Tätigkeitsbericht 2005

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

Schengen-Auswirkungen auf das KDSG

Mit der Zustimmung der Schweiz zu Schengen / Dublin kommt ein grosser gesetzlicher Anpassungsbedarf auf die kantonalen Datenschutzgesetze zu. In Graubünden kann diesem Vorgang relativ gelassen entgegengeblickt werden. Zum einen ist ein entsprechendes Gesetz bereits in Kraft und zum zweiten hat es der kantonale Gesetzgeber in kluger Voraussicht vermieden, ein umfassendes, detailliertes Werk zu verabschieden. Vielmehr wird im kantonalen Datenschutzgesetz (KDSG[1]) in materieller Hinsicht fast integral auf das eidgenössische Datenschutzgesetz (DSG[2]) verwiesen. Dies hat den Vorteil, dass auf kantonaler Ebene kaum Handlungsbedarf für materielle Änderungen besteht. Die zurzeit laufende Revision des DSG wird auch auf die konkrete kantonale Umsetzung Auswirkungen haben. Da jedoch davon ausgegangen werden kann, dass das revidierte Gesetzeswerk den europäischen Anforderungen zu genügen vermag, gilt dies auch für das KDSG. In unserem Kanton reduziert sich die Überprüfung des KDSG mit den europäischen Vorgaben auf den formalen Bereich, insbesondere das Klagerecht, die Anzeigebefugnis und die Unabhängigkeit des Datenschutzbeauftragten (DSB). Manchmal ist weniger mehr.

Kantonaler Datenschutzbeauftragter:

RA Thomas Casanova

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

II. Schengen / Dublin

Allgemeines

Das Volk hat am 5. Juni 2005 der Teilnahme der Schweiz an Schengen / Dublin zugestimmt. Das Dublin-Abkommen regelt die Assoziierung der Schweiz an die unter dem Stichwort «Dublin II» bekannte Richtlinie der EU sowie an Eurodac. «Dublin II» regelt die Kriterien, nach welchen zu bestimmen ist, welcher an Dublin teilnehmende Staat für die Behandlung eines Asylgesuches zuständig ist. Die Zielsetzung besteht darin, dass jeder Asylgesuchsteller nur in einem Staat ein Asylgesuch stellen kann. Die Datenbank Eurodac, in der die Fingerabdrücke der Gesuchsteller registriert werden, dient der Überprüfung, ob ein Gesuchsteller bereits in einem andern an Dublin teilnehmenden Land ein Gesuch eingereicht hat. Ist dies der Fall, kann der Gesuchsteller an diesen Staat verwiesen werden.

Mit Bezug auf die dactylographische Erfassung von illegal in die Schweiz einreisenden oder sich illegal in der Schweiz aufhaltenden Personen ist vorgesehen, dass die zuständigen kantonalen Stellen diese vornehmen und die erfassten Daten an das zuständige Bundesamt weiterleiten. Für die Abnahme und Bearbeitung von Fingerabdrücken sind die Datenschutzvorschriften der Eurodac-Verordnung[1] sowie ganz allgemein das Datenschutzniveau der Datenschutzrichtlinie der EU einzuhalten.

Im Rahmen der Schengener Zusammenarbeit haben die teilnehmenden Staaten ihre Personenkontrollen an den Binnengrenzen aufgehoben und gleichzeitig zur Stärkung der inneren Sicherheit eine Reihe von Ausgleichsmassnahmen beschlossen. Dazu gehören insbesondere die Verstärkung der Kontrollen an den Aussengrenzen des Schengenraumes, eine gemeinsame Visumspolitik für Kurzaufenthalte, die Verbesserung der Zusammenarbeit im Bereich der Rechtshilfe in Strafsachen sowie die Intensivierung der grenzüberschreitenden Polizeizusammenarbeit. Zu den wichtigsten Instrumenten dieser Zusammenarbeit gehört das Schengener Informationssystem (SIS), eine europaweite Fahndungsdatenbank. Diese hat sich als effizientes Mittel im Kampf gegen grenzüberschreitendes Verbrechen bewährt. Der rasche computergesteuerte Informationsaustausch erhöht die Wirksamkeit von Kontrollen und entsprechend auch die Fahndungserfolge bei internationalen Ausschreibungen. Es liegt auf der Hand, dass bei diesem intensiven Datenaustausch flankierende datenschutzrechtliche Massnahmen getroffen werden müssen.

---

[1] Verordnung (EG) Nr. 2725/2000 des Rates vom 11. 12. 2000; ABl. L 316 vom 15. 12. 2000, S. 1 ff.

Aus innerstaatlicher Sicht ist festzuhalten, dass aufgrund unseres föderativen Systems die Kantone für die rechtskonforme Datenschutz-Kontrolle der Datenbearbeitungen durch kantonale Behörden besorgt sein müssen. Die kantonale Datenschutzaufsicht hat dabei den Anforderungen der EU-Richtlinien, insbesondere Art. 28 EU-Datenschutzrichtlinie[2], zu genügen. Danach haben die Kantone eine öffentliche Stelle zu bezeichnen, welche die Umsetzung und Anwendung der einzelstaatlichen Vorschriften zu überwachen hat. Diese Aufgabe ist in völliger Unabhängigkeit wahrzunehmen, und die Kontrollstelle muss über Untersuchungs- und Weisungsbefugnisse verfügen. Schliesslich stipuliert besagter Art. 28 ein Klagerecht oder eine Anzeigebefugnis zugunsten der Kontrollstelle.

