Tätigkeitsbericht 2025

Datenschutzbeauftragter des Kantons Graubünden

Datenschutzbeauftragter des Kantons Graubünden

RA Thomas Casanova · Kornplatz 2 · 7001 Chur
Telefon 081 256 55 58 · dsb@staka.gr.ch

Impressum
Gestaltung / Druck: Casutt Druck & Werbetechnik AG, Chur
Gedruckt auf Cyclus Recycling-Papier aus 100% speziell sortierten Druckerei- und Büroabfällen

Inhalt

I. Schlusswort

Mit dem vorliegenden Tätigkeitsbericht schliesst eine Ära: Nach 23 Jahren übergebe ich das Amt des Datenschutzbeauftragten in neue Hände. In dieser Zeit hat sich der Datenschutz von einer vergleichsweisen unbekannten Regulierung zu einem zentralen Pfeiler in der Verwaltung, Wirtschaft und Gesellschaft entwickelt. Die Herausforderungen haben sich stetig gewandelt – von der Einführung technischer Schutzmassnahmen über die Umsetzung datenschutzrechtlicher Grundsätze bis hin zur Bewältigung der digitalen Transformation.

Blickt man in die Zukunft, zeigen sich neue Risiken: Die zunehmende Digitalisierung, der Einsatz künstlicher Intelligenz, vernetzte Systeme und globale Datenflüsse verlangen weiterhin Aufmerksamkeit, Innovationsbereitschaft und ein konsequentes proaktives Handeln. Datenschutz bleibt ein dynamisches Feld, das sich ständig weiterentwickelt.

Ich möchte allen danken, die in diesen Jahren zur Stärkung des Datenschutzes beigetragen haben – seien es Mitarbeitende der Behörden, unser Verband oder meine Fachkollegen und -kolleginnen. Ohne ihr Engagement und ihre konstruktive Zusammenarbeit wäre die Entwicklung eines wirksamen und modernen Datenschutzrechts nicht möglich gewesen. Ich bin überzeugt, dass das Amt unter der neuen Leitung die Herausforderungen der Zukunft meistern und den Schutz personenbezogener Daten weiterhin zuverlässig gewährleisten wird.

Adieu

Kantonaler Datenschutzbeauftragter:

Thomas Casanova

II. Die Entwicklung des Datenschutzes im Spannungsfeld der Informationstechnologie

1. Einleitung

Der Schutz personenbezogener Daten hat sich seit den Anfängen der Computertechnik von einer rein technischen Herausforderung zu einem zentralen gesellschaftlichen, rechtlichen und wirtschaftlichen Thema gewandelt. Insbesondere das Aufkommen des Internets, sozialer Medien, Smartphones wie dem iPhone, Cloud-Diensten, Phishing-Techniken und die jüngste Entwicklung künstlicher Intelligenz (KI) eröffneten nicht nur neue Möglichkeiten für Wirtschaft, Verwaltung und Gesellschaft, sondern stellen auch das Datenschutzrecht vor nie dagewesene Herausforderungen.

Während die Informationstechnologie in den letzten Jahrzehnten exponentiell an Leistungsfähigkeit und Reichweite gewonnen hat, haben sich zugleich die Risiken für die Privatsphäre dramatisch erhöht.

Im Folgenden werden die Wechselwirkung zwischen technologischen Innovationen und datenschutzrechtlichen Rahmenbedingungen nachgezeichnet, zentrale Meilensteine identifiziert und daraus Leitlinien für die zukünftige Gestaltung von Datenschutz Strategien abgeleitet.

2. Historischer Überblick

Datenschutz als eigenes Rechtsgebiet entstand in Europa als Antwort auf die zunehmende Digitalisierung. In der Schweiz basierte der Datenschutz lange Zeit auf verfassungsrechtlichen Grundsätzen, insbesondere aus Artikel 13 der Bundesverfassung (BV), der das Recht auf Achtung des Privat- und Familienlebens sowie des Brief- und Fernmeldegeheimnisses schützt.

Das erste umfassende Datenschutzgesetz war das Bundesgesetz über den Datenschutz (DSG) von 1992, das am 1. Juli 1993 in Kraft trat. Dieses Gesetz regelte erstmals den datenschutzrechtlichen Schutz natürlicher Personen gegenüber Datenbearbeitungen durch Behörden und private Organisationen. Mit der massiven Verbreitung des Internets, von E-Mail-Diensten, Smartphones und sozialen Netzwerken wurden die Anforderungen an den Datenschutz vielschichtiger. Die ursprüngliche Gesetzesfassung war in einem Zeitalter entstanden, in dem das World Wide Web kaum über universitäre Forschung hinaus verbreitet war.

Daher begann Ende der 2010er-Jahre eine umfassende Revision, die das Gesetz technologisch und international aktualisieren sollte. Die revidierte Fassung des Schweizer Datenschutzgesetzes trat am 1. September 2023 in Kraft. Sie bringt das nationale Recht näher an internationale Standards, insbesondere vergleichbar mit der EU-Datenschutz-Grundverordnung (DSGVO), und stärkt damit Rechte von Betroffenen sowie Pflichten für Verantwortliche. Am 1. Januar 2026 tritt das revidierte kantonale Datenschutzgesetz (KDSG) in Kraft. Es lehnt sich weitgehend an das revidierte DSG an. Mit der Einführung werden zudem die aufsichtsrechtlichen Kompetenzen gestärkt, insbesondere durch eine deutliche Erhöhung von Budget und Personalbestand.

3. Digitale Transformation und rechtlicher Anpassungsbedarf im Datenschutz

Die fortschreitende Miniaturisierung von Hardware und die Skalierbarkeit von Cloud Infrastrukturen haben die Möglichkeit geschaffen, Petabytes an personenbezogenen Daten in Echtzeit zu analysieren. Diese Leistungsfähigkeit erhöht das Risiko von Profilbildung, selbst bei angeblich anonymisierten Datensätzen. Neue Datenformen – Standortinformationen, biometrische Merkmale und Verhaltensprofile – ermöglichen tiefere Einblicke in das Privatleben. Künstliche Intelligenz und maschinelles Lernen stellen weitere Herausforderungen dar. Exakte Analyse und generative Modelle erzeugen nicht nur Erkenntnisse, sondern auch neue Daten.

Einsatz von Funkwasserzählern

Eine Gemeinde fragt an, ob es für den Einbau von Funkwasserzählern eine besondere gesetzliche Grundlage braucht. In vielen Gemeinden steht die Umrüstung von herkömmlichen Wasserzählern auf elektronisch ablesbare Geräte (Funkwasserzähler) an.

