Tätigkeitsbericht 2009

Datenschutzbeauftragter des Kantons Graubünden

Datenschutzbeauftragter des Kantons Graubünden

RA Thomas Casanova · Arcas 22 · 7002 Chur
Telefon 081 250 79 40 · Telefax 081 252 63 46
datenschutzbeauftragter@staka.gr.ch

Inhalt

I. Vorwort

Es lebe der Skandal

Die Sensibilisierung für den Datenschutz hat in den letzten Jahren markant zugenommen. Mit dazu beigetragen haben die in regelmässiger Abfolge zu Tage tretenden Versäumnisse von Unternehmen und Behörden. Es entspricht nun einmal einer Tatsache, dass das Verständnis und die Berechtigung für Vorschriften erst erkannt werden, wenn Schaden entsteht oder wenn man davon direkt betroffen ist.

Daten sind ein kostbares Gut. Selbst Staaten sind bereit, dafür Millionenbeträge zu bezahlen. Die IT-Industrie hat den Wert von Daten schon längst erkannt. Anbietern von Diensten, die mit der Bekanntgabe von Daten verbunden sind (vgl. bspw. facebook), gelingt es, innert wenigen Jahren ihren Wert von Null auf Milliarden zu steigern.

Leider ist dem Einzelnen dennoch nicht immer bewusst, welchen Wert seine Daten für ihn persönlich haben. Vielfach unbedarft werden sie fremden Personen oder Organisationen anvertraut. Gedanken wer was mit diesen Daten anstellt, kommen schon gar nicht auf. Daher fehlt oft die Erkenntnis, die persönlichen Daten zu schützen und restriktiv mit ihnen umzugehen. Die permanente Aufklärung der Bevölkerung und der Behörden bildet daher mit eine Haupt- und Daueraufgabe der Datenschutzbeauftragten. So widersprüchlich es sich anhört, hilft dabei die regelmässige Aufdeckung eines Datenskandals.

Kantonaler Datenschutzbeauftragter:

RA Thomas Casanova

II. Ausgewählte Themen

1. Datenverknüpfungen im Gesundheitswesen[1]

Allgemeines

Im Gesundheitswesen stehen der Patient und die Patientin im Mittelpunkt. Ausgehend von diesen Personen ergibt sich eine Vielzahl von Verbindungen. Dabei ist die Krankengeschichte das zentrale Gefäss, in welchem sich Informationen über Patienten ansammeln. Anschaulich manifestiert sich die Datenflut am Beispiel eines Spitals. Die Verbindungen oder eben Verknüpfungen im Bereiche der Spitäler reichen fast ins Uferlose. Es liegt auf der Hand, dass aufgrund des technisch Machbaren die Begehrlichkeiten und der Druck auf die Spitäler zunehmen. Die verschiedenen Akteure im Gesundheitswesen wollen Zugang zu Spitaldaten. Aus Gründen des Persönlichkeitsschutzes ist jedoch das bis anhin geltende eingeschränkte Regime zu schützen.

Eine allgemein gültige Begriffsbestimmung für Verknüpfung besteht nicht. Im Zusammenhang mit Datenschutz bildet eine Verknüpfung die Verbindung von Daten, sei dies nun durch direkten Zugriff auf Datensätze, das Zusammenführen oder die Zurverfügungstellung von Daten. Es werden in jedem Fall datenschutzrelevante Bereiche tangiert. Der mögliche Anwendungsbereich ist also sehr breit gestreut.

Rechtliche Rahmenbedingungen

Der Patient und die Patientin, um deren Daten es letztendlich geht, stehen im Vordergrund. Folgerichtig hat der Persönlichkeitsschutz bzw. die Datenschutzgesetzgebung den entsprechenden Stellenwert. Der Datenschutz als eine Querschnittsmaterie ist sowohl für den privaten wie für den öffentlichen Sektor von grosser Bedeutung, und zwar unabhängig davon, in welchen spezifischen Kontexten sich dieser Umgang vollzieht[2]. Je nach Konstellation kommt im Gesundheitswesen das jeweilige kantonale oder das eidgenössische Datenschutzrecht zur Anwendung. Die zu beachtenden Prinzipien bleiben jedoch dieselben, weshalb auf die unterschiedlichen rechtlichen Erörterungen für private und öffentliche Spi-

---

[1] Verkürzte Wiedergabe eines Vortrages, gehalten anlässlich des 3. Schweizerischen Datenschutztages in Fribourg.

[2] Herbert Burkert, ZBl. 7/2007, S. 375.

täler verzichtet werden kann[3]. In der Praxis bereiten oft die Grundsätze der Rechtmässigkeit, der Verhältnismässigkeit und der Zweckmässigkeit Mühe.

Die heute beinahe überall abgeschlossene Entwicklung der papiermässigen Krankengeschichte zum elektronischen Patientendossier hat diese Sensibilität noch verstärkt[4]. Das medizinische Behandlungsverhältnis basiert bekanntlich auf dem privaten Auftragsrecht[5]. Der selbständige Arzt und das private Spital arbeiten auf dieser Grundlage. Daneben kennen wir die Behandlung am öffentlichen Spital nach öffentlichem Recht. Unabhängig davon werden immer schützenswerte Daten bearbeitet, welche Dritten nicht bekannt gegeben werden dürfen[6]. Es bedarf entweder eines Rechtfertigungsgrundes oder einer gesetzlichen Grundlage. Vor diesem Hintergrund sind sämtliche Verknüpfungen zu prüfen.

Der Aspekt des Rechtfertigungsgrundes gemäss Art. 13 DSG wird im Folgenden ausser Acht gelassen.

Den einschlägigen Gesetzen im Gesundheitsbereich (KVG, UVG, IVG, AHVG, ATSG) können keine Grundlagen entnommen werden, die ein systematisches Verknüpfen von Daten durch Dritte zulassen.

Spitalinterne Verknüpfungen

Beim internen Datenaustausch ist nach dem Prinzip der Verhältnismässigkeit dafür zu sorgen, dass nur die geeigneten und erforderlichen Daten an die jeweils berechtigten Stellen gelangen[7]. Der adäquate Datenfluss erlangt bei elektronischen Krankengeschichten eine besondere Bedeutung. Der Einsatz von Informationssystemen ermöglicht eine umfassende und effiziente Bearbeitung von Patientendaten. In den meisten Spitälern ist ein Klinikinformationssystem (KIS) bereits eingeführt, elektronische Bildarchi-

[3] Vgl. Art. 4 DSG; §8 ff. IDG Kt. ZH, 170.4; Art. 2 KDSG Kt. GR.

[4] Bruno Baeriswyl: Entwicklungen und Perspektiven des Datenschutzes in öffentlich-rechtlichen Krankenhäusern – Erfahrungen aus dem Kanton Zürich, in: Datenschutz im Gesundheitswesen, Forum Gesundheitsrecht, Zürich 2001, S. 57.

[5] Lukas S. Brühwiler-Frésey, Medizinischer Behandlungsvertrag und Datenrecht, Zürich 1996, S. 3.

[6] Art. 12 Abs. 2 lit. c DSG; Art. 17 Abs. 2 DSG.

[7] Bruno Baeriswyl, a. a. O., in: Datenschutz im Gesundheitswesen, Forum Gesundheitsrecht, Zürich 2001, S. 60.

vierung oder das elektronische Rezept bilden noch die Ausnahme, bestehen aber ebenso.

Im Zusammenhang mit der Behandlung von Personen dürfen Daten verschiedener Abteilungen und unterschiedlicher Anwendungen verbunden und zu einer Einheit zusammengeführt werden. Ausgehend von der Zentrumsstellung der Patientin und des Patienten sind alle Verbindungen zulässig, die für den Betroffenen direkten Bezug zur Behandlung haben. So kann aus dem KIS die Leistungserfassung extrahiert werden. Die administrativen Daten dürfen mit dem KIS verbunden werden oder der elektronische Rechnungsversand darf auf den Erhebungen des KIS basieren. Anwendungen, die nicht dem Behandlungsziel (worunter letztendlich auch die Rechnungsstellung zu verstehen ist) dienen, dürfen nicht verknüpft werden.

Outsourcing

Spitäler gehen dazu über, vielfältige Aufgaben Dritten zu übertragen. Auslagerungen werden in Art. 10a DSG ausdrücklich vorgesehen. Mit der kürzlich eingeführten Bestimmung soll der zunehmenden Arbeitsteilung in der heutigen Berufswelt Rechnung getragen werden. Eine Bearbeitung von Daten durch Dritte ist statthaft, wenn die Daten durch den Dritten nur so bearbeitet werden, wie der Auftraggeber es selbst tun dürfte und wenn keine gesetzliche oder vertragliche Geheimhaltungspflicht sie verbietet. Der Datenbearbeitung durch Dritte werden somit bewusst Grenzen gesetzt.

Der EDOEB stellt in seinem 14. Tätigkeitsbericht[8] fest, dass eine Übertragung der Patientendatenbearbeitung an Dritte infolge des strafrechtlich relevanten Berufsgeheimnisses des Arztes grundsätzlich nur bei Vorliegen der Einwilligung sämtlicher betroffener Personen zulässig ist, ausser der Zugriff beziehe sich lediglich auf nicht medizinische Daten. Die Praxis sieht indessen anders aus. Ärzte, Praxisgemeinschaften, Spitäler und Kliniken lassen zunehmend den ganzen IT-Bereich durch externe Anbieter erledigen. Die Datenbearbeitung reicht dabei von der einfachen Rechnungsstellung bis zur Echtzeitüberwachung von technischen Geräten während Behandlungen oder Operationen. Unweigerlich wird damit die Anwendung

[8] EDOEB, 14. Tätigkeitsbericht 2006/2007, S. 51.

von Art. 321 StGB [9] tangiert, wonach Ärzten und ihren Hilfspersonen das Offenbaren von Patientengeheimnissen verboten ist.

Die vorliegende Problematik manifestiert sich im Ausdruck «Hilfsperson». Können Inkasso- und IT-Dienstleister als Hilfspersonen im Sinne des StGB qualifiziert werden? Der EDOEB ist dezidiert der Meinung, der Hilfspersonenstatus sei bei IT-Unternehmungen nicht gegeben, da die unterstützende Person unter Leitung und Aufsicht des Geheimnisträgers tätig sein müsse [10]. Dieser Meinung wird vor allem von Praktikern widersprochen. Als Hilfsperson wird bezeichnet, wer bei der Berufstätigkeit des Geheimnisträgers in einer Weise mitwirkt, dass er grundsätzlich von den dabei wahrgenommenen Tatsachen ebenfalls Kenntnis erhält [11]. Nicht von Relevanz ist die Stellung. Vielmehr genügt es, wenn sie den Geheimnisträger in irgendeiner Funktion bei der Erfüllung seiner Aufgaben unterstützt und dabei Kenntnis von Geheimnissen der betreuten Person erhält [12]. Entgegen der Meinung des EDOEB kann ein IT-Unternehmen sehr wohl Hilfsperson des Geheimnisträgers sein. Eine adäquate Leitung und Aufsicht durch den Arzt ist lediglich eine Frage der Organisation. Vertraglich kann ohne weiteres festgelegt werden, wer für die Bearbeitung von Gesundheitsdaten extern zuständig ist bzw. unter welcher Verantwortung die Bearbeitung erfolgt. Technisch einfach ist die Protokollierung der konkret auf die Daten zugreifenden Mitarbeitenden. Ein allfälliger Verstoss kann also im Nachhinein ermittelt werden. Würde der Meinung des EDOEB gefolgt, könnte in einem grossen Spital, beispielsweise im Unispital Zürich oder im Inselspital Bern, faktisch eine geteilte Datenbearbeitung nicht erfolgen. Das computergestützte Patientenhandling vom Eintritt über die Klinikinformationssysteme bis zur Rechnungsstellung nach dem Austritt ist nur möglich, wenn – sei dies nun spitalintern oder -extern – eine Vielzahl von Spezialisten in ihren Bereichen Hand in Hand arbeiten.