Daraus resultiert Handlungsbedarf. Im Bereich der Unabhängigkeit wird die Wahl und Anstellung der Kontrollstelle tangiert. Das Wahlorgan, die administrative Zuordnung und der gewährte Ressourcenbedarf bilden weitere Aspekte. In Graubünden wählt die Regierung einen DSB. Die Wahl der Kontrollstelle durch den Grossen Rat wäre vor dem Hintergrund der demokratischen Legitimation vorteilhafter. Indessen ist eine Wahl durch das Parlament nicht zwingend erforderlich, zumal auf Bundesebene ebenfalls die Exekutive Wahlorgan ist. Die Anstellung des DSB über einen regulären Arbeitsvertrag entspricht den europäischen Vorgaben nicht. Ob das in Graubünden zur Anwendung gelangende Rechtsinstrument des Auftrages jedoch den strengen Vorgaben genügt, bleibt abzuwarten. Gut gelöst ist in unserem Kanton hingegen die administrative Zuordnung des DSB. Administrativ ist der Datenschutz in der Standeskanzlei angesiedelt, budgetmässig mit einem eigenen Konto. Faktisch steht und fällt der Datenschutz mit den der Datenschutzaufsicht gewährten personellen und finanziellen Ressourcen. Über das Budget befindet der Grosse Rat. Er ist berechtigt und verantwortlich für das Sprechen der erforderlichen Mittel. Dieses Recht kann der Legislative nicht durch gesetzliche Fesseln genommen werden. Vielmehr sind die Anliegen und der Nutzen des Datenschutzes permanent zu kommunizieren. Können die Parlamentarier dafür sensibilisiert werden, werden ebenfalls die erforderlichen Mittel für die Umsetzung der gesetzlichen Vor-

[2] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. 10. 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr; ABl. L 281 vom 23. 11. 1995, S. 31 ff.

gaben bereitgestellt. Zu berücksichtigen ist dabei, dass die Datenbearbeitungen mit Schengen / Dublin zunehmen, das Risiko der Verletzung der Grundrechte betroffener Personen wächst und sich europaweit auswirkt und die EU-Datenschutzrichtlinie ein zusätzliches Gewicht auf Kontrollen legt.

Polizeiliche Meldepflicht der Beherbergung

In Graubünden besteht eine gesetzliche Meldepflicht von Hotelgästen. In Art. 11 Gastwirtschaftsgesetz (BR 945.100) wird festgehalten, dass die Regierung diese Meldepflicht zu regeln hat. Die Ausführungsgesetzgebung zum Gastwirtschaftsgesetz bestimmt eingehend den Geltungsbereich, die Aufnahme der Daten sowie die Weiterleitung des Meldescheins. Die Beherberger sind gesetzlich verpflichtet, die amtlichen Meldescheine auszufüllen und an die örtlich zuständige Dienststelle der Kantonspolizei weiterzuleiten (vgl. Art. 2 ff. Ausführungsbestimmungen zum Gastwirtschaftsgesetz; BR 945.110). In Art. 26 der Strafprozessordnung (StPO; BR 350.000) wird festgelegt, dass mit Haft bis zu acht Tagen oder mit Busse bestraft wird, wer im amtlichen Meldeschein für die polizeiliche Kontrolle der Beherbergten unrichtige Angaben über seine Person oder seine Begleiter macht oder diese Angaben verweigert.

In Art. 6 KDSG wird der Rechtsschutz geregelt. Damit wird dem Postulat, wonach eine gerichtliche Überprüfung für die Betroffenen möglich sein soll, Rechnung getragen. Art. 28 Abs. 3 Einzug 3 EU-Datenschutzrichtlinie sieht darüber hinaus ein Klagerecht oder eine Anzeigebefugnis jeder Kontrollstelle vor. Dieses Anliegen wird durch Art. 6 KDSG nicht abgedeckt. Das schweizerische Rechtssystem kennt das Instrument der Anzeige lediglich im Strafverfahren. Dabei hat die anzeigende Person keine Parteistellung. Eine Gerichtsbehörde wird in der Regel nur im Rahmen eines streitigen Verfahrens tätig. Vor diesem Hintergrund erscheint die Umsetzung eines Anzeigerechtes wenig sinnvoll. Auf Bundesebene wird jedenfalls darauf verzichtet. Indessen statuiert die Teilrevision des eidgenössischen Datenschutzgesetzes in Art. 27 Abs. 6 DSG ausdrücklich ein Klagerecht des DSB. In Nachachtung der gesetzlichen Vorgaben ist der kantonalen Aufsichtsstelle ebenfalls ein Klagerecht einzuräumen. Ob noch weitere Bestimmungen des KDSG angepasst werden müssen, wird sich weisen.

Weitere Bemerkungen

Für den polizeilichen Bereich kommt die EU-Datenschutzrichtlinie nicht zur Anwendung. Das kantonale Recht muss jedoch in jedem Fall das Niveau des Europaübereinkommens STE Nr. 108[3] bzw. der Empfehlung

[3] Übereinkommen vom 28.01.1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SR 0.235.1).

Nr. R (87) 15 des Ministerkomitees des Europarates über den Gebrauch von Personendaten im Polizeisektor aufweisen. Erforderlich ist auch im polizeilichen Bereich, dass die Datenbearbeitung durch eine unabhängige Kontrollinstanz überwacht wird. Da grundsätzlich dieselben Anforderungen betreffend die Unabhängigkeit erfüllt werden müssen, wie sie für den DSB gelten, würde es aus organisatorischen Gründen wenig Sinn machen, eine zweite Datenschutzstelle für diesen Bereich zu schaffen. Formal ist jedoch im polizeilichen Bereich eine unabhängige Kontrollinstanz vorzusehen.

III. Ausgewählte Themen

1. Datensperre

Eine Datensperre können Bürgerinnen und Bürger jederzeit mittels schriftlicher Mitteilung an die zuständige Amtsstelle veranlassen. Gemäss Art. 20 Abs. 1 DSG muss ein schutzwürdiges Interesse glaubhaft gemacht werden. An diesen Interessennachweis dürfen keine hohen Anforderungen gestellt werden.[1] Dies bedeutet für die Verwaltung, dass sie das Sperrgesuch entgegennehmen muss und die notwendigen Massnahmen in die Wege zu leiten hat, damit keine Bekanntgabe dieser Daten an Drittpersonen erfolgt. Die Sperrung umfasst dabei sämtliche Daten, die über die gesuchstellende Person bei der jeweiligen Amtstelle vorhanden sind.[2]

