu lassen. Auch Absender auf Briefen sind für jede Person lesbar, die den Briefkasten leeren kann. Sollte dies vom Schuldner nicht gewünscht sein, muss er in seiner Wohngemeinschaft entsprechende Vorkehrungen treffen. Was die Kenntnisnahme durch den Postboten betrifft, ist wiederum festzuhalten, dass er dem Amtsgeheimnis und dem Postgeheimnis untersteht. Eine offene Zustellung der Vorladung an einem anderen Ort als dem heimischen Briefkasten (z.B. am Arbeitsplatz) wäre aufgrund des Datenschutzes jedoch nicht zulässig; sie müsste durch eine Zustellung in einem verschlossenen Couvert ersetzt werden.

Ergebnis

Da der Postbote nach Bundesrecht auf zwei Exemplaren eines Zahlungsbefehls bescheinigen muss, an wen und wann er diesen zugestellt hat, und er darüber hinaus sowohl dem Amts- wie auch dem Postgeheimnis untersteht, ist die offene Zustellung datenschutzkonform. Ebenso ist das Einwerfen von offenen Vorladungen in den Briefkasten des Schuldners aus datenschutzrechtlicher Sicht zu rechtfertigen, denn die Vorladung dient der Durchführung des Betreibungsverfahrens und ist bei Einwurf in den heimischen Briefkasten des Schuldners auch verhältnismässig.

1 Art. 72 Abs. 1 SchKG.
2 Art. 72 Abs. 2 SchKG.
3 Art. 15 Abs. 1 Postorganisationsgesetz in Verbindung mit Art. 22 Abs. 1 Bundespersonalgesetz.
4 Art. 320 StGB.
5 Art. 321ter StGB.

Fall 5 Die Weiterreichung des psychiatrischen Gerichtsgutachtens

Die IV-Stelle Basel-Stadt möchte, dass ihr das Amt für Justizvollzug zur Erfüllung ihrer gesetzlichen Aufgabe ein forensisch-psychiatrisches Gutachten herausgibt, welches im Rahmen des Strafverfahrens über einen Angeklagten erstellt worden ist. Sie brauche die Angaben für die Festlegung einer IV-Rente des inzwischen verurteilten Straftäters. Muss/darf das Amt für Justizvollzug das Gutachten herausgeben?

Wenn ein öffentliches Organ des Kantons Basel-Stadt ein Gutachten über eine bestimmte Person an ein anderes öffentliches Organ weitergibt, dann handelt es sich um ein Bearbeiten von Personendaten. Darauf findet das baselstädtische Datenschutzgesetz (und künftig das Informations- und Datenschutzgesetz) Anwendung. Ein forensisch-psychiatrisches Gutachten enthält aber nicht nur Angaben zur Person wie Alter, Geschlecht usw., sondern insbesondere auch Angaben zum (psychischen und physischen) Gesundheitszustand, zur Tat und oft eine Rückfallprognose. Das sind nicht bloss «gewöhnliche» Personendaten, sondern besonders schützenswerte Personendaten (nach IDG: besondere Personendaten)[1].

Für das Bearbeiten – und als Unterfall des Bearbeitens: für das Bekanntgeben – von besonderen Personendaten gelten qualifizierte Voraussetzungen. Besondere Personendaten dürfen (u.a.) bekannt gegeben werden, wenn ein Gesetz (und nicht bloss eine Verordnung) dazu ausdrücklich verpflichtet oder ermächtigt oder dies zur Erfüllung einer in einem Gesetz (und nicht bloss in einer Verordnung) klar umschriebenen Aufgabe zwingend notwendig ist[2].

Die IV-Stelle Basel-Stadt kann sich für ihr Bekanntgabebegehren auf ein Bundesgesetz stützen[3]. Eine Bestimmung verpflichtet Behörden von Bund und Kantonen, auf schriftliche und begründete Anfrage einer Sozialversicherung hin diejenigen Daten bekannt zu geben, welche für die Festsetzung, Änderung oder Rückforderung von Leistungen erfoderlich sind. Im vorliegenden Fall soll die IV-Stelle Basel-Stadt die Leistungen für die inhaftierte Person festsetzen, was klar unter die zitierte Bestimmung zu subsumieren ist.

Damit besteht die erforderliche formellgesetzliche Grundlage, welche die Datenbekanntgabe kantonaler Behörden an die Sozialversicherungen vorsieht. Das Amt für Justizvollzug ist demnach verpflichtet, der IV-Stelle Basel-Stadt die erforderlichen Informationen mitzuteilen.

Das heisst nun allerdings keineswegs, dass das Amt für Justizvollzug der IV-Stelle einfach eine Kopie des Gutachtens schicken darf. Das Bundesgesetz spricht von « diejenigen Daten (...), welche für die Festsetzung, Änderung oder Rückforderung von Leistungen erforderlich sind». Auch das Datenschutzgesetz (wie auch künftig das Informations- und Datenschutzgesetz) verlangt, dass jedes Datenbearbeiten verhältnismässig sein muss. Verhältnismässig ist eine Datenbekanntgabe, wenn

— die bekannt gegebenen Daten zur Zweckerreichung geeignet sind,
— die bekannt gegebenen Daten zur Zweckerreichung erforderlich (bei besonderen Personendaten: zwingend notwendig) sind, d.h. wenn die Aufgabe ohne die Daten nicht erfüllt werden kann, und wenn
— die Datenbekanntgabe der betroffenen Person zumutbar ist, d.h. wenn zwischen Zweck und Eingriff ein vernünftiges Verhältnis besteht.

Nicht alle im Gutachten enthaltenen besonderen Personendaten sind für die Aufgabenerfüllung der IV-Stelle, d.h. für die Festsetzung einer IV-Rente zwingend notwendig. Das Amt für Justizvollzug muss also, um verhältnismässig zu handeln, konkret abwägen, welche Informationen die IV-Stelle für diese Aufgabe benötigt. Dies kann dazu führen, dass grosse Teile des Gutachtens eingeschwärzt oder abgedeckt werden müssen. Der Datenschutzbeauftragte empfiehlt in solchen Fällen anzugeben, weshalb einzelne Passagen aus dem Gutachten nicht weitergegeben wurden (z.B. «Diese Passage enthält Informationen zum Tathergang»). Sollte der Empfänger oder die Empfängerin der Ansicht sein, dass gerade eine solche Information ebenfalls für die Festsetzung der Ansprüche notwendig sei, so kann sie dies begründen und eine Nachreichung verlangen.