Die Einführung von Funkwasserzählern erfordert eine gesetzliche Grundlage. Die Voraussetzungen für Einbau und Ablesung von Wasserzählern sind in der Regel im kommunalen Wasserreglement geregelt. Soll eine funkmässige Ablesung eingeführt werden, ist dieses entsprechend anzupassen.

Zudem ist der datenschutzrechtliche Grundsatz der Verhältnismässigkeit zwingend einzuhalten. Zweck der Ablesung ist ausschliesslich die Ermittlung des Wasserverbrauchs zur Gebührenberechnung. Systeme, die den Verbrauch in kurzen Intervallen erfassen und über längere Zeit speichern, gehen über das Erforderliche hinaus und sind daher unzulässig (vgl. BGE 147 I 346).

Zusammengefasst setzt der Einsatz von Funkwasserzählern sowohl eine ausreichende gesetzliche Grundlage als auch eine verhältnismässige technische Umsetzung voraus.

Die rasante Entwicklung der Informationstechnologie verändert seit Jahren die Art, wie Daten entstehen, verarbeitet und genutzt werden. Mit der Verbreitung leistungsfähiger Cloud-Infrastrukturen werden personenbezogene Daten zunehmend ausserhalb des eigenen Einflussbereichs gespeichert und über Ländergrenzen hinweg ausgetauscht. Das schafft neue Abhängigkeiten und stellt hohe Anforderungen an Datensicherheit, Kontrollmöglichkeiten und Verantwortlichkeiten zwischen Anbietern und Kunden. Gleichzeitig ermöglichen Big-Data-Technologien und künstliche Intelligenz automatisierte Auswertungen riesiger Datenmengen. Dadurch entstehen wertvolle neue Erkenntnisse, etwa für personalisierte Angebote oder Entscheidungsunterstützung. Zugleich drohen neuartige Risiken wie Profiling, Diskriminierung oder mangelnde Transparenz komplexer Algorithmen.

Auch das Internet of Things führt zu datenschutzrechtlichen Herausforderungen. Millionen vernetzter Geräte erfassen kontinuierlich Daten aus dem Alltag der Menschen – häufig unbemerkt. Diese ständige Datengenerierung verlangt wirksame Konzepte für Datensparsamkeit, Sicherheit und Zweckbindung. Hinzu kommen Cyberangriffe, die zunehmend pro-

fessioneller und häufiger auftreten. Sie machen deutlich, dass klassische Sicherheitsmassnahmen nicht mehr ausreichen und umfassende technische und organisatorische Vorkehrungen erforderlich sind.

Schliesslich verändert die Blockchain-Technologie bestehende Grundsätze des Datenschutzes. Die Unveränderbarkeit gespeicherter Informationen stärkt zwar die Integrität, steht jedoch im Konflikt zu Löschpflichten und dem Recht auf Vergessenwerden. Neue technische und rechtliche Ansätze sind nötig, um beide Anforderungen miteinander zu vereinbaren. Insgesamt zeigt sich, dass die digitale Transformation den rechtlichen Rahmen laufend auf den Prüfstand stellt. Datenschutzgesetze müssen flexibler, technologieneutraler und risikobasierter ausgestaltet werden, um sowohl Innovationspotenziale als auch den Schutz der Persönlichkeit angemessen sicherzustellen. Das geltende Gesetz ist in weiten Teilen technologieneutral gestaltet, dennoch bleibt ein kontinuierlicher Handlungsbedarf bestehen. Den rasanten Entwicklungen im IT-Bereich kann nur durch konsequent proaktives Handeln begegnet werden. Dies erfordert einen hohen Professionalisierungsgrad der Datenschutzbehörden sowie ausreichende personelle und finanzielle Ressourcen.

4. Chancen und Risiken von KI-Technologien im Datenschutzkontext

Die nächste Phase digitaler Transformation wird wesentlich durch künstliche Intelligenz geprägt sein. KI-gestützte Systeme können hochkomplexe Datenbearbeitungen automatisieren, Muster aus grossen Datenmengen extrahieren und Entscheidungen treffen, die traditionell menschlicher Expertise vorbehalten waren. Aus datenschutzrechtlicher Perspektive ergeben sich daraus sowohl Chancen als auch Risiken, die das Datenschutzrecht der kommenden Jahre weiterhin herausfordern werden.

Künstliche Intelligenz bietet im Bereich Datenschutz und IT-Sicherheit vielfältige Chancen. So kann sie die Datensicherheit erheblich verbessern, indem Sicherheitsrisiken frühzeitig erkannt und Angriffe automatisiert abgewehrt werden. Systeme zur Anomalieerkennung, zur Abwehr von PhishingAttacken oder zur Identifikation verdächtiger Login-Muster ermöglichen eine effizientere Cyberabwehr, als es rein menschliche Kontrollmechanismen leisten könnten. Darüber hinaus unterstützt KI die Umsetzung des Grundsatzes der Datensparsamkeit. Intelligente Verarbeitungskonzepte tragen dazu bei, personenbezogene Daten weniger zentralisiert zu verarbeiten und besser kontrollierbar zu machen. Schliesslich kann KI die Stärkung der Betroffenenrechte fördern. KI-gestützte Tools ermöglichen es, Auskunftsanfragen automatisiert zu bearbeiten, transparente Risikoanalysen für Verbraucher bereitzustellen oder Datenschutzinformationen verständlich aufzubereiten. Digitale Assistenzsysteme können Betroffene so aktiv dabei unterstützen, ihre Rechte wahrzunehmen und informierte Entscheidungen über ihre Daten zu treffen.

Künstliche Intelligenz birgt nicht nur Chancen, sondern auch erhebliche Risiken für Datenschutz und informationelle Selbstbestimmung. Viele KI-Modelle bleiben Black Boxes, deren Entscheidungen schwer nachvollziehbar sind. Werden automatisierte Systeme beispielsweise zur Bestimmung der

Einschreibeverfahren in der Kantonsbibliothek

Da sich Nutzerinnen und Nutzer der Kantonsbibliothek auch vor Ort einschreiben können, besteht neben der Anmeldung über App oder Internet eine gleichwertige analoge Alternative. Entscheidet sich eine Person für den digitalen Anmeldeweg, erfolgt dies somit freiwillig. Aus datenschutzrechtlicher Sicht ist entscheidend, dass kein faktischer oder rechtlicher Zwang zur digitalen Übermittlung personenbezogener Daten besteht. Die Aufrechterhaltung einer Einschreibemöglichkeit vor Ort ist daher von zentraler Bedeutung, um die Freiwilligkeit der Wahl sicherzustellen. Positiv hervorzuheben ist zudem die Information, wonach die übermittelten Daten nach erfolgter Verifizierung gelöscht werden. Diese Mitteilung entspricht dem datenschutzrechtlichen Transparenzgebot und stärkt das Vertrauen der Nutzerinnen und Nutzer in den Umgang mit ihren Daten.

