Tätigkeitsbericht 2016

Datenschutzbeauftragter des Kantons Graubünden

Datenschutzbeauftragter des Kantons Graubünden

RA Thomas Casanova · Kornplatz 2 · 7002 Chur
Telefon 081 256 55 58 · Telefax 081 256 55 54
dsb@staka.gr.ch

Inhalt

I. Vorwort

Es vergeht kein Jahr, in welchem keine datenschutzrelevanten Entwicklungen vorgestellt werden oder sich bereits auf dem Markt durchgesetzt haben. Smarte Kühlschränke und Heizsysteme, interaktive Bücher oder selbstfahrende Autos werden als selbstverständliche Konsumgüter angepriesen und natürlich auch dementsprechend vermarktet. Diese intelligenten Objekte sollen uns den Alltag vereinfachen und einen Mehrwert schaffen. Kaum einmal werden dabei die Gefahren einer vollumfänglichen Vernetzung kommuniziert. In Anbetracht der sicher unbestreitbaren Vorteile solcher Neuentwicklungen neigt der Konsument dazu, die damit einhergehenden Nachteile zu ignorieren und zu verdrängen. Immer wieder hört man die Aussage, was interessiert einen Grosskonzern meine individuellen Daten. Eine solche Haltung ist zwar nachvollziehbar, darf aber nicht geteilt werden. Daten sind das Gold des digitalen Zeitalters und Gold sollte man nicht ohne Grund verschenken. Auf die eigenen Daten muss Acht gegeben werden. Die Konsumenten haben es letztendlich in der Hand, gegen eine ausufernde Speicherung und Verwertung von Daten anzugehen. Dabei sind sie von der Politik zu unterstützen, indem Rahmenbedingungen geschaffen werden, die eine Entwicklung nicht verhindert, aber in einem Masse kanalisiert, dass die individuellen Freiheitsrechte gewahrt bleiben. Dies ist zugegeben ein schwieriges Unterfangen, indessen ein bedeutender gesellschaftlicher Auftrag.

Kantonaler Datenschutzbeauftragter:

Thomas Casanova

II. Outsourcing – Datenbearbeitung durch Dritte[1]

Unter Outsourcing im öffentlich-rechtlichen Bereich wird der Rückgriff auf die Ressourcen verwaltungsexterner Dritter verstanden, die im Auftrag der Behörde bestimmte Produkte herstellen oder Dienstleistungen erbringen, um die Erfüllung öffentlicher Aufgaben zu ermöglichen oder zu fördern.[2] Ein Outsourcing liegt auch dann vor, wenn eine Behörde innerhalb desselben Kantons eine Auslagerung zu einer anderen öffentlichen Verwaltung vornimmt.[3] Dieser aktuell festzustellenden Tendenz der Auslagerung der Datenverarbeitung folgt auch der Kanton Graubünden, wobei teils auf Cloud Computing gesetzt wird. Die Software, die Speicherkapazität oder die Rechnerleistung wird dabei über ein Netzwerk bedarfsorientiert bezogen, d.h. gemietet.[4]

Selbst wenn ein Outsourcing verschiedene Vorteile mit sich bringt und der Behörde die Konzentration auf ihre Kernkompetenz ermöglicht, darf die datenschutzrechtliche Komponente nicht ausser Acht gelassen werden. Der Aufsatz befasst sich mit den hiesigen gesetzlichen Vorgaben eines Outsourcings durch kantonale Behörden. Oft weisen Auslagerungen insbesondere bei Cloud Computing einen Auslandbezug auf, wodurch die Datenbearbeitung durch Dritte weiteren gesetzlichen Anforderungen genügen muss. Schliesslich wird am Rande die Auswirkungen auf die Verantwortlichkeit und die Rechtsbehelfe betroffener Personen ausgeführt.

---

[1] verfasst von RA Mlaw Flavia Brülisauer.

[2] TRÜEB/ZOBL, Steuerdaten in der Cloud, in: BAERISWYL/RUDIN/HÄMMERLI/SCHWEIZER/KARJOTH/VASELLA (Hrsg.), digma, Zeitschrift für Datenrecht und Informationssicherheit, 16. Jahrgang, Heft 3, Zürich 2016, S. 102 f. Das so verstandene Outsourcing ist abzugrenzen von der Aufgabenprivatisierung (Übertragung öffentlicher Aufgaben an Private).

[3] SURY, Outsourcing bei kantonalen Behörden, in: BAERISWYL/RUDIN/HÄMMERLI/SCHWEIZER/KARJOTH/VASELLA (Hrsg.), digma, Zeitschrift für Datenrecht und Informationssicherheit, 16. Jahrgang, Heft 3, Zürich 2016, S. 108.

[4] EIDGENÖSSISCHER DATENSCHUTZ- UND ÖFFENTLICHKEITSBEAUFTRAGTER (EDÖB), Erläuterungen zu Cloud Computing, S. 1, abrufbar unter: https://www.edoeb.admin.ch/datenschutz/00626/00876/01203/index.html?lang=de.

1. Kantonales Outsourcing

Das Datenschutzgesetz sieht vor, dass die Bearbeitung von Personendaten unter gewissen Bedingungen einem Dritten übertragen werden kann.[5] Art. 10a DSG setzt für ein Outsourcing kumulativ voraus, dass sich die Übertragung auf eine Vereinbarung (oder ein Gesetz) stützt, dass die Daten nur so bearbeitet werden, wie der Auftraggeber selbst es tun dürfte, dass keine widersprechenden Geheimhaltungsverpflichtungen vorliegen und dass die Datensicherheit und deren Überwachung gewährleistet sein muss.[6]

1.1. Vereinbarung (oder Gesetz)

Die Auslagerung einer Datenbearbeitung hat auf einer Vereinbarung zwischen der Behörde und dem Dritten zu beruhen. Vor dem Hintergrund, dass derjenige, der Personendaten übermittelt, nachzuweisen hat, dass er alle erforderlichen Massnahmen zur Gewährleistung eines angemessenen Schutzniveaus getroffen hat, empfiehlt es sich, sämtliche Subunternehmer in die Vereinbarung miteinzubeziehen.[7]

1.2. Bearbeitung wie Auftraggeber

Die Daten dürfen vom Auftragnehmer nach Art. 10a Abs. 1 lit. a DSG zudem nur so bearbeitet werden, wie der Auftraggeber selbst es tun dürfte. Die Bedingung ist dahingehend zu konkretisieren, als dass der Auftragnehmer die Daten nur so bearbeiten darf, wie ihn der Auftraggeber darüber hinaus ermächtigt.[8]

---

[5] Art. 10a des Datenschutzgesetzes (DSG; SR 235.1) i.V.m. Art. 2 Abs. 2 des Kantonalen Datenschutzgesetzes (KDSG; BR 171.100). Die Vorschriften des Bundesgesetzes für die Bearbeitung von Personendaten durch Bundesorgane finden auf kantonaler Ebene sinngemäss Anwendung. Im Nachfolgenden wird daher direkt auf die Bestimmungen des DSG Bezug genommen.

[6] Art. 10a Abs. 1 und 2 DSG; BAERISWYL, in: BAERISWYL/PÄRLI (Hrsg.) Handkommentar DSG, Bern 2015, N 18 zu Art. 10a DSG.

[7] EDÖB, Erläuterungen zu Cloud Computing, a.a.O., S. 3. Zur Verantwortlichkeit siehe nachfolgend Ziffer 3.

[8] BAERISWYL, a.a.O., N 24 zu Art. 10a DSG.