Ergebnis

Für die Bekanntgabe von besonderen Personendaten braucht es eine gesetzliche Grundlage in einem Gesetz im formellen Sinn. Selbst wenn diese gegeben ist, dürfen aber nur diejenigen Informationen weitergegeben werden, welche das empfangende öffentliche Organ zur Aufgabenerfüllung konkret benötigt. Bei einem forensisch-psychiatrischen Gutachten, das an die IV-Stelle weitergegeben werden soll, weil es Angaben zur Festsetzung der IV-Rente der betroffenen Person benötigt, sind alle Angaben, welche genau für diesen Zweck nicht zwingend notwendig sind, abzudecken oder einzuschwärzen.

1 § 2 Abs. 2 DSG, künftig § 3 Abs. 4 lit. a IDG.
2 § 21 Abs. 2 IDG, ebenso noch § 6 i.V.m. § 10 DSG.
3 Art. 32 Abs. 1 lit. a ATSG.

Fall 6 Die diskreten Konkubinatspartner

Der eine Partner eines Konkubinatspaares stellt einen Antrag auf Krankenkassenprämien-Verbilligung. Der Entscheid des Amtes für Sozialbeiträge schlüsselt aber nicht nur seine eigenen Vermögensverhältnisse auf, sondern auch die der Partnerin. Die beiden hatten zuvor bewusst und gewollt gegenseitig keinen Einblick in die Vermögensverhältnisse und fühlen sich nun ihrer Privatsphäre verletzt. Zu Recht?

Bei einem Antrag auf Prämienverbilligung wird der Anspruch aufgrund des Einkommens der massgeblichen Haushaltseinheit berechnet[1]. Ein Konkubinatspaar, welches seit mehr als fünf Jahren in einem gemeinsamen Haushalt lebt, gilt nach den Bestimmungen der Sozialleistungs-Harmonisierungsverordnung[2] als gefestigte faktische Lebensgemeinschaft. Eine gefestigte faktische Lebensgemeinschaft wird nach den Bestimmungen des Sozialleistungs-Harmonisierungsgesetzes wie die Ehe als Haushaltseinheit behandelt[3]. Damit wird das anrechenbare Einkommen beider Konkubinatspartner Teil der Berechnung des Anspruchs auf Prämienverbilligung des einen Partners.

Der Entscheid, ob jemandem eine Prämienverbilligung zusteht oder nicht, stellt eine anfechtbare Verfügung dar. Die Pflicht des Amts für Sozialbeiträge, Verfügungen zu begründen, ergibt sich aus der Kantonsverfassung[4] und ist Ausdruck des Anspruchs auf rechtliches Gehör. Die Begründung einer Verfügung genügt dem Anspruch auf rechtliches Gehör jedoch nur, wenn die Betroffenen dadurch in die Lage versetzt werden, die Tragweite der Entscheidung zu beurteilen; insbesondere sollen die Betroffenen aufgrund der Begründung entscheiden können, ob sie die Verfügung anfechten, also mit einem Rekurs an die nächsthöhere Instanz weiterziehen wollen. Das Amt für Sozialbeiträge ist somit von Verfassungs wegen verpflichtet, offenzulegen, wie der Entscheid bezüglich des Anspruchs auf Prämienverbilligung zustande kam.

Aus dieser Begründungspflicht ergibt sich, dass dem antragstellenden Konkubinatspartner die Berechnungsgrundlage für den Anspruch auf Prämienverbilligung offen gelegt werden muss. Ist das anrechenbare Einkommen eines Konkubinatspartners Teil dieser Berechnung, müssen ihm auch diese Angaben vorgelegt werden, da er sonst nicht nachvollziehen kann, wie sein Antrag berechnet wurde.

Die vom Datenschutzgesetz verlangte gesetzliche Grundlage für eine Datenbekanntgabe ist hier somit einerseits in der Begründungspflicht des Amts für Sozialbeiträge und andererseits in der gesetzlich vorgeschriebenen Berechnungsweise für Ansprüche auf Prämienverbilligung zu sehen.

Ergebnis

Wenn Konkubinatspaare seit mehr als fünf Jahren zusammenleben, müssen die Vermögens- und Einkommensverhältnisse beider Partner bei der Berechnung des Anspruchs auf Prämienverbilligung berücksichtigt werden, da diese aufgrund der Haushaltseinheit vorgenommen werden muss. Das Amt für Sozialbeiträge ist sodann von Gesetzes wegen verpflichtet, dem Antragsteller darzulegen, wie der Entscheid bezüglich der beantragten Prämienverbilligung zustande kam. Die Bekanntgabe des anrechenbaren Einkommens des Konkubinatspartners an den Antragssteller erweist sich in diesem Fall als rechtlich zulässig.

1 § 4 SoHaG.
2 § 1 Abs. 1 lit. b SoHaV.
3 § 5 SoHaG.
4 § 12 lit. b KV.

Fall 7 Informationen über Ausschaffungshäftlinge

Ein gesamtschweizerisches Pilotprojekt des Schweizerischen Roten Kreuzes (SRK) will die Rückführung von Ausschaffungshäftlingen humanitär begleiten. In diesem Zusammenhang ersucht das SRK Basel-Stadt das Migrationsamt, den Datenbestand der am Projekt teilnehmenden Personen zu vervollständigen. Darf das Migrationsamt die verlangten Personendaten an das SRK weitergeben?

Will ein Häftling die Dienstleistung des SRK in Anspruch nehmen, so geschieht dies auf freiwilliger Basis. Alle bereits bestehenden Daten erhebt das SRK direkt bei den betroffenen Personen, also bei den Ausschaffungshäftlingen. Bei den vom Migrationsamt gewünschten Angaben handelt es sich also um solche, die bei den Häftlingen selbst nicht erhoben werden konnten; in erster Linie betrifft es den Haftantritt oder die Haftart. Dem SRK sollen die erhobenen Daten zu rein statistischen Zwecken dienen.