Es empfiehlt sich, den Hinweis auf die Möglichkeit der Einschreibung vor Ort auch ausdrücklich in die digitale Kommunikation – insbesondere in der App sowie auf der Website – aufzunehmen. Dadurch wird sichergestellt, dass alle Nutzerinnen und Nutzer aktiv auf die analoge Alternative aufmerksam gemacht werden und eine informierte Entscheidung treffen können.

Kreditwürdigkeit, von Versicherungstarifen oder im Bewerbungsprozess eingesetzt, entstehen Risiken diskriminierender oder fehlerhafter Entscheidungen. Damit entsteht ein Spannungsfeld zwischen technischer Innovation und dem Schutz der Persönlichkeitsrechte, wobei datenschutzrechtlich zentral bleibt, wie die «Erklärbarkeit» solcher Systeme technisch und rechtlich sichergestellt werden kann. Darüber hinaus ermöglicht KI eine bislang unerreichte Skalierbarkeit der Datenanalyse. Sensible Daten können zusammengeführt, analysiert und zu verhaltensbasierten Vorhersagen genutzt werden – sowohl rechtmässig als auch potenziell missbräuchlich. Dies erhöht die Gefahr, dass Personen in ihrer informationellen Selbstbestimmung faktisch entmachtet werden. Ein weiteres Risiko ergibt sich aus der Abhängigkeit von globalen Technologieanbietern. KI-Infrastrukturen werden überwiegend von grossen Cloud- und Plattformanbietern bereitgestellt, was die Datensouveränität der Schweiz beeinträchtigen kann. Vor diesem Hintergrund wird diskutiert, ob nationale oder souveräne KI- und Cloud-Strategien notwendig sind, um datenintensive Prozesse nicht ausschliesslich im Ausland abzuwickeln. Schliesslich eröffnen KI-Anwendungen regulatorische Grauzonen. Obwohl das revidierte Datenschutzgesetz grundsätzlich technologieneutral gestaltet ist, wirft KI neue Fragen auf – etwa hinsichtlich Zweckbindung, Verantwortlichkeit für autonome Entscheidungen oder Transparenz gegenüber Betroffenen. Die künftige Rechtsprechung wird entscheidend klären, wie bestehende Datenschutzgarantien auf KI-Systeme angewendet werden können.

5. Proaktiver Datenschutz in Zeiten rascher IT-Entwicklung

Behörden und Unternehmen stehen im Zuge der digitalen Transformation vor der Herausforderung, personenbezogene Daten effektiv zu schützen und auf neue Risiken angemessen zu reagieren. Zunächst müssen sie neue Technologien systematisch auf mögliche Gefahren prüfen und bei besonders sensiblen Daten Datenschutz-Folgenabschätzungen durchführen, um Risiken frühzeitig zu erkennen. Technische und organisatorische Schutzmassnahmen wie Verschlüsselung, Zugriffskontrollen, Sicherheitsrichtlinien und Notfallpläne sind dabei zentral, um Daten vor unbefugtem Zugriff, Verlust oder Manipulation zu sichern. Ebenso wichtig sind die Schulung und Sensibilisierung der Mitarbeitenden, da menschliche Fehler oft die grösste Schwachstelle darstellen.

Transparenz und Rechenschaftspflicht bilden ein weiteres Fundament: Behörden und Unternehmen müssen nachvollziehbar dokumentieren, welche Daten wofür verarbeitet werden, und jederzeit die Einhaltung gesetzlicher Vorgaben nachweisen können. Der Umgang mit neuen Technologien wie KI, Cloud-Computing oder Blockchain erfordert zudem spezifische Anpassungen, etwa die Anonymisierung von Daten oder Off-Chain-Speicherung. Ergänzend müssen sie ein wirksames Krisen-Management etablieren, um Datenschutzverletzungen schnell zu erkennen, zu melden und zu beheben. Schliesslich sichern rechtskonforme Verträge und klare Governance-Strukturen, insbesondere bei Dienstleistern oder internationalen Datenübertragungen, die Verantwortlichkeiten und die Einhaltung von Sicherheitsanforderungen ab. Zusammengefasst erfordert die digitale Transformation ein aktives Risikomanagement, geeignete Schutzmassnahmen, kritische Technologieprüfung und eine umfassende Sensibilisierung, um Datenschutz und Datensicherheit dauerhaft zu gewährleisten.

6. Fazit

Die Geschichte des Datenschutzes ist eng verwoben mit den Fortschritten der Informationstechnologie. Jede neue technische Möglichkeit – sei es die Skalierbarkeit von Cloud Infrastrukturen, die Leistungsfähigkeit von KI Modellen oder die Dezentralisierung durch Blockchain – eröffnet sowohl Chancen für innovative Dienste als auch neue Angriffsflächen für den Missbrauch personenbezogener Daten. Die regulatorische Landschaft hat darauf reagiert, indem sie zunehmend umfassende Prinzipien etabliert und gleichzeitig versucht, Flexibilität für technologische Weiterentwicklungen zu bewahren. Für Unternehmen, Gesetzgeber und die Gesellschaft gilt es, diesen dynamischen Dialog aktiv zu gestalten: Technik muss von vornherein datenschutzfreundlich konzipiert werden, während der Rechtsrahmen flexibel genug bleiben muss, um auf noch unbekannte Entwicklungen reagieren zu können. Nur so lässt sich ein Gleichgewicht zwischen Innovation und dem Grundrecht auf informationelle Selbstbestimmung erreichen.

III. Das neue kantonale Datenschutzgesetz

Die Totalrevision des Datenschutzgesetzes des Kantons Graubünden (KDSG) stellt eine grundlegende Neuausrichtung des kantonalen Datenschutzrechts dar. Das ursprüngliche Gesetz aus dem Jahr 2002 vermochte den Anforderungen der fortschreitenden Digitalisierung sowie den Entwicklungen im nationalen und internationalen Datenschutzrecht nicht mehr zu genügen. Insbesondere die Revision des eidgenössischen Datenschutzgesetzes sowie die zunehmende Bedeutung europäischer Datenschutzstandards machten eine umfassende Anpassung erforderlich. Vor diesem Hintergrund trat das revidierte KDSG per 1. Januar 2026 in Kraft.