1.3. Geheimhaltungspflichten

Im Weiteren dürfen einem Outsourcing keine Geheimhaltungspflichten wie Amts-, Spezial- oder auch Berufsgeheimnisse[9] entgegenstehen. Dies heisst allerdings nicht, dass jede Geheimhaltungspflicht eine Bearbeitung durch Dritte ausschliesst.[10] Wird dem Auftragnehmer vertraglich die Geheimhaltungspflicht überbunden, steht das Amtsgeheimnis einem Outsourcing grundsätzlich nicht entgegen. Bei den Spezialgeheimnissen verhält es sich grundsätzlich gleich.[11] Dagegen ist das Berufsgeheimnis «differenziert zu betrachten».[12] Besondere Probleme ergeben sich schliesslich, wenn die Datenbearbeitung durch einen Auftragnehmer im Ausland erfolgen soll, da Geheimhaltungspflichten nach schweizerischem Recht im Ausland nicht denselben Schutz geniessen wie im Inland.[13]

1.4. Gewährleistung der Datensicherheit

Dem Auftraggeber obliegt es schliesslich neben der inhaltlichen Definition der spezifischen organisatorischen und technischen Massnahmen[14], sich darüber vor allem auch zu vergewissern.[15] «Dies bedeutet in erster Linie, dass der Auftraggeber dem Auftragnehmer klare Vorgaben für Sicherheitsmassnahmen macht und deren Umsetzung und Einhaltung kontrolliert. […] Der Auftraggeber hat sich generell zu versichern, dass die in seinem Bereich angemessenen Sicherheitsmassnahmen umgesetzt werden und kann sich nicht darauf verlassen, dass der Auftragnehmer diese selbständig umsetzt.»[16] Darüber hinaus hat die auslagernde Behörde ganz allgemein den Sorgfaltspflichten hinsichtlich Auswahl, Instruktion und Überwachung des Dritten nachzukommen.[17]

---

[9] Vgl. u.a. Art. 320 f. des Schweizerisches Strafgesetzbuches (StGB; SR 311.0).
[10] BAERISWYL, a.a.O., N 29 zu Art. 10a DSG.
[11] BAERISWYL, a.a.O., N 33 f. zu Art. 10a DSG.
[12] BAERISWYL, a.a.O., N 35 f. zu Art. 10a DSG; ausführlich dazu WOHLERS, Outsourcing durch Berufsgeheimnisträger, in: BAERISWYL/RUDIN/HÄMMERLI/SCHWEIZER/KARJOTH/VASELLA (Hrsg.), digma, Zeitschrift für Datenrecht und Informationssicherheit, 16. Jahrgang, Heft 3, Zürich 2016, S. 114 ff.
[13] BÜHLER/RAMPINI, in: MAURER-LAMBROU/BLECHTA (Hrsg.), Basler Kommentar DSG, 3. A., Basel 2014, N 15 zu Art. 10a DSG.
[14] Vgl. dazu Art. 8–10 der Verordnung zum Bundesgesetz über den Datenschutz [VDSG; SR 235.11]).
[15] BAERISWYL, a.a.O., N 37 f. zu Art. 10a DSG.
[16] BAERISWYL, a.a.O., N 37 f. zu Art. 10a DSG. Vgl. auch Art. 6 Abs. 4 und Art. 8 Abs. 4 VDSG.
[17] BBl 1988, 463; SURY, a.a.O., S. 111.

2. Datenübermittlung ins Ausland[18]

Die aufgezeigten gesetzlichen Anforderungen an ein Outsourcing gelten unabhängig davon, ob die Datenbearbeitung durch einen Auftragnehmer im In- oder Ausland erfolgt. Befindet er sich im Ausland, gelten zusätzlich die Vorgaben von Art. 6 DSG.[19] Danach dürfen Personendaten nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet wird, namentlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet.[20] Unter diesen Umständen dürfen Personendaten nur ins Ausland bekannt gegeben werden, wenn eine der in Art. 6 Abs. 2 DSG aufgeführten Bedingungen erfüllt sind.[21] Fehlt eine Gesetzgebung, die einen angemessenen Schutz gewährleistet, können Personendaten ins Ausland danach bekannt gegeben werden, wenn beispielsweise durch Vertrag ein angemessener Schutz im Ausland gewährleistet wird, die betroffene Person einwilligt oder die Bekanntgabe im Einzelfall für die Wahrung der überwiegenden öffentlichen Interessen oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich ist.[22]

Korrigenda

Im Tätigkeitsbericht 2015, S. 11, wurde über die Nutzung der Online-Bibliothek berichtet. Entgegen dieser Ausführungen erlangt die Kantonsbibliothek keine Kenntnisse über Recherchedetails von der Nutzung der E-Bibliothek. Das Protokoll zeigt anonymisierte Benutzerdaten an, gestützt darauf die Bibliothek zugeordnet und die Rechnung erstellt werden kann. Die Rechnung der E-Bibliothek an die Kantonsbibliothek kann nicht mit Anmeldekennwörtern von Nutzern versehen werden, da die E-Bibliothek keine Kenntnisse über diese Kennwörter besitzt.

[18] Das allgemeine Zugänglichmachen von Personendaten mittels automatischer Informations- und Kommunikationsdienste wie Internet zwecks Information der Öffentlichkeit gilt nicht als Datenübermittlung ins Ausland (Art. 5 VDSG, EDÖB, Erläuterungen zur Übermittlung von Personendaten ins Ausland nach revidiertem DSG, S. 4, abrufbar unter: https://www.edoeb.admin.ch/datenschutz/00626/00753/index.html?lang=de).

[19] EDÖB, Datenübermittlung ins Ausland im Rahmen eines Outsourcing, S. 1, abrufbar unter: https://www.edoeb.admin.ch/dokumentation/00153/00184/00189/index.html?lang=de; a.M. BAERISWYL, a.a.O., N 43 zu Art. 10a DSG.

[20] Art. 6 Abs. 1 DSG. Die Angemessenheit ist unter Berücksichtigung der im betreffenden Staat anwendbaren Rechtsvorschriften allgemeiner und sektorieller Art zu beurteilen. Dabei sind das Übereinkommen STE 108 und die im Zusatzprotokoll aufgestellten Grundsätze in der Gesetzgebung und in der Rechtspraxis miteinzubeziehen, EDÖB, Erläuterungen zur Übermittlung von Personendaten ins Ausland nach revidiertem DSG, a.a.O., S. 5 f. Der EDÖB publiziert eine Liste jener Staaten, welche die entsprechenden Anforderungen erfüllen: https://www.edoeb.admin.ch/datenschutz/00626/00753/index.html?lang=de.

[21] EDÖB, Erläuterungen zu Cloud Computing, a.a.O., S. 3.

[22] Art. 6 Abs. 2 DSG. Weitere Ausführungen dazu in EDÖB, Erläuterungen zur Übermittlung von Personendaten ins Ausland nach revidiertem DSG, a.a.O., S. 6 ff. In den Fällen von Art. 6 Abs. 2 lit. a und g DSG obliegt dem Inhaber einer Datensammlung gegenüber dem EDÖB zudem eine Informationspflicht (Art. 6 Abs. 3 DSG i.V.m. Art. 6 VDSG). Die Information soll dem EDÖB ermöglichen, die Angemessenheit der Schutzmassnahmen zu prüfen, so EDÖB, Erläuterungen zur Übermittlung von Personendaten ins Ausland nach revidiertem DSG, a.a.O., S. 10 f.