Für das Datenbearbeiten des SRK gilt das Bundesdatenschutzgesetz. Wenn jedoch das Migrationsamts als Amtsstelle des Justiz- und Sicherheitsdepartements Personendaten bearbeitet (hier: bekannt geben soll), ist das kantonale Datenschutzgesetz anwendbar.

Das kantonale Datenschutzgesetz trifft in Bezug auf die Datenbekanntgabe – wie künftig auch das Informations- und Datenschutzgesetz – eine Unterscheidung zwischen der «gewöhnlichen» Datenbekanntgabe unter öffentlichen Organen und an Private[1] einerseits und der Datenbekanntgabe zu einem nicht personenbezogenen Zweck[2] andererseits. Im Normalfall geht es bei der Datenbekanntgabe um eine Bekanntgabe zu personenbezogenen Zwecken im Rahmen der Erfüllung der gesetzlichen Aufgabe: der durch das Datenbearbeiten angestrebte Erkenntnisgewinn zielt auf die betroffene Person. Das Migrationsamt bezieht Daten der Sozialhilfe, um darüber entscheiden zu können, ob sie einer konkreten Ausländerin die Aufenthaltsbewilligung verlängern oder entziehen soll.

Hier geht es dem SRK nicht um eine Erkenntnis in Bezug auf den einzelnen, bestimmten Ausschaffungshäftling, sondern um eine allgemeine, über den Einzelfall hinausreichende Erkenntnis. Mit anderen Worten: Es geht um ein Datenbearbeiten zu einem nicht personenbezogenen Zweck. Die Bekanntgabe von Personendaten zu einem nicht personenbezogenen Zweck – Forschung, Statistik, Planung – wird vom Datenschutzgesetz speziell geregelt[3]. Dabei unterscheidet es die Bekanntgabe an andere öffentliche Organe und an Private.

Wenn immer möglich sind für nicht personenbezogene Zwecke nicht Personendaten bekannt zu geben. Kann der Zweck auch mit anonymisierten oder pseudonymisierten Daten erreicht werden, dann ist es nicht erforderlich und damit auch unverhältnismässig, «scharfe» Personendaten an Dritte herauszugeben. Damit entfällt auch die Gefahr, dass Personendaten in falsche Hände geraten und missbraucht werden können. Wenn aber – wie im hier vorliegenden Fall – Daten aus verschiedenen Quellen ausgewertet werden sollen, um Zusammenhänge oder Abhängigkeiten zu erkennen, dann können die Personendaten nicht vorgängig anonymisiert werden, weil sie sonst logischerweise nicht mehr zueinander in Bezug gesetzt werden können.

Mit der Bekanntgabe zu einem nicht personenbezogenen Zweck sind aber weitere Voraussetzungen und Auflagen verbunden – das Informations- und Datenschutzgesetz wird sie künftig systematischer regeln[4]. Vorausgesetzt ist, dass keine besondere gesetzliche Geheimhaltungspflicht entgegensteht. Die Personendaten dürfen für keinen anderen Zweck verwendet werden und nicht an Dritte weitergegeben werden. Die Empfängerin hat für die Informationssicherheit zu sorgen. Die Ergebnisse der nicht personenbezogenen Bearbeitung dürfen nur so bekannt gegeben werden, dass keine Rückschlüsse auf betroffene Personen möglich sind.

Um die Einhaltung der Auflagen sicherzustellen, hat das öffentliche Organ, das die Daten bekannt gibt, die Empfängerin vor der Datenherausgabe eine entsprechende Verpflichtungserklärung unterzeichnen zu lassen.

Ergebnis

Die Bekanntgabe von Personendaten für nicht personenbezogene Zwecke – Forschung, Statistik, Planung – wird vom Datenschutzgesetz (und auch künftig vom Informations- und Datenschutzgesetz) privilegiert. Nur wenn sich der nicht personenbezogene Zweck nicht mit anonymisierten oder pseudonymisierten Daten erreichen lässt, dürfen Personendaten herausgegeben werden. Ebenso darf keine besondere gesetzliche Geheimhaltungspflicht die Datenbekanntgabe verbieten. Die Empfängerin muss sich ausserdem verpflichten, die Personendaten zu anonymisieren oder zu pseudonymisieren, sobald es der Bearbeitungszweck zulässt, die Daten für keinen anderen Zweck zu bearbeiten und Dritten nicht zugänglich zu machen. Überdies dürfen die Ergebnisse nur so bekannt gegeben werden, dass keinerlei Rückschlüsse auf betroffene Personen möglich sind.
Das Migrationsamt darf somit – wenn die Voraussetzungen erfüllt und eine Verpflichtungserklärung unterzeichnet ist – dem SRK die verlangten Daten bekannt geben.

1 §§ 10 und 11 DSG.
2 § 15 Abs. 2 DSG.
3 § 15 Abs. 2 DSG, künftig § 22 IDG.
4 § 22 Abs. 1 (Vorbehalt der Geheimhaltungsbestimmung), Abs. 2 (Anonymisierungs-/Pseudonymisierungspflicht, keine Rückschlüsse aus der Veröffentlichung der Resultate), Abs. 4 (Zweckänderungsverbot, Weitergabeverbot, Informationssicherheit) IDG.

Fall 8 Der beliebte «Geschenkkoffer»

Eine Werbefirma will Schwangere und junge Mütter besuchen und ihnen einen «Geschenkkoffer» überreichen. Zu diesem Zweck verlangt sie von den Spitälern die Bekanntgabe der Namen, Adressen und Geburtstermine der «Zielpersonen». Die Spitäler verweigern dies jedoch aus Datenschutzgründen. Der Datenschutzbeauftragten soll nun eine «Unbedenklichkeitserklärung» zuhanden der Spitäler abgeben. Ist die Datenbekanntgabe durch die Spitäler zulässig?