[9] SR 311.0.
[10] Basler Kommentar, StGB II, Niklaus Oberholzer, Art. 321 N 6.
[11] Stefan Trechsel, Schweizerisches Strafgesetzbuch, Kurzkommentar, 2. Auflage, Zürich 1997, Art. 321 N 13.
[12] Basler Kommentar, StGB II, Niklaus Oberholzer, Art. 321 N 6.

Fall Management

«Durch Krankheit oder Unfall arbeitsunfähig gewordene Erwerbstätige bekommen dank dem Case-Management wieder eine Perspektive. Der Case-Manager begleitet und unterstützt den Versicherten. Er koordiniert alle nötigen Massnahmen von Invalidenversicherung, Ärzten, Spitälern, Arbeitgebern und weitern Institutionen.» [13] Zur administrativen Fallabwicklung setzen Krankenversicherer zunehmend sogenannte «Fall-Manager» in den Spitälern ein. Deren Koordinationstätigkeit regeln die Versicherer in Vereinbarungen mit den Spitälern. Zwar können diese Vereinbarungen begrifflich und inhaltlich voneinander abweichen. Es geht jedoch stets darum, dass Krankenversicherungen Case-Manager einsetzen, die als alleinige Ansprechpartner für das Spital Behandlungsprozesse koordinieren. Dadurch sollen die Qualität der Behandlung verbessert und die Kosten gesenkt werden. Die Koordination der Case-Manager setzt einen Informationsaustausch zwischen allen Beteiligten voraus [14]. Weder im KVG noch in kantonalen Gesundheitsgesetzen ist das Case-Management vorgesehen. Es fehlt also an einer gesetzlichen Grundlage. Ebenso weisen die meisten Verträge keine Bestimmung auf, wonach eine ausdrückliche Einwilligung des Betroffenen in das Case-Management vorgesehen ist.

Schlussbetrachtung

Verknüpfungen zwischen öffentlich-rechtlichen Spitälern und Dritten bedürfen einer gesetzlichen Grundlage, wenn Gesundheitsdaten bearbeitet werden. In der Regel fehlt es an dieser Voraussetzung. In der Praxis wird diese auf der Verfassung beruhende Tatsache vielfach ignoriert. Diese Gegebenheiten ändern nichts daran, dass entweder auf Verknüpfungen verzichtet wird oder auf Gesetzesstufe nachgebessert werden muss.

Unter Privaten dürfen Daten nur verknüpft werden, wenn ein Rechtfertigungsgrund im Sinne von Art. 13 DSG vorliegt.

---

[13] http://www.helsana.ch/dokument_show.cfm/uc_h_unser_standpunkt_juni07

[14] DSB Kt. ZH, Tätigkeitsbericht Nr. 14, 2008, S. 10.

2. GPS-Systeme in Fahrzeugen des Werkbetriebes

Ausgangslage

Eine Gemeinde beabsichtigt, zur Optimierung der Betriebsführung die Fahrzeugflotte des Werkbetriebes mit GPS-Geräten auszurüsten.

Es stellt sich die Frage, ob der Einbau von GPS-Geräten in Fahrzeugen zu einer ungerechtfertigten Überwachung der Arbeitnehmenden führt.

Gesetzliche Grundlage

Das Bearbeiten von Personendaten hat die Grundsätze der Rechtmässigkeit zu beachten (Art. 2 Abs. 1 kantonales Datenschutzgesetz [KDSG][1]). Unter Personendaten sind alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen, zu verstehen (Art. 3 lit. a eidgenössisches Datenschutzgesetz [DSG][2]). Mittels Auswertung von GPS-Daten kann der Arbeitsablauf eines Mitarbeitenden detailgenau nachgezeichnet werden. Mit der Abfrage von GPS-Daten werden demnach offensichtlich Personendaten bearbeitet.

Die Tätigkeit des Werkbetriebes stützt sich mehrheitlich auf ein Gesetz über die Abfallentsorgung. Darin werden in der Regel die Aufgaben des Werkbetriebes umschrieben. Zur Optimierung des Arbeitsablaufes können technische Hilfsmittel zum Einsatz gebracht werden. Dagegen ist grundsätzlich nichts einzuwenden.

Die Kontrolle und Registrierung von GPS-Daten führen nun zwangsläufig zu einer gänzlichen Überwachungsmöglichkeit der Mitarbeitenden. Gemäss Art. 26 der Verordnung 3 zum Arbeitsgesetz (ArGV 3)[3] dürfen Überwachungs- und Kontrollsysteme, die das Verhalten der Arbeitnehmer am Arbeitsplatz überwachen sollen, nicht eingesetzt werden. Gemäss Art. 4 lit. c ArGV 1 in Verbindung mit Art. 2 Abs. 2 ArG ist die Arbeitsgesetzgebung auf Betriebe der Gemeinden für die Abfuhr anwendbar. Folgerichtig ist Art. 26 ArGV 3 zu beachten.

[1] BR 171.100.
[2] SR 235.1.
[3] SR 822.113.

Überwachung der Arbeitnehmenden

Art. 26 ArGV 3 lautet:
«Überwachungs- und Kontrollsysteme, die das Verhalten der Arbeitnehmer am Arbeitsplatz überwachen sollen, dürfen nicht eingesetzt werden. Sind Überwachungs- oder Kontrollsysteme aus andern Gründen erforderlich, sind sie insbesondere so zu gestalten und anzuordnen, dass die Gesundheit und die Bewegungsfreiheit der Arbeitnehmer dadurch nicht beeinträchtigt werden.»

Gemäss Auskunft des Verantwortlichen dient der Einbau von GPS-Geräten nicht zur Überwachung der Mitarbeitenden. Vielmehr könne anhand der ermittelten Daten der Einsatz des Fuhrparks optimiert werden. Daneben würden die ermittelten Daten im Falle von Haftpflichtansprüchen (insbesondere im Winterdienst) wichtige Angaben liefern. Sie könnten für die detaillierte Rechnungsstellung an Dritte herangezogen werden, da neben der Position der Fahrzeuge eine Vielzahl von anderen wichtigen Daten erhoben werden (z. B. Einsatz Pflug, Einsatz Streuer, Pressmenge Kehricht etc.).

Ausgehend von der Anwendung von Art. 26 Abs. 2 ArGV 3 stellt sich die Frage, welche Massnahmen vorzukehren und zumutbar sind, damit eine unverhältnismässige Überwachung der Mitarbeitenden ausgeschlossen werden kann. Das Bundesgericht hat sich in einem wegleitenden Entscheid (vgl. BGE 130 II 425; Praxis 2005, Nr. 71) eingehend mit dem Einsatz von GPS-Geräten beschäftigt. Nach der bundesgerichtlichen Rechtssprechung kommt es bei der Frage, ob ein Überwachungssystem zulässig ist oder nicht, weniger auf die Art der Überwachung oder deren Wirkung an, als vielmehr auf die Gründe, die zur Errichtung geführt haben oder die Ziele, die damit verfolgt werden. Je nach den Umständen und der Art der Tätigkeit ist es nicht ausgeschlossen, dass Gründe im Zusammenhang mit der Organisation oder der Planung der Arbeit die Einrichtung von gewissen Überwachungssystemen, rechtfertigen können. Art. 26 ArGV 3 verbietet ein Überwachungssystem, wenn es allein oder vorwiegend bezweckt, das Verhalten der Arbeitnehmer an und für sich zu überwachen. Demgegenüber ist ein Einsatz erlaubt, obwohl objektiv betrachtet auch hier eine Überwachung stattfindet, wenn legitime Gründe vorliegen, die in der Natur des Arbeitsverhältnisses selber liegen. Schliesslich muss das gewählte Überwachungssystem vor dem Hintergrund sämtlicher Umstände im Vergleich zum beabsichtigten Zweck ein verhältnismässiges Mittel darstellen

und die Arbeitnehmer müssen im Voraus über den Einsatz des Systems informiert werden.

Das Bundesgericht hat sich eingehend mit dem Einsatz von GPS-Systemen beschäftigt. Es kam zum Schluss, dass ein GPS-System verhältnismässig ist, wenn die Überwachung nur indirekt und zeitweilig erfolgt sowie nur Teilaspekte betrifft. In diesem Zusammenhang hält das Bundesgericht fest:

«Wenn es das GPS-System dem Arbeitgeber hingegen erlaubt, die Reiseroute der von den Serviceleuten verwendeten Fahrzeugen dauernd und in Echtzeit zu verfolgen, könnte es sich im Verhältnis zum verfolgten Ziel um ein unverhältnismässiges Überwachungsmittel handeln.

In der Tat ist die Schwere der Beeinträchtigung der Gesundheit, der Persönlichkeit und der Bewegungsfreiheit der betroffenen Arbeitnehmer verschieden, je nachdem, ob sie vom Arbeitgeber dauernd und in Echtzeit überwacht werden oder ob eine Kontrolle erst «a posteriori», am Ende des Tages, erfolgt, und diese darin besteht, die Arbeitsrapporte mit den Informationen des GPS-Systems zu vergleichen.»

In ersterem Fall hielt das Bundesgericht zugunsten der Arbeitnehmenden fest, dass eine Stresssituation bestehe, die durch das Gefühl des ständigen Überwachtseins durch den Arbeitgeber hervorgerufen werde. Dies sei im zweiten Fall nicht gegeben.

Zusammenfassung

Zusammenfassend kann festgehalten werden, dass der Einbau eines GPS-Systems nicht grundsätzlich gegen Art. 26 ArGV 3 (vgl. auch Art. 328 OR) verstösst. Wesentlich ist ein verhältnismässiger Einsatz der technischen Möglichkeiten. Dazu gehört der Verzicht auf Echtzeitüberwachung. Das Bundesgericht hält richtigerweise fest, dass eine permanente über den ganzen Tag sich ausdehnende Überwachung die Gesundheit, die Bewegungsfreiheit und die Persönlichkeit der Arbeitnehmenden unverhältnismässig stark beeinträchtigt. Der Einbau des GPS-Systems muss somit in der Art und Weise erfolgen, dass eine Echtzeitüberwachung nicht möglich ist.

3. Aufbewahrung von Internetprotokollen

Der EDOEB hält in seinem Leitfaden über Internet und E-Mail-Überwachung am Arbeitsplatz [1] auf S. 14 was folgt fest:

«Ob Protokollierungen eingesetzt werden dürfen, wer und wie lange darauf Zugriff hat, muss nach den Kriterien der Zweck- und Verhältnismässigkeit entschieden werden. Ein Hinweis auf jede eingesetzte Protokollierung, deren Zweck, Inhalt und Aufbewahrungsdauer sollte aus Transparenzgründen im internen Überwachungsreglement erwähnt werden.» «Die Aufbewahrungsdauer der Protokollierungen steht in direktem Zusammenhang mit ihrem Zweck und muss im Nutzungs- und Überwachungsreglement transparent mitgeteilt werden. Dem Arbeitgeber obliegt keine gesetzliche Aufbewahrungspflicht im Zusammenhang mit Protokollierungen.»