Wichtig ist zu vermerken, dass diese Sperrung nur in Bezug auf die Bekanntgabe von Daten an private Personen oder Organisationen zum Tragen kommt. Sofern gesetzliche Mitteilungsrechte und -pflichten für die Bekanntgabe dieser Daten an andere Amtsstellen bestehen, sind diese von einer Datensperre nicht betroffen. In zwei Fällen ist eine Datenbekanntgabe an private Personen und Organisationen trotz Sperre zulässig:

– Das öffentliche Organ ist von Gesetzes wegen zur Weitergabe der Information verpflichtet.[3]

– Die um Datenbekanntgabe ersuchende Person macht glaubhaft, dass die Sperrung sie in der Verfolgung eigener Rechte gegenüber der betroffenen Person behindert.[4] Gemeint ist in diesem Zusammenhang, dass eine Beurteilung nach den gesamten Umständen zur Überzeugung führt, dass die Angaben des Gesuchstellers stimmen. Ein Schuldner soll sich beispielsweise nicht durch eine Datensperre seinen Gläubigern entziehen können. Sofern eine Person die notwendigen Dokumente vorlegt, welche das Bestehen einer Forderung glaubhaft machen, ist die Adresse dieses Schuldners durch die Einwohnerkontrolle trotz Datensperre bekannt zu geben. Die Datensperre wirkt somit nur in den Fällen, bei welchen für die Verwaltung keine gesetzliche Verpflichtung zur Datenbekanntgabe an Dritte besteht.

---

[1] Als Begründung für die Sperrung sollte in den meisten Fällen der Wunsch der Person auf Schutz ihrer Persönlichkeit genügen.

[2] Urs Maurer/Nedim Peter Vogt (Hrsg.), Kommentar zum Schweizerischen Datenschutzgesetz, Art. 20 N 1.

[3] Beispielsweise aufgrund gesetzlicher Bestimmungen, die eine Publikation und somit eine Bekanntgabe von Daten an Drittpersonen vorsehen.

[4] Fakten, die Zeitschrift für Datenschutz des Kantons Zürich, 2/1999, S. 11 f.

Damit ist die Frage des praktischen Vorgehens noch nicht beantwortet. Das Glaubhaftmachen von eigenen Rechten wie auch von einer Behinderung bei deren Durchsetzung macht nur die Berechtigung der um Datenbekanntgabe ersuchenden Seite wahrscheinlich. Die Position der Gegenseite wird noch mit keinem Wort gewürdigt. Folgerichtig ist die Amtsstelle zu einer Anhörung der Gegenseite verpflichtet. Hat die betroffene Person im konkreten Einzelfall nichts gegen die Bekanntgabe ihrer Daten einzuwenden, kann die gesuchstellende Person oder Organisation die Antwort ohne weiteres erhalten. Ist die betroffene Person mit der Durchbrechung der Sperre nicht einverstanden, muss sie ihre Gründe näher ausführen.[5] Dabei können ihre Einwände die unterschiedlichsten Bereiche beschlagen. Entweder wird bereits das Bestehen von Ansprüchen bestritten, sei es, dass solche gar nie rechtsgültig entstanden oder aber infolge Zeitablaufs oder Erfüllung nicht mehr vorhanden sind. Oder die betroffene Person kann auf ihre besonderen Lebensumstände hinweisen und beispielsweise geltend machen, sie sei zu ihrer persönlichen Sicherheit darauf angewiesen, ihren Wohnort möglichst geheim zu halten. Gründe können sodann gegenüber der konkret gesuchstellenden Person bestehen, wenn beispielsweise die Befürchtung geäussert wird, die Angaben sollten lediglich dazu dienen, um weiterhin Nachstellungen und Belästigungen zu ermöglichen. Selbstverständlich ist von der betroffenen Person kein Mehr an Beweiskraft für ihre Weigerung zu fordern als von der gesuchstellenden Person oder Organisation zum Nachweis des Rechtsanspruches und der Behinderung in der Rechtsverfolgung. Es genügt somit, dass eine gewisse Wahrscheinlichkeit für die Richtigkeit der Aussage spricht. Wird von der einen Seite eine Bekanntgabe gesperrter Daten gefordert und von der andern eine Durchbrechung der Sperre abgelehnt, liegt die Entscheidung bei der zuständigen Behörde. Sie hat die von beiden Seiten vorgebrachten Interessen zu gewichten und sorgfältig gegeneinander abzuwägen, wobei keinem der beteiligten Interessen der Vorrang zu geben ist.

Kommt die Behörde nach Abwägung aller Argumente zum Schluss, dass sich im konkreten Einzelfall eine Durchbrechung der Sperre nicht rechtfertigt, erlässt sie eine begründete Verfügung. Damit erhält die gesuchstellende Person oder Organisation die Möglichkeit, den Sachverhalt bei der nächsthöheren Instanz überprüfen zu lassen und allenfalls einen anders lautenden Entscheid zu erwirken. Das gleiche Prozedere gilt bei einem Beschluss, die Sperre im konkreten Einzelfall zu durchbrechen. Selbstver-

[5] Fakten, die Zeitschrift für Datenschutz des Kantons Zürich, 1/2000, S. 6.

ständlich dürfen bei einer derartigen Verfügung nicht direkt die Daten bekannt gegeben werden, ansonsten würde die betroffene Person nämlich der Möglichkeit beraubt, den Sachverhalt durch die nächsthöhere Instanz überprüfen zu lassen.

Der Amtsstelle kann der Entscheid nach Würdigung der gesamten Umstände nicht abgenommen werden.

