Tätigkeitsbericht 2002

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

Datenschutz: Fluch oder Chance?

Seit dem 1. Mai 2002 ist das kantonale Datenschutzgesetz in Kraft. Die Behörden des Kantons, der Bezirke, Kreise, Gemeinden sowie der Gemeindeverbindungen unterstehen diesen Regelungen. Manch ein Behördenvertreter wird sich fragen, ob schon wieder neue mit Aufgaben verbundene Gesetzesbestimmungen erforderlich sind. Ist dies tatsächlich so? Der Datenschutz leitet sich aus Art. 13 Abs. 2 BV ab, wonach jede Person Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten hat. Entsprechend mussten sich die staatlichen Organe schon bis anhin mit Datenschutz befassen. Ihren Niederschlag fand diese Pflicht in mannigfaltigen, unterschiedlich ausgestalteten kommunalen, regionalen und kantonalen Datenschutzreglementen. Mit Einführung der für den ganzen Kanton gültigen Lösung ist nicht nur eine einheitliche Gesetzesgrundlage geschaffen worden. Das Institut der Aufsichtsstelle führt auch zu einer einheitlichen Gesetzesanwendung. Probleme datenschutzrechtlicher Natur können dem Datenschutzbeauftragten unterbreitet werden. Er ist vorwiegend beratend und kontrollierend tätig, ohne dass der Entscheidungsspielraum der Verwaltung eingeschränkt wird.

Vor dem Hintergrund des Persönlichkeitsschutzes und der zunehmenden Tendenzen, das Öffentlichkeitsprinzip der Verwaltung einzuführen, nimmt das Gemeinwesen die Verantwortung in einem für Bürgerinnen und Bürger sensiblen Bereich wahr. Wenn betroffene Personen vereinfacht ihre Rechte geltend machen können, profitiert letztendlich auch der Staat. Offene und transparente Information und Kommunikation schaffen Vertrauen und verbessern allein schon dadurch die zu erbringende Dienstleistung. Pointiert ausgedrückt resultiert aus dem Datenschutz ein Kundennutzen. Nutzen wir deshalb die Chance.

Justiz-, Polizei- und Sanitätsdepartement
Graubünden

Der Vorsteher:

Martin Schmid
Regierungsrat

Der Datenschutzbeauftragte erstattet jährlich Bericht über seine Tätigkeit. Dieser wird veröffentlicht[1]. Der vorliegende Bericht deckt den Zeitraum zwischen 1. Mai 2002 und 31. Dezember 2002 ab. Er richtet sich an zwei Zielgruppen, nämlich an die Bürgerinnen und Bürger sowie die Mitarbeitenden der öffentlichen Verwaltungen.

Das eidgenössische Datenschutzgesetz (DSG) schreibt den Kantonen vor, ein Kontrollorgan für den Datenschutz einzurichten[2]. Diese Bestimmung ist seit dem 1. Januar 1993 in Kraft. Sie ist zwingend. Graubünden tat sich in der Umsetzung der gesetzgeberischen Vorgabe schwer. Im Herbst 1997 führte das JPSD ein Vernehmlassungsverfahren durch. Die daraufhin geäusserte Kritik veranlasste die Regierung, den Gesetzesentwurf einer umfassenden Überarbeitung zu unterziehen. Das Parlament behandelte in der Novembersession 2000 die entsprechende Botschaft[3] und verabschiedete das Datenschutzgesetz mit 81:0 Stimmen zuhanden der Volksabstimmung[4].

Das am 1. Mai 2002 in Kraft getretene kantonale Datenschutzgesetz (KDSG)[5] löst die Datenschutzrichtlinien für die kantonale Verwaltung, von der Regierung am 21. November 1988 erlassen, ab. Mit dem KDSG hat der Kanton Graubünden eine Rahmengesetzgebung geschaffen, die sich stark an das DSG[6] anlehnt, indem die sinngemässe Anwendung des DSG ausdrücklich festgelegt wird[7]. Der Vorteil dieser Konzeption liegt darin, dass auf eine reichhaltige Entscheidsammlung und eine gefestigte Praxis[8] abgestellt werden kann. Definitionen können ohne weiteres übernommen und auf Wiederholungen kann verzichtet werden. Demgegenüber fehlen ausgesprochen kantonsspezifische Regelungen, wie z.B. Bestimmungen über die Einwohnerkontrolle. Insgesamt überzeugt die schlanke Gesetzgebung.

---

[1] Art. 8 lit. g KDSG
[2] Art. 37 Abs. 2 DSG: Die Kantone bestimmen ein Kontrollorgan, welches für die Einhaltung des Datenschutzes sorgt.
[3] Botschaft Nr. 5/2000, Seite 493 ff.
[4] AGRP 2000, Seite 537.
[5] BR 171.100
[6] SR 235.1
[7] Art. 2 Abs. 2 KDSG
[8] Entscheide der Eidgenössischen Datenschutzkommission; Jahresbericht EDSB.

Die Bestimmungen des KDSG gelten auch für die Gemeinden, Gemeindeverbindungen und Kreise. Gleiches gilt für den Datenschutzbeauftragten. Ursprünglich war vorgesehen, den Gemeinden einen gesetzgeberischen Spielraum zu belassen, indem diese eigene Bestimmungen hätten erlassen können und die Aufsicht gemeindeweise geregelt worden wäre. Im Sinne einer Vereinfachung und zur Sicherung des Fachwissens wurde die in der Botschaft enthaltene Bestimmung gestrichen.[9] Das KDSG gilt somit für alle Verwaltungsebenen.

Kantonaler Datenschutzbeauftragter:

Thomas Casanova

[9] GRP 2000, Seite 434 f.

II. Einführung

Grundsätze des Datenschutzes

Allgemeines

Ausgangspunkt der Betrachtungen bildet die Bundesverfassung. Hinter der entsprechenden Norm[1] steht der Gedanke, dass grundsätzlich jeder selber bestimmen soll, wem und wann er oder sie persönliche Lebenssachverhalte, Gedanken, Empfindungen oder Emotionen offenbaren will[2]. Der verfassungsrechtliche Schutz betrifft dabei jedes staatliche Erheben, Sammeln, Verarbeiten, Aufbewahren oder Weitergeben von Daten, die einen Bezug zur Privatsphäre einer Person haben. Eine Einschränkung dieses Schutzes ist gemäss geltender Lehre und Rechtsprechung nur unter den allgemeinen Voraussetzungen von Grundrechtseinschränkungen zulässig, nämlich wenn eine gesetzliche Grundlage dies ausdrücklich vorsieht, wenn ein überwiegendes öffentliches Interesse besteht und wenn der Grundsatz der Verhältnismässigkeit gewahrt ist[3].

Definitionen[1]

Personendaten: Alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen.

Persönlichkeitsprofil: Eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt.

Bearbeiten: Jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten.

Bekanntgeben: Das Zugänglichmachen von Personendaten wie das Einsichtgewähren, Weitergeben oder Veröffentlichen.

Datensammlung: Jeder Bestand von Personendaten, der so aufgebaut ist, dass die Daten nach betroffenen Personen erschliessbar sind.

[1] Art. 3 DSG

Der Gedanke des Datenschutzes wird auf eidgenössischer Ebene im eidgenössischen Datenschutzgesetz und auf kantonaler Ebene im kantonalen Datenschutzgesetz konkretisiert. Während sich das eidgenössische Datenschutzgesetz in erster Linie auf die Bundesorgane und Private bezieht, regelt das kantonale Datenschutzgesetz den Umgang der Behörden und Amtsstellen mit Personendaten von Kanton bis Gemeinde[4].

Mit Bezug auf den Datenschutz ist wichtig zu wissen, was alles unter den Begriff «Daten» fällt. Mit dem Datenschutzgesetz werden sämtliche Angaben, die sich auf eine Person beziehen, vor widerrechtlichem Bearbeiten ge-

[1] Art. 13 Abs. 2 BV
[2] Jörg Paul Müller, Grundrechte in der Schweiz, 3. Auflage, Seite 45.
[3] Als Verweigerungsgrund der Datenbekanntgabe wird in Art. 19 Abs. 4 DSG darüber hinaus ausdrücklich ein offensichtlich schutzwürdiges Interesse einer betroffenen Person genannt.
[4] Art. 1 Abs. 1 + 2 KDSG

schützt[5]. Das Medium, auf welchem die Daten aufgezeichnet werden, ist unbedeutend. Es gibt keine freien Daten, die nach Datenschutzgesetz voraussetzungslos bearbeitet werden dürfen[6].