Ähnlich äussert sich der EDOEB in seinem Merkblatt «Elektronische Spuren und Datenschutz» [2] auf S. 13:

«Die Benutzer haben keinen direkten Zugang zu den Spuren, die vom Unternehmen kontrolliert werden. Deshalb muss das Unternehmen es als seine Pflicht betrachten, die Benutzer unter anderem über das Vorhandensein, die Aufbewahrungsdauer und die Vernichtungspolitik zu informieren und darlegen, wer zu welchen Daten Zugang hat und wozu. Das Unternehmen hat also für vollständige Transparenz zu sorgen.» «Bei den Protokollen, die vom Unternehmen kontrolliert werden, sollte die Archivierungsdauer für Online-Daten nicht mehr als einen Monat und bei Offline-Daten nicht mehr als sechs Monate betragen.»

Es kann also festgehalten werden, dass den Arbeitgeber keine gesetzliche Pflicht trifft, Protokollierungen über eine längere Zeitdauer aufzubewahren. Aus Datenschutzgründen wird berechtigterweise Transparenz gefordert. Die Mitarbeitenden sollen wissen, wo welche Daten wie lange aufbewahrt werden und wer auf diese Zugriff hat.

Abschliessend ist die Frage zu klären, ob eine Behörde, welche verwaltungsintern IT-Dienstleistungen anbietet dem Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) [3] untersteht. Gemäss Art. 1 Abs. 2 gilt das BÜPF für alle staatlichen, konzessionierten oder

---

[1] Abrufbar unter: http://www.edoeb.admin.ch/dokumentation/00445/00472/index.html?lang=de.
[2] Abrufbar unter http://www.edoeb.admin.ch/themen/00794/00928/00929/index.html?lang=de.
[3] SR 780.1.

meldepflichtigen Anbieterinnen von Post- und Fernmeldedienstleistungen sowie für Internetanbieterinnen. Demgegenüber müssen Betreiber von internen Fernmeldenetzen und Hauszentralen lediglich die Überwachung dulden. Die Definition für den Begriff Internet-Anbieterin findet sich in der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF)[4]. Unter dieser Formulierung wird was folgt verstanden: Fernmeldedienstanbieterin oder Teil einer Fernmeldedienstanbieterin, die der Öffentlichkeit fernmeldetechnische Übertragungen von Informationen auf der Basis der IP-Technologien (Netzprotokoll im Internet [Internet Protocol]) unter Verwendung öffentlicher IP-Adressen anbietet (vgl. Art. 2 lit. a VÜPF). Personen, die über die Beschaffung, die Erstellung und den Betrieb dieser Einrichtungen entscheiden, werden als Betreiberinnen von internen Fernmeldenetzen oder Hauszentralen bezeichnet (vgl. Art. 2 lit. b VÜPF). Es ist nun so, dass das Amt der Öffentlichkeit keine fernmeldetechnischen Übertragungen anbietet. Vielmehr bildet es Teil der Arbeitsorganisation. Folgerichtig kommt das BÜPF auf das Amt nicht zur Anwendung. Damit entfällt auch die Vorschrift der sechsmonatigen Aufbewahrung der Daten gemäss Art. 15 Abs. 3 BÜPF. Eine Rückfrage beim EDOEB hat diese Ansicht bestätigt. Auf Stufe Bund wird das Bundesamt für Informatik ebenfalls nicht dem BÜPF unterstellt.

Es ist somit dem Arbeitgeber überlassen, gestützt auf den Anwendungszweck und das Prinzip der Verhältnismässigkeit die Aufbewahrungsdauer festzulegen.

Zum Schluss ist festzuhalten, dass diese Aussagen nicht für allenfalls vom Gemeinwesen beauftragte private Anbieter gelten, die als Provider arbeiten. Für jede Unternehmung ist im Einzelnen abzuklären, ob sie dem BÜPF und damit der verlängerten Aufbewahrungspflicht unterstehen.

[4] SR 780.11.

4. Uebermittlung von Personendaten von Nichtmitgliedern an die Reformierte Kirchgemeinde

Anzeige an die Vormundschaftsbehörde

Gemäss Art. 41 Abs. 2 EGzZGB ist derjenige, der von einem Fall, der zu Kinderschutzmassnahmen Anlass geben kann, Kenntnis erhält, verpflichtet, Anzeige zu erstatten[1]. In Art. 307 ZGB wird allgemein formuliert, wonach bei Gefährdung des Wohls des Kindes, ohne dass die Eltern für Abhilfe sorgen, geeignete Massnahmen zum Schutze des Kindes zu treffen sind. Beim Kindswohl wird unterschieden zwischen Gefährdung des körperlichen Wohls (körperliche Misshandlung, Fehlernährung, mangelnde Körper- und Gesundheitspflege etc.), der Gefährdung des geistigen Wohls (Erschwerung der Kontakte mit dem besuchsberechtigten Elternteil, fehlende Zusammenarbeit mit Schulbehörden, Konflikte bei Berufswahlentscheiden, fehlende Erziehungs- und Durchsetzungsfähigkeit, fehlende Bereitschaft zur Förderung bei allgemein schulischen Schwächen etc.) und der Kombination physischer und psychischer Beeinträchtigungen. Ob und gegebenenfalls welche Massnahmen erforderlich sind, bestimmt die Vormundschaftsbehörde. Falls ein Mitarbeitender der Behörde der Ansicht ist, es liege ein wichtiger Grund im Sinne des Gesetzes vor, ist er somit berechtigt, die Vormundschaftsbehörde zu informieren.

[1] Vgl. Tätigkeitsbericht 2008, Seite 16 ff.

Die Reformierte Kirchgemeinde möchte Personendaten von Nichtmitgliedern zum Aufbau einer Familienerfassung bei der Gemeinde beziehen.

Es handelt sich bei Angaben über die Religionszugehörigkeit in den meisten Fällen um besonders schützenswerte Personendaten gemäss Art. 3 lit. c Ziff. 1 DSG. Gemäss Art. 17 Abs. 2 DSG dürfen diese Daten nur bearbeitet werden, wenn ein Gesetz im formellen Sinn es ausdrücklich vorsieht. Die Ausnahmen für eine Weitergabe der Daten ohne gesetzliche Grundlage werden in der genannten Bestimmung abschliessend genannt. Daten können ausnahmsweise weitergegeben werden, wenn sie für eine in einem Gesetz im formellen Sinn klar umschriebene Aufgabe unentbehrlich sind, wenn die Rechte der betroffenen Person nicht gefährdet sind oder wenn die betroffene Person im Einzelfall zugestimmt hat.

Vorliegend ist lediglich der erste Fall von praktischer Bedeutung. Die Reformierte Kirchgemeinde ist für die Erfüllung ihrer Aufgaben nicht zwingend auf die Daten von Personen, die einer andern oder keiner Religionsgemeinschaft angehören, angewiesen. Die Unkenntnis hindert die Reformierte Kirchgemeinde nicht, ihre Aufgaben zu erfüllen, zumal sie gegenüber Mitgliedern anderer Religionsgemeinschaften ohnehin keinerlei Rechte besitzt. Allein schon aufgrund der Anwendung von Art. 17 DSG ist eine Weitergabe der verlangten Personendaten nicht möglich.

Sowohl Art. 4 DSG als auch Art. 2 Abs. 2 KDSG statuieren das Verhältnismässigkeitsprinzip. Ausfluss dieses Grundsatzes, vor allem in Verbindung mit Art. 4 Abs. 4 DSG, wonach die Beschaffung von Personendaten für die betroffene Person erkennbar sein muss, besteht darin, dass Daten primär

bei den betroffenen Personen zu erheben sind. Aufgrund der erstellten Datenbank hat die Reformierte Kirchgemeinde Kenntnis von den sogenannten «Mischehen». Es ist ihr ohne Weiteres zuzumuten, diese Personen anzuschreiben und die verlangten Daten anzufordern. Allein schon aus Gründen der Transparenz drängt sich ein solches Vorgehen auf. Auf alle Fälle sind die betroffenen Personen frei in ihrer Entscheidung, ob sie die verlangten Daten der Reformierten Kirchgemeinde weiterleiten möchten oder nicht.

Der Ausnahmekatalog von Art. 19 DSG ist für besonders schützenswerte Personendaten gemäss Art. 17 DSG nicht anwendbar. Mit der Gesetzesrevision aus dem Jahre 2006, in Kraft seit 1. Januar 2008, gilt das neue Regime. Selbst wenn aber auf Art. 19 DSG abgestellt werden würde, kann eine systematische Datenbekanntgabe ebenfalls nicht erfolgen. Der EDOEB machte wiederholt darauf aufmerksam, dass regelmässige Datenbekanntgaben mittels Listen an andere Behörden und die Übernahme in andere Datensammlungen eine ausdrückliche Rechtsgrundlage verlangen, in welcher auch die erforderlichen Grenzen der Datenbearbeitung und die Sicherheit zu regeln sind. Er weist explizit darauf hin, dass für die Bekanntgabe besonders schützenswerter Personendaten es zudem einer ausdrücklichen Regelung in einem formellen Gesetz bedarf (Maurer-Lambrou / Vogt, Basler Kommentar, Datenschutzgesetz, 2. Auflage, Art. 19, N 23).

III. Fälle aus der Praxis

1. Akteneinsichtsrecht der Opferhilfe

Es stellt sich die Frage, ob die Opferhilfe-Fachstelle (OHF) im Zusammenhang mit Gesuchen um Ausrichtung einer Genugtuung und/oder Entschädigung Unterlagen bei der Opferhilfe-Beratungsstelle (OHB) anfordern kann.

Massgebend für die Beantwortung dieser Fragestellung sind das Opferhilfegesetz (OHG)[1] und die dazugehörige kantonale Vollziehungsverordnung (VVzOHG)[2]. Gemäss Art. 29 Abs. 2 OHG stellt die zuständige kantonale Behörde den Sachverhalt von Amtes wegen fest. In der Botschaft zum VVzOHG (Botschaft vom 11. Mai 1993, S. 150) wird in den Bemerkungen zu den einzelnen Artikeln mit Bezug auf die Anwendung von Art. 4 ausdrücklich auf die Untersuchungsmaxime hingewiesen. Die Untersuchungsmaxime besagt, dass die Behörde, ohne an die Anträge der Betroffenen gebunden zu sein, selbständig den Sachverhalt erforschen und die Wahrheit autonom suchen kann. Dieses Vorgehen wird im Privatrecht insbesondere dann beschritten, wenn schwache Parteien geschützt werden müssen (z. B. Adoption, Besuchsrecht der Kinder). Die spezifische Anwendung im Privatrecht gibt daher einen weiteren Hinweis auf die Abklärungsbefugnisse im Rahmen des OHG. Das Amt hat gestützt auf Art. 4 VVzOHG weit reichende Kompetenzen.

Gemäss Art. 2 Abs. 1 VVzOHG ist das kantonale Sozialamt für die Beurteilung von Entschädigungs- und Genugtuungsansprüchen zuständig. Diese Aufgabe übernimmt innerhalb des Sozialamtes die OHF. Folgerichtig kann die OHF im Sinne von Art. 4 Abs. 1 VVzOHG die zweckmässigen Erhebungen vornehmen. Es liegt auf der Hand, dass für die Beurteilung eines Falles Dokumente der OHB, welche Daten der gesuchstellenden Person bearbeitet, unter Umständen eine grosse Relevanz aufweisen und daher auch beigezogen werden dürfen. Mit andern Worten ist die OHB verpflichtet, der OHF Auskünfte zu erteilen.

Art. 11 OHG kommt im Zusammenhang mit der Abklärung von Genugtuungs- und/oder Entschädigungsansprüchen nicht zur Anwendung, bzw. geht Art. 29 Abs. 2 OHG Art. 11 OHG vor. Gemäss Art. 19 DSG in Verbin-

---

[1] SR 312.5.
[2] BR 549.100.

dung mit Art. 2 Abs. 2 KDSG dürfen Behörden Personendaten bekannt geben, wenn dafür Rechtsgrundlagen bestehen. In diesem Zusammenhang wird auf Art. 17 DSG verwiesen. Danach dürfen besonders schützenswerte Personendaten sowie Persönlichkeitsprofile nur bearbeitet werden, wenn ein Gesetz im formellen Sinn es ausdrücklich vorsieht. Diese gesetzliche Grundlage findet sich nun in Art. 29 Abs. 2 OHG, in welchem die Untersuchungsmaxime statuiert wird. Die OHB kann also Unterlagen, welche für die OHF zur Beurteilung ihrer Aufgabe erforderlich sind, dieser übergeben.