Ziel der Revision ist es, ein zeitgemässes Datenschutzniveau sicherzustellen und die Vereinbarkeit mit übergeordnetem Recht, namentlich dem Bundesrecht sowie einschlägigen völkerrechtlichen Verpflichtungen, zu gewährleisten. Der kantonale Gesetzgeber verfolgte dabei einen zurückhaltenden Regelungsansatz, indem er sich im Wesentlichen auf die Umsetzung zwingender Vorgaben beschränkte und auf eine darüberhinausgehende Ausdehnung der Regulierung bewusst verzichtete. Gleichwohl trägt das revidierte Gesetz den Herausforderungen moderner Datenbearbeitungen – insbesondere im Kontext digitaler Prozesse und umfangreicher Datenverarbeitungen – Rechnung.

Eine wesentliche Neuerung liegt in der gesetzessystematischen Ausgestaltung. Während das frühere Recht in erheblichem Umfang auf dynamische Verweisungen zum Bundesrecht abstellte, wurden die entsprechenden Regelungsinhalte nun eigenständig in das kantonale Gesetz integriert. Dies führt zu einer erhöhten Normklarheit und Systematik, geht jedoch mit einer reduzierten Anpassungsflexibilität einher. Der gewachsene Regelungsbedarf zeigt sich auch im deutlich erweiterten Umfang des Gesetzes, dessen Bestimmungen von ursprünglich 13 auf neu 41 Artikel angewachsen sind.

Im materiellen Gehalt ist insbesondere die Stärkung der Rechte der betroffenen Personen hervorzuheben. Das revidierte KDSG erweitert die individuellen Abwehr- und Mitwirkungsrechte und trägt damit dem verfassungsrechtlich verankerten Anspruch auf informationelle Selbstbestimmung Rechnung. Gleichzeitig werden die Pflichten der öffentlichen Organe substantiell ausgebaut. Diese sind künftig verpflichtet, angemessene technische und organisatorische Massnahmen zur Gewährleistung der Datensicherheit zu treffen und sich dabei an vorgegebenen Mindeststandards zu orientieren. Zudem wird bei Datenbearbeitungen mit er-

höhtem Risiko die Durchführung von Datenschutz-Folgenabschätzungen verlangt, wodurch potenzielle Eingriffe in die Persönlichkeitsrechte frühzeitig identifiziert und begrenzt werden sollen.

Ferner übernimmt das revidierte Gesetz zentrale Instrumente eines modernen Datenschutzrechts. Dazu zählt insbesondere die Regulierung von Datenbearbeitungen mit erhöhtem Gefährdungspotenzial, namentlich im Bereich des Profilings. Diese Regelungen tragen den Risiken automatisierter Datenverarbeitungen Rechnung, welche geeignet sind, Persönlichkeitsprofile zu erstellen und damit in erheblicher Weise in die Privatsphäre einzugreifen.

Ein weiterer Schwerpunkt der Revision liegt in der institutionellen Stärkung der Datenschutzaufsicht. Die zuständige Aufsichtsbehörde wird in ihrer Unabhängigkeit gestärkt und mit erweiterten Kompetenzen sowie zusätzlichen personellen Ressourcen ausgestattet. Dadurch soll eine effektivere Kontrolle der Einhaltung datenschutzrechtlicher Vorschriften gewährleistet werden. Inhaltlich konzentriert sich die Revision dabei vornehmlich auf das formelle Datenschutzrecht, indem sie insbesondere Verfahrensfragen, Zuständigkeiten und Aufsichtsmechanismen neu regelt, ohne in spezialgesetzlichen Materien tiefgreifende Änderungen vorzunehmen.

In der Gesamtwürdigung ist die Revision als notwendiger und sachgerechter Schritt zur Modernisierung des kantonalen Datenschutzrechts zu qualifizieren. Sie trägt den aktuellen rechtlichen und technischen Entwicklungen Rechnung und stärkt den Schutz der Persönlichkeitsrechte. Dennoch bestehen punktuell Auslegungs- und Abgrenzungsfragen, insbesondere im Zusammenhang mit neuen Technologien und automatisierten Datenbearbeitungen. Zudem ist nicht zu verkennen, dass die erweiterten gesetzlichen Anforderungen mit einem erhöhten Vollzugsaufwand für die öffentlichen Organe einhergehen.

Zusammenfassend schafft das revidierte Datenschutzgesetz des Kantons Graubünden eine zeitgemässe und im Grundsatz kohärente Regelungsgrundlage, welche den Anforderungen des digitalen Zeitalters gerecht wird, auch wenn in einzelnen Bereichen weiterhin Konkretisierungsbedarf besteht.

IV. Fälle aus der Praxis

1. Einsicht in Daten Verstorbener und Fortwirkung von Geheimnisschutz

Ausgangspunkt bildet Art. 31 Abs. 1 ZGB, wonach die Persönlichkeit mit dem Tod endet. Das schweizerische Zivilrecht kennt grundsätzlich keinen über den Tod hinaus fortwirkenden Persönlichkeitsschutz. Dies wurde auch durch die Rechtsprechung bestätigt (vgl. BGer 5A_496/2014). Konsequenterweise entfallen damit auch persönlichkeitsrechtliche Ansprüche wie etwa das datenschutzrechtliche Sperrrecht. Trotz Wegfalls des Persönlichkeitsschutzes bedeutet dies jedoch nicht, dass Personendaten Verstorbener frei zugänglich wären. Das Datenschutzgesetz knüpft zwar primär an den Schutz lebender natürlicher Personen an, regelt aber mittelbar auch den Umgang mit Daten Verstorbener, insbesondere durch die Anforderungen an die Datenbekanntgabe durch Behörden.

Gemäss Art. 34 DSG dürfen Personendaten nur bekanntgegeben werden, wenn eine gesetzliche Grundlage besteht. Dieser Grundsatz gilt unabhängig davon, ob die betroffene Person noch lebt, da er auch die Rechtmässigkeit staatlichen Handelns und den Schutz öffentlicher Interessen bezweckt. Eine Bekanntgabe ohne ausdrückliche gesetzliche Grundlage ist gemäss Art. 36 Abs. 2 DSG nur ausnahmsweise zulässig, insbesondere wenn:

- die Bekanntgabe für den Empfänger zur Erfüllung einer gesetzlichen Aufgabe unentbehrlich ist,
- sie zum Schutz von Leben oder körperlicher Unversehrtheit Dritter erforderlich ist, oder
- die Daten allgemein zugänglich sind.