Nach Einschätzung des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten wird in vielen Fällen der Auftraggeber daher nicht umhin kommen, mit dem Auftragnehmer vertragliche Datenschutzgarantien abzuschliessen.[23] Die Datenschutzkonformität einer Datenübermittlung ist dabei aufgrund der gesamten Umstände der Bekanntgabe im Einzelfall zu beurteilen.[24]

3. Verantwortlichkeit

Die Datenbearbeitung durch verwaltungsexterne Stellen ist nach dem Gesagten zugelassen, wobei allerdings die Verantwortlichkeit für den Datenschutz bei der auslagernden Behörde verbleibt.[25] Mit anderen Worten haftet der Inhaber der Datensammlung für Nachteile, die sich aus einer Verletzung seiner Sorgfaltspflicht ergeben.[26] Auch bei einer Verletzung der Geheimhaltungspflichten durch den Dritten haftet die Behörde gegenüber der betroffenen Person. Der Auftraggeber ist daher gut beraten, wenn er die vertragliche Geheimhaltungspflicht mit einer Konventionalstrafe absichert.[27]

Neben den Rechtsbehelfen von Art. 28 ZGB kann die betroffene Person insbesondere verlangen, dass die Datenbearbeitung gesperrt wird, keine Daten an Dritte bekannt gegeben oder die Personendaten berichtigt oder vernichtet werden.[28] Nach Ansicht von TRÜEB und ZOBL steht es der in ihrer Persönlichkeit verletzten Person frei, zusätzlich gegen den Auftragnehmer beziehungsweise solidarisch gegen den Auftraggeber und den Auftragnehmer vorzugehen.[29] Bei einer Datenübermittlung ins Ausland wird die betroffene Person von dieser Alternative nicht zuletzt aufgrund eines allfälligen ausländischen Gerichtsstandes wohl absehen.

---

[23] EDÖB, Erläuterungen zu Cloud Computing, a.a.O., S. 3.

[24] EDÖB, Erläuterungen zur Übermittlung von Personendaten ins Ausland nach revidiertem DSG, a.a.O., S. 4.

[25] Art. 10a und 16 DSG. Vgl. statt vieler BAERISWYL, a.a.O., N 2 zu Art. 10a DSG; EDÖB, Erläuterungen zur Übermittlung von Personendaten ins Ausland nach revidiertem DSG, a.a.O., S. 11; SURY, a.a.O., S. 111.

[26] Vgl. statt vieler EDÖB, Erläuterungen zur Übermittlung von Personendaten ins Ausland nach revidiertem DSG, a.a.O., S. 11.

[27] BAERISWYL, a.a.O., N 30 zu Art. 10a DSG.

[28] Art. 15 DSG.

[29] TRÜEB/ZOBL, Steuerdaten in der Cloud, a.a.O., S. 107.

4. Würdigung

Selbst wenn ein Outsourcing heutzutage vermehrt eingesetzt wird, darf nicht leichthin davon ausgegangen werden, dass die Datenbearbeitung durch Dritte keine Risiken in sich birgt. Entsprechend hoch ist der Massstab bei der Auswahl, Instruktion und vor allem auch bei der regelmässigen Überwachung des Auftragnehmers anzusetzen. Die organisatorischen und technischen (Sicherheits-)Massnahmen haben zudem jederzeit gewährleistet zu sein. Allein mit der Vereinbarung über die Einhaltung der datenschutzrechtlichen Vorgaben ist es somit nicht getan, wobei ein Auslandbezug weitere Schwierigkeiten mit sich bringt. So fehlt bei Cloud Computing oft die Übersicht, wo genau die Daten gespeichert sind, was eine Gewährleistung der Datensicherheit nur schwer zulässt.

Akteneinsicht betreffend IV-Akten

Gemäss Art. 47 ATSG steht der berechtigten Person grundsätzlich ein Akteneinsichtsrecht zu, sofern keine überwiegenden Privatinteressen entgegenstehen.

Das Recht auf Einsicht in die Akten eines laufenden Verfahrens ist Teilgehalt des verfassungsmässigen Anspruchs auf rechtliches Gehör (Art. 29 Abs. 2 BV). Das Akteneinsichtsrecht stellt sicher, dass am Verfahren beteiligte Personen die Entscheidgrundlagen kennen und sich wirksam zur Sache äussern können.[1] Das Recht auf Akteneinsicht gilt indessen nicht absolut. Es kann wie jeder grundrechtliche Anspruch unter den Voraussetzungen von Art. 36 BV eingeschränkt werden. Als Gründe der Verweigerung nennen die Spezialgesetze als auch das Datenschutzgesetz ein überwiegendes öffentliches oder privates Interesse sowie eine besondere gesetzliche Grundlage. Bei der Einsichtnahme in IV-Akten fällt ein überwiegendes öffentliches Interesse offensichtlich ausser Betracht. Ebenso sind in der Regel keine schutzwürdigen Drittinteressen erkennbar. Schliesslich sieht Art. 47 ATSG eine Akteneinsicht ausdrücklich vor. Zu berücksichtigen ist jedoch Art. 47 Abs. 2 ATSG. Stellt sich die IV auf den Standpunkt, eine Bekanntgabe könne sich auf die Gesundheit des Berechtigten nachteilig auswirken, hat sie dem Gesuchsteller diesen Umstand bekannt zu geben. Dieser hat sodann die Möglichkeit, einen Arzt zu bestimmen, der seine Interessen wahrnimmt.

[1] MARK HÄUSLER/RETO FERRARI-VISCA, Das Recht auf Akteneinsicht im Verwaltungs- und Verwaltungsjustizverfahren in: Jusletter 8. August 2011.

III. Fälle aus der Praxis

1. Zugriff auf das Personen- und Objektregister

Gestützt auf Art. 451 Abs. 2 ZGB kann jedermann, der ein Interesse glaubhaft macht, von der Erwachsenenschutzbehörde Auskunft über das Vorliegen und die Wirkungen einer Massnahme des Erwachsenenschutzes verlangen. Bis anhin erhielten die Betreibungs- und Konkursämter von den Erwachsenenschutzbehörden jeweils Auskunft über die sie interessierenden Massnahmen. Mit Einführung des Gesetzes über die Einwohnerregister und weitere Personen- und Objektregister (ERG) wurde eine Datenplattform geschaffen, auf welche verschiedenste Institutionen Zugriff über ein Abrufverfahren haben.

In Art. 32 ERG wird auf den Datenschutz explizit Bezug genommen. In dieser Bestimmung wurde auch die Voraussetzung für die grundsätzliche Weitergabe von Daten geschaffen. Art. 30b ERG konkretisiert den Zugriff über ein Abrufverfahren. Danach erhalten Dienststellen des Kantons, die von der Regierung bezeichneten öffentlich-rechtlichen Anstalten des Kantons und Gemeinden das Recht, online Daten abzufragen. Das sogenannte Abrufverfahren ist ein automatisiertes Verfahren, welches die Bekanntgabe von Personendaten an Dritte ohne Intervention des bekanntgebenden Organs durch Abruf ermöglicht. Der Datenherr verliert komplett die Kontrolle über die Bearbeitung der Personendaten, da das informationssuchende Organ sich diese selber zielgerichtet beschaffen kann und sein Gesuch nicht begründen muss. Art. 19 Abs. 3 Satz 1 DSG fordert für die Bekanntgabe ordentlicher Personendaten eine materielle gesetzliche Grundlage, während das Abrufverfahren für die Zugänglichmachung besonders schützenswerter Personendaten sowie Persönlichkeitsprofile in einem Gesetz im formellen Sinn ausdrücklich vorgesehen sein muss. Die formell-gesetzliche Grundlage allein, die nur die für die Bearbeitung erforderlich machenden Aufgaben regelt, genügt jedoch nicht; vielmehr müssen das Organ, welches Zugang hat, der Zugangszweck und der Umfang der Zugangsberechtigung bezeichnet werden.[1]

[1] JENNIFER EHRENSPERGER in: MAURER-LAMBROU/BLECHTA (Hrsg.), Basler Kommentar zum Datenschutz- und Öffentlichkeitsgesetz, Art. 19, N 52; WALDMANN/BICKEL in: BELSER/EPINEY/WALDMANN (Hrsg.), Datenschutzrecht, §12, N 97.