2. Arztzeugnis

Weitergabe von Daten zu Forschungszwecken

Ein Institut der Universität Bern erwartet von der Gemeinde eine Zusammenstellung von Personendaten. Es stellt sich in diesem Zusammenhang die Frage, ob die Einwohnerkontrolle dem Anliegen der Universität Bern nachkommen kann. Das KDSG verweist in Art. 2 auf die Bundesgesetzgebung. Gemäss Art. 22 DSG reiht Abs. 1 lit. a – c die kumulativ zu erfüllenden Voraussetzungen für die Bearbeitung von Personendaten auf. Eine ähnliche Bestimmung kennt auch das bernische Datenschutzgesetz. Das Institut untersteht als Behörde dieser Gesetzgebung.
In Art. 22 Abs. 2 DSG wird darauf hingewiesen, dass für die Weitergabe von Daten das Zweckbindungsgebot, die formell-gesetzliche Grundlage bei der Datenbearbeitung besonders schützenswerter Personendaten und Persönlichkeitsprofile sowie die Rechtsgrundlage bei Bekanntgabe von Personendaten nicht erfüllt sein müssen. Eine Weiterleitung der verlangten Angaben kann trotzdem nur erfolgen, wenn das Universitätsinstitut sich verpflichtet, den Vorgaben des DSG nachzukommen und aufzeigt, welche Massnahmen zur Anonymisierung, insbesondere mit Bezug auf die Veröffentlichung der Daten, getroffen werden.

Ein Arbeitgeber meldet sich beim Spitalarzt und verlangt betreffend einen bestimmten Arbeitnehmer das diesem abgegebene Arztzeugnis bzw. er verlangt vom Arzt eine Bestätigung, wonach das vom Arbeitnehmer an den Arbeitgeber übergebene Arztzeugnis nicht manipuliert worden ist.

Es sind unterschiedliche Varianten zu berücksichtigen:

a) Krankheit
Gemäss KVG ist jede Person mit Wohnsitz in der Schweiz verpflichtet, sich für die Krankenpflege versichern zu lassen. Gegenstand der Versicherungspflicht bildet einzig die Krankenpflege. Die damit zusammenhängenden Kosten haben keinen Berührungspunkt mit einem Arbeitsverhältnis. Mithin entfällt eine Mitteilungspflicht an den Arbeitgeber von vorne herein.

b) Unfall
Im Rahmen eines Unfallereignisses ist ebenfalls der Erwerbsausfall gedeckt. Zwangsläufig wird das Arbeitsverhältnis tangiert. Für die Bearbeitung eines Unfallereignisses ist der Versicherungsträger zuständig. Gemäss Art. 28 Abs. 1 ATSG haben der Versicherte und sein Arbeitgeber beim Vollzug unentgeltlich mitzuwirken. Dazu gehört auch die Auskunftserteilung. Personen, die Versicherungsleistungen beanspruchen, haben alle Personen und Stellen, namentlich Ärztinnen und Ärzte im Einzelfall zu ermächtigen, die Auskünfte zu erteilen, die für die Abklärung von Leistungsansprüchen erforderlich sind (Art. 28 Abs. 3 ATSG). Die Personen und Stellen sind zur Auskunft verpflichtet. Demgegenüber haben Personen, die an der Durchführung der Sozialversicherungsgesetze beteiligt sind, gegenüber Dritten Verschwiegenheit zu bewahren (Art. 33 ATSG). Art. 97 UVG (Datenbekanntgabe) greift im vorliegenden Fall nicht.

Gemäss Art. 43 ATSG ist der Versicherungsträger für die erforderlichen Abklärungen zuständig. Der Arbeitgeber ist somit nicht berechtigt, von beteiligten Ärztinnen und Ärzten Unterlagen anzufordern. Sein Ansprechpartner ist der Versicherungsträger. Bei Ungereimtheiten hat er sich an diesen zu wenden.

c) Krankentaggeldversicherung / Arbeitsrecht
Die Krankentaggeldversicherung ist nicht obligatorisch. Daher sind die entsprechenden allgemeinen Vertragsbestimmungen zu beachten.

Indessen darf der Arbeitgeber unabhängig davon gestützt auf Art. 328b OR Daten über den Arbeitnehmer bearbeiten, soweit sie für die Durchführung des Arbeitsverhältnisses erforderlich sind. Auf die Anwendung der Datenschutzgesetzgebung wird ausdrücklich hingewiesen. Es stellt sich mithin die Frage, ob der Arbeitgeber die Echtheit einer ihm vorgelegten Urkunde überprüfen darf. Es ist davon auszugehen, dass ein Arztzeugnis für die Durchführung des Arbeitsverhältnisses relevant ist.

Gemäss Art. 3 lit. e DSG ist der Begriff des Bearbeitens weit zu fassen. Es dürfen Daten zu Kontrollzwecken bearbeitet werden (vgl. Honsell / Vogt / Wiegand, Basler Kommentar, Obligationenrecht, Art. 328b, N. 24). Der Arbeitgeber ist also grundsätzlich befugt, abzuklären, ob die ihm überlassenen Dokumente richtig sind. Art. 5 Abs. 1 DSG schreibt die Vergewisserung über die Richtigkeit ausdrücklich vor. Folgerichtig kann der Arbeitgeber beim zuständigen Spitalarzt anfragen, ob ein ihm vorgelegtes Arztzeugnis den Tatsachen entspricht. Er kann jedoch nicht ein Arztzeugnis anfordern. Hiezu ist er auch unter Anwendung der arbeitsvertraglichen Bestimmungen nicht befugt.

Wenn der Arbeitgeber dem zuständigen Spitalarzt ein Arztzeugnis zukommen lässt verbunden mit der Frage, ob dieses Dokument richtig sei, kann der Spitalarzt die Richtigkeit bzw. die Unrichtigkeit bestätigen.

3. Brandschutzkontrolle

Es wird angefragt, ob ein Gemeindefeuerpolizist trotz Aufforderung dies nicht zu tun, anlässlich einer Kontrolle in einer Tiefgarage Fotografien erstellen und diese an Dritte weiterleiten kann.

Massgebend für die Beantwortung dieser Frage ist die kantonale Feuerpolizeiverordnung (FPV)[1]. In Art. 1 FPV wird die Gemeinde für die Feuerpolizei und das Feuerwehrwesen verantwortlich erklärt. Unter dem Titel Schadenverhütung wird in Art. 15 FPV ausdrücklich auf die Brandschutzkontrolle eingegangen. Die Gemeinden sind zur regelmässigen Kontrolle von Bauten mit erhöhter Brandgefahr, darunter fallen auch Autoeinstellhallen, verpflichtet. Die Brandschutzkontrolle ist, wenn möglich, im Beisein des Besitzers oder seines Vertreters vorzunehmen. Dem Eigentümer ist ebenfalls auf Verlangen hin Gelegenheit zu geben, der Kontrolle beizuwohnen. Die Beanstandungen sind ohne Verzug dem Eigentümer, dem Besitzer, dem Gemeindevorstand und dem kantonalen Feuerpolizeiamt schriftlich mitzuteilen.

Dürfen nun Fotos angefertigt und diese an Dritte weitergeben werden?

Vorab zur Problematik der Fotografie. Die Gemeindebehörde ist grundsätzlich verpflichtet, die Feuerpolizeiverordnung durchzusetzen und Kontrollen durchzuführen (vgl. Art. 15 Abs. 1 FPV). Sie hat darüber einen schriftlichen Bericht zu verfassen. Ob dabei Fotografien angefertigt werden dürfen, geht nicht aus dem Gesetzestext hervor. Es sind daher die Bearbeitungsgrundsätze von Personendaten heranzuziehen.

Das staatliche Handeln muss zur Verwirklichung eines im öffentlichen Interesse liegenden Ziels geeignet und notwendig sein. Die Datenbearbeitung dient vorliegend der Feststellung von Mängeln bei Bauten und Anlagen bezogen auf eine mögliche Feuergefährlichkeit. Gesetzlich abgedeckt ist die Verpflichtung, schriftlich eine Mängelaufnahme zu verfassen und an verschiedene Beteiligte weiterzuleiten. Unzweifelhaft kann mittels einer Fotografie schnell und unkompliziert ein Sachverhalt festgestellt werden. Für die Beurteilung, ob ein solches Vorgehen rechtens ist, ist auf objektive Kriterien im Einzelfall abzustellen. Vorliegend ist ein Autoabstellplatz fotografiert worden, auf welchem Lampen, ein Eisengestell, eine Leiter und ein Klapptisch zu sehen sind. Objektiv beurteilt ist der Betroffen aufgrund

---

[1] BR 838.100.

der erstellten Fotografie in seiner Persönlichkeit kaum verletzt. Demgegenüber steht die Pflicht der Behörde, die bestehenden Mängel aufzunehmen. Dem geringen Eingriff in die Persönlichkeit steht die Verpflichtung der Gemeinde gegenüber, ein kantonales Gesetz zu vollziehen. Eine Fotografie ist geeignet, um auf einfache Art und Weise einen Sachverhalt zu dokumentieren. Sie dient aber insbesondere auch zu Beweiszwecken in einem möglichen Einspracheverfahren. Die Behörde handelte den Verhältnissen entsprechend und damit angemessen.

Ein zweiter Punkt beschlägt die Problematik der Weitergabe der Daten. Massgebend ist auch hier das Gesetz. Gemäss Art. 19 Abs. 2 FPV sind Beanstandungen ohne Verzug dem Eigentümer, dem Besitzer, dem Gemeindevorstand und dem kantonalen Feuerpolizeiamt schriftlich mitzuteilen. In der Regel wird der Eigentümer durch den Hauswart und die Verwaltung gegen aussen vertreten. Von einer derartigen Vertretungseigenschaft darf der Kontrolleur ausgehen. Es ist deshalb nicht zu beanstanden, wenn die genannten Personen gestützt auf Art. 19 Abs. 2 FPV von den Beanstandungen erfahren haben.

Mit Bezug auf die Archivierung der Unterlagen besteht keine kantonal gesetzliche Regelung. Gemäss Auskunft der kantonalen Feuerpolizei werden die Unterlagen nach Abschluss des Verfahrens in der Regel vernichtet. Da indessen keine gesetzliche Regelung besteht, ist auch ein anderes Vorgehen statthaft. Dabei orientiert sich die öffentliche Hand an den Gegebenheiten in der Privatwirtschaft. Insbesondere im Obligationenrecht werden Archivierungsregeln festgehalten. Es hat sich eine Aufbewahrungszeit von 10 Jahren eingebürgert. Diese Frist wird von vielen Gemeinwesen übernommen. Zweckmässigerweise werden also Verfahrensunterlagen spätestens nach 10 Jahre vernichtet.