Die Werbefirma stellt sich auf den Standpunkt, dass eine Schwangerschaft nicht unter das Datenschutzgesetz falle, da diese – naturbedingt – früher oder später für jedermann ersichtlich sei. Zudem erfreue sich der Geschenkkoffer bei den «Zielpersonen», den Schwangeren und «frischgebackenen Müttern» (so das Schreiben der Werbefirma), grosser Beliebtheit.

Namen und Adressen sind zweifellos Personendaten. Wenn öffentlichrechtliche Spitäler des Kantons Basel-Stadt und Privatspitäler, welchen der Kanton eine öffentliche Aufgabe übertragen hat, Personendaten bekannt geben, fällt dies in den Geltungsbereich des baselstädtischen Datenschutzgesetzes.

Personendaten dürfen bekannt gegeben werden, wenn dafür eine gesetzliche Grundlage besteht oder das Bekanntgeben zur Erfüllung einer gesetzlichen Aufgabe erforderlich ist[1]. Ausserdem ist die Datenbekanntgabe von öffentlichen Organen an Private zulässig, wenn die betroffene Person ausdrücklich zugestimmt hat oder, falls sie dazu nicht in der Lage ist, die Bekanntgabe in ihrem Interesse liegt und ihre Zustimmung in guten Treuen vorausgesetzt werden darf[2]. Ein typischer Anwendungsfall liegt vor, wenn z.B. Gesundheitsdaten für die Behandlung einer anderswo verunfallten und nicht ansprechbaren Person bekannt gegeben werden müssen.

Eine Rechtsgrundlage oder eine gesetzliche Aufgabe, welche die Spitäler nur mit der Bekanntgabe von Namen und Adressen von Schwangeren und jungen Müttern an die Werbefirma erfüllen könnten, ist nicht ersichtlich. Die von der Werbefirma angeführte Beliebtheit vermag die erforderliche Rechtsgrundlage keineswegs zu ersetzen. Eine Zustimmung der betroffenen Personen kann die Werbefirma ebenfalls nicht vorweisen, sonst bräuchte sie die Bekanntgabe ja gar nicht mehr zu verlangen. Weil die Schwangeren und jungen Mütter auch durchaus in der Lage sind, selber zuzustimmen, darf auch keine «presumptive Einwilligung» angenommen werden. Die gesetzlichen Voraussetzungen für die Datenbekanntgabe sind somit nicht gegeben.

Eine sog. Listenauskunft, wie sie neuerdings das Aufenthaltsgesetz vorsieht («Die Einwohnerkontrolle kann Privaten, nach bestimmten Kriterien geordnet, Familiennamen, Vornamen, Geburtsdatum und Adresse bekannt geben von Personen, die in der Gemeinde wohnen, wenn die Daten ausschliesslich für schützenswerte ideelle Zwecke verwendet werden …»[3]), erlaubt einzig der Einwohnerkontrolle die Datenbekanntgabe, nicht aber den Spitälern. Im Übrigen ist der Zweck, zu dem die Daten verlangt werden, ein kommerzieller, womit auch das Erfordernis des schützenswerten ideellen Zwecks nicht erfüllt wäre.

Hingegen wäre das folgende Vorgehen datenschutzkonform: Wenn die Spitäler von der Beliebtheit der Besuche der Damen der Werbefirma überzeugt sind, könnten sie allenfalls den Schwangeren bzw. Müttern ein Informationsblatt aushändigen. Mit einem Bestelltalon könnten diese dann selber der Werbefirma Name, Adresse und Geburtstermin bekannt geben. Allerdings kann eine Werbefirma die Spitäler nicht zu einem solchen Vorgehen verpflichten und diese werden sich gut überlegen müssen, ob sie zu solchen Marketingaktivitäten Hand bieten wollen. Ausserdem können Werbefirmen auch wie bis anhin die «Geschenkkoffer» den Spitälern, Geburtshäusern und Geburtshilfe-Praxen anvertrauen, die sie dann beispielsweise bei Beratungsgesprächen, Vorbereitungsanlässen oder nach der Geburt den Schwangeren bzw. Müttern aushändigen. So kommen diese in den Genuss der Promotionen, ohne dass ihre Daten bearbeitet werden müssen.

Ergebnis

Die Spitäler haben zutreffend festgestellt, dass die rechtlichen Voraussetzungen für eine Bekanntgabe von Namen, Adressen und Geburtsterminen von Schwangeren und jungen Müttern nicht gegeben sind.

1 § 11 i.V.m. § 5 DSG; künftig § 21 Abs. 1 IDG.
2 So künftig § 21 Abs. 1 lit. c und § 21 Abs. 2 lit. c IDG; § 11 Abs. 1 lit. a DSG verlangt auch im Falle der ausdrücklichen Zustimmung noch, dass die Bekanntgabe – offensichtlich nach dem Urteil der Behörde, welche die Daten bekannt geben soll – im Interesse der betroffenen Person liegt – ein reichlich paternalistischer Ansatz.
3 § 30 Abs. 6 Aufenthaltsgesetz.

Fall 9 Eine Antwort, die ein bisschen zu viel verrät

Ein Rekurs an ein Departement und eine Eingabe an vier Mitglieder des Regierungsrates werden aus Gründen der Verfahrensökonomie in einem einzigen Schreiben beantwortet. Ist das zulässig? Auch wenn dabei die anderen Mitglieder des Regierungsrates etwas erfahren, das im Schreiben an sie nicht erwähnt war?

Eine Person reicht bei einem Departement Rekurs gegen eine Verfügung einer Amtsstelle dieses Departements ein. Ausserdem wendet sie sich mit einem Brief an vier Mitglieder des Regierungsrates – u.a. auch an die/den Vorsteher(in) des Departements, bei welchem der Rekurs hängig ist. Diese(r) Vorsteher(in) reagiert in einem Schreiben an die Person, worin sie/er einerseits den Eingang des Rekurses bestätigt (Absatz 1) und anderseits Stellung nimmt zu Fragen, die der/die Rekurrent(in) im Schreiben an die vier Mitglieder des Regierungsrates aufgeworfen hat (die folgenden Absätze). Aus Gründen der Verfahrensökonomie wurden in diesem Fall beide Teile (Rekurs-Eingangsbestätigung einerseits und Antwort auf das Schreiben an die vier Mitglieder des Regierungsrates anderseits) miteinander in demselben Schreiben behandelt.