2. Benutzerberechtigungs-Konzept im Spitalwesen

Der Zugriffsberechtigung auf Daten kommt in einer Spitalzentrale besondere Bedeutung zu. Diese Bedeutung akzentuiert sich, wenn die Patientendaten mittels eines elektronischen Systems (KIS) aufbereitet und archiviert werden. Die Unternehmung Safe & Legal AG hat zuhanden der Gesundheits- und Fürsorgedirektion des Kantons Bern umfassend und detailliert die Problematik der Benutzerberechtigung analysiert.[1]

Von der Notwendigkeit eines Benutzerberechtigungskonzeptes im Rahmen eines KIS darf ausgegangen werden. Vorab sind die gesetzlichen Geheimhaltungsvorschriften[2] zu berücksichtigen. Daneben gilt es auch die Bearbeitungsprinzipien des Datenschutzes, wie insbesondere der Grundsatz der Verhältnismässigkeit und das Zweckbindungsgebot, zu beachten. Daraus folgt, dass ein Zugriff nur auf solche Patientendaten möglich sein darf, die von den involvierten Mitarbeitenden für die medizinische Behandlung und / oder die administrative Betreuung des konkreten Falles benötigt werden. Dabei sind die folgenden Rahmenbedingungen zu beachten:

- Die Informations- und Kommunikationsprozesse in einem Spital sind sehr komplex.
- Eine grosse Zahl der Mitarbeitenden ist mit sehr unterschiedlichen Aufgaben und Informationsbedürfnissen involviert.
- In der Regel besteht eine vergleichsweise hohe interne und externe Fluktuation der Mitarbeitenden.
- Besonderheiten, wie Schichtdienst der Mitarbeitenden und die Gewährleistung eines funktionierenden Notfalldienstes, müssen berücksichtigt werden.

Allein schon aufgrund der strafrechtlichen Begründung wird von einem Patienteninformationssystem verlangt, dass Informationen selektiv nur jenen Benutzern zugänglich gemacht werden, die diese Informationen auch tatsächlich kennen dürfen. Aus dem Prinzip der Verhältnismässigkeit ergibt sich die Forderung, dass nur Personen auf Patientendaten zugreifen dürfen, welche die Information für die Erfüllung der ihnen überbundenen Aufgaben tatsächlich benötigen. Ein selektiver Zugriff auf die für die jeweilige Aufgabenerfüllung notwendigen Daten ist somit zwingend gegeben.

---

[1] Safe & Legal AG für Datenschutz und Managementconsulting, 3003 Bern; Datenschutz-Rahmenkonzept für den Datenschutz und die Datensicherheit in den Berner Spitälern und Kliniken.

[2] Art. 320 StGB (SR 311.0), Verletzung des Amtsgeheimnisses; Art. 321 StGB, Verletzung des Berufsgeheimnisses.

Welche Patientendaten für welche Funktionen mit welchen Bearbeitungsrechten von einer Anwendung zur Verfügung gestellt werden, ist anhand der betrieblichen Bedürfnisse festzulegen und auf ihre Datenschutzkonformität hin objektiv zu überprüfen, namentlich unter den vorgängig erwähnten Aspekten. Ob eine Anwendung der Datenschutzgesetzgebung entspricht, hängt entscheidend davon ab, wie konsequent diese Grundsätze bei der Konzeption, Inbetriebnahme und insbesondere während des Betriebes eines Informationssystems umgesetzt werden. Die datenschutzgerechte Ausgestaltung der Benutzerrechte ist in erster Linie Sache der Entscheidungsverantwortlichen. Welche Rollen es in einem Spital gibt und welche Funktionen wahrzunehmen sind, muss spezifisch festgelegt werden.[3] Einzelne Benutzerrollen können dabei unter Umständen mehrere Funktionen wahrnehmen, was aber nicht dazu führen darf, dass der Einfachheit halber Benutzerrollen definiert werden, die alle Patientendaten einsehen dürfen.

Ein gänzliches Öffnen der Patientendossiers z. B. für die gesamte Ärzteschaft oder das gesamte Betreuerteam ist datenschutzwidrig. Es ist zwingend ein selektives Verfahren zu wählen, das vorzugsweise nur einen Datenzugriff über eine zwischengeschaltete Verknüpfung zulässt. Die Ärzteschaft hat mithin entsprechend dem jeweiligen Wirkungskreis Einsicht in Krankengeschichten. Ganz andere Kriterien spielen bei den Bereichen Administration, Pflegepersonal und Hotellerie eine Rolle. Die Zuordnung zweckmässiger Zugriffsberechtigungen ist anspruchsvoll, aber gerechtfertigt.

[3] Z. B. Patientenadministration, ärztliche Behandlung, pflegerische Betreuung, Hotellerie.

3. Gemeindeversammlungsprotokoll im Internet

Das Internet, wie es sich heute darstellt, ist ein Geflecht aus vielen tausenden von Netzen und Millionen von Hosts. Diese an das Internet angeschlossenen Rechner sind in der Regel lokale Netze. Organisatorisch sind sie zumeist im regionalen Netzwerk verbunden. Das weltumspannende Internet bietet so ein homogenes Erscheinungsbild, obwohl es technisch auf einem heterogenen Konglomerat an Netzwerken aufgebaut ist. Im Internet können Informationen von jedermann angeboten und angesehen werden. Eine wichtige Konsequenz daraus ist die fehlende Kontrollierbarkeit. Noch problematischer ist jedoch die Tatsache, dass persönliche Daten sehr leicht sammelbar, speicherbar und sehr schnell und einfach verteilbar sind. Das Missbrauchspotential ist enorm gross. Das Internet ist eine fast unerschöpfliche, globale Informationsquelle und ein blitzschnelles Kommunikationsmedium. Das Internet hat somit eine ganz andere Dimension als die herkömmlichen Kommunikationsmittel. Folgerichtig ist dem Persönlichkeitsschutz bei Daten, welche in das Internet gestellt werden, erhöhte Aufmerksamkeit zu schenken.

Das Internet ist ein «Archiv für die Ewigkeit». Es gibt spezialisierte Suchmaschinen, welche Kopien von aktuellen Websites archivieren. Informationen bleiben so selbst dann allen zugänglich, wenn die entsprechenden Dateien im eigenen Web-Auftritt gelöscht sind. Was nicht der ganzen Menschheit für immer und ewig bekannt gegeben werden soll, ist deshalb nicht im Internet zu publizieren. So ist es zum Beispiel keinesfalls zwingend, dass ein lokales Publikationsorgan im Verhältnis 1:1 ins Internet gestellt wird. Was bereits in Papierform veröffentlicht wurde, darf nicht automatisch auch ins Internet gestellt werden. Ob etwas im Internet veröffentlicht werden kann, ist eine Frage, die selbst bei bereits erfolgter gedruckter Publikation eigenständig und unabhängig zu prüfen ist. Insbesondere stellt sich jeweils die Frage, ob Regelungen für die Internetpublikation vorliegen.