Gemeindeprotokoll auf der Website

Massgabe für die Veröffentlichung bildet die Verfassung der Gemeinde. In der Regel stehen die Protokolle der Gemeindeversammlung jedem Stimmberechtigten zur Einsicht offen. Die Veröffentlichung ist gemäss Gemeindeverfassung somit in zweifacher Hinsicht eingeschränkt (vgl. Tätigkeitsbericht 2005, Seite 12). Zum einen ist nur jeder und jede Stimmberechtigte befugt, Einsicht in das Protokoll zu nehmen und zum zweiten wird mit dem Begriff «Einsicht» darauf hingewiesen, dass ein Stimmberechtigter oder eine Stimmberechtigte selbst aktiv werden muss. Das Gemeindeversammlungsprotokoll kann bei der Behörde eingesehen werden. Demgegenüber stellt die Publikation des Protokolls der Gemeindeversammlung im Internet eine weltweite Veröffentlichung dar. Jedermann kann zu jeder Zeit das Protokoll einsehen und Auszüge aus dem Protokoll auf den eigenen Computer herunterladen. Für die Einsichtnahme in das Protokoll ist keine Legitimation erforderlich, ausser die Gemeinde würde mit Passwörtern arbeiten, was aber wahrscheinlich allein schon aus Gründen der Praktikabilität nicht in Frage kommt. Auf alle Fälle enthält die Gemeindeverfassung in aller Regel nicht die erforderliche gesetzliche Grundlage für die Veröffentlichung des Protokolls der Gemeindeversammlung im Internet.

In periodischer Abfolge werden Vertrauenspersonen der Krankenkassen in Heime gesandt zur Überprüfung der Pflegeleistungen und Pflegeziele. Im Zusammenhang damit werden diesen Personen ohne Genehmigung der Betroffenen alle Pflegeunterlagen zur Verfügung gestellt.

Hinzuweisen ist auf ein Urteil des Bundesgerichtes (BGE 133 V 359), wonach in der Stadt Zürich die Helsana mit Bezug auf 16 namentlich genannte Patientinnen und Patienten verschiedene Gesundheitsunterlagen von Heimen verlangte, um die Einteilung der Pflegestufen überprüfen zu können. Das Bundesgericht hielt in seinem Urteil fest, dass es zulässig sei, Stichproben vorzunehmen, d. h. einen zufällig ausgewählten Teil einer Kontrolle zu unterziehen. Mit Sicherheit ist es jedoch nicht zulässig, den Vertrauenspersonen der Krankenversicherer unbesehen alle Pflegeunterlagen zur Verfügung zu stellen. Ein massgebendes in der Gesetzgebung verankertes Prinzip (vgl. Art. 2 Abs. 1 KDSG) bildet der Grundsatz der Verhältnismässigkeit. Es sind also nur diejenigen Dokumente abzugeben, welche erforderlich sind, um die Wirtschaftlichkeit gemäss Art. 56 KVG überprüfen zu können. Hiezu hielt das Bundesgericht im vorgenannten Entscheid fest: «Die Wirtschaftlichkeitskontrolle, die der Versicherer gemäss Art. 56 Abs. 2 KVG vornehmen muss, dient der Kontrolle über die Leistungserbringer. Schon aus dieser Zielsetzung ergibt sich, dass entgegen einer in der Literatur zum Teil vertretenen Ansicht nicht vom Leistungserbringer zu beurteilen ist, welche Angaben er dem Versicherer liefert, würde doch sonst der zu Kontrollierende selber den Umfang der Kontrolle festlegen. Vielmehr richtet sich der Umfang der Auskunftspflicht danach, was der Versicherer für die Durchsetzung seiner Rechte und der Pflicht zur Kontrolle der Wirtschaftlichkeit gemäss Art. 32 KVG als notwendig erachtet. Die Auskunftspflicht unterliegt freilich dem Verhältnismässigkeitsprinzip; sie kann sich

sowohl im Lichte des Datenschutzrechtes als auch unter Berücksichtigung der administrativen Belastung für den Leistungserbringer nur auf Angaben erstrecken, die objektiv erforderlich und geeignet sind, um die Wirtschaftlichkeit der Leistungen überprüfen zu können.» Vor dem Hintergrund des massgebenden Bundesgerichtsurteils ist dem Krankenversicherer zuzumuten, vorgängig mitzuteilen, in welche Dossiers im Sinne einer Stichprobe Einsicht verlangt wird. Das Heim kann dann vor Eintreffen der Vertrauensperson des Krankenversicherers die Krankengeschichte bereit legen und allenfalls nicht relevante Dokumente aus der Krankengeschichte entfernen. Für die Beurteilung der Leistungspflicht sind die Vertrauenspersonen der Krankenversicherer nicht auf die Einsicht in die gesamte Krankengeschichte angewiesen. In der Krankengeschichte müssen diejenigen Dokumente verbleiben, welche Aufschluss geben über die Einteilung in die entsprechende BESA-Stufe.

Die Bereitstellung aller Patientenunterlagen wird selbst nach dem sehr weitgehenden Urteil des Bundesgerichtes ganz eindeutig als nicht verhältnismässig angesehen. Der Krankenversicherer ist ohnehin verpflichtet, die Überprüfung vorzubereiten. Daher ist eine vorgängige Mitteilung betreffend die Überprüfung von Dossiers durchaus legitim. Die Verweigerung der Einsichtnahme in Krankenakten kann jedoch nicht durchgesetzt werden.

5. Kreisrechnung

Die jährliche Kreisrechnung wird in sehr detaillierter Form jeweils den Gemeindepräsidenten zugestellt. Aus der Rechnung ist beispielsweise ersichtlich, wer welche vormundschaftliche Massnahme erhalten hat oder welche Personen strafrechtlich verfolgt wurden. Es stellt sich die Frage, ob ein derart hoher Detaillierungsgrad erforderlich ist.

Die Kreise sind Körperschaften des öffentlichen Rechtes mit eigener Rechtspersönlichkeit (Art. 70 KV). Gemäss Verfassung des Kreises leisten die Gemeinden eine Defizitgarantie. Das Verwaltungsdefizit wird jährlich nach einem bestimmen Schlüssel (Einwohnerzahl, Steueraufkommen) auf die Gemeinden aufgeteilt. Die Gemeinden besitzen folgerichtig das Recht, angemessen über die Kreisrechnung dokumentiert zu werden. Vorliegend stellt sich die Frage, wie detailliert die Kreisrechnung abgefasst werden soll.

Die Kreisbehörde untersteht dem kantonalen Datenschutzgesetz (KDSG; vgl. Art. 1 Abs. 3 KDSG). In Art. 2 KDSG werden die Grundsätze für das Bearbeiten von Personendaten genannt, nämlich das Prinzip der Rechtmässigkeit, der Verhältnismässigkeit, der Zweckmässigkeit, der Zweckgebundenheit, der Richtigkeit und der Datensicherheit.

Die Anwendung des Prinzips der Verhältnismässigkeit muss einer näheren Prüfung unterzogen werden. Der Grundsatz der Verhältnismässigkeit hat Verfassungsrang (vgl. Art. 5 Abs. 2 BV). Ein Verhalten ist dann verhältnismässig, wenn die Massnahme geeignet ist, das angestrebte Ziel zu erreichen (Zwecktauglichkeit), und diejenige ist, welche die privaten Interessen am meisten schont (geringstmöglicher Eingriff). Schliesslich muss die Massnahme auch durch ein überwiegendes staatliches Interesse gerechtfertigt sein (vgl. Maurer – Lambrou / Vogt, Basler Kommentar, Datenschutzgesetz, Art. 4, N 9). Aus diesem allgemein geltenden Grundsatz lässt sich für die Datenbearbeitung ableiten, dass ein Datenbearbeiter nur diejenigen Daten beschaffen und bearbeiten darf, die er für einen bestimmten Zweck objektiv tatsächlich benötigt (BGE 125 II 473). Konkret ist mithin abzuklären, ob die Namensnennung in der Kreisrechnung für die Gemeinde erforderlich ist, um ihrer eingeschränkten Prüfungspflicht nachkommen zu können.

Es ist davon auszugehen, dass die Kreisrechnung – wie verfassungsmässig vorgesehen – durch die Rechnungsrevisoren geprüft und vom Kreisrat abgenommen wird. Die Weiterleitung an die Gemeinden bezweckt einzig,

diese über ihre Beteiligung zu informieren. Eine materielle Prüfung erfolgt nicht, zumal die Beiträge der Gemeinden nach formellen, statischen Kriterien erhoben werden. Es ist deshalb nicht einzusehen, weshalb auf dieser Ebene irgendwelche Personendaten in der Rechnung aufscheinen sollen.

Es stellt sich vielmehr sogar die Frage, ob selbst in der internen Rechnung insbesondere Personendaten der Vormundschaftsbehörde Eingang finden. Gemäss Art. 360 ZGB haben die vormundschaftlichen Organe (Vormundschaftsbehörde, Vormund und Beistand) sowohl eine öffentlich-rechtliche Aufgabe zu vertreten, als auch die Interessen ihrer Klienten wahrzunehmen. Im Zuge der Erfüllung ihrer Aufgaben erhalten sie regelmässig besonders schützenswerte Personendaten (vgl. Art. 3 lit. c DSG). Nach neuer Lehrmeinung ist aus dem Vormundschaftsrecht selber die grundsätzliche Schweigepflicht der vormundschaftlichen Organe mit Bezug auf die Informationen, die sie im Zusammenhang mit der Ausübung ihrer vormundschaftlichen Aufgabe erhalten, als ungeschriebener Rechtssatz herzuleiten (Honsell / Vogt / Geiser, Basler Kommentar, Zivilgesetzbuch I, Art. 360, N 11). Ohne Recht und Pflicht zur Geheimhaltung würden die Organe das Vertrauensverhältnis zu der jeweils betroffenen schutzbedürftigen Person gar nicht finden oder spätestens dann verlieren, wenn die Geheimnisse preisgegeben würden. Das Vormundschaftsgeheimnis ist dermassen grundlegend im Wesen des Vormundschaftsrechtes, dass eine andere Lösung einen Widerspruch des ZGB mit sich selbst darstellen würde (Basler Kommentar, ZGB I, a. a. O. N 11). Die Pflicht zur Verschwiegenheit ergibt sich sodann gestützt auf Art. 8 Abs. 1 EMRK und aus Art. 28 ZGB. Das Vormundschaftsgeheimnis umfasst neben der Schweigepflicht der vormundschaftlichen Organe deren Schweigerecht gegenüber Behörden und privaten Dritten. Das Vormundschaftsgeheimnis gilt grundsätzlich generell und absolut (Basler Kommentar, ZGB I, a. a. O. N 19). Vor diesem Hintergrund erstaunt es, dass offenbar eine Vielzahl von Personendaten der Vormundschaftsbehörde Eingang in die Kreisrechnung findet. Die Vormundschaftsbehörde muss ihre bis anhin gepflegte Praxis sicherlich überdenken.

6. Gebrauch des persönlichen PC's bei Prüfungen

Der PC bietet vielfältige Möglichkeiten für die Erweiterung des Schulunterrichtes. Es besteht aber auch die Gefahr, dass er zweckentfremdend genutzt und insbesondere bei Prüfungen als unerlaubtes Hilfsmittel missbraucht wird. Aus diesem Grund verbieten z. B. die HTW Chur und die Uni St. Gallen auf den Gebrauch von privaten PC's anlässlich von Prüfungen. Die Uni St. Gallen lässt nicht einmal über das gewöhnliche Mass hinausgehende Rechner zu. Ganz grundsätzlich stellt sich die Frage, ob die Zulassung von Computern überhaupt möglich ist, vor dem Hintergrund des grossen Aufwandes der Überprüfung auf unzulässige Inhalte. Dies insbesondere wenn man sich vergegenwärtigt, welche Vielzahl von Möglichkeiten es gibt, Texte, Tabellen, Links etc. in einem PC zu verstecken.