Die Person stört sich daran, dass in diesem Schreiben die Tatsache der Rekurserhebung wie auch Name und Geburtsdatum ihrer Tochter erwähnt werden. Beides hatte sie in ihrem Brief an die Mitglieder des Regierungsrates nicht erwähnt. Zweifelsohne handelt es sich hierbei um ein Bekanntgeben von Personendaten im Sinne des Datenschutzgesetzes[1]. Ein öffentliches Organ darf Personendaten bearbeiten, wenn dafür eine gesetzliche Grundlage besteht oder das Bearbeiten zur Erfüllung einer gesetzlichen Aufgabe erforderlich ist[2]; ausserdem muss das Bearbeiten der Daten verhältnismässig sein[3]. Dass das Departement der Rekurrentin/dem Rekurrenten gegenüber einerseits den Eingang des Rekurses bestätigen darf, ist nicht zu bestreiten. Dass es anderseits zu den von ihr im Schreiben an die vier Mitglieder des Regierungsrates aufgeworfenen Fragen Stellung nehmen und diese Stellungnahme auch den anderen Adressaten ihres Briefes zur Kenntnis bringen darf, ist wohl ebenso wenig zu bestreiten. Hingegen ist es zur Aufgabenerfüllung nicht notwendig und damit unverhältnismässig, im gleichen Schreiben die Tatsache der Rekurserhebung und in Verbindung damit Name und Geburtsdatum der Tochter zu erwähnen. Allerdings erscheint uns der Verstoss gegen das Verhältnismässigkeitsprinzip mindestens in Bezug auf die Nennung von Name und Geburtsdatum der Tochter nicht schwerwiegend – es sind Angaben, die von der Einwohnerkontrolle (vorbehältlich einer Bekanntgabesperrung[4]) selbst an beliebige Private voraussetzungslos bekannt gegeben dürfen[5].

Es bleibt die Bekanntgabe der Tatsache der Rekurserhebung an die anderen drei Mitglieder des Regierungsrates. Dafür fehlt die Rechtsgrundlage, und sie ist auch zur Aufgabenerfüllung nicht erforderlich. Dass allenfalls später im Laufe des Rekursverfahrens alle Mitglieder des Regierungsrates (als Rekursinstanz) in den Besitz dieser Angaben gekommen wären, vermag die rechtliche Beurteilung nicht zu ändern, da der Rekurs nicht zwingend bis zum Regierungsrat gelangen muss: Er könnte vorher vom Departement bereits gutgeheissen werden, die Rekurrentin/der Rekurrent könnte bei einer Abweisung auf den Weiterzug verzichten und schliesslich könnte der Regierungsrat den Rekurs dem Verwaltungsgericht zum Entscheid überweisen, ohne selber materiell darauf einzutreten («Sprungrekurs»)[6], so dass die anderen Mitglieder des Regierungsrates von der Rekurserhebung tatsächlich oder (beim Sprungrekurs) praktisch nichts erfahren. Allerdings muss hier auch deutlich festgehalten werden, dass es sich in Würdigung aller Umstände nur um eine sehr geringfügige Datenschutzverletzung handelt – was der Person, die sich auf diesem «Nebenschauplatz» der eigentlichen Auseinander-setzung an den Datenschutzbeauftragten gewandt hat, auch klar mitgeteilt wurde.

Ergebnis

Werden von einem öffentlichen Organ unterschiedliche Eingaben, die an verschiedene öffentliche Stellen gingen, in einem einzigen Schreiben beantwortet und Kopien der Antwort an alle Empfänger der Eingaben versandt, ist darauf zu achten, dass diesen Empfängern keine Daten bekannt gegeben werden, die diese zur Erfüllung ihrer gesetzlichen Aufgabe gar nicht benötigen. Wir empfehlen, in gleich gelagerten Fällen künftig mit separaten Schreiben zu reagieren, was die beteiligten Stellen im betroffenen Departement auch bereits zugesagt haben.

1 § 2 Abs. 1 DSG; künftig § 3 Abs. 3 und 6 IDG.
2 § 5 Abs. 1 DSG; künftig § 9 Abs. 1 IDG.
3 § 5 Abs. 2 DSG; künftig § 9 Abs. 3 IDG.
4 § 13 DSG; künftig § 28 IDG.
5 § 12 Abs. 1 Aufenthaltsgesetz.
6 § 42 OG.

Fall 10 Das E-Mail-Konto der ehemaligen Mitarbeiterin

Fast alle Mitarbeiter(innen) der Verwaltung verfügen über ein persönliches E-Mail-Konto. Was passiert mit den (geschäftsrelevanten, aber möglicherweise auch privaten) Nachrichten, die sich in den entsprechenden Postfächern befinden, wenn Mitarbeiter(innen) innerhalb der Verwaltung den Job wechseln, aus dem öffentlichen Dienst austreten oder gar ableben? Wie kann präventiv darauf hin gearbeitet werden, dass ein Zugriff auf Postfächer nicht notwendig wird?

Wenn es nur unpersönliche E-Mail-Konten (rechtsabteilung.staatskanzlei@bs.ch) gäbe, wäre der Zugriff auf die Postfächer kaum ein Datenschutzproblem. Wenn aber jemand aus Ihrem Bekanntenkreis Ihre E-Mail-Adresse (vorname.name@bs.ch) rekonstruieren kann, dann können sich in Ihrem Posteingang auch höchstpersönliche Mitteilungen befinden. Auch im Gesendet-Postfach sind persönliche E-Mails nicht ausgeschlossen, da die nicht überbordende private Nutzung des E-Mails nicht verboten ist. Dem Zugriff des Arbeitgebers auf private Mails steht aber das Grundrecht auf informationelle Selbstbestimmung der Mitarbeiter(innen) entgegen – und allenfalls sogar dasjenige der externen Absender(innen) von privaten Mails an eine dienstliche Mail-Adresse.