Je nach Zusammenhang kann eine ganz normale Angabe wie Name, Vorname, Wohnort, Geburtsdatum eine besondere Empfindlichkeit in Bezug auf die betreffende Person haben. Besonders schützenswerte Personendaten wie religiöse, weltanschauliche und politische Ansichten, Daten über den geistigen und körperlichen Gesundheitszustand, Massnahmen der sozialen, vormundschaftlichen, fürsorgerischen Hilfe sowie Strafverfolgung und Verurteilung sind besonders strengen Massstäben des Schutzes unterstellt[7].

Bei der Bearbeitung von Daten müssen die allgemein gültigen verwaltungsrechtlichen Grundsätze[8] beachtet werden. Gegen den ausdrücklichen Willen der betroffenen Personen dürfen Daten nur erhoben werden, wenn eine entsprechende Rechtsgrundlage besteht. Der Datenschutz geht aber nie so weit, dass eine von Gesetzes wegen vorgegebene Aufgabe nicht mehr erfüllt werden kann. Bürger und Bürgerinnen sind jedoch immer über die Aufnahme von Daten zu informieren. Die Akteneinträge und Berichte sind so kurz wie möglich und so ausführlich wie nötig abzufassen. Dabei dürfen nur diejenigen Personendaten bearbeitet werden, welche zur Erfüllung des Auftrages notwendig sind. Dem Umstand der raschen Veränderung von Situationen ist Rechnung zu tragen. Es empfiehlt sich daher, Berichte, Gutachten etc. mit dem Hinweis auf ihre Vertraulichkeit und zeitlich beschränkte Gültigkeit zu versehen. Die Daten müssen richtig sein, und sie sind zu datieren. Jede Person hat Anspruch auf Berichtigung von falschen Daten. Bei der Bearbeitung von Daten ist eine grösstmögliche Transparenz anzustreben.

Grundsätzlich besitzen die betroffenen Personen das uneingeschränkte Recht auf Auskunft betreffend die über sie geführten Akten. Sie können dieses Recht jederzeit geltend machen. Die Auskunft kann nur verweigert, eingeschränkt oder mit Auflagen verbunden werden, wenn

- eine gesetzliche Bestimmung dies verlangt oder ermöglicht, oder
- wesentliche öffentliche Interessen gegenüberstehen (z.B. Interessen einer noch nicht abgeschlossenen Untersuchung), oder
- überwiegend schützenswerte Interessen einer Drittperson dies verlangen[9].

[5] Art. 1 Abs. 1 KDSG
[6] Urs Maurer, Nedim Peter Vogt (Hrsg.), Kommentar zum Schweizerischen Datenschutzgesetz, Art. 2 N 4.
[7] Art. 3 lit. c DSG, Art. 17 Abs. 2 DSG
[8] Art. 4 KDSG
[9] Art. 19 Abs. 4 DSG

Jede urteilsfähige Person kann Auskunft verlangen, d.h. auch Kinder und Jugendliche nach ihrem Grad der Urteilsfähigkeit. Das Recht auf Auskunft bezieht sich nur auf Daten der eigenen Person. Daten über Drittpersonen unterliegen nicht der uneingeschränkten Auskunftspflicht, sondern die Auskunft richtet sich nach den Grundsätzen bei Auskunft an Drittpersonen. Befinden sich in den Akten Gutachten und Berichte, welche durch andere Personen erstellt wurden, so ist auch diesbezüglich Auskunft zu erteilen. Eine Berufung auf die gesetzliche Schweigepflicht ist nicht möglich.

Die Auskunft ist in der Regel schriftlich zu erteilen. Die betroffene Person kann kostenlos eine Kopie bzw. einen Auszug verlangen. Wird die Auskunft aus Gründen der Interessenabwägung aufgeschoben, eingeschränkt oder verweigert, ist dies in den Akten zu vermerken und der betroffenen Person schriftlich mitzuteilen.

Auskünfte an Drittpersonen dürfen nur bekannt gegeben werden, wenn

- eine gesetzliche Grundlage besteht, oder
- ein überwiegendes öffentliches oder privates Interesse an der Bekanntgabe besteht[10], oder
- die betroffene Person in die Bekanntgabe ausdrücklich oder stillschweigend einwilligt.

Benötigt eine öffentliche Stelle zur Erfüllung ihres eigenen gesetzlichen Auftrages Informationen, welche sie nur mit unverhältnismässigem Aufwand selber beschaffen könnte, so kann diese Stelle bei anderen öffentlichen oder privaten Stellen um Amtshilfe nachsuchen. Daten können bekannt gegeben werden, wenn

- ein Gesuch der öffentlichen Stelle vorliegt,
- die Daten zur Erfüllung einer öffentlichen Aufgabe dienen,
- nicht eine andere verhältnismässige Beschaffung möglich ist,
- der ursprüngliche Zweck der Datenbeschaffung nicht verletzt wird[11].

Sollte die angefragte Person unter dem Amtsgeheimnis stehen, braucht sie in diesem Fall keine formelle behördliche Entbindung von der Schweigepflicht.

---

[10] Art. 19 Abs. 1 lit. d DSG: … der Empfänger glaubhaft macht, dass die betroffene Person die Einwilligung verweigert oder die Bekanntgabe sperrt, um ihm die Durchsetzung von Rechtsansprüchen oder die Wahrnehmung anderer schutzwürdiger Interessen zu verwehren; der betroffenen Person ist vorher wenn möglich Gelegenheit zur Stellungnahme zu geben.

[11] Urs Maurer, Nedim Peter Vogt (Hrsg.), Kommentar zum Schweizerischen Datenschutzgesetz, Art. 19 N 6.

Daten dürfen nicht in unbefugte Hände geraten und sind deshalb von den bearbeitenden Stellen mit organisatorischen und technischen Massnahmen zu schützen. Diese müssen angemessen sein und dem Stand der Technik entsprechen. Die Anforderungen an die Datensicherheit sind bei sensibler Datenbearbeitung entsprechend höher.

Die Bearbeitung von Daten mittels EDV verlangt heute von der Verwaltung zusätzliche Massnahmen im Bereiche der Datensicherheit. Nicht nur die Verfügbarkeit, sondern auch die Vertraulichkeit und die Integrität der Daten müssen sichergestellt sein. Wenn elektronische Daten über Netzwerke ausgetauscht werden, sind deshalb Massnahmen zur Überprüfung der Echtheit zu treffen.

Konkret umgesetzt auf die alltägliche Tätigkeit heisst dies:

- bei Abwesenheit sind die Büros zu schliessen,
- besonders schützenswerte Personendaten, z.B. Falldossiers, sind nur verschlossen aufzubewahren,
- für die Benutzung von EDV-Anwendungen sind Passwörter und Zugriffsberechtigungslisten unumgänglich,
- sensible Personendaten dürfen nur verschlüsselt über unsichere Netze (Internet) übertragen werden.

Die Aufgaben des Datenschutzbeauftragten

Grundlage für die Tätigkeit des Datenschutzbeauftragten bildet Art. 8 KDSG. Danach übt der Datenschutzbeauftragte stichwortartig zusammengefasst folgende Funktionen aus:

- Überwachung
- Registrierung
- Beratung
- Vermittlung
- Berichterstattung.

Der Datenschutzbeauftragte ist befugt, ungeachtet allfälliger Geheimhaltungsvorschriften bei Behörden Auskünfte über das Bearbeiten von Personendaten einzuholen, Einsicht in Datensammlungen und ihre Unterlagen zu nehmen und sich das Bearbeiten von Personendaten vorführen zu lassen[12].

[12] Art. 9 Abs. 2 KDSG

Dennoch versteht sich der Datenschutzbeauftragte als Dienststelle, die allen Beteiligten, ob Private oder Amtsstelle, zur Verfügung steht. Das Ziel des Datenschutzbeauftragten besteht darin, den Schutz der Persönlichkeit sicherzustellen, ohne eine öffentliche Aufgabe zu verunmöglichen. Es liegt auf der Hand, dass diese beiden Zielvorgaben zuweilen zu Interessenkollisionen führen können. Die Interessenabwägung erfolgt indessen nicht im gesetzesfreien Raum, sondern vielmehr in Beachtung der vorgegebenen Grundsätze[13] und der bestehenden reichhaltigen Literatur und Judikatur. Bisweilen lassen sich Konflikte nicht vermeiden, zumal Datenschutz eine Querschnittsmaterie ist, die sich mit allen Bereichen staatlichen Handelns auseinanderzusetzen hat, in denen Personendaten bearbeitet werden. Die Komplexität wird durch die rechtlichen und technischen Entwicklungen noch verstärkt.