Es stellt sich nun die Frage, ob für den Datenaustausch zwischen dem zentralen Personen- und Objektregister und einem Betreibungs- und Konkursamt die erforderlichen gesetzlichen Grundlagen gegeben sind und ob ein Betreibungs- und Konkursamt überhaupt Zugriff auf die Daten des Personen- und Objektregisters haben kann. Gemäss Art. 30b ERG haben Dienststellen des Kantons, speziell bezeichnete öffentlich-rechtliche Anstalten des Kantons sowie Gemeindebehörden Zugriff auf die Daten der Datenplattform. In Art. 20 ff. ERV wird der Datenaustausch mit den einzelnen Institutionen näher beschrieben. Es geht insbesondere um den Datenaustausch mit dem Bund, zwischen den Gemeinden und dem Kanton.

Kann nun ein Betreibungs- und Konkursamt als Dienststelle des Kantons qualifiziert werden? Gemäss Art. 1 SchKG bildet das Gebiet jedes Kantons für die Durchführung der Schuldbetreibungen und der Konkurse einen oder mehrere Kreise. Die Kantone bestimmen Zahl und Grösse der Kreise.

Der Kanton haftet für Schäden, den die für die Durchführung verantwortlichen Personen widerrechtlich verursachen (Art. 5 SchKG). Die Organisation der schuldbetreibungsrechtlichen Behörden und die Entschädigung derselben ist grundsätzlich ebenfalls Sache der Kantone. Gemäss Gesetz müssen die Kantone die geschaffenen Kreise allerdings mit Betreibungs- und Konkursämtern versehen und diese mit genügend Personal ausstatten. Streng rechtlich können Betreibungs- und Konkursämter keine Dienststellen des Kantons bilden. In diesem Sinne äussert sich auch der Gesetzgeber: «Wollen andere Behörden oder Institutionen einen Zugriff auf das kantonale Personenregister, so muss dafür grundsätzlich eine spezialgesetzliche Bestimmung vorhanden sein bzw. geschaffen werden. Im ERG selbst wird diesbezüglich nur der Zugriff der kantonalen Verwaltung (Dienststellen), der öffentlich-rechtlichen Anstalten des Kantons und der Gemeinden geregelt.»[2]

Auf S. 25 der Botschaft hält die Regierung ausdrücklich fest: «Aufgrund der subsidiären Anwendbarkeit der kantonalen und eidgenössischen Datenschutzgesetzgebung (also immer dann, wenn das ERG keine abschliessenden Regelungen enthält) und somit gestützt auf Art. 2 Abs. 2 KDSG in Verbindung mit Art. 17 Abs. 2 DSG darf auf besonders schützenswerte

[2] Botschaft der Regierung an den Grossen Rat, Heft Nr. 1, 2014–2015, S. 24.

Fahrbewilligung ins Dischmatal

Im Dischmatal besteht vom 20. Dezember bis 31. März eine Sperrung für den Individualverkehr. Es gelten aber verschiedene Ausnahmen. Wenn nun ein Fahrzeuglenker der Ansicht ist, auf ihn sei dieser Ausnahmekatalog anwendbar, muss er den dafür bestimmten Umstand nachweisen. Im Datenschutzrecht ist das Prinzip der Verhältnismässigkeit verankert. Eine Behörde kann also diejenigen Daten anfordern, die erforderlich sind, um den gesetzlichen Auftrag zu erfüllen. Es ist kein Verstoss gegen den Datenschutz erkennbar, wenn die Gemeinde verlangt, dass eine Person, die eine Bewilligung wünscht, mitteilt, gestützt auf welchen Bewilligungsgrund sie einen Anspruch auf die Ausstellung einer Fahrbewilligung geltend macht. Die Befreiung von der Bewilligungspflicht zieht keinen Datenaustausch mit sich und ist datenschutzrechtlich unproblematisch.

Personendaten nur unter weitergehenden Voraussetzungen zugegriffen werden, namentlich wenn ein spezielles Gesetz konkret den Zugriff erlaubt oder es für eine in einem Gesetz im formellen Sinn klar umschriebene Aufgabe unentbehrlich ist. Sollten solche Daten im Personenregister geführt sein und sollte eine Dienststelle bzw. eine öffentlich-rechtliche Anstalt oder eine kommunale Behörde Zugriff auf solche Daten benötigen, muss folglich dafür gesorgt sein, dass die Voraussetzungen erfüllt sind.»

Klarerweise kann festgestellt werden, dass das Gesetz über Einwohnerregister und weitere Personen- und Objektregister keine genügende gesetzliche Grundlage für die Betreibungs- und Konkursämter bildet, um im Rahmen eines Abrufverfahrens auf besonders schützenswerte Personendaten zugreifen zu können, welche auf der kantonalen Datenplattform gespeichert werden. Art. 451 ZGB kann ganz offensichtlich nicht als Grundlage für die Installation eines Abrufverfahrens gelten.

2. *Weitergabe von Einwohnerdaten an die Landeskirchen*

Das kantonale Datenschutzgesetz gilt auch für die Kirchgemeinden. Es stellt sich vorliegend die Frage, ob ein Einwohnerdienst Mutationen betreffend Mitglieder der Landeskirche an die zuständige innerkirchliche Institution weiterleiten darf. Mangels einer gesetzlichen Grundlage kann ein Online-Zugriff (Abrufverfahren) nicht eingerichtet werden (vgl. Art. 19 Abs. 3 DSG); dies vorneweg. Eine Weiterleitung von Daten kann also nur im Einzelfall ausgelöst durch die Einwohnerdienste erfolgen. Zudem werden unter dem Titel Zweck und Zugriff in Art. 30b ERG die Behörden genannt, welche Zugriff auf die Daten der Gemeinden, welche auf einer Datenplattform verwaltet werden, erhalten. Die Aufzählung ist abschliessend. Öffentlich-rechtliche Körperschaften werden nicht genannt. Danach erhalten die Landeskirchen keinen Zugriff auf diese Datenplattform.

Gemäss Art. 3 lit. c Ziff. 1 DSG werden Daten über die religiösen Ansichten oder Tätigkeiten als besonders schützenswert qualifiziert. In diesem Zusammenhang stellt sich die Frage, ob Daten über die Mitgliedschaft in einer Landeskirche als sensitiv gelten. Der DSB Graubünden nimmt mit Bezug darauf eine offene Haltung ein. Vor dem Hintergrund der Definition der besonders schützenswerten Personendaten, wonach diese die Persönlichkeit der betroffenen Person in erhöhtem Masse berühren, insbesondere wenn sie den Geheimbericht, das Privatleben oder das Ansehen und die soziale Geltung betreffen[1], weist die Nennung der Konfession bzw. die Mitgliedschaft in einer Landeskirche keinen erhöhten Schutzbereich auf. Diese Meinung wird jedoch von der herrschenden Lehre nicht geteilt. Danach gelten Angaben zur Konfession als besonders schützenswert[2]. Gemäss Art. 17 Abs. 2 DSG bedarf es für die Bearbeitung besonders schützenswerter Personendaten einer besonderen gesetzlichen Grundlage. Dazu gehört ebenfalls die Weitergabe von Daten (vgl. Art. 3 lit. e DSG). Gestützt auf Art. 1 Abs. 1 ERG in Verbindung mit Art. 6 lit. l Bundesgesetz über die Harmonisierung der Einwohnerregister und anderer amtlicher Personenregister (RHG[3]), enthält das Einwohnerregister die Angaben zur Zugehörigkeit zu einer öffentlich-rechtlichen oder

[1] Botschaft DSG, S. 446, BBl 1988 II 413–534.

[2] GABOR P. BLECHTA in: MAURER-LAMBROU/BLECHTA (Hrsg.), Basler Kommentar zum Datenschutz- und Öffentlichkeitsgesetz, Art. 3, N 32; YVONNE JÖHRI in: Handkommentar zum Datenschutzgesetz, Art. 3, N 47; BEAT RUDIN in: Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Zürich, §3, N 21; BEAT RUDIN in: Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Basel-Stadt, §3, N 36.

[3] SR 431.02.