Der Zugriff auf E-Mails von Mitarbeiter(inne)n durch Dritte stellt ein Bearbeiten von Personendaten dar. Es muss durch eine gesetzliche Grundlage legitimiert, durch ein öffentliches Interesse gerechtfertigt und ausserdem verhältnismässig sein. Eine gesetzliche Grundlage ist nicht ersichtlich – abgesehen von Fällen, in denen der Verdacht auf die Begehung strafbarer Handlungen besteht, worauf die Strafverfolgungsbehörde gestützt auf die Strafprozessordnung aktiv werden darf. Nach einer Weisung der Informatik-Konferenz[1] muss sichergestellt sein, dass die Bearbeitung eingehender E-Mails auch bei unvorhergesehenen Abwesenheiten von mehr als zwei Tagen gewährleistet ist; allerdings überlässt die Weisung die konkrete Umsetzung den Amtsstellen. Ein Zugriff Dritter auf ein E-Mail-Konto dürfte ausschliesslich als Ausnahmelösung vorgesehen werden (abgesehen von sog. Sekretariatslösungen für Leitungspersonen) – nebenbei bemerkt untersagt eine weitere Weisung[2] explizit die Weitergabe von Passwörtern an andere Personen.

Umso wichtiger dürfte es sein, darauf hinzuwirken, dass es gar nicht nötig wird, auf Postfächer von anderen Personen zuzugreifen. Der Datenschutzbeauftragte schlägt dazu folgendes Vorgehen vor:

— Die Mitarbeiter(innen) sind anzuhalten, ihre privaten und geschäftlichen E-Mails zu trennen und entsprechend zu markieren.
— Posteingangsfächer sollen wöchentlich geleert und ihre Inhalte abgelegt werden. Die Mitarbeiter(innen) sind regelmässig darauf aufmerksam zu machen. So wird vermieden, dass Geschäftsmails in einem Posteingang «verstauben» und sich beim Austritt einer Mitarbeiterin/eines Mitarbeiters die Frage nach dem Zugriff stellt.
— Vor einem geplanten Austritt sind die Mitarbeiter(innen) aufzufordern, ihre Postfächer zu leeren bzw. die Inhalte abzulegen.
— Das nicht mehr benötigte Benutzerkonto ist so rasch als möglich auf «inaktiv» zu setzen, so dass eingehende Mails gar nicht mehr angenommen werden. Die «Unzustellbarkeits-Meldung» soll darauf hinweisen, dass eingehende E-Mails nicht umgeleitet werden, und erwähnen, an wen sich Sender von Mails mit ihren Anliegen nun wenden können.

Auch bei bloss vorübergehenden Abwesenheiten soll keine automatische Weiterleitung eingerichtet werden, sondern nur eine Abwesenheitsmeldung, in welcher der Zeitpunkt der Rückkehr ins Büro erwähnt wird und die zuständigen Anlaufstellen, falls ein Sender nicht bis zur Rückkehr warten kann. Eine automatische Weiterleitung kann Persönlichkeitsrechte verletzen: Eine Mitarbeiterin will sich z.B. bei der übernächsten Vorgesetzten über ihren direkten Vorgesetzten beschweren. Die Adressatin hat aber eine automatische Umleitung zu ihrem Stellvertreter eingerichtet – ausgerechnet zu dem Vorgesetzten, über den sich die Mitarbeiterin in ihrem Mail beklagt ... Eine Abwesenheitsmeldung kann von Mitarbeiter(inne)n mit Remote-Access zu Kalender und E-Mail auch von zu Hause aus eingerichtet werden.

Sollten trotz aller Vorkehren neu eingegangene E-Mails «liegen bleiben», so dass sich ein Zugriff auf das Account nicht vermeiden lässt, so wäre das Einschalten einer neutralen Stelle denkbar.

Ergebnis

Beim Zugriff auf E-Mail-Konten von ehemaligen Mitarbeiter(inne)n besteht eine erhebliche Gefahr, dass Persönlichkeitsrechte verletzt werden. Es kann aber mit geeigneten Massnahmen präventiv darauf hingewirkt werden, dass sich im Normalfall das Problem vermeiden lässt. Auf eine automatische Weiterleitung von E-Mail ist – auch bei bloss vorübergehenden Abwesenheiten (Ferien, geplanter Spitalaufenthalt) – zu verzichten.

1 Weisung der Informatik-Konferenz vom 1. November 2007 zur Nutzung von E-Mails und zur Handhabung elektronischer Kalender.
2 Weisung der Informatik-Konferenz Basel-Stadt vom 22. Oktober 2003 für die Benutzung von Informatikmitteln in der Verwaltung des Kantons Basel-Stadt (mit Änderungen vom 15. September 2004).

Fall 11 Die Bekanntgabe «auf Ersuchen hin»

Verwaltungsbehörden haben der Steuerverwaltung «auf Ersuchen hin» alle erforderlichen Auskünfte zu erteilen. Sie können von sich aus Mitteilung machen, wenn nach Wahrnehmungen in ihrer amtlichen Tätigkeit die Wahrscheinlichkeit einer unvollständigen Versteuerung besteht. Muss das Amt für Umweltschutz und Energie (AUE) künftig generell die Namen und Adressen von Förderbeitrags-Empfänger(inne)n an die Steuerverwaltung liefern, wenn es diese einmal verlangt?

Wer eine Liegenschaft energetisch saniert, kann vom Kanton Förderbeiträge nach Energiegesetz erhalten. Jeweils zu Jahresbeginn soll von der Energiefachstelle im AUE eine Liste mit den betroffenen Liegenschaften, den Zahlungsempfänger(inne)n sowie den im Vorjahr ausgerichteten Summen an die Steuerverwaltung geliefert werden. Anhand der Daten soll bei den Steuererklärungen geprüft werden, ob die Subventionen von den Investitionen abgezogen worden sind.

Aus § 140 Abs. 1 Steuergesetz ergeben sich zwei Tatbestände:

— Die Verwaltungs- und Gerichtsbehörden des Kantons und seiner Gemeinden erteilen auf Ersuchen hin der Steuerverwaltung die erforderlichen Auskünfte (Satz 1).