Unabhängig von diesen einleitenden Bemerkungen handelt es sich beim Lesen und Überprüfen von Dateien um eine Bearbeitung von Personendaten (vgl. Art. 3 lit. e DSG). Gemäss Art. 2 Abs. 1 KDSG sind beim Bearbeiten von Personendaten die Grundsätze der Rechtmässigkeit, der Verhältnismässigkeit, der Zweckmässigkeit, der Zweckgebundenheit, der Richtigkeit und der Datensicherheit zu beachten. Mithin braucht es für den Eingriff in die Privatsphäre eine gesetzliche Grundlage (vgl. Art. 17 Abs. 1 DSG). Diese ist vorliegend nicht gegeben. Art. 19 Abs. 1 DSG unterscheidet vier Fälle, bei welchen eine Bearbeitung auch bei fehlender gesetzlicher Grundlage möglich ist, nämlich:

a) wenn die Daten für die Erfüllung der gesetzlichen Pflicht unentbehrlich sind,
b) wenn die Person im Einzelfall eingewilligt hat,
c) wenn die Daten allgemein zugänglich sind und
d) bei einer ungerechtfertigten Verweigerung.

Vorliegend sind lediglich die Fälle a) und b) von praktischer Bedeutung.

Die Schule könnte sich auf den Standpunkt stellen, die Durchsuchung eines PC's auf prüfungsrelevante Daten sei für die Erfüllung der gesetzlichen Pflicht einer korrekten Ablegung einer Prüfung unentbehrlich. Diesem Argument könnte entgegengehalten werden, dass für die Ablegung der Prüfung ein PC gar nicht erforderlich ist und entsprechend die Basis für die Einsicht in Daten eines persönlichen PC's nicht gegeben sind. Mit einem Verzicht auf die Zulassung von privaten PC's kann dennoch eine reguläre Prüfung abgenommen und damit die gesetzliche Pflicht erfüllt werden.

Vorstellbar wäre das vorgängige Einholen einer Einwilligung zur Einsicht in die PC-Daten. Eine solche Einwilligung muss jedoch auf freiwilliger Basis erfolgen. Mit anderen Worten darf die Verweigerung einer Einwilligung nicht mit Nachteilen verbunden sein. Entweder werden den Schülern, die nicht in die Einsichtnahme in ihre PC's eingewilligt haben, hauseigene PC's zur Verfügung gestellt, oder die Prüfung kann auch ohne Zuhilfenahme von PC's abgelegt werden. Der zweite Fall wird wahrscheinlich in der Praxis nicht vorliegen, ansonsten wäre die Pflicht, bei der Prüfung ein PC zu gebrauchen, ohnehin unnütz.

Bei der Zustimmung zur Dateneinsicht ist auf grosse Transparenz zu achten. Es darf nicht der Eindruck erweckt werden, dass bei einer Weigerung der Zustimmung ein Nachteil entstehen könnte. In einem solchen Fall würde es sich datenschutzrechtlich nicht mehr um eine Einwilligung handeln. Die Schülerschaft ist also in angemessener Weise zu informieren (vgl. Art. 4 Abs. 5 DSG).

Im Weiteren müsste ein Reglement erstellt werden, das Auskunft gibt, wie beim Verdacht auf Unregelmässigkeiten vorgegangen würde, wer beispielsweise Einsicht nehmen dürfte, ob die oder der Geprüfte an der Einsichtnahme zugegen sein könnte, welche Daten kopiert werden dürften etc.

In Anbetracht der Tatsache, dass auf PC's, insbesondere bei Jugendlichen, vielfach sehr Intimes gespeichert wird, eine Kontrolle auf Missbrauch mit erheblichem Aufwand verbunden ist, da prüfungsrelevante Daten auf einfache Weise gut versteckt werden können, und die Weigerung einer Einwilligung mit keinerlei Nachteilen verbunden sein darf, wird empfohlen, auf die Zulassung von persönlichen PC's bei Prüfungen zu verzichten.

7. Verwendung von Adressen im Zusammenhang mit einem Referendum

Krankengeschichte

Im Zusammenhang mit Abklärungen in einem Einzelfall wurde festgestellt, dass aus der Krankengeschichte eines Spitals nicht hervorgeht, an welche Drittpersonen ausserhalb des Spitals Unterlagen zugestellt worden sind. Konkret sind Teile der Krankengeschichte an die zuständige Krankenkasse versandt worden, ohne dass in der Krankengeschichte ein Hinweis zu finden war.
Die Krankenkassen wenden sich mit konkreten Anfragen, welche mit einem Antwortcouvert versehen sind, direkt an die Ärzte. Diese antworten vielfach handschriftlich. Ein Eintrag in die Krankengeschichte unterbleibt, nicht zuletzt aufgrund der Tatsache, dass diese aktuell nicht immer greifbar ist.
Auf die Qualität von Gesundheitsdaten (vgl. Art. 3 lit. c DSG) muss nicht näher eingangen werden. Hinzuweisen ist aber auf Art. 8 Abs. 2 DSG. Danach muss der Inhaber der Datensammlung den betroffenen Personen unter anderem mitteilen können, wer Datenempfänger ist. Aus der Krankengeschichte muss somit zwingend hervorgehen, was wann an wen zugestellt worden ist. Unabhängig von der datenschutzrechtlichen Relevanz sollte aus Gründen der Transparenz eine Krankengeschichte diese Information ohnehin beinhalten.

Es geht um die Frage, ob ein Referendumskomitee Unterschriftenlisten für eigene Zwecke nutzen darf.

Die Verfassung des Gemeinwesens verweist in Art. 7 e im Zusammenhang mit dem anzuwendenden Recht auf das Gesetz über die Ausübung der politischen Rechte im Kanton Graubünden (GPR)[1]. Gemäss Art. 81 Abs. 2 GPR werden eingereichte Unterschriftslisten nicht zurück gegeben und können auch nicht eingesehen werden. Der Zweck der Unterschriftensammlung besteht darin, ein dem fakultativen Referendum unterstelltes Geschäft dem Souverän vorzulegen. Dafür sind gemäss Art. 7 lit. b der Verfassung des Gemeinwesens 300 Unterschriften von Einwohnern und Einwohnerinnen erforderlich. Ein anderer Zweck ist nicht gegeben. Art. 2 Abs. 1 KDSG befasst sich mit den bei der Bearbeitung von Personendaten anzuwendenden Grundsätzen. Es sind dies das Prinzip der Rechtmässigkeit, der Verhältnismässigkeit, der Zweckmässigkeit, der Zweckgebundenheit, der Richtigkeit und der Datensicherheit. In Art. 2 Abs. 2 KDSG wird ausdrücklich auf die sinngemässe Anwendung des DSG hingewiesen. Nach dessen Art. 4 dürfen Personendaten nur rechtmässig bearbeitet werden. Unter Bearbeiten wird gemäss Art. 3 lit. e DSG jeder Umgang mit Personendaten verstanden, insbesondere das Beschaffen, das Verwenden und Bekanntgeben. Die Bearbeitung der Personendaten hat nach Treu und Glauben zu erfolgen. Diese dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist (Art. 4 Abs. 3 DSG).

Vorliegend mussten in sinngemässer Anwendung von Art. 79 GPR spezielle Unterschriftslisten geschaffen werden, die einen Mindestinhalt

[1] BR 150.100.

aufzuweisen hatten. Aus diesen Unterschriftslisten geht klar und eindeutig hervor, wofür eine Einwohnerin oder ein Einwohner seine Adressdaten bekannt gibt. Die Unterschriftensammlung bezweckt einzig und allein die Durchführung einer Volksabstimmung zu einem bestimmten Geschäft. Die in Art. 2 KDSG und Art. 4 DSG aufgeführten wichtigsten materiellen Grundsätze sind bei der Bearbeitung von Personendaten einzuhalten. Ein Privater begeht eine Persönlichkeitsverletzung, wenn er diese Grundsätze missachtet und keinen Rechtfertigungsgrund nach Art. 12 ff. DSG anführen kann (Maurer – Lambrou / Vogt, Basler Kommentar, Datenschutzgesetz, Art. 4, N 4).

Es ist noch einmal auf die Zweckbindung bei der Bearbeitung von Personendaten hinzuweisen. Eine betroffene Person muss nicht hinnehmen, dass die erhobenen Daten einem andern Zweck zugeführt werden. Gerade im Bereich der Ausübung von politischen Rechten ist mit Bezug auf die Weiterverwendung von Daten grösste Zurückhaltung geboten. Darauf weisen auch die eidgenössischen und kantonalen Bestimmungen im Zusammenhang mit der Ausübung der politischen Rechte hin (vgl. Art. 64 Abs. 2 BPR, Art. 19 Abs. 6 VPR, Art. 60 Abs. 2 GPR, Art. 81 Abs. 2 GPR). Als unzulässige Zweckänderung wurde beispielsweise die Sammlung von Adressen im Zusammenhang mit einer Initiative gewertet, welche von den Initianten später zu andern Zwecken weiterverwendet werden sollte (BBl. 1988 II 451).

Gestützt auf das Prinzip der Zweckbindung dürfen somit eingeholte und dem Staat übergebene Unterschriften lediglich für die Durchführung einer Urnenabstimmung Verwendung finden.

8. Weitergabe von Personendaten

Eine Person, welche in der kantonalen Verwaltung arbeitete, löste aufgrund von schwerwiegenden Differenzen ihren Arbeitsvertrag im gegenseitigen Einverständnis auf. Sie bewarb sich in der Folge wieder beim selben Arbeitgeber, indessen bei einer anderen Dienststelle, in einem anderen Departement. Zur Ausfertigung des Arbeitsvertrages mit dem Antrag auf Anstellung kamen die Unterlagen zum Personalamt, das bereits bei der Auflösung des früheren Arbeitsvertrages involviert gewesen war. Der zuständige Sachbearbeiter nahm mit der antragstellenden Dienststelle Kontakt auf und riet von einer Anstellung ab.

Es stellt sich in diesem Zusammenhang die Frage, ob das Personalamt diese Dienststelle kontaktieren darf und inwiefern über das Vorgefallene Informationen weitergegeben werden dürfen. Darüber hinaus soll abgeklärt werden, ob ohne Ermächtigung der betroffenen Person Referenzauskünfte kantonsintern eingeholt werden dürfen.

Massgebend für die Beurteilung der aufgeworfenen Fragen sind neben der Datenschutzgesetzgebung das kantonale Personalgesetz (PG)[1] sowie die dazugehörende Verordnung (PV)[2].

Gemäss Art. 3 PG regelt das Personalgesetz das Arbeitsverhältnis der kantonalen Mitarbeitenden. Mit der Bezeichnung Kanton sind die kantonale Verwaltung, die selbständigen kantonalen Anstalten und die Gerichte gemeint. Arbeitgeber für alle Mitarbeitenden, welche dem Personalgesetz unterstehen, ist folgerichtig der Kanton. Es wird keine Unterscheidung zwischen einzelnen Departementen oder gar Dienststellen gemacht. Ausfluss dieser rechtlichen Vorgabe bildet das zentral für alle Dienststellen tätige Personalamt. Gemäss dem Regierungs- und Verwaltungsorganisationsgesetz (RVOG)[3] gliedert sich die Kantonale Verwaltung in fünf Departemente. Diese umfassen Verwaltungseinheiten, die den Departementen unterstellt sind. Die Aufgaben der einzelnen Bereiche und damit auch der Dienststellen werden von der Regierung in einer Verordnung geregelt (vgl. Art. 10 Regierungs- und Verwaltungsorganisationsverordnung [RVOV][4]).

---

[1] BR 170.400.
[2] BR 170.410.
[3] BR 170.300.
[4] BR 170.310.