Abrufverfahren

Die gesetzliche Grundlage für ein Abrufverfahren findet sich in Art. 19 Abs. 3 DSG. Personendaten dürfen nur im Abrufverfahren zugänglich gemacht werden, wenn dies ausdrücklich vorgesehen ist. Es gelten also erhöhte Anforderungen an die Rechtsgrundlage. Art. 19 Abs. 3 Satz 1 DSG fordert für die Bekanntgabe ordentlicher Personendaten eine materielle gesetzliche Grundlage, während das Abrufverfahren für die Zugänglichmachung besonders schützenswerter Personendaten sowie Persönlichkeitsprofile in einem Gesetz im formellen Sinn ausdrücklich vorgesehen sein muss.

Der EDÖB hat die Anforderungen an die Rechtsgrundlagen u.a. wie folgt konkretisiert: «Wird im Zusammenhang mit dem Abrufverfahren ein grosses und verzweigtes EDV-System bei der Datenbearbeitung eingesetzt, in welchem in erheblichem Umfang und von verschiedenen Personendaten, namentlich besonders schützenswerte Personendaten oder Persönlichkeitsprofile bearbeitet werden, muss dieses ebenfalls im Gesetz im formellen Sinn ausdrücklich erwähnt werden. Zudem wird bei Zugriff von verschiedenen Behörden oder der Verknüpfung von Datensammlungen vom verantwortlichen Organ ein Bearbeitungsreglement verlangt.»

Es entscheidet diejenige Behörde, welche die Datenherrschaft über Personendaten ausübt, ob ein Abrufverfahren verankert werden soll. Allein schon aus Gründen der Transparenz muss im jeweiligen Gesetz, gestützt worauf Personendaten bearbeitet werden, das Abrufverfahren legiferiert werden.

auf andere Weise vom Kanton anerkannten Religionsgemeinschaft. Die gesetzliche Grundlage für die Bearbeitung dieser Daten ist damit gegeben.

Für die Erfüllung der Aufgaben einer Landeskirche sind diese darauf angewiesen, dass sie über die Mutationen in ihrem Mitgliederkreis orientiert werden. Die Zugehörigkeit zur entsprechenden kantonalen oder kommunalen Landeskirche ist abhängig vom Wohnsitz. Nur die Einwohnerdienste sind verbindlich in der Lage, über An- und Abmeldungen von Einwohnern Auskunft zu erteilen. Nun dürfen Behördendaten bekannt geben, wenn diese für den Empfänger im Einzelfall für die Erfüllung seiner gesetzlichen Aufgaben unentbehrlich sind (Art. 19 Abs. 1 lit. a DSG). Art. 32 Abs. 2 ERG sieht des Weiteren eine Datenbekanntgabe vor, wenn ein Interesse glaubhaft gemacht wird. In Anwendung der vorgenannten Bestimmungen sind die Einwohnerdienste berechtigt, den Landeskirchen Mutationsmeldungen über Angehörige ihrer Mitglieder bekannt zu geben.

Mühe bereitet die Datenbekanntgabe von Zuzügern, die keine Religions- bzw. Konfessionsangehörigkeit angeben. Die Einwohnerregister sind gesetzlich verpflichtet, die Zugehörigkeit zu einer öffentlich-rechtlichen Religionsgemeinschaft zu prüfen (vgl. Art. 6 lit. l RHG). Im Zusammenhang mit dem Zuzug von Personen, die keine Angaben zur Religionszugehörigkeit machen, kann dies für einen Einwohnerdienst zu Abklärungen führen. Gemäss Art. 10 RHG müssen die Kantone die notwendigen Vorschriften für den Datenaustausch beim Weg- oder Zuzug von Einwohnerinnen und Einwohnern regeln. Der Austausch findet elektronisch und in verschlüsselter Form statt (Art. 10 Abs. 2 RHG). Folgerichtig wird ein Einwohnerdienst in Kenntnis gesetzt, ob eine Diskrepanz zwischen den

Angaben des Zuzügers und den gespeicherten Daten des Wegzugortes besteht. In einem solchen Fall ist der Einwohnerdienst gestützt auf das Prinzip der Datenintegrität verpflichtet, diesen Umstand zu klären. Die Landeskirchen sind höchstens ausnahmsweise miteinzubeziehen.

Es kann festgestellt werden, dass die Landeskirchen auf die Zusammenarbeit mit den Einwohnerdiensten angewiesen sind und berechtigterweise Mutationsmeldungen ihrer Mitglieder seitens der Einwohnerdienste erhalten dürfen.

Sperrrecht

Eine Person, welche ihre persönlichen Daten gesperrt haben will, hat ein schutzwürdiges Interesse glaubhaft zu machen (Art. 20 DSG). An diese Voraussetzung dürfen keine hohen Anforderungen gestellt werden. Eine Datensperre wirkt nicht absolut. Sie steht unter dem Vorbehalt von Art. 19 Abs. 1bis DSG. Es ist also möglich, gesperrte Daten inner- und ausserkantonal an Amtsstellen bekannt zu geben. Art. 20 Abs. 2 lit. b DSG lässt die Bekanntgabe zu, wenn eine Behörde dadurch gehindert würde, seine Aufgabe ordnungsgemäss zu erfüllen. Aus diesem Grund dürfte eine bestehende Datensperre im Verkehr mit anderen Behörden in der Regel ohne Wirkung bleiben.[1] Stichwortartig lässt sich ausführen:

In Graubünden ist eine Datensperre möglich. Der Betroffene muss sich an jede Amtsstelle einzeln wenden und mitteilen, welche Daten er gesperrt haben will. Eine besondere Form wird an diese Anfrage nicht gestellt.

Grundsätzlich ist es so, dass gesperrte Daten an andere Amtsstellen weitergegeben werden, wenn eine gesetzliche Grundlage besteht oder die Amtsstelle nachweisen kann, dass sie für die Erfüllung der eigenen Aufgabe darauf angewiesen ist.

Die Datensperre muss den Amtsstellen, an welche damit belastete Personendaten weitergegeben werden, mitgeteilt werden. Auch diese Amtsstellen sind an die Datensperre gebunden.

[1] JANA MOSER in: MAURER-LAMBROU/BLECHTA (Hrsg.), Basler Kommentar zum Datenschutz- und Öffentlichkeitsgesetz, Art. 20, N 16.

3. Weitergabe von Patientendaten an die SUVA/UVG-Versicherer

Die Unfallversicherer müssen zweckbestimmt immer wieder medizinisches Fachwissen von Ärzten nutzen, verfügen aber über keine gesetzliche Regelung, welche den Beizug oder die Einsetzung von Vertrauensärzten vorsieht. Die Datenbekanntgabe hat daher direkt an den Unfallversicherer zu erfolgen. Der Umfang der Datenbekanntgabe ist in Art. 54a UVG und in Art. 69a Abs. 1 UVV geregelt. Diese Bestimmungen stellen einen gesetzlichen Rechtfertigungsgrund gemäss Art. 17 Abs. 2 DSG dar, weshalb der behandelnde Arzt und andere Leistungserbringer von der Schweigepflicht gemäss Art. 321 StGB entbunden sind. Art. 54a UVG, Art. 69a Abs. 1 lit. a–c UVV und Art. 97 UVG stellen genügende gesetzliche Grundlagen dar für die Datenbekanntgabe des Arztes bzw. des Leistungserbringers an den Unfallversicherer und sind massgebend für die Art und den Umfang deren Auskunftserteilung. Eine Datenbekanntgabe im Rahmen dieser Gesetzesbestimmungen schliesst eine Verletzung des Berufs- und/oder des Amtsgeheimnisses aus. Eine Ermächtigung des Patienten bzw. der versicherten Person ist im Einzelfall nicht erforderlich.

Gestützt auf diese Ausgangslage fragt ein Unfallversicherer ein Spital an, ob der Berichtsversand von Austritts-, OP-, Notfall- und Sprechstundenberichten sowie Berichten zur MRI/CT-Bildgebung neu nicht unaufgefordert, d.h. ohne Nachfrage des Unfallversicherers, erfolgen könne.