Im Internet dürfen keine Daten veröffentlicht werden, welche dem Amtsgeheimnis oder anderen gesetzlichen Geheimhaltungspflichten unterstehen. Personendaten dürfen zudem nur im Internet publiziert werden, wenn eine ausdrückliche Rechtsgrundlage, welche die Veröffentlichung im Internet erlaubt, besteht.

Protokolle der Gemeindeversammlung enthalten häufig Personendaten. Sofern nicht eine ausdrückliche gesetzliche Grundlage für eine Internetpublikation vorhanden ist oder eine ausdrückliche Einwilligung der betroffenen Person vorliegt, sind diese Dokumente nur anonymisiert im Internet

zu veröffentlichen. Eine Bestimmung auf kommunaler Ebene, wonach Einsicht in ein Gemeindeversammlungsprotokoll genommen werden darf oder dieses auf Verlangen vorgelesen werden muss, genügt nicht als gesetzliche Grundlage für das Aufschalten der vollständigen Protokolle auf der Homepage einer Gemeinde.

IV. Fälle aus der Praxis

1. Privater Telefonverkehr am Arbeitsplatz

Kann ein kantonaler Amtsleiter vom Amt für Informatik einen Detailauszug der gewählten Rufnummern ab dem geschäftlichen Mobiltelefon eines Mitarbeitenden verlangen?[1]

Ohne ausdrückliche Einschränkung oder Verbot privater Telefongespräche am Arbeitsplatz darf der Mitarbeitende davon ausgehen, dass das private Telefonieren im Rahmen des Verhältnismässigen zulässig ist und dass keine Überwachung vorgenommen wird. Die kantonale Verwaltung handhabt das private Telefonieren auf diese Weise. Dabei ist der Mitarbeitende verpflichtet, seine privaten Telefongespräche als solche zu deklarieren und auch zu bezahlen.

Vorliegend geht es um die Protokollierung der telefonischen Randdaten. Diese werden beim Amt für Informatik aufbewahrt. Eine Bekanntgabe der angewählten Nummern privater Gespräche ist grundsätzlich nicht gestattet. Es stellt sich indessen die Frage, ob eine Aufzeichnung zur Verhinderung der missbräuchlichen Verwendung des Telefons zu privaten Zwecken erfolgen darf. Darunter versteht man sowohl die Missachtung einer Einschränkung der privaten Nutzung des Telefons als auch die unverhältnismässige Beanspruchung einer an sich gestatteten Telefonnutzung zu privaten Zwecken. Schliesslich fällt die Nichtdeklaration von privaten Telefongesprächen ebenfalls darunter. Die Überwachung des privaten Telefonmissbrauches muss auf Anzeichen beruhen, die sich nicht auf eine präventive Kontrolle der Randdaten stützen. Verdachtsmomente bilden beispielsweise übermässig hohe Telefonkosten eines Mitarbeitenden im Vergleich zu Mitarbeitenden in ähnlicher Stellung, ein Leistungseinbruch oder die wiederholte Feststellung des Missbrauches vor Ort. Erhärten sich solche Verdachtsmomente, ist der betroffene Mitarbeitende darüber zu informieren unter Hinweis darauf, dass gelegentlich oder permanent in die Zukunft gerichtet Aufzeichnungen und Auswertungen der vollständigen Randdaten vorgenommen werden können. Eine Überprüfung ist somit immer in die Zukunft gerichtet. Eine Ausnahme bildet der besondere Fall der Telefonbenutzung zur Begehung einer Straftat, welcher vorliegend jedoch nicht interessiert.

[1] Vgl. Erläuterungen zur Telefonüberwachung am Arbeitsplatz, http:\\www.edsb.ch\d\themen\weitere\telefonueberwachung_d.pdf.

Das Amt für Informatik hat somit vom anfragenden Amtsleiter eine schriftliche Bestätigung zu verlangen, wonach der Mitarbeitende über die Kontrolle der Randdaten orientiert worden ist. Es ist sodann gemeinsam festzulegen, über welchen Zeitraum und in welchem Ausmass eine Überprüfung erfolgen soll. Eine in die Vergangenheit gerichtete Anfrage ist abschlägig zu beantworten.

2. Herausgabe der Adressen von Inhabern privater Fischereirechte

Es wird angefragt, ob Personendaten betreffend die privaten Fischereirechte an eine Vereinigung weitergegeben werden dürfen.

Gemäss Art. 19 DSG dürfen Personendaten in wenigen Einzelfällen an Dritte bekanntgegeben werden. Einfach gestaltet sich der Fall, wenn eine gesetzliche Grundlage besteht. Das kantonale Fischereigesetz (KFG[1]) sieht keine voraussetzungslose Weitergabe von Daten vor. Insbesondere die Art. 27 ff. KFG lassen keinen diesbezüglichen Schluss zu. Folgerichtig muss überprüft werden, ob eine der anderen in Art. 19 DSG genannten Voraussetzungen erfüllt ist. In Frage kommen höchstens die in Art. 19 lit. b und c DSG festgehaltenen Tatbestände. Eine Weitergabe ist demnach möglich, wenn die betroffene Person im Einzelfall in die Bekanntgabe eingewilligt hat oder die Einwilligung nach den Umständen vorausgesetzt werden darf oder wenn die betroffene Person ihre Daten allgemein zugänglich gemacht hat. Letzteres kann vorliegend ausgeschlossen werden, ansonsten müsste nicht nachgefragt werden. Ebenfalls liegt keine Einwilligung in die Bekanntgabe vor. Damit verbleibt einzig die Prüfung, ob allenfalls die Einwilligung zur Bekanntgabe nach den Umständen vorausgesetzt werden darf. Es mag durchaus sein, dass einzelne Inhaber von privaten Fischereirechten einer bestimmten Vereinigung positiv gegenüberstehen. Das Gegenteil kann aber auch zutreffen. Auf jeden Fall sind die Umstände nicht derart, dass eine Einwilligung vorausgesetzt werden darf. Mithin fehlt es an einer Voraussetzung für die Bekanntgabe von Personendaten.