— Die Verwaltungs- und Gerichtsbehörden des Kantons und seiner Gemeinden können von sich aus Mitteilung an die Steuerverwaltung machen wenn nach Wahrnehmungen in ihrer amtlichen Tätigkeit die Wahrscheinlichkeit einer unvollständigen Versteuerung besteht (Satz 2).

Die beiden Tatbestände unterscheiden sich durch die Initiative zur Datenbekanntgabe: Im ersten Fall steht ein Ersuchen der Steuerverwaltung am Anfang. Im zweiten Fall werden die anderen Behörden von sich aus tätig; Voraussetzung ist allerdings ein hinreichender Verdacht («die Wahrscheinlichkeit») einer unvollständigen Versteuerung. Beim Begehren der Steuerverwaltung handelt es sich klarerweise um den ersten Fall; die Wahrscheinlichkeit einer unvollständigen Versteuerung soll nach der Vorstellung der Steuerverwaltung mitnichten Voraussetzung für die Datenbekanntgabe sein. Wird aber die vom Gesetzgeber formulierte Voraussetzung des «Ersuchens» nicht ausgehebelt, wenn mit einem Mail («… inskünftig von Ihrem Amt zu Beginn jeden Jahres eine Liste über die im zurückliegenden Jahr ausgerichteten Förderbeiträge erhalten») ein für allemal «ersucht» wird?

Nach unserer Beurteilung kann der Gesetzgeber mit der Voraussetzung «auf Ersuchen hin» nur gemeint haben, dass auf Seiten des öffentlichen Organs, welches die Datenbekanntgabe verlangt, ein Anlass dazu vorhanden sein muss – etwa dass ein Steuerpflichtiger Sanierungsaufwendungen abziehen will, ohne dass ersichtlich ist, ob allfällige Förderbeiträge berücksichtigt sind. Hätte der Gesetzgeber eine voraussetzungslose generelle Informationspflicht der Verwaltungsbehörden gewollt, so hätte er eine entsprechend klare Regelung getroffen. Das hat er weder im Steuergesetz noch im Energiegesetz oder in der Energieverordnung getan.

Die Steuerverwaltung stellt sich auf den Standpunkt, der Passus «auf Ersuchen hin» bedeute nur, dass der Anstoss zum Amtshilfeverfahren von der Steuerbehörde aus gehen muss – im Gegensatz zu der vom Dateneigentümer «von sich aus» vorgenommenen Datenübermittlung. Die analoge Regelung im Bundesgesetz über die direkte Bundessteuer werde nach Praxis und Rechtsprechung nicht als Beschränkung auf den Einzelfall ausgelegt. Nicht gestattet seien einzig Suchaktionen (fishing expeditions).

Wir verstehen das Bemühen, dafür zu sorgen, dass die Steuergesetze wirkungsvoll vollzogen werden können. Wir können das Anliegen nachvollziehen, dass dort, wo der Kanton Private mit Leistungen unterstützt, diese Leistungen auch bei der Steuerveranlagung korrekt berücksichtigt werden. Wir erachten es aber weiterhin als unbefriedigend, dass verdachtsunabhängig Daten unter Behörden ausgetauscht werden, ohne dass der Gesetzgeber diesen Datenaustausch bewusst rechtfertigt. Es ist unseres Erachtens rechtsstaatlich problematisch, wenn eine Datenbekanntgabe im Rahmen der Amtshilfe ins Belieben eines öffentlichen Organs gestellt wird – ob die Steuerverwaltung ein solches «Ersuchen» stellt, ist offensichtlich völlig ihrem Ermessen anheim gestellt. Wir beugen uns aber der Rechtsprechung und Praxis.

Ergebnis

Die Bekanntgabe an die Steuerverwaltung «auf Ersuchen hin» ist nach Rechtsprechung und Praxis zulässig, auch wenn die Steuerverwaltung nur ein einziges Mal für alle Zukunft darum «ersucht». Wir erachten es aber als unbefriedigend, dass verdachtsunabhängig Daten unter Behörden ausgetauscht werden, ohne dass der Gesetzgeber diesen Datenaustausch bewusst rechtfertigt. Wir richten daher an alle rechtsetzenden Organe die Empfehlung, künftig unmissverständlich festzulegen, unter welchen Voraussetzungen Daten bekannt gegeben werden dürfen. Wir empfehlen zudem, im Sinne des gesetzlichen Erfordernisses der Erkennbarkeit der Datenbeschaffung in den Verfügungen der Energiefachstelle einen Hinweis anzubringen, dass die entsprechenden Daten der Steuerverwaltung mitgeteilt werden.

Fall 12 Im Zweifel an die Staatsanwaltschaft

Eine Vorgesetzte erhält Kenntnis vom Verdacht, dass ein(e) Mitarbeiter(in) eine Straftat begangen hat – Amtsgeheimnisverletzung, Bestechlichkeit, Konsum harter Pornografie ...Darf sie auf eigene Faust zu ermitteln beginnen? Soll sie die verdächtige Person darauf ansprechen? Kann man den Fall vielleicht «unter den Teppich kehren», damit der Verwaltung kein Imageverlust entsteht?

Bei einem öffentlichen Organ taucht der Verdacht auf, dass ein(e) Mitarbeiter(in) sich strafbar gemacht haben könnte. Eine Mitarbeiterin könnte beispielsweise Informationen, die sie im ihrer dienstlichen Funktion über einen Kunden der Amtsstelle zur Kenntnis bekommen hat, per E-Mail an Dritte weitergeben. Oder ein Mitarbeiter könnte gegenüber einem regelmässigen Lieferanten der Amtsstelle in einem E-Mail «Wünsche» angemeldet haben, beispielsweise er würde sich über eine Einladung zu einem Wochenende in einem Wellness-Hotel freuen. Oder mehrfach haben Kolleg(inn)en eines Mitarbeiters festgestellt, dass er Websites mit harter Pornografie aufgerufen hat.