Es ist nun tatsächlich so, dass die Kompetenzen des Unfallversicherers weiter gehen als diejenigen des Krankenversicherers. Dennoch ist auch die Unfallversicherung an das allgemeine Prinzip der Verhältnismässigkeit gebunden (vgl. Art. 4 Abs. 2 DSG). Aufbauend auf dem vorgenannten Grundsatz darf der Unfallversicherer diejenigen Akten anfordern, die erforderlich und notwendig sind für die Abklärung, ob es sich um einen Unfall handelt, die Behandlung adäquat ist oder weitergehende medizinische Massnahmen erforderlich sind. In der Regel wird der Unfallversicherer auf die Austritts-, OP-, Notfall- und Sprechstundenberichte sowie bildgebende Unterlagen angewiesen sein. Diese Frage kann jedoch nicht abschliessend beantwortet werden. Vielmehr ist festzustellen, ob es einen Grundbedarf von Akten gibt, die in jedem Fall für die seriöse Abklärung eines Falles erforderlich sind. Wenn dem so ist, kann ein Spital ohne weiteres diese Unterlagen unaufgefordert dem Unfallversicherer mitteilen. Es handelt sich dabei nicht um einen automatischen Informationsaustausch (Abrufverfahren). Dieses zeichnet sich bekanntlich dadurch aus, dass der Datenherr die Herrschaft über die eigenen Daten verliert. Vorliegend entscheidet indessen immer das Spital, ob und welche Daten gelie-

fert werden. Auch wenn grundsätzlich unaufgefordert Daten übermittelt werden, kann das Spital jederzeit intervenieren und in speziellen Einzelfällen eine andere Praxis anwenden. Gegen eine unaufgeforderte Berichterstattung ist aus datenschutzrechtlicher Sicht nichts einzuwenden. Kriterium muss jedoch die Relevanz der Daten für die Bearbeitung des Falles durch den Unfallversicherer sein. Wenn gewährleistet wird, dass ein Grundstock an Unterlagen in jedem Fall gebraucht wird, können diese unaufgefordert zugestellt werden.

Der Unfallversicherer hat nur Anspruch auf Daten, die für die Beurteilung der Leistungspflicht erforderlich sind. Einer Lösung, wonach automatisch sämtliche Daten unaufgefordert an den Unfallversicherer weitergeleitet werden, kann deshalb nicht beigepflichtet werden. Ein solches System kann auch nicht eingeführt werden, zumal eine ungeprüfte Übermittlung von sämtlichen Spitalakten an den Unfallversicherer faktisch einem Abrufverfahren gleich käme. Dafür fehlt aber ganz offensichtlich die gesetzliche Grundlage.

Private Daten auf dem Geschäftscomputer

Ein Grundsatz lautet: Privates bleibt privat. Der Arbeitgeber hat grundsätzlich kein Recht, auf die privaten Daten zu greifen. Wenn der Arbeitgeber seinen Arbeitenden erlaubt, ein als privat bezeichnetes Laufwerk zu betreiben, gibt er gleichzeitig sein Einverständnis, in einem vertretbaren Mass private Daten auf dem Geschäftscomputer zu halten. Diesen Umstand hat er zu respektieren. Die Dienststelle hat kein Zugriffsrecht auf diese Daten. Vermutet der Arbeitgeber, auf diesem Laufwerk seien Geschäftsdaten gespeichert, kann er allenfalls die Strafverfolgungsbehörde einschalten. In einer zivilen Auseinandersetzung entscheidet der Richter über eine Edition. Als Sofortmassnahme ist lediglich einer Speicherung dieser Daten denkbar.

4. Absenderadressierung von amtlichen Dokumenten

Die Kantonspolizei Graubünden hat einem fehlbaren Lenker eine Bussverfügung zugestellt. In der Absenderzeile des mit einem Fenster versehenen Couverts konnte für alle erkennbar folgender Absender nachgelesen werden: «Kantonspolizei Graubünden, Verkehrspolizei Radarbüro, Ringstrasse 2, 7000 Chur 1». Es stellt sich die Frage, ob diese Praxis datenschutzrechtlich konform ist.

Der Kanton Graubünden ist bestrebt, gegen aussen einheitlich aufzutreten. In der Verordnung über die Deckung des Bürobedarfs in der Kantonalen Verwaltung[1] wird in Art. 4 u.a. vorgegeben, dass die Gestaltung von Drucksachen einem einheitlichen Erscheinungsbild zu folgen hat. Die Gestaltung im Einzelnen wird von der Drucksachen- und Materialzentrale in einer Richtlinie «Corporate Design» vorgegeben. Konkretisiert wird der einheitliche Auftritt in der Richtlinie zur Umsetzung des Erscheinungsbildes für Drucksachen der Kantonalen Verwaltung. Mit Bezug auf die Adressetiketten bzw. dem Adressfenster verlangt der Kanton die Nennung des zuständigen Amtes mit der Adresse. Für die Einhaltung der Vorgaben gemäss der Richtlinie «Corporate Design» sind die Dienststellen verantwortlich. Die Kantonspolizei Graubünden hat diese Weisung in dem Sinne umgesetzt, dass neben der Amtsstelle zusätzlich die zuständige Abteilung genannt wird (in obenstehendem Beispiel «Verkehrspolizei Radarbüro»). Es stellt sich die Frage, ob die Weisung des Kantons und die Umsetzung durch die Kantonspolizei den datenschutzrechtlichen Vorgaben genügen.

Die Post hat das ausschliessliche Recht, Briefe bis 50g zu befördern (Art. 18 Abs. 1 Postgesetz[2]). Im Zusammenhang mit der Beförderung von Briefen macht die Post konkrete Vorgaben betreffend die korrekte Adressierung und Gestaltung[3]. Die Post verlangt neben der Zustelladresse die Angaben des Absenders.

---

[1] BR 170.700.

[2] SR 783.0.

[3] vgl. Weisungen der Post AG betreffend korrekte Adressierung und Gestaltung.

Um einen reibungslosen Postverkehr (insbesondere bei Rücksendungen) abwickeln zu können, ist die Post auf die Bekanntgabe des Absenders angewiesen. Mit Bezug darauf ist sie in die Lage zu versetzen, eine Rücksendung vornehmen zu können. Es genügt bspw. die Bekanntgabe einer Postfachnummer mit dem dazugehörigen Ort. Daher ist der Postkunde relativ frei, welche konkreten Angaben gegenüber der Post gemacht werden sollen.

Demgegenüber verlangt der Kanton in seiner Weisung die Nennung der Amtsstelle mit Adresse. In der Regel ist dieses Vorgehen nicht zu beanstanden. Wenn indessen besonders schützenswerte Personendaten (vgl. Art. 3 lit. c DSG) übermittelt werden, sind erhöhte Anforderungen an die Bekanntgabe der Absenderdaten zu stellen. Der Begriff der besonders schützenswerten Personendaten ist insofern formaler Natur, als die Frage, ob eine Information nach Datenschutzgesetz besonders schützenswert ist, nicht davon abhängt, ob sie vom Datenbearbeiter oder von der betroffenen Person als besonders sensitiv eingestuft wird oder allenfalls unter den Bestimmungen anderer Gesetze besonders geschützt wird. Entscheidend ist allein, ob es sich um Daten handelt, die unter Art. 3 lit. c DSG aufgeführt sind.[4] Im vorliegenden Fall wurden Daten betreffend eine Ordnungsbusse weitergeleitet. Informationen über Ordnungsbussen werden unter den Begriff administrative oder strafrechtliche Verfolgungen und Sanktionen subsumiert und stellen deshalb besonders schützenswerte Personendaten dar.[5] Die Polizei ist deshalb gehalten, möglichst neutrale Angaben bei der Bekanntgabe des Absenders aufzuführen. Zumindest darf aufgrund des Absenders nicht auf das Verfahren geschlossen werden können. Da ein Briefverkehr mit der Polizei sich in der Regel auf ein administratives oder strafrechtliches Verfahren stützt, ist es grundsätzlich empfehlenswert, dass die Kantonspolizei Graubünden in ihrer Absenderliste nicht auf ihr Amt hinweist. Zumindest ist auf die Bezeichnung einer internen Abteilung zu verzichten. Grundsätzlich muss die Post einzig in die Lage versetzt werden, eine Rücksendung vornehmen zu können. Es genügt damit der Hinweis auf den Kanton Graubünden

[4] GABOR P. BLECHTA in: MAURER-LAMBROU/BLECHTA (Hrsg.), Basler Kommentar zum Datenschutz- und Öffentlichkeitsgesetz, Art. 3, N 29.