Dem Anliegen des Anfragers könnte dennoch Rechnung getragen werden, indem das kantonale Amt, allenfalls gegen Erhebung eines Unkostenbeitrages, die Unterlagen des Anfragers dem Inhaber privater Fischereirechte zukommen lässt. Auf diese Weise könnte jeder Inhaber von privaten Fischereirechten selbst entscheiden, ob eine Kontaktnahme mit dem Anfrager angestrebt werden soll oder nicht.

[1] BR 760.100.

3. Einsicht in Krankengeschichte

Aus Sicht des Datenschutzes muss geklärt werden, ob die nächsten Angehörigen das Recht haben, Einsicht in die Krankengeschichte einer verstorbenen Person zu nehmen.

Gesundheitsdaten sind besonders schützenswerte Personendaten.[1] Die Bearbeitung dieser besonders schützenswerten Personendaten erfordert deshalb die nötige Sensibilität. Des Weiteren sind die Gesundheitsdaten durch die ärztliche Schweigepflicht respektive das Patientengeheimnis geschützt.[2] Nur die betroffene Person kann als Geheimnisherr die Medizinalperson bzw. die Institution von der Schweigepflicht entbinden. Mit ihrem Tod geht diese Möglichkeit unter, die Schweigepflicht bleibt jedoch bestehen. In Frage kommt dann nur noch deren Aufhebung durch das Sanitätsdepartement.[3] Das kantonale Sanitätsdepartement hat in jedem Fall eine Interessenabwägung vorzunehmen und zu entscheiden, ob die Interessen der nahen Verwandten an der Kenntnis der Gesundheitsdaten schwerer wiegen als das Interesse des Verstorbenen an der weiteren Geheimhaltung seiner Daten.

Vertrauensarzt

Gemäss Art. 51 kantonale Personalverordnung (PV; BR 170.400) kann das Personal- und Organisationsamt eine vertrauensärztliche Untersuchung anordnen. Eine solche Untersuchung muss zwingend Bezug zu der Arbeitstätigkeit bzw. Arbeitsunfähigkeit des Patienten haben. Der Vertrauensarzt kann Abklärungen tätigen, welche im Zusammenhang mit der Berufsausübung stehen. Dazu kann auch eine Befragung des Vorgesetzten gehören. Dabei ist das Prinzip der Verhältnismässigkeit zu beachten. Massgebend ist der Grund für die medizinische Untersuchung. Die entsprechenden Handlungen haben sich darauf zu beschränken.

Die Hinterbliebenen sind unter keinem Titel berechtigt, umfassend Einblick in Krankengeschichten zu nehmen. Andererseits benötigen sie allenfalls detaillierte Informationen, falls sie den Verdacht hegen, die behandelnden Ärzte seien für den Tod ihres Verwandten verantwortlich. Mit Bezug darauf hat das Obergericht des Kantons Schaffhausen entschieden, die hinterbliebenen Personen müssten einen Arzt ihres Vertrauens mit der Einsicht in die vollständige Krankengeschichte betrauen. Dieser Vertrauensarzt dürfe allerdings die Hinterbliebenen oder deren Rechtsvertreter nur insofern über den Inhalt der Krankengeschichte informieren, als daraus Schlüsse für eine allfällige Fehlbehandlung gezogen werden können.[4] Das

---

[1] Vgl. Art. 3 lit. c DSG.

[2] Gestützt auf Art. 20 Gesundheitsgesetz des Kantons Graubünden (BR 500.000) ist das Recht auf Schutz der Persönlichkeit der Patienten gewährleistet.

[3] Vgl. Art. 48 Abs. 2 Gesundheitsgesetz.

[4] ZBl 91, Seite 364 ff.

Bundesgericht hat zu einem späteren Zeitpunkt Bezug auf dieses Urteil genommen und die Lösung als gerechtfertigt erklärt.

Zusammenfassend kann festgehalten werden, dass die nahen Verwandten einer verstorbenen Person keinen selbstständigen Anspruch auf Einsicht oder gar Herausgabe der Krankengeschichte haben. Die Einsichtnahme in die vollständige Krankengeschichte einer verstorbenen Person kann lediglich über einen Arzt des Vertrauens erfolgen.

4. Einsicht in Unterlagen einer Supervision

Ein Arbeitnehmer möchte wissen, ob er das Recht hat, Einsicht in einen Bericht zu nehmen, welcher im Rahmen einer Supervision erstellt worden ist.

Bei der Beurteilung dieser Frage wird davon ausgegangen, dass der Arbeitgeber eine entsprechende Institution beauftragt hat, eine Supervision durchzuführen. Zwischen dieser Unternehmung und der Arbeitnehmerin oder dem Arbeitnehmer ist es zu keiner vertraglichen Bindung gekommen. Die Auskünfte, welche Arbeitnehmer oder Arbeitnehmerin im Rahmen der Supervision erteilten, gründen auf dem Arbeitsvertrag mit dem Arbeitgeber.

REHA-Management

Im Zusammenhang mit der Tätigkeit von REHA-Managern kommen regelmässig heikle Punkte zur Sprache (Aussagen über Krankheit, Arbeitsklima, Arbeitskollegen usw.). Diese Aussagen dürfen vom REHA-Manager nicht an den Vorgesetzten des Patienten weitergeleitet werden. Die Informationen, welche den REHA-Managern gegeben werden, haben teilweise besonders schützenswerten Charakter. Solche Daten dürfen nur bearbeitet werden, wenn ein formelles Gesetz es ausdrücklich vorsieht. Die gesetzliche Grundlage in Art. 51 PV genügt nicht. Ein Ausnahmetatbestand nach Art. 19 DSG liegt nicht vor.