Grundsatz der Gesetzmässigkeit:
Jede Datenbearbeitung muss auf einer gesetzlichen Grundlage beruhen.

Grundsatz der Verhältnismässigkeit:
Datenbearbeitung darf den Umfang des Notwendigen und des Geeigneten nicht übersteigen.

Grundsatz der Zweckgebundenheit:
Die Verwendung der Daten darf nur zu dem vorgegebenen Zweck erfolgen.

Grundsatz der Richtigkeit:
Die zu bearbeitenden Daten müssen richtig und vollständig sein.

Grundsatz der Datensicherheit:
Daten müssen durch geeignete Massnahmen ausreichend gesichert sein.

Ähnlich einem Ombudsmann kann der Datenschutzbeauftragte bei Verletzung der Datenschutzvorschriften die Verantwortlichen oder deren vorgesetzte Behörde auffordern, die geeigneten Massnahmen zu ergreifen[14], und im Weigerungsfalle die Regierung bzw. den Gemeindevorstand anrufen. Eigentliche Sanktionsmittel besitzt der Datenschutzbeauftragte jedoch keine[15].

Als zentrales Element der Tätigkeit des Datenschutzbeauftragten ist die Weisungsungebundenheit herauszustreichen. Der Datenschutzbeauftragte erfüllt seine Aufgaben fachlich selbständig, unabhängig und extern von der Verwaltung[16]. Diese gesetzlichen Vorgaben garantieren einen glaubwürdigen Datenschutz in der Öffentlichkeit.

Der Datenschutzbeauftragte arbeitet eng mit anderen Datenschutzaufsichtsstellen zusammen. Dadurch wird eine Angleichung der Praxis betreffend die datenschutzrechtliche Anwendung von kantonalen und kommunalen Gesetzen angestrebt und gleichzeitig versucht, eine hohe fachliche Kompetenz zu entwickeln.

---

[13] Art. 2 Abs. 2 KDSG
[14] Art. 9 Abs. 3 KDSG
[15] Art. 9 Abs. 4 KDSG
[16] Art. 7 Abs. 2 KDSG

III. Ausgewählte Themen

1. Aufbewahrung von Personalakten

Gesetzliche Grundlagen

In der Regel verweisen die kommunalen Personalverordnungen auf die kantonale Personalgesetzgebung oder das Obligationenrecht. In der kantonalen Personalverordnung (PV) finden sich zwei Bestimmungen, die explizit den Datenschutz beschlagen. In Art. 40 PV wird mit Bezug auf das Einsichtsrecht in die persönlichen Daten auf die kantonalen Bestimmungen über den Datenschutz verwiesen. Art. 64 PV enthält eine generelle Norm, wonach die mit der Personalverwaltung beauftragten Stellen berechtigt sind, Personendaten zu erheben und zu bearbeiten. Daneben gelten zumeist die Bestimmungen des Obligationenrechtes. Art. 1a Abs. 3 PV verweist ausdrücklich auf deren Anwendung. Gemäss Art. 328 Abs. 1 OR ist der Arbeitgeber verpflichtet, die Persönlichkeit der Mitarbeitenden zu achten und zu schützen. Es trifft ihn die Fürsorgepflicht. Der allgemeine Persönlichkeitsschutz nach Art. 27 und 28 ZGB wird im Arbeitsrecht durch Art. 328 Abs. 1 OR konkretisiert. Der Arbeitgeber hat also alle Eingriffe in die Persönlichkeit der Mitarbeitenden zu unterlassen, die nicht durch den Arbeitsvertrag gerechtfertigt sind. Ausfluss dieser Schutzfunktion bildet der neu geschaffene Art. 328b OR, worin ausdrücklich auf den Datenschutz verwiesen wird[1].

Inhalt der Personalakte

Grundsätzlich steht dem Arbeitgeber das Recht zu, sich über die Mitarbeitenden ein Bild zu machen und zu diesem Zwecke Angaben zur Person sowie Unterlagen über deren Fähigkeiten und Leistungen zu sammeln[2]. Die Beschaffung und Weitergabe der Informationen ist dann frei, wenn das Interesse des Arbeitgebers an dieser Beschaffung das Interesse des Betroffenen an der Geheimhaltung überwiegt[3]. Es kann somit keine generelle Angabe über die einzelnen Aktenstücke, welche Eingang in ein Personaldossier finden, gemacht werden. Vielmehr ist die Relevanz im Einzelfall abzuklären. Der Arbeitgeber darf Notizen und Berichte über das Verhalten von Mitarbeitenden nur dann im Personaldossier aufbewahren, soweit sie für das Arbeitsverhältnis von Bedeutung sind. Sicherlich gehören Qualifikationen und Beurteilungen zu den wichtigsten Personaldaten. Wesentlich erscheint, eine gewisse Objektivierung eines Personaldossiers zu erreichen.

---

[1] Weitere Normen, die datenschutzrechtliche Relevanz haben, sind die Art. 330a und 341 sowie Art. 362 OR.

[2] Nef, ZSR 1973 I 328.

[3] Rehbinder, Berner Kommentar, VI 2/2/1, 1985, OR 328 N 14.

Dies kann durch die Festlegung eines Standardinhaltes erreicht werden. Darüber hinaus sollte in jedem Dossier festgehalten werden, wann ein Dokument Aufnahme gefunden hat und wie lange dieses voraussichtlich im Dossier verbleiben soll. Auf diese Weise wird auf eine einfache Art grosse Transparenz geschaffen. Finden sich bedeutungslose oder bedeutungslos gewordene Dokumente im Personaldossier, so sind diese durch eine regelmässige Triage des Dossiers zu entfernen.

Graue Dossiers

Das Personalsossier mit seinen schriftlichen Aufzeichnungen gilt nicht als eine Datenbearbeitung zum ausschliesslich persönlichen Gebrauch des Arbeitgebers und unterliegt somit dem Geltungsbereich des Datenschutzgesetzes, insbesondere dem Auskunftsrecht. Mit der Erstellung von «grauen» Dossiers, in die Mitarbeitende keine Einsicht haben, werden die Persönlichkeitsrechte der Mitarbeitenden umgangen. Betroffen ist in erster Linie das Auskunftsrecht bezüglich Informationen, die wegen ihrer Brisanz Angestellten verheimlicht werden. Dadurch wird das Berichtigungs- und Bestreitungsrecht verunmöglicht. Der Arbeitgeber kann zwar das Auskunftsrecht einschränken, aufschieben oder verweigern. Die entsprechenden Voraussetzungen müssen aber gegeben sein. Die Datenschutzgesetzgebung verpflichtet den Inhaber von Datensammlungen, den Grund für die Einschränkung der Auskunft mitzuteilen. Die Betroffenen müssen gestützt darauf die Möglichkeit besitzen, die Zulässigkeit und die Stichhaltigkeit der Beschränkung zu überprüfen bzw. richterlich überprüfen zu lassen.

Auskunftspflicht

Grundsätzlich besitzen alle Mitarbeitenden das uneingeschränkte Recht auf Auskunft betreffend die Personalakte[4]. Dieses Recht kann jederzeit geltend gemacht werden. Die Auskunft kann nur verweigert werden, wenn eine gesetzliche Bestimmung dies verlangt, wesentliche öffentliche Interessen gegenüberstehen oder überwiegend schützenswerte Interessen einer Drittperson zu beachten sind. Dem Einsichtsrecht vollständig unterworfen sind Unterlagen mit medizinischem Inhalt sowie psychologische Gutachten und Tests. Indessen besteht kein Einsichtsrecht in persönliche Notizen des Arbeitgebers. Ebenso wenig besteht dieses in Unterlagen betreffend Personal- und Karriereplanung.

Aufbewahrung der Personalakte

Die Aufbewahrungsdauer einer Personalakte kann nicht allgemein in Jahren angegeben werden. Grundsätzlich sind Dokumente, welche für die weitere Durchführung des Arbeitsvertrages an Bedeutung verloren haben, aus dem Personaldossier zu entfernen.