[5] BEAT RUDIN in: Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Basel-Stadt, §3, N 39.

Veröffentlichung von Fotos

Fotos von Mitarbeitenden sollen im Internet veröffentlicht werden. Massgebend ist Art. 328b OR. Danach darf der Arbeitgeber Daten über den Arbeitnehmer nur bearbeiten, soweit sie dessen Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrages erforderlich sind. Es muss also zwangsläufig eine Interessenabwägung vorgenommen werden, in dem Sinne, dass die Frage beantwortet wird, ob die Veröffentlichung von persönlichen Daten im Internet für die Durchführung des Arbeitsvertrages erforderlich ist. Ein Foto ist nicht Teil der geschuldeten Arbeitsleistung. Ein Arbeitgeber darf nicht ohne Zustimmung des jeweiligen Mitarbeiters Fotos veröffentlichen. Dies betrifft jede Art der Veröffentlichung. Die Verwendung kann auch nicht mit der Loyalitätspflicht des Arbeitnehmers begründet werden, weil sich daraus keine Verpflichtung ergibt, die Veröffentlichung des Fotos zu dulden. Nur wenn das überwiegende berechtigte Interesse des Arbeitgebers die Verwendung des Fotos erfordert, liegt keine Verletzung von schutzwürdigen Geheimhaltungsinteressen vor und ist keine Zustimmung der Mitarbeiter erforderlich. Es liegt also eine Verletzung der Persönlichkeit vor, wenn die betroffene Person keine Einwilligung zum Bild und dessen Veröffentlichung gegeben hat oder die Verletzung nicht durch ein überwiegendes privates oder öffentliches Interesse oder durch ein Gesetz gerechtfertigt ist.

---

[1] vgl. https://www.edoeb.admin.ch/datenschutz/00627/01167/index.html?lang=de

und die Adresse. In der Praxis hat sich jedoch gezeigt, dass der Hinweis auf den Kanton Graubünden ohne Bezeichnung der Dienststelle zu Schwierigkeiten geführt hat. Soll in einem solchen Fall eine Rücksendung richtig zugeordnet werden, müsste zwangsläufig eine Drittperson, die mit dem Fall nichts zu tun hat, die Post öffnen. Im Kanton Graubünden ist es so geregelt, dass nicht eindeutig zustellbare Rücksendungen an die Standeskanzlei gesandt werden, welche die Briefe öffnet und hernach eine interne Verteilung vornimmt. Ein solches Vorgehen ist aus datenschutzrechtlicher Sicht nicht erwünscht. Daher soll die Dienststelle genannt werden.

Die Problematik der dienststelleninternen Zustellung der Post kann auf einfache Weise gelöst werden, indem Abteilungen (sofern sie in der Absenderzeile aufscheinen sollen) anonymisiert werden. Damit ist gewährleistet, dass der interne Postdienst die Rücksendungen richtig zuordnen kann und den Anliegen des Datenschutzes entsprochen wird.

5. Sperrung von Grundbuchdaten

Gemäss Art. 20 DSG kann eine betroffene Person, die ein schutzwürdiges Interesse glaubhaft machen kann, vom verantwortlichen Bundesorgan (und gestützt auf Art. 2 KDSG auch von einem kantonalen Organ) die Bekanntgabe von bestimmten Personendaten sperren lassen. Ein Bundesorgan verweigert die Sperrung, wenn eine Rechtspflicht zur Bekanntgabe besteht (Art. 20 Abs. 2 lit. a DSG).

Der Sinn und Zweck der Sperrung liegt in der Einschränkung der Weiterverbreitung oder -nutzung durch Dritte. Dieser gesetzlich verankerte Anspruch der betroffenen Person entspricht dem Grundgedanken, dass jede Person das Herrschaftsrecht über ihre eigenen Personendaten haben soll. Er entspricht dem Recht auf individuelle, informationelle Selbstbestimmung und entspringt letztlich dem Recht auf persönliche Freiheit.[1] Gemäss Rechtsprechung darf an den Nachweis des schutzwürdigen Interesses keine hohen Anforderungen gestellt werden. Die Befürchtung einer möglichen Gefahr oder auch blossen Schikanen durch die Neugier Dritter ausgesetzt zu sein, genügt. Ein weitergehender Beweis, insbesondere konkrete Hinweise, dass sich eine Gefahr verwirklicht oder Schikanen tatsächlich vorkommen, sind nicht erforderlich.[2]

Näher abzuklären ist der Ausnahmetatbestand von Art. 20 Abs. 2 lit. a DSG. Gemäss dieser Bestimmung kann das Sperrrecht dort nicht durchgesetzt werden, wo die Behörde einer Rechtspflicht zur Bekanntgabe von Personendaten untersteht; die Behörde verfügt in diesem Fall über keinerlei Ermessensspielraum betreffend eine Datensperre. Für eine individuelle Interessenabwägung bleibt in diesem Fall kein Raum.[3] Vorliegend ist nun abzuklären, ob ein Eigentümer das Recht besitzt, seine im Grundbuch eingetragenen Eigentümerrechte sperren zu lassen. In diesem Zusammenhang stellt sich die Frage, ob Art. 970 ZGB und Art. 146c EGzZGB eine genügende Grundlage für die Verweigerung eines Sperrrechtes bilden. Leider finden sich weder in der Judikatur noch Literatur anschauliche Beispiele, woraus hervorgeht, welche Voraussetzungen eine

[1] JENNIFER EHRENSPERGER in: MAURER-LAMBROU/BLECHTA (Hrsg.), Basler Kommentar zum Datenschutz- und Öffentlichkeitsgesetz, Art. 20, N 1.
[2] VPB 68.69.
[3] VPB 70.45, Erwägung 4.4.

gesetzliche Grundlage aufweisen muss für die Anwendung von Art. 20 Abs. 2 lit. a DSG. Im Zusammenhang mit der Sperrung von Personendaten hielt die EDSK fest, dass Personendaten eines allgemein zugänglichen Registers gesperrt werden können (es ging um die Publikation von Motorfahrzeughalterdaten). Demgegenüber bejahte das Bundesgericht das Bestehen einer solchen Rechtspflicht hinsichtlich der Ausstellung von Steuerausweisen an Dritte betreffend den Kanton Zürich. Im Kommentar zum IDG des Kantons Basel-Stadt kann unter Durchbrechung der Sperre aufgrund gesetzlicher Verpflichtung nachgelesen werden: «Die Sperre der Bekanntgabe von Eigentümerdaten beim Grundbuchamt kann durchbrochen werden, weil dieses gesetzlich verpflichtet ist, jeder Person Auskunft über den Namen des Eigentümers zu geben.»[4] Massgabe für die Anwendung von Art. 20 Abs. 2 lit. a DSG ist die Verpflichtung der Behörde zur Datenbekanntgabe. Mit Bezug darauf gehört der anwendbare Art. 970 Abs. 2 ZGB in diesen Anwendungsbereich. Die Auskunft darüber, wer als Eigentümer eines Grundstücks im Grundbuch eingetragen ist, wird voraussetzungslos erteilt. Jede Person ist berechtigt, den Namen und die Identifikation des Eigentümers zu erhalten.[5] Insofern kann sich ein Eigentümer kaum auf das Sperrrecht berufen. Eine andere Frage betrifft die Anwendung von Art. 970a ZGB in Verbindung mit Art. 146c EGzZGB. In Art. 970a ZGB gibt der Bundesgesetzgeber an die Kantone die Kompetenz, die Veröffentlichung des Erwerbers vorzusehen. Es handelt sich dabei um eine sog. «Kann-Vorschrift». Mithin ist keine Verpflichtung damit verbunden. Art. 146c Abs. 1 EGzZGB lautet: «Der Kanton publiziert die ohne Interessennachweis einsehbaren Daten des Hauptbuchblattes im Internet.» Die Formulierung lässt auf eine Verpflichtung schliessen. Der Kanton wird verpflichtet, die Veröffentlichung über das Internet vorzunehmen. Insofern bleibt kein Handlungsspielraum. Aufgrund der gesetzlichen Vorgaben spricht vieles dafür, dass ein Sperrrecht im Bereich Grundbuch nicht durchgesetzt werden kann.