In Art. 8 DSG wird das Akteneinsichtsrecht ausdrücklich statuiert. Danach kann jede Person vom Inhaber einer Datensammlung Auskunft darüber verlangen, ob Daten über sie bearbeitet werden. Der Inhaber der Datensammlung muss der Person alle über sie in der Datensammlung vorhandenen Daten mitteilen. Dies ist auch dann der Fall, wenn die Personendaten durch einen Dritten bearbeitet[1] werden. Der Inhaber der Datensammlung bleibt auskunftspflichtig. Das in Art. 8 DSG statuierte Auskunftsrecht ist indessen nicht schrankenlos. In Art. 9 und 10 DSG werden die entsprechenden Ausnahmen normiert. Sie zielen darauf ab, im jeweiligen Einzelfall eine Güterabwägung zwischen Auskunftsbedürfnis und allenfalls bestehenden konträren Geheimhaltungsinteressen zu ermöglichen. Der Auskunftsanspruch in Art. 8 DSG ist die Regel; die Einschränkungen in Art. 9 f. DSG stellen demnach die Ausnahmen dazu dar. Daraus folgt, dass die Einschränkungen nicht als Generalermächtigung zur Geheimhaltung verstanden werden dürfen. Sie greifen nur dort und nur insoweit, als das Geheimhaltungsinteresse dasjenige an der Auskunft tatsächlich überwiegt. In Art. 9 Abs. 3 DSG wird dies wie folgt formuliert:

[1] Bearbeiten im Sinne des DSG bedeutet jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten (Art. 3 lit. e DSG).

> «Private als Inhaber einer Datensammlung können zudem die Auskunft verweigern, einschränken oder aufschieben, soweit eigene überwiegende Interessen es erfordern und sie die Personendaten nicht an Dritte bekanntgeben.»

Für die entsprechende Güterabwägung hat das Bundesgericht in seiner Rechtsprechung zum verfassungsmässigen Akteneinsichtsrecht den Grundsatz entwickelt, wonach legitime Geheimhaltungsinteressen Privater zu berücksichtigen sind, indem die einander entgegenstehenden Interessen an der Akteneinsicht auf der einen Seite und an deren Verweigerung auf der andern Seite im Einzelfall sorgfältig gegeneinander abzuwägen sind. Allein schon aus dieser Formulierung ist der grosse Ermessensspielraum des Inhabers der Datensammlung ersichtlich und damit die Schwierigkeit, eine präzise Antwort zu geben.

Klar ist auf jeden Fall, dass der Arbeitgeber das Einsichtsrecht insoweit einschränken kann – sofern er denn verpflichtet ist, überhaupt Einsicht zu gewähren –, als lediglich diejenigen Auszüge bekannt gegeben werden, welche einen direkten Bezug zur Einsicht verlangenden Person haben. Ein umfassendes Einsichtsrecht in die Unterlagen der Supervision besteht auf jeden Fall nicht.

5. Inkassoprobleme

Im Spital X sind vermehrt Inkassoprobleme feststellbar. Im Nachhinein stellt sich vielfach heraus, dass die betreffenden Patienten Sozialhilfeempfänger sind und die Abwicklung der Zahlung somit direkt über die Gemeinde hätte erfolgen können. Es stellt sich nun die Frage, ob die Rechnung in Zukunft nicht direkt der Gemeinde zugestellt werden kann.

Einsichtsrecht des Beistandes

Gestützt auf Art. 367 Abs. 3 ZGB gelten für den Beistand, soweit keine besonderen Vorschriften aufgestellt sind, die Bestimmungen über den Vormund. Mit Beendigung des Amtes gehen auch die in diesem Zusammenhang allfällig bestehenden Rechte unter. Gestützt auf Art. 439 ZGB hört die Vertretung durch den Beistand auf mit der Erledigung der Angelegenheit, für die er bestellt worden ist. Im Gesetz werden jedoch nicht alle Beendigungsgründe genannt. Eine Beistandschaft endet nach herrschender Lehre auch mit dem Tod der betroffenen Person. An diesem Umstand ändert die Tatsache nichts, dass die Rechtssicherheit gebietet, die Beistandschaft und damit die gesetzliche Vertretungsmacht durch einen behördlichen Entscheid zu beenden. Spätestens mit dem Tod erlöscht folgerichtig das Einsichtsrecht des Beistandes.

Es sind zwei Fälle denkbar:

a) Der Patient gibt bekannt, dass er Sozialhilfe bezieht.

b) Der Patient gibt nicht bekannt, dass er Sozialhilfe bezieht.

Zum Fall a)

Sofern der Patient darauf aufmerksam macht – oder auf entsprechende Frage bekannt gibt –, dass er Sozialhilfe bezieht, kann die Rechnung direkt der zuständigen Gemeinde zugestellt werden. Mit der Bekanntgabe des Bezuges von Sozialhilfe kann eine Zustimmung zur direkten Abwicklung der Spitalkosten über die Gemeinde angenommen werden. Art. 19 Abs. 1 lit. b DSG sieht diesen Sachverhalt ausdrücklich vor.

Zum Fall b)

Schwieriger gestaltet sich die Abwicklung der Kostenübernahme direkt mit der Gemeinde, wenn der Patient selbst nicht bekannt gibt, dass er Sozialhilfe empfängt. Ein Rechtfertigungsgrund für die Bekanntgabe von Personendaten gemäss Art. 19 DSG liegt für das Spital nicht vor. Es besteht auch keine gesetzliche Voraussetzung, wonach die Bezahlung und Rückforderung der Kosten direkt über die Gemeinde erfolgen kann. Es bleibt somit lediglich die Möglichkeit, im Nachhinein beim Patienten eine Zustimmung einzuholen.

6. Akteneinsicht in einem Kirchenprozess

Mit Bezug auf die Zuständigkeit ist auf den Unterschied zwischen der katholischen Landeskirche und der katholischen Kirche hinzuweisen. Letztere kann eigene Vorschriften erlassen, die nicht dem kantonalen Datenschutzrecht unterstellt sind. Die daraus resultierenden Zuständigkeiten können offen gelassen werden. Tatsache ist, dass die für das Verfahren gültige Prozessordnung (PO) die Akteneinsicht in den Art. 229 ff. PO eingehend regelt. Es stellt sich mithin die Frage, ob die genannten Bestimmungen vor den datenschutzrechtlichen Vorgaben standhalten mögen.