Die zehnjährige Verjährungsfrist von Art. 127 OR gilt nach vorherrschender Auffassung unter anderem für den Anspruch auf Erstellung, Begründung, Korrektur oder Ergänzung eines Arbeitszeugnisses[5]. Diese Ansprüche können bis zehn Jahre nach Beendigung des Arbeitsverhältnisses gel-

[4] 4. Tätigkeitsbericht EDSB 1996/1997, S. 25.

[5] Streiff/von Kaenel, Arbeitsvertrag, 5. Auflage, Zürich 1992, Art. 330a N 2 mit Verweisen.

tend gemacht werden. Von der Aufbewahrungspflicht des Arbeitgebers betroffen sind somit in erster Linie Angaben über Art und Dauer des Arbeitsverhältnisses, Aufgabenbeschreibung und Verantwortungsbereich, Beurteilungen von Leistung, Verhalten und Führung, Laufbahn, Weiterbildung und Austrittsgrund, aber auch Angaben über besondere Vorkommnisse. Relevant für die Erstellung eines Arbeitszeugnisses sind in der Regel nur die letzten zwei Mitarbeiterbeurteilungen. Frühere Beurteilungen sind somit spätestens mit dem Austritt der Mitarbeitenden aus der Personalakte zu entfernen und zu vernichten.

Daten über Fehlverhalten der Mitarbeitenden sind nach angemessener Zeit zu überprüfen und gegebenenfalls zu vernichten. Eine brauchbare zeitliche Grenze lässt sich aus der analogen Anwendung strafrechtlicher Normen ableiten. Beispielsweise beträgt die zulässige Höchstdauer der Aufbewahrung von Betriebsbussen zwei Jahre[6].

Bewerbungsunterlagen, wie z.B. Lebenslauf, frühere Arbeitszeugnisse, Ausbildungsdiplome etc. gehören den Mitarbeitenden. Sobald der Arbeitgeber kein berechtigtes Interesse mehr hat oder spätestens bei Beendigung des Arbeitsverhältnisses müssen diese Dokumente den Mitarbeitenden zurückgegeben werden. In der Regel sollte dies jedoch bereits nach Ablauf der Probezeit geschehen[7].

Akten, die dem Arbeitgeber gehören, an denen er aber kein berechtigtes Interesse mehr hat, müssen spätestens bei Beendigung des Arbeitsverhältnisses vernichtet oder den Mitarbeitenden ausgehändigt werden. Es geht hier insbesondere um frühere Qualifikationsunterlagen, aber auch um graphologische, psychologische oder medizinische Gutachten sowie Persönlichkeitstests. Auch solche Dokumente sollten in der Regel bereits ein bis zwei Jahre nach Erstellung vernichtet bzw. zurückgegeben werden[8].

Für die Aufbewahrung der Personalakten kann – wie dargelegt – keine generelle Aufbewahrungsdauer angegeben werden. Vielmehr ist eine kontinuierliche Überprüfung der Relevanz von Unterlagen für das Arbeitsverhältnis vorzunehmen. Dies gilt insbesondere bei Beendigung des Arbeitsverhältnisses. Ein nicht minder wichtiger Aspekt bildet die Sicherheit. Es ist selbstverständlich, dass die Personalakten, welche während des Arbeitsverhältnisses verschlossen und nur für den personalverantwortlichen Personenkreis zugänglich waren, auch nach Beendigung des Arbeitsverhältnisses unter demselben Sicherheitsaspekt archiviert werden.

---

[6] Rehbinder, Berner Kommentar, VI 2/2/1, 1985, OR 328 N 15.
[7] 9. Tätigkeitsbericht EDSB, 2001/2002, S. 76.
[8] 9. Tätigkeitsbericht EDSB, 2001/2002, S. 76.

2. Videoüberwachung

Allgemeines

Der Einsatz von Videogeräten zur Feststellung und zur Sicherung von Sachverhalten nimmt laufend und rasant zu. In der Schweiz sollen Schätzungen zufolge gegen 40 000 Überwachungskameras[1] installiert sein. Aktualität erhielt die Problematik der Videoüberwachung in Graubünden im Zusammenhang mit dem WEF.

Das Bearbeiten von Personendaten hat die Grundsätze der Rechtmässigkeit, der Verhältnismässigkeit, der Zweckmässigkeit, der Zweckgebundenheit, der Richtigkeit und der Datensicherheit zu beachten[2]. Diese elementaren Prinzipien sind auch bei der Videoüberwachung einzuhalten. Obwohl sich eine Person in der Öffentlichkeit der allgemeinen Beobachtung aussetzt, gibt sie damit kein Einverständnis, ihr Verhalten durch staatliche Organe aufnehmen, sicherstellen und verwerten zu lassen. Auch bei der Zuhilfenahme von Videogeräten sind die allgemein gültigen verwaltungsrechtlichen Grundsätze zu beachten[3].

Arten der Videoüberwachung

Da die Videoüberwachung unterschiedlichen Zwecken dient, lassen sich verschiedene Kategorien unterscheiden.

Die **observierende** Überwachung zielt auf die Überwachung von Objekten wie Strassen oder Gebäuden ab. Sie ist nicht auf Personen gerichtet. Ihr Ziel ist primär die Kontrolle und Steuerung oder die Gewährleistung der Sicherheit eines Gebäudes oder eines Grundstücks. Soweit sie nicht personenbezogen ist, hat sie keine datenschutzrechtliche Relevanz.

Bei der **invasiven** Überwachung wird die Beschattung einer bestimmten, tatverdächtigen Person angestrebt. Die Sicherstellung durch die Überführung oder Verhaftung dieser Person ist das Ziel dieser Massnahme. Für die Anordnung einer invasiven Überwachung wird neben einem dringenden Tatverdacht auch eine bestimmte Schwere des Delikts verlangt. Sodann findet eine richterliche Überprüfung der Massnahme statt.

---

[1] Sonntags Zeitung 26. Januar 2003, S. 101.

[2] Art. 2 Abs. 1 KDSG

[3] Vgl. Grundsätze des Datenschutzes Ziffer II hievor.

[4] Datenschutzbeauftragter des Kantons Zürich, Videoüberwachung durch öffentliche Organe, Juli 2002, http://www.datenschutz.ch;
B. Baeriswyl, in: digma, Zeitschrift für Datenrecht und Informationssicherheit, 2002, S. 26 ff.

Mit der **dissuasiven** Überwachung wird primär versucht, vorsorglich bestimmte öffentliche Räume zu beobachten. Sie dient der inneren Sicherheit und richtet sich gegen eine Vielzahl von unbestimmten Personen, die sich im überwachten Raum bewegen. Im Gegensatz zur observierenden Überwachung ist die dissuasive auf die Erkennbarkeit der Personen ausgerichtet. Letztere tangiert die Grundrechte ganz erheblich. Somit müssen die erforderlichen Voraussetzungen für den Eingriff in die Privatsphäre gegeben sein.

Gesetzliche Grundlage

Für einen schweren Eingriff in die Grundrechte bedarf es eines Gesetzes. Weniger weit reichende Eingriffe können auf Verordnungsstufe geregelt werden. Das Bundesgericht nimmt an, dass die Exekutive aufgrund der polizeilichen Generalklausel auch ohne ausdrückliche gesetzliche Grundlage diejenigen Massnahmen treffen darf, die zur Wiederherstellung der öffentlichen Sicherheit und Ordnung bei schweren Störungen oder zur Abwehr unmittelbar drohender schwerwiegender Gefährdungen dieser Ordnung unerlässlich sind. Eine solche Massnahme muss zeitlich und örtlich begrenzt sein.

Die polizeiliche Generalklausel kann bei der dissuasiven Videoüberwachung mangels genügender Bestimmtheit nicht als rechtliche Grundlage herangezogen werden. Bei dieser Art der Überwachung geht es in der Regel weder um schwere Störungen der öffentlichen Sicherheit und Ordnung noch um die Abwehr unmittelbar drohender schwerwiegender Gefährdungen.

In Graubünden fehlt es an der erforderlichen gesetzlichen Grundlage für eine dissuasive Videoüberwachung. Massgebend ist die grössrätliche Verordnung über die Kantonspolizei (KapoV)[5]. Aufgrund der heutigen Kompetenzregelung in der Kantonsverfassung, der dazu vorhandenen bundesgerichtlichen Rechtsprechung sowie der bis anhin erfolgten Rechtsetzung auf dieser Stufe bildet die KapoV wohl eine genügende gesetzliche Grundlage auch für die Einführung sicherheitspolizeilicher Befugnisse. Mit der kürzlich erlassenen Teilrevision wurde neu ein Art. 8a KapoV eingeführt.