Diese Ausnahmen sind restriktiv auszulegen und rechtfertigen keine generelle Einsichtsmöglichkeit für Angehörige. Insbesondere begründet das blosse Verwandtschaftsverhältnis keinen eigenständigen Anspruch auf Zugang zu Daten Verstorbener. Besondere Bedeutung kommt spezialgesetzlichen Geheimhaltungspflichten zu. Das Bundesgericht hat in BGE 129 I 302 ausdrücklich festgehalten, dass das Arztgeheimnis über den Tod hinaus fortwirkt. Demnach bleiben die in einem Patientendossier enthaltenen Informationen auch nach dem Ableben der betroffenen Person geschützt. Eine Offenlegung ist nur zulässig, wenn eine Entbindung vom Berufsgeheimnis erfolgt ist, etwa durch eine zuständige Behörde oder – soweit möglich – gestützt auf den mutmasslichen Willen der verstorbenen Person. Diese Grundsätze gelten nicht nur für medizinische Befunde im engeren

Sinn, sondern erfassen auch damit zusammenhängende Informationen wie etwa die Todesursache. Auch insoweit ist eine Bekanntgabe grundsätzlich nur zulässig, wenn die Voraussetzungen für eine Entbindung vom Arztgeheimnis erfüllt sind.

Zwar können Angehörige legitime Interessen an der Kenntnis bestimmter Informationen haben (z. B. zur Klärung von Erbfragen oder gesundheitlichen Risiken). Solche Interessen vermögen jedoch für sich allein keine Datenbekanntgabe zu rechtfertigen. Sie sind vielmehr im Rahmen der bestehenden gesetzlichen Ausnahmen oder spezialgesetzlichen Regelungen zu berücksichtigen und gegebenenfalls im Rahmen eines formellen Entbindungsverfahrens geltend zu machen.

Zusammenfassend ist festzuhalten: Mit dem Tod endet der zivilrechtliche Persönlichkeitsschutz, weshalb auch das Sperrrecht nicht mehr anwendbar ist. Die Bekanntgabe von Daten Verstorbener durch Behörden bleibt jedoch an die Voraussetzungen des Datenschutzrechts gebunden und bedarf grundsätzlich einer gesetzlichen Grundlage. Die Ausnahmetatbestände von Art. 36 Abs. 2 DSG sind restriktiv auszulegen und begründen keinen generellen Einsichtsanspruch von Angehörigen. Spezialgesetzliche Geheimhaltungspflichten, insbesondere das Arztgeheimnis, wirken über den Tod hinaus fort und schränken die Datenweitergabe erheblich ein. Damit ist der Zugang zu Daten Verstorbener insgesamt stark eingeschränkt und nur in klar geregelten Ausnahmefällen zulässig.

2. Einsicht in die Krankenakte

Gestützt auf das kantonale Datenschutzrecht (KDSG) richtet sich das Auskunftsrecht sinngemäss nach dem Bundesrecht. Gemäss Art. 2 Abs. 2 KDSG gelangen die Bestimmungen des Datenschutzgesetzes zur Anwendung, insbesondere Art. 25 DSG sowie die Art. 16 ff. DSV.

Gegenstand des Auskunftsrechts sind Personendaten im Sinne von Art. 5 lit. a DSG, mithin sämtliche Informationen, die sich auf eine bestimmte oder bestimmbare Person beziehen. Das Auskunftsrecht umfasst folglich alle über die betroffene Person vorhandenen Daten, unabhängig davon, ob diese in formellen Dossiers oder in internen Arbeitsunterlagen enthalten sind. Erfasst sind damit grundsätzlich auch interne Akten, Notizen oder elektronische Einträge, soweit sie Personendaten darstellen.

Einsichtsrecht der Geschäftsprüfungskommission (GPK)

Grundsätzlich verfügt die GPK über ein weitreichendes Einsichtsrecht. Dieses findet jedoch seine Grenzen in den datenschutzrechtlichen Grundprinzipien, insbesondere im Verhältnismässigkeitsprinzip. Danach sind der GPK nur jene Unterlagen bzw. Informationen zugänglich zu machen, die zur Erfüllung ihres gesetzlichen Auftrags erforderlich sind. Soweit der Zweck der Aufsicht auch ohne personenbezogene Angaben erreicht werden kann, sind diese zu anonymisieren oder zu schwärzen. Ist hingegen die Kenntnis von Identitäten für die Beurteilung eines konkreten Einzelfalls unerlässlich, kann auch eine ungeschwärzte Herausgabe gerechtfertigt sein.

Massgeblich ist somit stets eine einzelfallbezogene Interessenabwägung zwischen dem Informationsinteresse der GPK und dem Persönlichkeitsschutz der betroffenen Personen. Dabei ist sicherzustellen, dass die GPK ihren Auftrag wirksam wahrnehmen kann, ohne weitergehende Eingriffe in die Persönlichkeitsrechte vorzunehmen als notwendig.

Das Auskunftsrecht gilt als zentrales Betroffenenrecht. Es verschafft der betroffenen Person einen durchsetzbaren Anspruch gegenüber dem Verantwortlichen auf Information über die Datenbearbeitung. Dadurch wird es überhaupt erst möglich, die Einhaltung der datenschutzrechtlichen Grundsätze – insbesondere Rechtmässigkeit, Verhältnismässigkeit und Zweckbindung – effektiv zu überprüfen und gegebenenfalls durchzusetzen (vgl. Ralph Gramigna, in: Blechta/Vasella [Hrsg.], Basler Kommentar, DSG/ÖG, Art. 25, N 1).

Vor diesem Hintergrund ist festzuhalten, dass sich das Auskunftsrecht im medizinischen Kontext auf die gesamte Krankengeschichte erstreckt. Dazu gehören insbesondere ärztliche Berichte, Befunde, Verlaufsdokumentationen der Pflege, Diagnosen, Therapiedokumentationen sowie Korrespondenzen, soweit sie Personendaten enthalten. Ebenfalls umfasst ist das Zuweisungsschreiben der Hausärztin, zumal auch dieses personenbezogene medizinische Informationen enthält. Im Übrigen ist auch die Hausärztin verpflichtet, dieses auf Anfrage herauszugeben.

Einschränkungen des Auskunftsrechts sind in Art. 26 DSG abschliessend geregelt. Eine Verweigerung, Einschränkung oder Aufschiebung der Auskunft ist nur zulässig, wenn:

- eine gesetzliche Grundlage im formellen Sinn dies vorsieht,
- überwiegende Interessen Dritter dies erfordern,
- das Gesuch offensichtlich unbegründet ist,
- überwiegende öffentliche Interessen entgegenstehen oder
- die Bekanntgabe ein behördliches oder gerichtliches Verfahren gefährden würde.

Solche Einschränkungsgründe sind restriktiv auszulegen.

Daraus folgt, dass grundsätzlich ein umfassendes Einsichts- und Herausgaberecht der Krankenakte besteht. Hat die Klinik bestätigt, sämtliche vorhandenen Unterlagen ausgehändigt zu haben, ist sie an dieser Aussage zu messen. Sollten entgegen dieser Bestätigung weitere Unterlagen existieren und nicht herausgegeben worden sein, läge ein rechtswidriges Verhalten vor. Zu beachten ist allerdings, dass sich das Auskunftsrecht nur auf tatsächlich vorhandene Daten erstreckt. Sollten Unterlagen zwischenzeitlich vernichtet worden sein, besteht kein Anspruch auf Wiederherstellung; die Klinik wäre jedoch verpflichtet, eine entsprechende Vernichtung transparent zu machen und zu bestätigen.