Im Anhang 1 der RVOV werden das Personalmanagement und die damit zusammenhängenden Organisationsfragen dem Departement für Finanzen und Gemeinden zugewiesen. Es erstaunt deshalb nicht, dass das Personalamt sämtliche Dienststellen in arbeitsrechtlichen Fragen berät und unter anderem auch Anträge um Anstellungen kontrolliert. Demgegenüber sind gestützt auf Art. 63 PG unterschiedliche Instanzen für die Anstellung und Kündigung zuständig. Das Personalamt besitzt also lediglich beratende Funktion. Der Entscheid, ob eine Person angestellt wird, obliegt dem jeweiligen Linienvorgesetzten.

Wechselt eine Person innerhalb der kantonalen Verwaltung die Stelle, ist damit kein Wechsel des Arbeitgebers verbunden. Der Dienstaltersurlaub richtet sich beispielsweise nach dem letzten Eintritt beim Kanton und nicht etwa nach den Dienstjahren in einem jeweiligen Amt (Art. 51 PV). Gleiches gilt für die Ehrung von langjährigen Mitarbeitenden (Art. 53 PV; Art. 42 PG). Klar und eindeutig ist somit der Kanton als solcher Arbeitgeber eines kantonalen Mitarbeitenden.

Das Personalamt ist gemäss Anhang 1 zur RVOV für das Personalmanagement zuständig. Diese umfassende Aufgabe wird in Art 59 PG näher beschrieben. Danach unterstützt es die Regierung und die Verwaltung in der Umsetzung der Personalpolitik und in der einheitlichen Anwendung des Personalrechts. Das Personalamt bereitet die Verträge, Verfügungen und Beschlüsse personalrechtlicher Natur vor. Es prüft, ob die beabsichtigten Entscheide den personalrechtlichen Erlassen und der Praxis entsprechen, und kann in seinem Aufgabengebiet fachtechnische Weisungen erlassen. Als Querschnittsamt hat das Personalamt daher sicherlich die eingehenden Anstellungsanträge zu prüfen. Dazu gehören neben den rechtlichen Aspekten Vergleiche mit andern Ämtern hinsichtlich Lohneinreihung, Aufgabengebiet, Qualifikation etc. Eine Prüfung muss zwangsläufig auch eine Meinungsäusserung beinhalten. Das Personalamt darf somit der antragstellenden Dienststelle mitteilen, wenn es der Ansicht ist, eine Anstellung entspreche nicht kantonsinternen Richtlinien. Darüber hinaus kann es ebenfalls von einer Anstellung abraten, wenn in der Vergangenheit Probleme mit der anzustellenden Person aufgetreten sind. Aus Gründen des Persönlichkeitsschutzes und in Anwendung des Prinzips der Verhältnismässigkeit sind jedoch nur diejenigen Informationen weiterzugeben, die für die Neuanstellung von Belang sind, beispielsweise verminderte Belastbarkeit, unzureichende Eingliederung in ein Team etc. Das anstellende Amt ist jedoch nicht über den vorgefallenen Sachverhalt zu dokumentieren. Es

ist diesem zuzumuten, sich direkt an die anzustellende Person zu wenden und die erforderlichen Informationen bzw. Erlaubnisse einzuholen.

Art. 4 PG verweist im Zusammenhang mit dem Einholen von Referenzen auf die subsidiäre Anwendung des OR. Art. 328 OR beinhaltet ausdrücklich den Schutz der Persönlichkeit. In Art. 328b OR wird dieser Schutz im Zusammenhang mit der Bearbeitung von Personendaten konkretisiert. Das Einholen von Referenzen ist zunächst unzulässig (Honsell / Vogt / Wiegand, Basler Kommentar, Obligationenrecht I, Art. 328b, N 22; Art. 12 Abs. 2 lit. b DSG). Es stellt sich die Frage, ob diese unbestrittene Einschränkung auch für das kantonsinterne Einholen von Auskünften gilt. In Anwendung von Art. 17 und 19 DSG in Verbindung mit Art. 2 Abs. 1 KDSG und Art. 4 DSG ist diese Frage zu bejahen. Dem anstellenden Amt, das aufgrund der Bewerbungsunterlagen von der früheren Anstellung beim Kanton Kenntnis haben muss, ist es zuzumuten, für die Einholung von internen Referenzen die Zustimmung der betroffenen Person einzuholen (Basler Kommentar, a. a. O., Art. 320 OR, N 10), zumal es sich bei Referenzauskünften durchaus um besonders schützenswerte Personendaten handeln kann (Art. 3 lit. c DSG), selbst wenn sich eine allfällige Auskunftserteilung zwingend auf die Eignung für das Arbeitsverhältnis oder die Durchführung des Arbeitsvertrages beschränken muss. Allein die Tatsache, dass sich eine Person innerhalb des Betriebes beruflich verändert, gibt der ehemaligen, vorgesetzten und personalverantwortlichen Stelle keine Berechtigung, ohne weiteres Auskünfte zu erteilen (Art. 19 DSG). Die Einholung von Referenzen, ob kantonsintern oder -extern ist an die ausdrückliche Zustimmung der betroffenen Person gebunden.

9. Weitergabe von Schuldaten

Es wird angefragt, unter welchen Bedingungen Schuldaten von Mittelschulen an private Dritte weitergegeben werden dürfen.

Vorab stellt sich die Frage, ob insbesondere private Mittelschulen dem KDSG unterstellt sind. Gemäss Art. 1 KDSG dient das Gesetz dem Schutz von Personen vor widerrechtlichem Bearbeiten von Personendaten durch Behörden. Als Behörden im Sinne des Gesetzes gelten nicht nur Amtsstellen des Kantons und der Bezirke, sondern auch öffentlich-rechtliche Anstalten, Stiftungen und Körperschaften des Kantons und der Bezirke sowie Private, soweit ihnen öffentliche Aufgaben übertragen sind. Es kann also davon ausgegangen werden, dass sämtliche Mittelschulen des Kantons Graubünden dem KDSG unterstellt sind. In der praktischen Anwendung ändert sich ohnehin wenig, selbst wenn dies nicht so wäre. Lediglich die Zuständigkeit wäre eine andere. Da das KDSG im Sinne eines Rahmengesetzes gestützt auf Art. 2 Abs. 2 KDSG integral auf das DSG verweist, macht es materiell-rechtlich keinen Unterschied, ob nun eine Schule als Privatperson oder als Behörde im Sinne des KDSG zu qualifizieren ist.

Die Bekanntgabe von Personendaten an Drittpersonen wird in Art. 19 DSG behandelt. Angestellte einer Mittelschule sind in ihrer privaten Tätigkeit als Drittpersonen zu behandeln. Personendaten dürfen nur bekannt gegeben werden, wenn dafür eine Rechtsgrundlage besteht, oder wenn die Daten für den Empfänger im Einzelfall zur Erfüllung seiner gesetzlichen Aufgaben unentbehrlich sind, die betroffene Person im Einzelfall eingewilligt hat oder die betroffene Person ihre Daten allgemein zugänglich gemacht hat und eine Bekanntgabe nicht ausdrücklich untersagt wurde. Diese Aufzählung in Art. 19 DSG ist abschliessend. Vorliegend kann davon ausgegangen werden, dass eine Rechtsgrundlage für die Datenbekanntgabe an Privatpersonen fehlt.

Im Weiteren ist die Voraussetzung gemäss Art. 19 Abs. 1 lit. a DSG, wonach die Daten für den Empfänger im Einzelfall zur Erfüllung seiner gesetzlichen Aufgabe unentbehrlich sind, in der Regel ebenfalls nicht gegeben. Es ist auch davon auszugehen, dass die betroffenen Personen ihre Daten nicht allgemein zugänglich gemacht haben. Diese Zugänglichmachung muss ohnehin im Zusammenhang mit der Institution Schule gesehen werden.

Es verbleibt somit die Einwilligung gemäss Art. 19 Abs. 1 lit. b DSG. Im Zuge der Revision des DSG ist die vorgenannte Bestimmung angepasst worden. Währenddem früher eine Weitergabe möglich war, wenn die Ein-

willigung der betroffenen Person nach den Umständen vorausgesetzt werden konnte, ist dieser Passus nunmehr gestrichen worden. Folgerichtig wurde Art. 19 DSG verschärft. Hinzuweisen ist schliesslich auf Art. 19 Abs. 2 DSG. Danach dürfen auf Anfrage Name, Vorname, Adresse und Geburtsdatum einer Person auch bekannt gegeben werden, wenn die Voraussetzungen von Art. 19 Abs. 1 DSG nicht erfüllt sind. Diese Bestimmung bezieht sich jedoch nur auf Einzelanfragen. Systematische Bekanntgaben sind durch sie nicht gedeckt (vgl. Maurer – Lambrou / Vogt, Basler Kommentar, Datenschutzgesetz, Art. 19, N 63). Bei der Bekanntgabe von Personendaten ist ganz grundsätzlich immer eine Interessenabwägung vorzunehmen. Ein angefragtes Organ gewährt die Datenbekanntgabe nur, wenn diese nach dem Recht, dem es untersteht, zulässig ist und insbesondere keine Geheimhaltungsbestimmungen die Datenbekanntgabe verbieten (Basler Kommentar, a. a. O., Art. 19, N 27). Eine Datenbekanntgabe an eine aussenstehende Drittperson scheitert daher regelmässig an den berechtigten, datenschutzrechtlichen Schranken.

Schulhomepage

Können Fotos von Schülern auf der Schulhomepage ohne schriftliche Zustimmung der Eltern veröffentlicht werden[1].

Bei der Publikation von Fotos, insbesondere Fotos von Ausflügen ist Vorsicht geboten. Die Betreiber der Homepage müssen darauf achten, dass die Fotos keinen komprimitierenden Inhalt aufweisen. Es sind grundsätzlich nur alltägliche Situationen zu publizieren.

Mit Bezug auf die Zustimmung der mündigen SchülerInnen bzw. der Erziehungsberechtigten ist auf die Personenbezogenheit hinzuweisen. Die Personenbezogenheit ist sicherlich gegeben, wenn die Fotos mit den einzelnen Namen verbunden werden. Daher sind Namen zu vermeiden. Die Kinder bzw. die Erziehungsberechtigten sind darauf hinzuweisen, dass Fotos ins Internet gestellt werden. Dadurch erhalten sie die Möglichkeit, dagegen zu opponieren. Falls ein Elternteil nicht wünscht, dass ihr Kind im Internet erscheint, ist diesem Ansinnen Rechnung zu tragen, und ein Bild ist von der Homepage zu entfernen. Bei Fotos von Schulausflügen, Schulaufführungen und dergleichen dürfte dies zu keinen Problemen führen. Anders verhält es sich bei der Publikation von Klassenfotos, wenn nur eine Person sich dagegen ausspricht. Gegebenfalls müsste jedoch diesem Anliegen durch Einfärbung der bestimmten Person Rechnung getragen werden.

[1] Vgl. Merklätter DSB BL, Welche Personendaten über Schülerinnen und Schüler, Lehrpersonen und Schulratsmitglieder dürfen auf Schulwebsites veröffentlicht werden?; Empfehlung Internet in der Schule, http://www.baselland.ch/main_publikationen-htm.309820.0.html.

10. Weiterleitung von Fotos

In der Notfallabteilung des Kantonsspitals Graubünden werden regelmässig Fotos von speziellen Verletzungen gemacht. Diese Fotos werden in der Notfallabteilung archiviert und sind unter dem Namen des jeweiligen Patienten abrufbar. Es kommt nun vor, dass diese Fotos an die weiterbehandelnden Ärzte zuhanden der KG abgegeben werden. Im Weitern kommt es vor, dass ausnahmsweise der behandelte Patient bzw. die behandelte Patientin nachfragt. Darüber hinaus dienen sie zur Aufklärung von Straftaten, zumeist im Zusammenhang mit häuslicher Gewalt. Und schliesslich melden andere Abteilungen Ansprüche an.