[5] BR 613.100

Danach kann die Kantonspolizei zur Wahrung der Sicherheit und Ordnung sowie zur Gefahrenabwehr ereignisbezogen die notwendigen Massnahmen anordnen. Art. 10 KapoV hält zudem fest, dass die Kantonspolizei nach dem Grundsatz der Verhältnismässigkeit und mit Bewilligung des Vorstehers des Justiz- und Polizeidepartementes technische Mittel einsetzen darf. Mit dem Wort «ereignisbezogen» in Art 8a KapoV wollte der Gesetzgeber jedoch zum Ausdruck bringen, dass eine präventive Massnahme nicht von dieser neu geschaffenen Bestimmung gedeckt ist. Der Ausdruck «ereignisbezogen» ist wohl nicht derart einschränkend auszulegen, dass lediglich während des eigentlichen Geschehens interveniert werden darf. Jedes Ereignis oder auch jeder Anlass hat einen Vorlauf und einen Nachgang. Im Umfeld des zeitlichen Vorlaufes als auch danach müssen polizeiliche Massnahmen, die einen Bezug zum Ereignis haben, möglich sein. Selbst bei grosszügiger Auslegung von Art. 8a KapoV genügt dieser aber nicht als Grundlage für eine dissuasive Überwachung, zumal neben der Ereignisbezogenheit die Komponenten «Wahrung der Sicherheit und Ordnung» oder «Gefahrenabwehr» ebenfalls gegeben sein müssen.

[6] Gemäss Botschaft Heft Nr. 7/2001/2002, S. 425, ist im Begriff «ereignisbezogen» auch der Ausdruck «anlassbezogen» mitenthalten.

3. Geo-Informationssysteme

Unter dem Begriff «Geo-Daten» ist eine Summe verschiedener geografischer Daten über den Boden, die Umwelt, die Natur und den bebauten und unbebauten Boden zu verstehen[1]. Geo-Informationen sind somit orts- und raumbezogene Daten, die die Gegebenheiten eines Landes umfassend beschreiben. In der modernen Kommunikationsgesellschaft bilden sie die Basis für Abläufe, Pläne, Massnahmen und Entscheidungen aller Art.

Das geografische Informations-System (GIS) ist ein Werkzeug, um Raumdaten mit Hilfe der EDV zu erfassen, zu verknüpfen, zu bearbeiten, darzustellen und auszuwerten[2]. Im Kanton Graubünden existiert keine gesetzliche Grundlage für die Bearbeitung von Geo-Daten. Es gibt hingegen zahlreiche Gesetze und Verordnungen, welche die GIS-Tätigkeit ansatzweise regeln[3].

Die Datenschutzgesetzgebung dient dem Schutz von Personen vor widerrechtlichem Bearbeiten von Personendaten durch Behörden[4]. Geografische Daten beinhalten typischerweise keine Personendaten. Die Persönlichkeit und deren Schutz wird indessen tangiert, sobald raumbezogene Daten einen Detaillierungsgrad aufweisen, der Personen identifizierbar macht. Aufgrund der technologischen Entwicklung ist es ohne weiteres möglich, die Ebenen verschiedener einzelner Pläne zu verknüpfen und mit Daten anderer Datenbanken zu verbinden[5]. Ein anschauliches Beispiel findet sich auf der Internetseite der Stadt Chur[6]. Über den Parzellenplan kann unter Zuhilfenahme des Icons «Information» direkt auf den jeweiligen Eigentümer einer Parzelle geschlossen werden. Das kantonale Datenschutzgesetz statuiert in Art. 2 das Prinzip der Zweckgebundenheit. Personenbezogene Daten dürfen nur zu einem Zweck bearbeitet werden, der für die betroffene Person transparent ist, indem er gesetzlich vorgesehen ist. Dieses Zweckbindungsgebot wird durchbrochen, wenn Daten in einer Datenverknüpfung zur Verfügung gestellt oder in einem GIS mit andern Daten

---

[1] M. Huser, Geodaten im Spannungsfeld von Grundbuch, Vermessung und GIS, in: ZBGR 83 (2002), S. 66.

[2] gis@2002+, Geografisches Informationssystem der Kantonalen Verwaltung Graubünden, Bericht zur heutigen Lage und künftigen Ausrichtung, S. 4. z.B. Verordnung über die amtliche Vermessung im Kanton Graubünden (BR 217.250).

[3] Verordnung über den Einsatz der Informatik in der Kantonalen Verwaltung Graubünden (BR 170.500).

[4] Art. 1 DSG, Art. 1 Abs. 1 KDSG

[5] Tätigkeitsbericht Datenschutzbeauftragter des Kantons Zürich 5/99, S. 19.

[6] http://www.chur.ch/d/stadtplan/index.cfm?tid=1

kombiniert werden. Die Kombination führt auch zu einer anderen Eingriffsqualität bezüglich Privatsphäre[7]. Das vorgenannte Beispiel widerspricht dem Prinzip der Zweckgebundenheit und darüber hinaus auch dem Grundsatz der Rechtmässigkeit. Jede Datenbearbeitung im öffentlichen Bereich bedarf einer gesetzlichen Grundlage. Dies ergibt sich aus den allgemeinen Verwaltungsrechtsprinzipien. Auf welcher Regelungsstufe eine entsprechende Grundlage zu schaffen ist, beurteilt sich nach der Schwere des Eingriffs in die Privatsphäre. Es ist eine Technikfolgenabschätzung vorzunehmen. Im Bereich der Raumdatenbearbeitungen fehlt eine solche bisher. Raumdatenbearbeitungen werden gesellschaftlich, politisch und wirtschaftlich noch mehr an Bedeutung gewinnen und viele Lebensbereiche durchdringen[8]. Bei der öffentlichen Zugänglichmachung von GIS-Daten darf grundsätzlich nicht nur auf den Nutzen für den Nachfrager abgestellt werden. Vielmehr ist das Augenmerk ebenfalls auf einen möglichen Missbrauch zu richten[9]. Die berechtigten Ansprüche der Allgemeinheit enden dort, wo der geschützte Bereich des Privaten übermässig beansprucht wird. Die schützenswerten Interessen des Einzelnen stehen immer auf der gleichen Stufe wie die berechtigten Anliegen von Nachfragern. Eine rechtskonforme Handhabung von GIS-Daten ruft nach einem Geo-Informationsgesetz.

[7] Marco Fey, Rechtliche Aspekte von GIS, in: digma, Zeitschrift für Datenrecht und Informationssicherheit, 2002, S. 170 ff.

[8] Marco Fey, ebenda, S. 172.

[9] 5. Tätigkeitsbericht EDSB 1997/1998, S. 72.

4. Datensperre

Jede Person hat das Recht auf Sperrung schützwürdiger Personendaten[1]. Die Sperrung der Bekanntgabe von Personendaten hat zum Ziel, die Weiterbearbeitung oder -nutzung durch Dritte einzuschränken. Eine Datensperre können Bürgerinnen und Bürger jederzeit mittels schriftlicher Mitteilung an die zuständige kantonale oder kommunale Amtsstelle veranlassen. Die Geltendmachung dieses Sperrrechtes ist nicht von einem Interessennachweis abhängig, da die kantonale Regelung an weniger weitgehende Voraussetzungen geknüpft ist als die bundesrechtliche.[2] Die Verwaltung hat grundsätzlich ein Sperrgesuch entgegenzunehmen und die erforderlichen Massnahmen in die Wege zu leiten. Die Sperrung umfasst dabei sämtliche Daten, die über diese Person bei der jeweiligen Amtsstelle bestehen.[3]

Gemäss den Bestimmungen von Art. 20 Abs. 2 DSG kann das verantwortliche Organ die Sperrung der betroffenen Person verweigern oder aufheben, wenn «eine Rechtspflicht zur Bekanntgabe besteht oder die Erfüllung seiner Aufgabe sonst gefährdet wäre». Im ersten Fall basiert die Verpflichtung zur Bekanntgabe der Daten auf einer rechtlichen Grundlage. Diese rechtliche Verpflichtung lässt den verantwortlichen Organen keinen Ermessensspielraum, um die Bekanntgabe abzulehnen.[4] Im zweiten Fall würde durch die Sperrung der Datenbekanntgabe die Erfüllung der Aufgaben des bekannt gebenden Organs gefährdet. Das Risiko der Gefährdung muss genügend konkret sein. Es darf sich dabei nicht um eine vage Eventualität der Gefährdung handeln. Das verantwortliche Organ muss grundsätzlich nicht mehr in der Lage sein, ohne Bekanntgabe seine Aufgabe zu erfüllen. Zumindest müsste sich die Aufgabenerfüllung als besonders schwierig oder gar unmöglich erweisen[5].