Hinsichtlich einer allfälligen nachträglichen Manipulation von Daten ist der Nachweis naturgemäss schwierig zu führen. Allerdings verfügen moderne Klinikinformationssysteme regelmässig über Protokollierungs- und Versionierungsfunktionen, welche Änderungen an Datensätzen nachvollziehbar machen (sog. Audit-Trails). Auch insoweit kann ein Anspruch auf Transparenz bestehen.

3. Einsicht in die Laufakten im Rahmen des Strafvollzugs

Gemäss Art. 25 DSG besteht ein Anspruch auf Auskunft über sämtliche Akten der betroffenen Person. Dieser Anspruch ist umfassend und bildet ein zentrales Instrument zur Durchsetzung der datenschutzrechtlichen Garantien. Er soll es der betroffenen Person ermöglichen, die Rechtmässigkeit der Datenbearbeitung effektiv zu überprüfen.

Einschränkungen dieses Anspruchs sind nur unter den engen Voraussetzungen von Art. 26 DSG zulässig. Insbesondere bedarf eine Verweigerung der Auskunft einer hinreichenden gesetzlichen Grundlage im formellen Sinn (Art. 26 Abs. 1 lit. a DSG). Solche Einschränkungen sind restriktiv auszulegen. Die Verweigerung der Einsicht in die Laufakte wurde vorliegend auf die Richtlinien über die Laufakte des Ostschweizer Strafvollzugskonkordats gestützt. Diese sehen vor, dass es sich bei der Laufakte um ein internes Arbeitsinstrument handle, in das kein Einsichtsrecht bestehe. Diese Argumentation überzeugt rechtlich nicht. Bei den genannten Richtlinien handelt es sich nicht um ein Gesetz im formellen Sinn, sondern um verwaltungsinterne Normen. Sie vermögen daher das gesetzlich garantierte Auskunftsrecht nicht einzuschränken. Das zugrunde liegende Konkordat vom 29. Oktober 2004 (BR 350.400) enthält seinerseits keine Bestimmungen, welche das Akteneinsichtsrecht ausdrücklich beschränken würden. Insbesondere regelt Art. 12 Abs. 2 des Konkordats lediglich die Weiterleitung von Vollzugsakten, nicht aber deren Einsicht.

Damit fehlt es an der erforderlichen gesetzlichen Grundlage, um das Auskunftsrecht einzuschränken. Die Berufung auf die Richtlinien erweist sich folglich als unzureichend. Auch die übrigen in Art. 26 DSG vorgesehenen Einschränkungsgründe sind nicht ersichtlich. Namentlich bestehen im vorliegenden Fall keine Anhaltspunkte dafür, dass ein Gesuch offensichtlich unbegründet oder rechtsmissbräuchlich wäre (Art. 26 Abs. 1 lit. c DSG). Diese Ausnahme ist ohnehin eng auszulegen und greift nur in klaren Ausnahmefällen. Vor diesem Hintergrund ist die Verweigerung der Einsicht in die Laufakte als rechtswidrig zu qualifizieren.

4. Informationssicherheitsereignis

1. Allgemeines

Im Rahmen eines Pilotprojektes, wurden durch ein Amt scharfe Daten an eine beauftragte Unternehmung gesendet. Bei den übermittelten Personendaten handelte es sich mehrheitlich um normal schützenswerte Personendaten. Jedoch sind auch besonders schützenswerte Personendaten über verwaltungs- und strafrechtliche Belange übermittelt worden. Insgesamt ist somit davon auszugehen, dass besonders schützenswerte Personendaten nicht autorisierten Personen zugestellt wurden. Es handelt sich um zirka 182 Exporte. Aus dem Testsystem wurden Daten von 210 eingewiesenen Personen geliefert. 10 bis 15 Personen hätten die Möglichkeit gehabt, auf diese nicht anonymisierten Daten zugreifen zu können.

2. Rechtliches

Gemäss Art. 24 DSG meldet der Verantwortliche so rasch als möglich eine Verletzung der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt. Diese Meldung ist erfolgt.

Die in Art. 24 DSG geregelten Meldepflichten haben gemeinsam, dass stets eine Verletzung der Datensicherheit vorausgesetzt wird. Gemäss Legaldefinition von Art. 5 lit. a DSG handelt es sich um eine Verletzung der Sicherheit, die dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verloren gehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden. Vorliegend sind Personendaten Unbefugten zugänglich gemacht worden. Eine Verletzung der Datensicherheit kann festgestellt werden.

Eine Meldung ist nur in denjenigen Fällen vorgesehen, in denen die Verletzung der Datensicherheit voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt, wobei Behörden eine Meldung erstatten, wenn ein hohes Risiko für die Grundrechte besteht. Vorliegend sind besonders schützenswerte Personendaten betroffen. Allein schon deshalb rechtfertigt sich eine Meldung.

Im zu beurteilenden Fall muss abgeklärt werden, ob eine Information der betroffenen Personen angezeigt erscheint. Massgebend ist Art. 24 Abs. 4 und 5 DSG. Die betroffene Person muss nur ausnahmsweise über die Verletzung der Datensicherheit informiert werden (Botschaft DSG-Revision 2017, 7065). Der Zweck der Meldepflicht besteht darin, dass die

betroffene Person in die Lage versetzt wird, sich vor den möglichen Folgen der Verletzung zu schützen oder diese abzumildern. Massgebend ist also in erster Linie, ob durch die Information der betroffenen Person die Risiken für deren Persönlichkeit oder Grundrechte reduziert werden können. Dies ist insbesondere dann der Fall, wenn die betroffene Person selbst in der Lage ist, bestimmte Massnahmen zu ihrem Schutz zu treffen (Roland Mathys, Kenzo Thomann, in: Blechta/Vasella (Hrsg.), Datenschutzgesetz, Öffentlichkeitsgesetz, Basler Kommentar, 4. Auflage, Art. 24, Note 64 ff.). Zum Schutz der betroffenen Person nicht erforderlich ist eine Information hingegen dann, wenn sich die negativen Folgen bereits verwirklicht haben oder wenn die betroffene Person nichts Relevantes dagegen ausrichten kann.