Gemäss Art. 229 § 3 PO wird den Parteien ein umfassendes Akteneinsichtsrecht gewährt, wobei dieses in Fällen sehr schwerer Gefahr, gestützt auf Art. 230 PO, partiell verweigert werden kann. Die Herausgabe der Akten an die Anwälte wird in Art. 235 PO geregelt. Indessen ist nicht vorgesehen, die Akten an die Parteien zu übergeben. Einzig darin könnte ein Verstoss gegen die Datenschutzgesetzgebung erblickt werden. Gemäss Art. 8 Abs. 5 DSG hat die Auskunft in der Regel schriftlich in Form eines Ausdruckes oder einer Fotokopie sowie kostenlos zu erfolgen. Der Gesetzgeber hat sich relativ eindeutig geäussert. Gemäss Art. 9 Abs. 3 DSG können Private die Auskunft verweigern, einschränken oder aufschieben, soweit eigene überwiegende Interessen es erfordern und sie die Personendaten nicht an Dritte bekannt geben. Hinzuweisen ist ebenfalls auf Art. 9 Abs. 1 lit. b DSG betreffend Auskunftsverweigerung wegen überwiegender Interessen Dritter.

Vorliegend ist erstellt, dass die Akten nur den Beteiligten und dem Gericht zugänglich gemacht werden, mithin nicht für Dritte. Insofern könnte Art. 9 Abs. 3 DSG zur Anwendung kommen. Wenn nun aber eine Einschränkung des Einsichtsrechtes denkbar ist, muss zweifelsohne auch die Verweigerung der Erstellung einer Kopie von Aktenstücken möglich sein. Nicht unberücksichtigt darf Art. 9 Abs. 1 lit. b DSG bleiben. Das Akteneinsichtsrecht findet seine Grenze in den berechtigten Interessen Dritter auf Persönlichkeitsschutz. Es ist durchaus vorstellbar, dass von den Parteien und den Zeugen äusserst intime Meinungsäusserungen abverlangt werden. Vor diesem Hintergrund rechtfertigt es sich, von der Herausgabe von Aktenstücken in Kopieform Abstand zu nehmen, wenn das Interesse der Auskunft erteilenden Person auf Diskretion höher gewichtet wird als das Recht, Kopien von Aussagen zu verlangen.

Zusammenfassend kann festgestellt werden, dass das Akteneinsichtsrecht gewährt wird und die Verweigerung der Ausfertigung von Kopien aus Gründen des Persönlichkeitsschutzes Dritter in der Datenschutzgesetzgebung eine Stütze findet.

V. Verbände/Weiterbildung

DSB + CPD.CH vereinigt alle kantonalen DSB. Angeschlossen ist auch der Vertreter des Fürstentums Liechtenstein. Im Jahre 2005 gab der eidgenössische Datenschutzbeauftragte (EDSB) seinen Austritt aus dem Verband bekannt. Er wollte ein Vetorecht des EDSB in die Statuten aufgenommen haben. Dies wurde ihm verweigert. In speziellen Sachthemen wird weiterhin zusammengearbeitet.

Im Rahmen der Lehrlingsausbildung wird dem Bereich Datenschutz ein gebührender Platz eingeräumt. Der DSB kann den Auszubildenden an vier Nachmittagen die Belange des Datenschutzes näher bringen.

Eine Weiterbildungsveranstaltung für Mitarbeitende der kantonalen Verwaltung war dem Datenschutz gewidmet. Die gut besuchte Veranstaltung zeigte auf, dass der Datenschutz in der täglichen Arbeit einen hohen Stellenwert einnimmt.

VI. Statistik Anfragen DSB 2005

Wer \ Was	Kurzanfragen	Berichte	Empfehlungen	Kontrollen	Vernehmlassungen	Referate	Kurse	Weiterbildung/Verbände
Kantonale Dienste								
Allgemeine Verwaltung							1	
DIV			1		1			
JPSD	10		1		4			
EKUD	3		1					
FMD	5							
BVFD								
öff. rechtliche Anstalten	3		1					
Gerichte								
Kreise	1		1					
Gemeindeverbände								
Gemeinden	21		1					
Bürgergemeinden								
Juristische Personen								
Private Personen	55	1	7					
Andere	1	1				2	3	6
Total	99	2	13		5	2	4	6

VII. Abkürzungsverzeichnis

ABl.	Amtsblatt der Europäischen Union (bis 2002 der Europäischen Gemeinschaften)
Abs.	Absatz
Art.	Artikel
BR	Bündner Rechtsbuch
BVFD	Bau-, Verkehrs- und Forstdepartement
bzw.	beziehungsweise
DIV	Departement des Innern und der Volkswirtschaft
DSB	Datenschutzbeauftragter
DSB + CPD.CH	Vereinigung der schweizerischen Datenschutzbeauftragten
DSG	eidgenössisches Datenschutzgesetz
EDSB	eidgenössischer Datenschutzbeauftragter
EG	Europäische Gemeinschaft
eidg.	eidgenössisch
EKUD	Erziehungs-, Kultur- und Umweltschutzdepartement
EU	Europäische Union
f. / ff.	folgend / folgende
FMD	Finanz- und Militärdepartement
Hrsg.	Herausgeber
JPSD	Justiz-, Polizei- und Sanitätsdepartement
KDSG	kantonales Datenschutzgesetz
KIS	Klinikinformationssystem
lit.	litera
N	Note
PO	kirchliche Prozessordnung
PV	kantonale Personalverordnung
Reha	Rehabilitation
S.	Seite
SIS	Schengener Informationssystem
SR	Sammlung der eidgenössischen Gesetze und systematische Sammlung des Bundesrechts (Systematische Rechtssammlung)
STE	Série des traités européens
StGB	Strafgesetzbuch
StPO	Gesetz über die Strafrechtspflege
usw.	und so weiter
vgl.	vergleiche

z.B.	zum Beispiel
ZBl	Schweizerisches Zentralblatt für Staats- und Verwaltungsrecht
ZGB	Zivilgesetzbuch

Impressum

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