Gemäss Art. 19 Abs. 1 lit. d DSG kann die Bekanntgabe ebenfalls erfolgen, wenn der «Empfänger glaubhaft macht, dass die betroffene Person die Einwilligung verweigert oder die Bekanntgabe sperrt, um ihm die Durchsetzung von Rechtsansprüchen oder die Wahrnehmung anderer schutzwürdiger Interessen zu verwehren.» Diese Bestimmung deckt den Fall ab, dass eine Person eine Datensperre erlässt, um einer Rechtspflicht zu entgehen (z.B. Alimentenzahlungen, Schuldbetreibung, etc.).

---

[1] Art. 1 Abs. 1 lit. e KDSG
[2] Art. 20 Abs 1 DSG
[3] Fakten, Die Zeitschrift für Datenschutz des Kantons Zürich, Nr. 2/96, S. 8.
[4] Es kann die Bekanntgabe nicht verweigern, indem es sich auf Art. 19 Abs. 4 DSG beruft.
[5] Urs Maurer, Nedim Peter Vogt (Hrsg.), Kommentar zum Schweizerischen Datenschutzgesetz, Art. 20 N 10.

Die Verwaltung wird verpflichtet, eine Interessenabwägung vorzunehmen zwischen der Glaubhaftmachung, dass die Sperrung die gesuchstellende Person in der Verfolgung eigener Interessen behindert, und dem schutzwürdigen Interesse der ihre Daten sperrenden Person. Folgerichtig ist die angegangene Behörde zu einer Anhörung beider Parteien verpflichtet.[6] Das verantwortliche Organ kann auf die Einholung einer Stellungnahme der betroffenen Person nur verzichten, wenn Rechtsansprüche oder legitime Drittinteressen aktuell gefährdet sind oder wenn die betroffene Person nicht erreichbar ist oder sich innerhalb der gesetzten Frist nicht geäussert hat.[7]

Anlegen von Musterordnern

Bei der Anlage, zumindest aber bei der Anwendung von Musterordnern handelt es sich um einen Tatbestand des Bekanntgebens von Daten. Dabei darf die Persönlichkeit der betroffenen Person nicht widerrechtlich verletzt werden. Solche Persönlichkeitsverletzungen können klageweise durchgesetzt werden. Grundsätzlich sollte auf die Anlage von Musterordnern verzichtet werden. Wenn hiezu dennoch ein Bedürfnis besteht, ist es zwingend erforderlich, eine Anonymisierung vorzunehmen, die Rückschlüsse auf Personen ausschliesst. Dabei genügt es im Einzelfall nicht, lediglich die Personennamen zu eliminieren. Rückschlüsse auf die Person lassen auch Ortsbezeichnungen und dergleichen zu. Selbst innerhalb von Amtsstellen ist Zurückhaltung zu üben. Dieser Grundsatz gilt noch vielmehr, wenn Musterordner eine Amtsstelle verlassen, sei dies zu Ausbildungs- oder Anwendungszwecken. Wird der Anonymisierung nicht vollumfänglich nachgelebt, ist die Datenschutzgesetzgebung verletzt.

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 beim Beschluss, die Sperre im konkreten Einzelfall zu durchbrechen. Selbstverständlich dürfen bei diesem Vorgehen die strittigen Daten nicht bekannt gegeben werden, ansonsten würde die betroffene Person der Möglichkeit beraubt, den Sachverhalt durch die nächsthöhere Instanz überprüfen zu lassen.[8] Diese Entscheide können beim kantonalen Verwaltungsgericht mit Rekurs angefochten werden.[9]

[6] Dies ergibt sich zwingend aus dem verfassungsmässigen Grundsatz des rechtlichen Gehörs.
[7] Urs Maurer, Nedim Peter Vogt (Hrsg.), Kommentar zum Schweizerischen Datenschutzgesetz, Art. 19 N 26.
[8] Fakten, Die Zeitschrift für Datenschutz des Kantons Zürich, Nr. 2/1999, S. 11 ff.
[9] Art. 6 Abs. 3 KDSG

IV. Fälle aus der Praxis

1. Listenauskünfte

Kann eine örtliche Partei von der Gemeinde eine Liste aller katholischen Stimmberechtigten verlangen, um diese Stimmberechtigten anzuschreiben und sie über die Zielsetzungen der Partei zu orientieren?

Gemäss Art. 2 KDSG wird bei der Bearbeitung von Personendaten, die auch die Weitergabe umfasst, die Einhaltung der Grundsätze der Rechtmässigkeit, der Verhältnismässigkeit, der Zweckmässigkeit, der Zweckgebundenheit, der Richtigkeit und der Datensicherheit verlangt. Diese im Datenschutzrecht vorherrschenden Prinzipien wurden in anderen Kantonen ausgedehnter konkretisiert. Das Bündner Datenschutzgesetz ist eher als Rahmengesetz zu qualifizieren. In der Ausgestaltung des Datenschutzes in anderen Kantonen wird eine Bekanntgabe durch Listenauskünfte gestattet, wenn ausschliesslich schützenswerte ideelle Zwecke verfolgt werden[1]. Eine Datenbekanntgabe zu kommerziellen Zwecken wird ausgeschlossen.[2]

Sofern Listenauskünfte erteilt werden sollen, muss im Einzelfall abgeklärt werden, was unter dem Begriff «schützenswerte ideelle Zwecke» zu verstehen ist. Die zuständige Behörde verfügt dabei über einen erheblichen Beurteilungsspielraum. Schützenswerte ideelle Zwecke verfolgen allgemein jene Vereine, Organisationen und Institutionen in den Bereichen Kultur, Freizeit, Sport, Politik usw., deren Aktivitäten zum Gemeinschaftsleben beitragen und im Interesse des Gemeinwohls erfolgen[3]. Die Praxis zeigt, dass die Abgrenzung bezüglich der schützenswerten ideellen Zwecke nicht immer leicht ist. Zum einen hat die Behörde sich darüber Rechenschaft abzugeben, ob die Zwecke, welche verfolgt werden, ideeller Natur sind. Zum andern stellt sich die Frage, ob die Listenauskunft lediglich für den bekannt gegebenen Zweck Verwendung findet oder ob eine weitergehende, dem Datenschutz zuwiderlaufende Bearbeitung offensichtlich möglich ist. In Anbetracht der Tatsache, dass die politischen Parteien eine staatstragende Funktion haben und die Zugehörigkeit zu der einen oder anderen Landeskirche gesellschaftlich kaum mehr von Bedeutung ist, kann eine Weitergabe der Adressen aller Katholiken zugestimmt werden.

---

[1] Beispiele:
§ 9 Abs. 3 Datenschutzgesetz des Kantons Zürich
§ 8 Abs. 3 lit. c Datenschutzgesetz des Kantons Zug

[2] Art. 5 Abs. 4 Gesetz über die Niederlassung der Schweizer, BR 130.200.

[3] Fakten, Die Zeitschrift für Datenschutz des Kantons Zürich, 3/96, S. 9.

2. Internetpublikation von Grundbuchdaten

Kann eine Gemeinde die Grundbuchdaten internetmässig publizieren?

Vorab ist festzustellen, dass die Veröffentlichung von Grundbuchdaten per Internet qualitativ etwas ganz anderes darstellt als die Bekanntgabe dieser Daten gegenüber Einzelpersonen. Das Internet als weltweit und zu jeder Zeit zugängliche Informationsplattform spricht als Zielpublikum theoretisch «die ganze Welt» an. Es ist ohne weiteres möglich, die publizierten Informationen abzuspeichern, auszuwerten und zu verknüpfen. Die Gefahren des Missbrauches im Internet sind nicht zu unterschätzen.