Im vorliegenden Fall wurden besonders schützenswerte Personendaten an eine nicht berechtigte Unternehmung zugestellt. Dieser Fehler wurde erkannt, und es wurden die richtigen Massnahmen getroffen, wobei der Datentransfer gestoppt und die bereits übermittelten Daten gelöscht wurden. Die betroffenen Personen müssen somit keine Vorkehrungen zu ihrem eigenen Schutz treffen. In Anbetracht der Tatsache, dass die fehlerhafte Übermittlung der Daten nur von wenigen Personen überhaupt eingesehen werden konnten und das beauftragte Unternehmen berechtigterweise mit der Bearbeitung von Daten beauftragt worden ist, rechtfertigt ebenfalls eine zurückhaltende Haltung. Mit dem Verantwortlichen ist auch der Datenschutzbeauftragte der Auffassung, dass eine Meldung an die Betroffenen vorliegend nicht erforderlich ist.

3. Weiteres Vorgehen

Die erforderlichen Sofortmassnahmen sind ergriffen worden. In Zukunft ist sicher zu stellen, dass keine aktuellen persönlichen Daten von betroffenen Personen übermittelt werden. Darüber hinaus ist die im Pilotprojekt involvierte Behörde insoweit in das Projekt einzubinden, dass regelmässige Kontrollen möglich sind.

5. Weitergabe von Grundstückdaten an das Bundesamt für Statistik

Ausgangspunkt bildet der Umstand, dass das Bundesamt für Statistik (BfS) vom kantonalen Amt für Immobilienbewertung die Herausgabe von Unterlagen der Grundbuchämter verlangt und sich dabei auf Art. 7 Abs. 2 des Bundesstatistikgesetzes (BStatG) beruft. Ziel ist ein Zugriff auf bestimmte Grundstück- bzw. Grundbuchdaten.

Zunächst ist zu klären, ob das Amt für Immobilienbewertung überhaupt befugt ist, die fraglichen Daten an eine Drittstelle wie das BfS weiterzugeben. Gemäss Art. 6 Abs. 3 DSG gilt das Prinzip der Zweckbindung: Personendaten dürfen nur zu einem bestimmten, für die betroffene Person erkennbaren Zweck beschafft und nur in einer mit diesem Zweck vereinbaren Weise bearbeitet werden. Der Begriff der Bearbeitung umfasst gemäss Art. 5 lit. d DSG ausdrücklich auch die Bekanntgabe. Die hier in Frage stehenden Daten – insbesondere aus Handänderungsanzeigen – werden primär für steuerliche Zwecke erhoben, namentlich zur Veranlagung von Grundstückgewinn- und Handänderungssteuern. Zwar nutzt das Amt diese Daten sekundär auch zur Marktbeobachtung und Bewertung, doch bleibt der ursprüngliche Erhebungszweck steuerrechtlicher Natur.

Eine Weitergabe an das BfS zu statistischen Zwecken stellt demgegenüber einen eigenständigen, vom ursprünglichen Zweck abweichenden Bearbeitungszweck dar. Mangels unmittelbarer Zwecknähe ist die erforderliche Zweckkompatibilität grundsätzlich zu verneinen. Eine solche Zweckänderung wäre nur zulässig, wenn sie sich auf eine hinreichende gesetzliche Grundlage stützen liesse oder klar im überwiegenden öffentlichen Interesse läge und verhältnismässig wäre. Nach Art. 36 Abs. 1 DSG dürfen Behörden Personendaten nur bekanntgeben, wenn dafür eine gesetzliche Grundlage besteht. Diese muss hinreichend bestimmt sein, insbesondere wenn es sich – wie vorliegend – um potenziell schützenswerte wirtschaftliche Informationen handelt. Die für das Amt für Immobilienbewertung einschlägigen kantonalen Bestimmungen regeln zwar die Datenerhebung und -verwendung im steuerlichen Kontext, enthalten jedoch keine ausdrückliche Ermächtigung zur Weitergabe an das BfS für statistische Zwecke. Eine solche Kompetenz lässt sich auch nicht implizit aus den bestehenden Normen ableiten. Art. 36 Abs. 2 DSG erlaubt eine Bekanntgabe ausnahmsweise auch ohne spezifische gesetzliche Grundlage, sofern die Daten für den Empfänger zur Erfüllung einer gesetzlichen Aufgabe unentbehrlich sind. Diese Bestimmung ist jedoch restriktiv auszulegen und auf Einzelfälle zugeschnitten. Sie dient nicht dazu, systematische oder dauerhafte Datenflüsse zwischen Behörden zu legitimieren. Das BfS

verfolgt vorliegend gerade keinen Einzelfallzweck, sondern beabsichtigt einen regelmässigen, teilweise automatisierten Zugriff auf umfangreiche Datensätze. Ein derartiger struktureller Datenaustausch sprengt den Anwendungsbereich von Art. 36 Abs. 2 DSG und setzt zwingend eine klare formell-gesetzliche Grundlage voraus.

Art. 7 Abs. 2 BStatG verpflichtet Behörden grundsätzlich zur Mitwirkung an statistischen Erhebungen des Bundes. Diese Bestimmung stellt jedoch keine generelle, unmittelbare Durchbrechung kantonaler Datenschutz- und Spezialgesetzgebungen dar. Vielmehr ist sie im Lichte der jeweiligen spezialgesetzlichen Regelungen sowie des Datenschutzrechts auszulegen. Insbesondere begründet Art. 7 Abs. 2 BStatG keine unmittelbare Pflicht eines kantonalen Fachamts, Daten weiterzugeben, über die es nicht originär verfügungsbefugt ist oder deren Weitergabe spezialgesetzlich eingeschränkt ist. Die Norm richtet sich primär an die jeweils zuständigen Dateninhaber.

Zu berücksichtigen ist sodann, dass das Grundbuchrecht bundesrechtlich geprägt ist. Das Zivilgesetzbuch (ZGB) enthält Regelungen zur Öffentlichkeit des Grundbuchs sowie zur Möglichkeit der Bekanntgabe von Grundstückpreisen. In den letzten Jahren ist tatsächlich eine gewisse Öffnung erfolgt, indem Kantonen ermöglicht wird, Transaktionsdaten – insbesondere Preise – zu veröffentlichen. Diese Entwicklung relativiert zwar den Schutzgehalt bestimmter Grundstückdaten, ersetzt jedoch nicht die Notwendigkeit einer klaren Zuständigkeitsordnung. Entscheidend ist, dass die Kompetenz zur Bekanntgabe solcher Daten grundsätzlich bei den Grundbuchbehörden bzw. den dafür zuständigen Aufsichtsstellen liegt. Vor diesem Hintergrund erscheint es systemwidrig, wenn das Amt für Immobilienbewertung als sekundärer Datenbearbeiter eine direkte Weitergabe an das BfS vornimmt. Die primäre Zuständigkeit für Grundbuchdaten liegt bei den Grundbuchämtern bzw. dem kantonalen Grundbuchinspektorat. Eine rechtlich saubere und systemkonforme Lösung besteht daher darin, dass das BfS sein Begehren direkt an die zuständige Grundbuchbehörde richtet. Alternativ kann das Amt für Immobilienbewertung die relevanten Informationen intern an das Grundbuchinspektorat weiterleiten, welches anschliessend in eigener Zuständigkeit und gestützt auf die einschlägigen bundesrechtlichen Vorgaben über die Datenbekanntgabe entscheidet.