Vorab stellt sich die Frage, ob eine Fotoaufnahme datenschutzrechtlich relevant ist. Das Datenschutzgesetz bezweckt den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden (vgl. Art. 1 DSG). Mithin muss aufgrund der Fotografie immer auf eine bestimmte Person geschlossen werden können. Wenn dies nicht der Fall ist, ist die Fotografie datenschutzrechtlich nicht relevant. Wenn beispielsweise ein schwerer Unterschenkelbruch dokumentiert wird, kann eine solche Detailaufnahme bei einem späteren Gebrauch zu Schulungs- oder andern Zwecken keiner konkreten Person zugeordnet werden, sofern die Aufnahme nicht mit weiteren Angaben wie Patientennummer, Adresse, Name des Patienten und anderem versehen ist.

Wenn indessen direkt oder indirekt auf die Patientin oder den Patienten geschlossen werden kann, handelt es sich um eine Bearbeitung von Daten im Sinne des Datenschutzgesetzes.

Gemäss Art. 3 lit. c Ziff. 2 DSG werden Daten über die Gesundheit als besonders schützenswerte Personendaten qualifiziert. Der Gesetzgeber gab damit zum Ausdruck, dass diese sensitiven Daten mit besonderer Vorsicht zu bearbeiten sind.

Im Folgenden soll auf einige in der Praxis sich ergebende Fälle hingewiesen werden:

a) Interner Unterricht
Datenschutzrelevante Fotos können für die interne Weiterbildung der Mitarbeitenden verwendet werden. Da die Mitarbeitenden der Notfallstation ohnehin Kenntnis der bei ihnen behandelten Patientinnen und Patienten haben und die Weiterbildung eine Kernaufgabe der Tätigkeit innerhalb der Notfallstation bildet, ist ein Gebrauch erstellter Fo-

Strafanzeige

Darf ein Mitarbeiter eines Sozialdienstes eine Strafanzeige an die Kantonspolizei richten, wenn ihm ein Klient im Zusammenhang mit der Beratung mitteilt, er sei der Täter in der Messerstecherei XY. Gemäss Art. 13 Sozialhilfegesetz sind die Mitarbeitenden der öffentlichen Sozialdienste zur Verschwiegenheit verpflichtet. Ausnahmen sieht das Gesetz nicht vor. Bekanntlich gilt jedoch der Grundsatz, wonach die Bekanntgabe von Personendaten eine gesetzliche Grundlage haben muss, nicht absolut. Es ist zu prüfen, ob ein Anwendungsfall von Art. 19 DSG vorliegt. Im zu beurteilenden Fall sind offensichtlich keine der verlangten Voraussetzungen gegeben. Gestützt auf die Datenschutzgesetzgebung ist demnach eine Strafanzeige nicht möglich. Gemäss Art. 69 StPO besteht für Behörden und kantonale Mitarbeiterinnen und Mitarbeiter eine Anzeigepflicht nur, soweit sie in anderen Erlassen vorgeschrieben ist. Mithin entfällt eine Anzeigepflicht gestützt auf die Strafprozessordnung. Hinzuweisen ist noch auf Art. 320 StGB. Danach macht sich jemand, dem ein Geheimnis offenbart wurde, das ihm in seiner Eigenschaft als Mitglied einer Behörde oder als Beamter anvertraut worden ist, oder das er in seiner amtlichen oder dienstlichen Stellung wahrgenommen hat, strafbar (vgl. auch Art. 35 DSG). Als Rechtfertigungsgrund wäre der Tatbestand des Notstandes (vgl. Art. 34 StGB) zu prüfen. Dieser kommt in der Regel aber nur zur Anwendung im Zusammenhang mit bevorstehenden Delikten. Ein Mitarbeiter des Sozialdienstes besitzt unter Vorbehalt von Art. 34 StGB keine Berechtigung zur Stellung einer Strafanzeige.

tografien im Zusammenhang mit dem Unterricht zulässig.

b) Aufnahme in die KG
Wenn der nachbehandelnde Arzt die Fotos anfordert, muss selbstverständlich ein Zusammenhang mit der Behandlung bestehen. Diese Fotos müssen Eingang in die KG finden, um ein vollständiges Akteneinsichtsrecht gewährleisten zu können.

c) Abgabe an die Patientin / den Patient
Eine Patientin oder ein Patient hat ein umfassendes Akteneinsichtsrecht. Mithin können Fotografien der Notfallstation der Patientin oder dem Patienten nicht vorenthalten werden.

d) Strafuntersuchungsbehörden
Das Datenschutzgesetz ist nicht anwendbar auf hängige Strafverfahren. Gestützt auf die Strafprozessordnung können Untersuchungsbehörden Akten heraus verlangen, soweit diese für das Strafverfahren benötigt werden.

e) Dritte
Dritten können Personendaten nur innert der engen Grenzen von Art. 17 und 19 DSG bekannt gegeben werden. Dritte im Sinne des Gesetzes sind ebenfalls Ärzte oder Abteilungen innerhalb des Spitals, die mit der aktuellen Behandlung der Patientin oder des Patienten nichts zu tun haben.

Danach können Personendaten nur bekannt gegeben werden, wenn dafür eine Rechtsgrundlage besteht. Im Einzelfall ist dies zu überprüfen. In der Regel kann sich ein Dritter nicht auf ein spezielles Gesetz berufen. Dennoch können Daten weitergegeben werden, wenn die Daten für den Empfänger im Einzelfall zur Erfüllung

seiner gesetzlichen Aufgabe unentbehrlich sind, die betroffene Person im Einzelfall eingewilligt hat oder die betroffene Person ihre Daten allgemein zugänglich gemacht hat. Eine Drittperson hat demgemäss darzutun, weshalb eine Fotografie der Notfallabteilung für die Erfüllung der eigenen gesetzlichen Aufgabe unentbehrlich ist. Grundsätzlich ist der Drittperson zuzumuten, sich vorerst direkt an die Patientin oder den Patienten zu wenden. Die Unentbehrlichkeit wird in der Praxis nur in seltenen Einzelfällen vorkommen.

Allein schon aus Gründen der Transparenz sollte, wenn immer möglich, das Einverständnis der betroffenen Person eingeholt werden (vgl. auch Art. 4 DSG). Bei der Einholung des Einverständnisses ist der Patientin oder dem Patienten mitzuteilen, wer Adressat der Fotografie ist und zu welchem Zweck diese Fotografie weitergeleitet werden soll. Die Patientin oder der Patient muss auch wissen, ob allenfalls weitere Kreise Einsicht in die Daten haben werden. Schliesslich ist die weitere Verwendung abzuklären. Es geht nicht an, dass datenschutzrelevante Fotografien von Dritten weiteren Personen zur Verfügung gestellt werden.

IV. Verbände

Privatim, die Vereinigung der Kantonalen Datenschutzbeauftragten erfüllt vor allem bei der Verfassung von Vernehmlassungen über eidgenössische Gesetze eine wichtige Rolle. Mit der Professionalisierung der Aufgabenbewältigungen konnte privatim vermehrt Spezialisten für die Lösung gesamtschweizerischer Probleme zuziehen. Vorgesehen ist, diesen Dienst noch zu erweitern. Daneben bilden die jährlichen Fachtagungen Basis für den Informations- und Meinungsaustausch. Wünschenswert wäre eine gemeinsame Plattform für in allen Kantonen auftretende gemeinsame Fragestellungen.

Die Arbeitsgruppe Gesundheit, welcher der DSB GR vorsteht, hat sich im Jahre 2009 unter anderem mit dem standardisierten Case-Management, dem Outsourcing von Aufgaben sowie mit dem Thema DRG befasst.

V. Statistik Anfragen DSB 2009

Wer \ Was	Kurzanfragen	Berichte	Empfehlungen	Kontrollen	Vernehmlassungen	Referate	Kurse	Weiterbildung/Verbände
Kantonale Dienste								
Allgemeine Verwaltung	2				1		1	
DVS	1		1					
DJSG	10	0	1		2			
EKUD	5	1	0		0			
DFG	3	1	1					
BVFD	2							
öff. rechtliche Anstalten	2		2	0				
Gerichte	0							
Kreise	2	0						
Gemeindeverbände								
Gemeinden	23	0	0		0			
Bürgergemeinden								
Juristische Personen								
Private Personen	48	2	4					
Andere	1		2			1	4	4
Total	99	4	11	0	3	1	5	4

VI. Abkürzungsverzeichnis

a.a.O.	am angegebenen Ort
Abs.	Absatz
AHVG	Bundesgesetz über die Alters- und Hinterlassenenversicherung
Art.	Artikel
ArG	Bundesgesetz über die Arbeit in Industrie, Gewerbe und Handel
ArGV	Verordnung zum Arbeitsgesetz
ATSG	Bundesgesetz über den Allgemeinen Teil des Sozialversicherungsrechtes
BBl	Bundesblatt
BESA	BewohnerInnen – Einstufungs- und Abrechnungssystem
BGE	Bundesgerichtsentscheid
BL	Kanton Basel-Landschaft
BPR	Bundesgesetz über die politischen Rechte
BR	Bündner Rechtsbuch
bspw.	beispielsweise
BÜPF	Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs
BV	Bundesverfassung
BVFD	Bau-, Verkehrs- und Forstdepartement
bzw.	beziehungsweise
DFG	Departement für Finanzen und Gemeinden
d. h.	das heisst
DJSG	Departement für Justiz, Sicherheit und Soziales
DSB	Datenschutzbeauftragter
DSG	Eidgenössisches Datenschutzgesetz
DVS	Departement für Volkswirtschaft und Soziales
EDOEB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EKUD	Erziehungs-, Kultur- und Umweltschutz-departement
etc.	et cetera
f. / ff.	folgend / folgende
FPV	Feuerpolizeiverordnung
GPR	Gesetz über die Ausübung der politischen Rechte im Kanton Graubünden
GPS	Global Positioning System
GR	Graubünden

IDG	Gesetz über die Information und den Datenschutz (Kanton Zürich)
IT	Informationstechnik
IVG	Bundesgesetz über die Invalidenversicherung
KDSG	Kantonales Datenschutzgesetz
KG	Krankengeschichte
KIS	Klinikinformationssystem
Kt.	Kanton
KV	Kantonsverfassung
KVG	Bundesgesetz über die Krankenversicherung
lit.	litera
N	Note
Nr.	Nummer
OHB	Opferhilfe – Beratungsstelle
OHF	Opferhilfe – Fachstelle
OHG	Opferhilfegesetz
OR	Obligationenrecht
PG	Kantonales Personalgesetz
PV	Kantonale Personalverordnung
RVoG	Kantonales Regierungs- und Verwaltungsorganisationsgesetz
RVoV	Kantonale Regierungs- und Verwaltungsorganisationsverordnung
S.	Seite
SR	Systematische Sammlung des Bundesrechts
StGB	Schweizerisches Strafgesetzbuch
StPO	Kantonale Strafprozessordnung
UVG	Bundesgesetz über die Unfallversicherung
usw.	und so weiter
vgl.	vergleiche
VPR	Verordnung über die politischen Rechte im Kanton Graubünden
VÜPF	Verordnung über die Überwachung des Post- und Fernmeldeverkehrs
VVzOHG	Vollziehungsverordnung zum Opferhilfegesetz
z. B.	zum Beispiel
ZGB	Schweizerisches Zivilgesetzbuch
ZH	Zürich
Ziff.	Ziffer

Impressum

Gestaltung: zanoni.kommunikation, Chur · **Druck:** Druckerei Casutt AG, Chur
Gedruckt auf Cyclus Recycling-Papier aus 100 % speziell sortierten Druckerei- und Büroabfällen