Gemäss Art. 970 Abs. 1 ZGB ist jedermann berechtigt, Auskunft zu erhalten, wer als Eigentümer eines Grundstückes im Grundbuch eingetragen ist. Grundsätzlich können nur die voraussetzungslos erhältlichen Daten Gegenstand einer frei zugänglichen Internetpublikation sein. Indessen regelt Art. 970 ZGB die Frage nach den Modalitäten der Auskunftserteilung nicht. Die Aufschaltung von Grundbuchdaten auf das Internet qualifiziert sich als Abrufverfahren[1]. Ein solches System wird einer besonderen rechtlichen Regelung unterworfen, weil der Auskunfterteilende grundsätzlich keine Möglichkeit hat, den Vorgang zu beeinflussen. Der Online-Zugriff ist abschliessend in Art. 111m Grundbuchverordnung (GBV) geregelt[2]. Unter diese abschliessende Regelung fällt auch der mögliche Kreis berechtigter Personen. Ein freier Zugang, wie es ein Zugriff via Internet bedeutet, ist nicht vorgesehen. Die vorgenannte Bestimmung gibt den Kantonen die Möglichkeit, Zugriffskriterien festzulegen. Mit Art. 35 kGBV[3] hat der Kanton Graubünden die Zugriffsmöglichkeiten des Art. 111m GBV übernommen. Die Aufzählung ist abschliessend. Somit ist ein Online-Verfahren ausgeschlossen.

Adressen von Vereinsmitgliedern[1]

Weitergabe an Dritte

Die Weitergabe von Mitgliederadressen eines Vereins an Dritte ist zulässig, wenn:

1. dies aus den Vereinsstatuten klar hervorgeht, oder
2. vorgängig die Einwilligung eines jeden Mitgliedes dazu eingeholt wird oder allen Mitgliedern unter vorgängiger Mitteilung des Empfängers und des Zwecks der Weitergabe ein Widerspruchsrecht eingeräumt wird, oder
3. eine rechtliche Verpflichtung dazu besteht.

(Jedem Mitglied steht es jederzeit absolut frei, von seinem Sperrrecht Gebrauch zu machen, respektive eine einmal gegebene Einwilligung teilweise oder ganz zu widerrufen.)

Weitergabe an Vereinsmitglieder

Die Aushändigung von Mitgliederlisten an Vereinsmitglieder ist zulässig, wenn:

1. die Liste zur Ausübung von Mitgliedschaftsrechten benötigt wird (z.B. Einberufung einer ausserordentlichen Mitgliederversammlung).
2. die Betroffenen ihre Einwilligung dazu gegeben haben.

[1] Auszug Merkblatt «Vereinsmitglieder» EDSB; http://www.edsb.ch/d/doku/merkblaetter/verein.htm

[1] Art. 19 Abs. 3 DSG
[2] SR 211.432.1
[3] BR 217.100

3. Wehrpflichtersatz und Steuerdatenbank

Kann im Zusammenhang mit der Veranlagung des Wehrpflichtersatzes das Kreiskommando auf die Daten der Steuerverwaltung online zugreifen?

In Art. 24 des Bundesgesetzes über den Wehrpflichtersatz (WPEG) wird die Amtshilfe umfassend geregelt. Art. 24 WPEG stützt sich auf das Bundesgesetz über die Schaffung und die Anpassung gesetzlicher Grundlagen für die Bearbeitung von Personendaten. Es besteht somit eine genügende gesetzliche Grundlage für den Datentransfer. Seitens der Steuerverwaltung aufgearbeitete Daten können somit dem Kreiskommando übergeben werden.

Problematischer wiegt die Frage der Implentierung eines Online-Zugriffs. Dabei handelt es sich um ein Abrufverfahren gemäss Art. 19 Abs. 3 DSG. Aus Sicht des Verfahrensablaufes entscheidet beim Abrufverfahren nicht mehr das bekannt gebende Organ, sondern der Datenempfänger, welche Daten zu welchem Zeitpunkt und in welchem Ausmass bekannt gegeben werden. Das bekannt gebende Organ verliert die Herrschaft über den Datenaustausch. Aus diesem Grund hat der Gesetzgeber die Legalitätsanforderungen bei der Verwendung von Abrufverfahren verstärkt und damit auf den Ausnahmecharakter hingewiesen. Das Abrufverfahren muss in einer gesetzlichen Grundlage speziell vorgesehen sein[1]. In Art. 19 Abs. 3 DSG wird der Begriff «ausdrücklich» verwendet. Folglich hat sich der Gesetzgeber eindeutig geäussert. Eine Bestimmung, welche lediglich feststellt, dass ein Organ Zugang zu den Informationssystemen oder zu den zur Ausübung seiner Aufgaben notwendigen Datensammlungen haben kann, genügt den Anforderungen der vorgenannten Bestimmung nicht. Das Abrufverfahren muss in der Rechtsgrundlage der Datensammlung, deren Daten bekannt gegeben werden, enthalten sein.

In der Botschaft über die Schaffung und die Anpassung gesetzlicher Grundlagen für die Bearbeitung von Personendaten[2] wird bereits in der Einführung festgestellt, dass Daten, welche über ein Abrufverfahren zugänglich gemacht werden sollen, über eine formelle gesetzliche Grundlage verfügen müssen. Es wird ausdrücklich Bezug genommen auf das Abruf-

[1] Urs Maurer, Nedim Peter Vogt (Hrsg.), Kommentar zum Schweizerischen Datenschutzgesetz, Art. 19 N 32.

[2] Bundesblatt 1999, S. 9005 ff.

verfahren im Zusammenhang mit Steuererlassen, worunter auch das Bundesgesetz über den Wehrpflichtersatz zu zählen ist[3]. Unter dem Titel «Normstruktur» wird in der Botschaft festgehalten[4]:

«Abs. 4 regelt die Amtshilfe mittels moderner Kommunikationsmittel von andern Ämtern an die Steuerverwaltung, nicht jedoch umgekehrt. Das andere Amt kann seine Daten damit der Steuerverwaltung im Einzelfall, auf Listen oder Disketten sowie durch ein Abrufverfahren weitergeben. Umgekehrt erhalten andere Ämter nur Informationen der Steuerverwaltung, wenn dies im Spezialgesetz vorgesehen ist. Nicht vorgesehen ist ein Abrufverfahren im Wehrpflichtersatzgesetz.»

Dementsprechend ist bei der Formulierung von Art. 4 WPEG – im Gegensatz beispielsweise zur Formulierung von Art. 39a des Bundesgesetzes über die Harmonisierung der direkten Steuern der Kantone und Gemeinden – auf die Formulierung eines Abrufverfahrens bewusst verzichtet worden. Art. 24 Abs. 5 WPEG, der auf den Datentransfer Bezug nimmt, ist nicht lückenhaft. In Einklang mit der Botschaft und der übrigen Gesetzgebung wurde auf die Legiferierung des Abrufverfahrens verzichtet. Konsequenterweise fehlt es beim Wehrpflichtersatz an einer entsprechenden ausdrücklichen gesetzlichen Grundlage für die Einrichtung eines Online-Systems im Sinne eines Abrufverfahrens.

Adoption und Akteneinsicht

Am 1. Januar 2003 ist Art. 268c Zivilgesetzbuch in Kraft getreten. Er lautet wie folgt:

«Hat das Kind das 18. Lebensjahr vollendet, so kann es jederzeit Auskunft über die Personalien seiner leiblichen Eltern verlangen; vorher kann es Auskunft verlangen, wenn es ein schutzwürdiges Interesse hat.

Bevor die Behörde oder Stelle, welche über die gewünschten Angaben verfügt, Auskunft erteilt, informiert sie wenn möglich die leiblichen Eltern. Lehnen diese den persönlichen Kontakt ab, so ist das Kind darüber zu informieren und auf die Persönlichkeitsrechte der leiblichen Eltern aufmerksam zu machen.

Die Kantone bezeichnen eine geeignete Stelle, welche das Kind auf Wunsch beratend unterstützt.»

Der Anspruch, die leiblichen Eltern zu kennen, steht dem volljährigen Adoptivkind von Verfassungs wegen unabhängig von einer Abwägung mit entgegenstehenden Interessen zu. Es handelt sich um ein unverzichtbares und nicht verwirkbares Recht. Der Gesetzgeber hat eine Güterabwägung zugunsten des volljährigen Adoptivkindes ohne Einschränkungen vorgenommen[1].

[1] BGE 1.P.460/2001/sta vom 4. März 2002

[3] Bundesblatt 1999, S. 9028.
[4] Bundesblatt 1999, S. 9029.

4. IPV-Daten an Krankenversicherer

Dürfen im Rahmen der individuellen Prämienverbilligung (IPV) Datenbestände des Kantons Graubünden an die Krankenkassen zugestellt werden?