[4] DANIELA WALDMEIER in: Praxiskommentar zum Informations- und Datenschutzgesetz Basel-Stadt, §28, N21.

[5] JÜRG SCHMID in: HONSELL/VOGT/GEISER (Hrsg.), Basler Kommentar zum ZGB, Art. 970, N 5 ff.

6. *Videoüberwachung Spitex*

Spitexmitarbeitende pflegen und betreuen Kunden in deren Räumlichkeiten. Es kommt vor, dass diese Räume von Angehörigen unter Zustimmung der Kunden aus Sicherheitsgründen videoüberwacht werden, um bei Unpässlichkeiten schneller reagieren zu können. Die Spitexmitarbeitenden werden zwangsläufig bei ihrer Arbeit gefilmt.

Vorab stellt sich die Frage, ob eine Videoüberwachung zulässig ist. Videoüberwachungssysteme dürfen nur dann eingesetzt werden, wenn sie rechtund verhältnismässig sind. Sie sind nur zulässig, wenn der Eingriff in die Persönlichkeit durch die Zustimmung der betroffenen Personen, durch ein überwiegendes privates Interesse oder durch ein Gesetz gerechtfertigt ist. Das Bundesgericht hat kürzlich in einer mietrechtlichen Auseinandersetzung entschieden, dass eine Videoüberwachung im Wohnbereich nicht an sich schon unzulässig sein. Es müsse jedoch in jedem Fall der Schutz der Privatsphäre gegen die Eigentumsgarantie abgewogen werden. Ähnlich verhält es sich im vorliegenden Fall. Grundsätzlich ist eine Videoüberwachung möglich. Indessen sind die Interessen der Mitarbeitenden der Spitex zu berücksichtigen.

Hinzuweisen ist auf das Arbeitsgesetz. Gemäss Art. 26 Abs. 1 ArGV 3 dürfen Überwachungs- und Kontrollsysteme, die das Verhalten der Arbeitnehmer am Arbeitsplatz überwachen sollen, nicht eingesetzt werden. Wenn diese Überwachungs- oder Kontrollsysteme aus anderen Gründen erforderlich sind, sind diese so anzuordnen, dass der Arbeitnehmer dadurch nicht beeinträchtigt wird. Auf den vorliegenden Fall bezogen bedeutet dies, dass während der Tätigkeit der Spitexmitarbeitenden die Kamera abgeschaltet oder so platziert wird, dass sich die Mitarbeitenden nicht beobachtet fühlen. Kann technisch kein Einfluss genommen werden, sind die Mitarbeitenden berechtigt, bspw. durch ein Tuch oder einen Aufkleber, die Videokamera zu verdunkeln.

IV. Referate/Kurse

Seit mehreren Jahren wird zusammen mit dem Verantwortlichen für die Informatiksicherheit ein kantonsinterner Kurs durchgeführt. Er erfreut sich grosser Beliebtheit. Das Ziel dieser Veranstaltung besteht darin, die Mitarbeitenden der kantonalen Verwaltung auf die Belange des Datenschutzes und der Datensicherheit zu sensibilisieren. Darüber hinaus werden ebenfalls alljährlich den Lernenden in ihren überbetrieblichen Kursen die Belange des Datenschutzes näher gebracht und schliesslich referiert der DSB alljährlich im Regionalspital Schiers.

V. Verbände

Privatim, die Vereinigung der kantonalen Datenschutzbeauftragten, hat sich ein neues Gesicht gegeben. Die Professionalisierung leidet indessen immer noch an den fehlenden Ressourcen. Positiv kann festgestellt werden, dass Adrian Lobsiger, der neu gewählte EDÖB, Interesse bekundet, aktiv bei Privatim mitzuarbeiten.

Nach 13-jähriger Mitgliedschaft in der Arbeitsgruppe Gesundheit hat der DSB GR diese Arbeitsgruppe verlassen.

VI. Statistik Anfragen DSB 2016

Wer \ Was	Kurzanfragen	Berichte	Empfehlungen	Kontrollen	Vernehmlassungen	Referate	Kurse	Weiterbildung/Verbände
Kantonale Dienste								
Allgemeine Verwaltung	1						1	1
DVS	6		1					
DJSG	15		1		2			
EKUD	4							
DFG	5							
BVFD	1							
öff. rechtliche Anstalten								
Gerichte								
Kreise								
Gemeindeverbände								
Gemeinden	22		1					
Bürgergemeinden								
Juristische Personen	5		2					
Private Personen	30	1	5					
Andere	7		2			6		3
Total	96	1	12	0	2	6	1	4

VII. Abkürzungsverzeichnis

a.a.O.	am angeführten Ort
Abs.	Absatz
a.M.	anderer Meinung
Art.	Artikel
ArGV 3	Verordnung 3 zum Arbeitsgesetz
ATSG	Allgemeiner Teil zum Sozialversicherungsgesetz
B	Botschaft
BG	Bundesgesetz
BGE	Bundesgerichtsentscheid
BGer	Bundesgericht
Bl	Blatt
BR	Bündner Rechtsbuch
BV	Bundesverfassung
BVFD	Bau-, Verkehrs- und Forstdepartement
bzw.	beziehungsweise
DJSG	Departement für Justiz, Sicherheit und Soziales
DSB	Datenschutzbeauftragter
DSG	Eidgenössisches Datenschutzgesetz
DVS	Departement für Volkswirtschaft und Soziales
EDOEB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDSK	Eidg. Datenschutz-Kommission
EGzZGB	Einführungsgesetz zum Zivilgesetzbuch
EKUD	Erziehungs-, Kultur- und Umweltschutzdepartement
ERG	Gesetz über die Einwohnerregister
ERV	Verordnung zu Gesetz über Einwohnerregister
etc.	et cetera
f./ff.	folgend/folgende
GR	Graubünden
Hrsg.	Herausgeber
i.V.m.	in Verbindung mit
KDSG	kantonales Datenschutzgesetz
KESB	Kinder- und Erwachsenenschutzbehörde
KV	Kantonsverfassung
lit.	litera
N	Note
OR	Obligationenrecht
RB	Rechtsbuch

RHG	BG über die Harmonisierung der Einwohnerregister und anderer amtlicher Personenregister
S	Seite
SchKG	Bundesgesetz über Schuldbetreibung und Konkurs
SR	Sammlung der eidgenössischen Gesetze und systematische Sammlung des Bundesrechts (Systematische Rechtssammlung)
StGB	Strafgesetzbuch
usw.	und so weiter
UVG	Unfallversicherungsgesetz
UVV	Verordnung zum Unfallversicherungsgesetz
VDSG	Verordnung zum eidgenössischen Datenschutzgesetz
vgl.	vergleiche
VPB	Verwaltungspraxis der Bundesbehörden
z.B.	zum Beispiel
ZGB	Zivilgesetzbuch
Ziff.	Ziffer

Impressum

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