Der Vorgesetzte der geschwätzigen Mitarbeiterin oder des begierigen Mitarbeiters bekommt den Verdacht mit, indem er beispielsweise von der betroffenen Person oder vom Lieferanten darauf angesprochen wird. Die Vorgesetzte des surfenden Mitarbeiters wird von dessen Kolleg(inn)en über das ungebührliche Surfverhalten informiert. Vielleicht haben die Vorgesetzten selber bereits Beobachtungen gemacht, die es nicht unwahrscheinlich erscheinen lassen, dass sich der Verdacht bestätigen könnte. Was sollen sie nun tun?

Sollen sie die Verdächtigten auf die Handlungen ansprechen und sie auffordern, sich künftig an die Regeln zu halten? Sollen sie von den Zentralen Informatikdiensten ZID die Log-Daten verlangen, um nachforschen zu können, ob sich der Verdacht erhärten lässt?

Im ersten Fall könnte es sich um eine Amtsgeheimnisverletzung handeln. Doch der Vorgesetzte ist sich dessen nicht sicher. Handelt es sich wirklich um etwas Geheimes, das bekannt gegeben worden sein soll? Selbst wenn die betroffene Person einen Ausdruck des E-Mails vorlegt, kann der Vorgesetzte das nicht sicher entscheiden. Vielleicht wird im E-Mail auch bloss bestätigt, dass etwas zutreffe – die bestätigte Information geht aber aus dem E-Mail nicht hervor. Im zweiten Fall könnte es sich um Bestechlichkeit handeln. Vielleicht wäre der Vorgesetzte nicht überrascht, wenn es bei dem Mitarbeiter, der ab und zu an Beschaffungen beteiligt ist oder mindestens gegen aussen gerne den Anschein vermittelt, als würde sein Urteil einiges wert sein. Ist es ein Mitarbeiter, der oft das Gefühl hat, er erhalte nicht genügend Wertschätzung? Und trotzdem: Muss die Formulierung eine Einladung zur Bestechung sein? Der Vorgesetzte ist sich nicht sicher. Im dritten Fall ist es möglicherweise harte, d.h. strafbare Pornografie – aber ist sich die Vorgesetzte sicher? Sie hat ja die Bilder nicht selber gesehen, und selbst wenn sie sie gesehen hätte: Könnte sie beurteilen, ob es sich um etwas Strafbares handelt?

Kurz: Überall stellt sich die Frage, ob es sich um strafbare Handlungen handelt. Wenn der Verdacht handfest genug ist, ist es nicht im Belieben der Vorgesetzten, darüber hinwegzusehen. Wenn es sich um strafbare Handlungen handelt, dann geht es um die Verwirklichung des Strafanspruchs des Staates. «Wir regeln das intern» ist keine rechtskonforme Lösung – es kann möglicherweise sogar selber strafrechtliche Folgen haben. Wenn sich die Vorgesetzten nicht sicher sind, ob es sich um strafbare Handlungen handelt, können sie den Fall der Staatsanwaltschaft zur Beurteilung unterbreiten. Die für diese Beurteilung zuständige und fachlich kompetente Behörde ist die Staatsanwaltschaft – nicht die oder der Vorgesetzte.

Die Schweiz ist international wegen schwacher Massnahmen zum Schutz vor Korruption unter Beobachtung – lieber von der Staatsanwaltschaft erfahren, dass ein Fall nicht zu einem Strafverfahren führt, als hinterher erleben müssen, dass es sich um einen schweren Fall gehandelt hat, den man aus falsch verstandener Loyalität unter den Teppich zu kehren versucht hat ...

Ergebnis

Besteht der Verdacht, dass strafbare Handlungen begangen worden sind, dann ist es nicht im Belieben der Vorgesetzten, Strafanzeige einzureichen. Falls den vorgesetzten Stellen unklar ist, ob der Verdacht zur Einleitung eines Strafverfahrens ausreicht, kann der Fall der Staatsanwaltschaft vor der Strafanzeige zur Beurteilung vorgelegt werden. Für eigene Ermittlungen durch die Vorgesetzten gibt es keine Rechtsgrundlagen; hingegen verfügt die Staatsanwaltschaft gestützt auf die Strafprozessordnung über alle nötigen Kompetenzen und Zwangsmittel.

Anhang

Verzeichnis der zitierten Gesetze und Materialen

Basel-Stadt

Aufenthaltsgesetz Gesetz vom 16. September 1998 über das Aufenthaltswesen (Aufenthaltsgesetz), SG 122.200.

BüRG Bürgerrechtsgesetz vom 29. April 1992 (BüRG, SG 121.100).

DSG Gesetz vom 18. März 1992 über den Schutz von Personendaten (Datenschutzgesetz, DSG), SG 153.260.

EnG Energiegesetz vom 9. September 1998 (EnG), SG 772.100.

EnV Verordnung vom 9. Februar 2010 zum Energiegesetz (Energieverordnung, EnV), SG 772.110.

IDG Gesetz vom 9. Juni 2010 über die Information und den Datenschutz (Informations- und Datenschutzgesetz, IDG), Kantonsblatt 2010, 914 ff.; noch nicht in Kraft.

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

OG Gesetz vom 22. April 1976 betreffend die Organisation des Regierungsrates und der Verwaltung des Kantons Basel-Stadt (Organisationsgesetz, OG), SG 153.100.

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).

SoHaG Gesetz vom 25. Juni 2008 über die Harmonisierung und Koordination von bedarfsabhängigen Sozialleistungen (Harmonisierungsgesetz Sozialleistungen, SoHaG), SG 890.700.

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

StG Gesetz vom 12. April 2000 über die direkten Steuern (Steuergesetz, StG), SG 640.100.

Bund, international

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

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

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

LMG Bundesgesetz vom 9. Oktober 1992 über Lebensmittel und Gebrauchsgegenstände (Lebensmittelgesetz, LMG), SR 817.0.

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

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

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
Dr. Beat Rudin, Advokat

Team
lic. iur. Andrea Klüser
lic. iur. Carmen Lindner
Dr. iur. Sandra Stämpfli
lic. iur. Barbara Widmer, LL.M., CIA

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