Die Voraussetzungen für die Datenbekanntgabe an Drittpersonen sind zu beachten. Die gesetzliche Grundlage für die Weitergabe von Versicherungsdaten findet sich in Art. 11 des Gesetzes über die Krankenversicherung und Prämienverbilligung (KPVG)[1]. Gemäss Art. 19 DSG in Verbindung mit Art. 17 DSG und Art. 2 Abs. 2 KDSG werden an die Rechtsgrundlagen für die Bekanntgabe von Daten hohe Anforderungen gestellt. Diesen gesetzlichen Vorgaben genügt Art. 11 KPVG grundsätzlich nicht. Art. 19 Abs. 1 lit. a und b DSG sieht indessen für bestimmte Fälle Abweichungen vor. Mit der Weitergabe von IPV-Datenbeständen an die Versicherer wird die direkte Auszahlung der Prämienverbilligung über die Versicherer angestrebt. Diese Vorgehensweise ist im KPVG ausdrücklich festgehalten. Die Übermittlung von Datensätzen an die Versicherer hat für die Versicherten durchaus Vorteile, da diese von der Bekanntgabe der Daten profitieren. Das System der Prämienverbilligung wird durch den vorgesehenen Ablauf für den Einzelnen einfacher. Aufgrund dieser Umstände darf vorausgesetzt werden, dass eine stillschweigende Einwilligung der Versicherten gemäss Art. 19 Abs. 1 lit. b DSG vorliegt. Im Übrigen wäre es völlig unverhältnismässig, von jeder betroffenen Person die konkrete ausdrückliche Bewilligung einzuholen[2].

[1] BR 542.100

[2] Urs Maurer, Nedim Peter Vogt (Hrsg.), Kommentar zum Schweizerischen Datenschutzgesetz, Art. 19 N 22.

V. Register der Datensammlungen

Das kantonale Datenschutzgesetz hat für die ihr Unterstellten[1] die Verpflichtung gebracht, innert einer vorgegebenen Frist[2] ein Register aufzubauen. Die Registrierung umfasst sämtliche Datensammlungen[3]. Das Register ist öffentlich und soll von jeder Person, die es wünscht, eingesehen werden können. Diese Vorgabe kann realistischerweise nur erreicht werden, wenn die einzelnen Register internetmässig aufgeschaltet werden. Für die Registrierung ist dasjenige Organ verantwortlich, das die Datensammlung zur Erfüllung seiner Aufgabe benötigt.

Ziel der Datenschutzgesetzgebung ist der Schutz der Grundrechte derjenigen Personen, über welche öffentliche Organe Daten bearbeiten. Eine Hauptvoraussetzung, um Datenschutz gewährleisten zu können, ist die Transparenz in der Datenbearbeitung. Das Register der Datensammlungen ist ein Instrument, welches einerseits den Organen ermöglicht, die Verantwortung im Bereich des Datenschutzes wahrzunehmen, und andererseits den betroffenen Personen erleichtert, ihre Rechte geltend zu machen. Die Registrierung der Datensammlungen bietet zudem die Chance, Verwaltungsabläufe zu optimieren und Effizienzpotenziale zu nutzen.

In einer ersten Phase beabsichtigt der Datenschutzbeauftragte, ein Musterregister für die politischen Gemeinden zu erarbeiten. Erst hernach werden gestützt auf die Erfahrungen mit den Gemeinden die weiteren dem Datenschutzgesetz unterstellten Behörden mit der Registrierung konfrontiert. Alle Gemeinden haben grundsätzlich dieselben Aufgaben. Es kann daher davon ausgegangen werden, dass sie unabhängig von der Grösse und Organisation zur Erfüllung ihres Auftrages weitgehend dieselben Daten benötigen und entsprechende Sammlungen führen. Ein Musterregister kann deshalb den Gemeinden die Registrierung ihrer eigenen Datensammlungen in verschiedener Hinsicht sehr erleichtern. Erstens gibt es ihnen einen Überblick über die wichtigsten in einer Gemeinde geführten Datensammlungen. Zweitens führt es bereits die Standarddaten, was die Sucharbeiten der einzelnen Gemeinden wesentlich reduziert. Drittens bildet es die Grundlage für die Überprüfung, ob die Datenbearbeitung in der Gemeinde sinnvoll und effizient wahrgenommen wird. Das Musterregister enthält

---

[1] Art. 1 KDSG

[2] Die Frist läuft am 1. Mai 2005 aus (Art. 12 Abs. 1 KDSG).

[3] Art. 8 lit. b KDSG; Art. 11 Abs. 2 DSG

eine Liste mit den in der Gemeinde üblicherweise geführten Datensammlungen. Die Liste orientiert sich an einem umfassenden Aufgabenkatalog. Sämtliche aufgeführten Datensammlungen werden auf ihre Registrierungspflicht und allfällige Zusammenfassungsmöglichkeiten hin überprüft. Das vorgesehene Musterregister ist als Leitfaden zu verstehen, d.h. jede Musterdatensammlung muss noch an die rechtlichen und faktischen Gegebenheiten der einzelnen Gemeinden angepasst werden. Der Musterordner wird unter Beizug von zwei auf diesem Gebiet spezialisierten Unternehmungen[4] erstellt. Für die Erarbeitung des Musterordners werden drei Pilotgemeinden evaluiert. Es ist vorgesehen, die Vorarbeiten bis Ende Juni 2003 abzuschliessen. Im zweiten Semester des Jahres 2003 erfolgt die Umsetzung in den Gemeinden. Die Registrierung der Datensammlungen innerhalb der kantonalen Verwaltung soll im Jahr 2004 erfolgen.

[4] Eine Unternehmung ist für die Erstellung des Musterregisters zuständig, die andere Unternehmung trägt die Verantwortung für die internetmässige Aufbereitung.

VI. Statistik

	Kurzantworten	Berichte	Empfehlungen	Kontrollen	Vernehmlassungen	Referate	erteilte Kurse	besuchte Weiterbildung
Kantonale Dienste								
Allgemeine Verwaltung								
DIV		4	4	1	1			
JPSD	2		2		1			
EKUD			2					
FMD			2					
BVFD								
öff.-rechtliche Anstalten	1	1	4					
Gerichte								
Kreise								
Gemeindeverbände								
Gemeinden	4	2	3			1	1	
Bürgergemeinden								
Juristische Personen		1	2					
Private Personen	5		3					
Andere						1		2
Total	12	10	22	1	2	2	1	2

VII. Abkürzungsverzeichnis

Abs.	Absatz
Art.	Artikel
AS	Amtliche Sammlung der Bundesgesetze und Verordnungen (Eidgenössische Gesetzessammlung; ab 1948: Sammlung der eidgenössischen Gesetze; ab 1987: Amtliche Sammlung des Bundesrechts)
B	Beschluss
BBl	Bundesblatt
BG	Bundesgesetz
BGE	Entscheidungen des Schweizerischen Bundesgerichts
BR	Bündner Rechtsbuch
BV	Bundesverfassung
BVFD	Bau-, Verkehrs- und Forstdepartement
DIV	Departement des Innern und der Volkswirtschaft
DSB	Datenschutzbeauftragter
DSG	Eidgenössisches Datenschutzgesetz
DSR	Datenschutzrichtlinien für die kantonale Verwaltung
E.	Erwägung
EDSB	Eidgenössischer Datenschutzbeauftragter
EDV	Elektronische Datenverarbeitung
Eidg.	eidgenössisch
EKUD	Erziehungs-, Kultur- und Umweltschutzdepartement
FMD	Finanz- und Militärdepartement
GIS	Geo-Informationssysteme
GRP	Grossratsprotokoll
Hrsg.	Herausgeber
IPV	Individuelle Prämienverbilligung
JPSD	Justiz-, Polizei- und Sanitätsdepartement
KDSG	Kantonales Datenschutzgesetz
KPVG	Kantonales Gesetz über die Krankenversicherung und Prämienverbilligung
N	Note
OR	Obligationenrecht
PV	Kantonale Personalverordnung
SR	Sammlung der eidgenössischen Gesetze und systematische Sammlung des Bundesrechts (Systematische Rechtssammlung)
vgl.	vergleiche
z.B.	zum Beispiel
ZGB	Zivilgesetzbuch
ZSR	Zeitschrift für Schweizerisches Recht
Ziff.	Ziffer

Impressum

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