Zusammenfassend fehlt es dem Amt für Immobilienbewertung an einer hinreichenden gesetzlichen Grundlage für die direkte und insbesondere

systematische Weitergabe von Grundbuchdaten an das BfS. Weder das Datenschutzrecht noch das Bundesstatistikgesetz vermögen eine solche Datenübermittlung in der vorliegenden Konstellation zu rechtfertigen.

6. Weitergabe von Mitarbeiterdaten an den Kanton

Im Zusammenhang mit einer arbeitsrechtlichen Auseinandersetzung wurde einer Mitarbeiterin der Elternberatung in einer Region des Kantons Graubünden gekündigt. Die Elternberatung ist organisatorisch einem Regionalspital angegliedert. Die betroffene Mitarbeiterin stellt sich die Frage, ob die Institution berechtigt war, persönliche Unterlagen im Zusammenhang mit der Kündigung an das Gesundheitsamt Graubünden weiterzuleiten.

Fehlerhafte formale Adressierung

Es bestehen Unstimmigkeiten hinsichtlich der formellen Adressierung durch ein kantonales Amt. Dabei handelt es sich jedoch um ein rein formales Problem. Es wird nicht geltend gemacht, dass Unterlagen einer unbeteiligten Drittperson zugestellt worden wären.

Gemäss Art. 1 Abs. 1 KDSG bezweckt das Datenschutzrecht den Schutz vor widerrechtlicher Bearbeitung von Personendaten durch Behörden. Die Zuständigkeit des entsprechenden Amtes für die Bearbeitung der Daten im Rahmen der amtlichen Tätigkeit ist unbestritten. Eine datenschutzrechtlich relevante Persönlichkeitsverletzung ist bei lediglich formalen Unzulänglichkeiten nicht ersichtlich. Bagatellfehler in der Adressierung – wie etwa das Fehlen eines Kommas oder die Schreibweise des Namens in Grossbuchstaben – sind datenschutzrechtlich unbeachtlich, solange die betroffene Person eindeutig identifiziert werden kann. Dies ist vorliegend der Fall. Eine unzulässige Bekanntgabe an Dritte oder eine sonstige missbräuchliche Datenbearbeitung ist weder geltend gemacht noch ersichtlich.

Die Frage, ob eine fehlerhafte Adressierung Auswirkungen auf die formgültige Eröffnung oder den Fristenlauf hat, ist ausschliesslich prozessrechtlicher Natur und nicht Gegenstand des Datenschutzrechts.

Gemäss Art. 5 Abs. 1 lit. b des Gesundheitsgesetzes des Kantons Graubünden (GesG) obliegt die Mütter- und Väterberatung dem Kanton. Nach Art. 1 Abs. 1bis der Verordnung zum Gesundheitsgesetz (VOzGesG) kann die Regierung diese Aufgabe an Dritte übertragen. Von dieser Möglichkeit wurde Gebrauch gemacht, indem zwischen der Regierung des Kantons Graubünden und der Regionalspital AG eine Leistungsvereinbarung über die Durchführung der Elternberatung abgeschlossen wurde.

Diese Vereinbarung regelt die Zusammenarbeit detailliert. So verpflichtet Ziffer 4.8 die Auftragnehmerin, dem Gesundheitsamt jährlich insbesondere Angaben zu den Qualifikationen der Mitarbeitenden zu übermitteln. Zudem sind gemäss Ziffer 4.9 personelle Veränderungen sowie auch Umstände unverzüglich zu melden, die den ordnungsgemässen Betrieb in fachlicher, organisatorischer oder finanzieller Hinsicht beeinträchtigen könnten.

Damit ist festzuhalten, dass die Weitergabe bestimmter personenbezogener Daten vertraglich ausdrücklich vorgesehen ist. Zu klären bleibt, ob darüber hinausgehende Unterlagen – insbesondere im Zusammenhang mit arbeitsrechtlichen Auseinandersetzungen – übermittelt werden dürfen.

Bei der Auslegung von Ziffer 4.9 ist zu berücksichtigen, dass der Kanton trotz Delegation der Aufgabenerfüllung die Gesamtverantwortung behält. Daraus ergibt sich ein legitimes Interesse an umfassender Information über personelle Vorgänge, soweit diese den ordnungsgemässen Betrieb der Leistungserbringung betreffen. Die vertraglich vorgesehenen Meldepflichten sind vor diesem Hintergrund weit auszulegen und umfassen auch relevante arbeitsrechtliche Konflikte. Folglich ist der Kanton berechtigt, über entsprechende Auseinandersetzungen informiert und – soweit erforderlich – auch dokumentiert zu werden.

Aus datenschutzrechtlicher Sicht ist die Weitergabe der hierfür notwendigen personenbezogenen Daten zulässig, da sie auf einer vertraglichen Grundlage beruht und zur Wahrnehmung der dem Kanton obliegenden Aufsichtsfunktion erforderlich ist. Das Vorgehen des Regionalspitals ist daher rechtlich nicht zu beanstanden.

VI. Abkürzungsverzeichnis

a.a.O.	am angeführten Ort
Abs.	Absatz
AFI	Kantonales Amt für Informatik
a.M.	anderer Meinung
Art.	Artikel
B	Botschaft
BBl	Bundesblatt
BfS	Bundesamt für Statistik
BG	Bundesgesetz
BGE	Bundesgerichtsentscheid
BGer	Bundesgericht
Bl	Blatt
BR	Bündner Rechtsbuch
BStaG	Bundesgesetz für Statistik
BV	Bundesverfassung
bzw.	beziehungsweise
DIEM	Departement für Infrastruktur, Energie und Mobilität
DFG	Departement für Finanzen und Gemeinden
DJSG	Departement für Justiz, Sicherheit und Gesundheit
DSB	Datenschutzbeauftragter
DSG	Bundesgesetz über den Datenschutz
DVS	Departement für Volkswirtschaft und Soziales
EDOEB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EKUD	Erziehungs-, Kultur- und Umweltschutzdepartement
ERG	Gesetz über die Einwohnerregister und weitere Personen- und Objektregister
etc.	et cetera
f./ff.	folgend/folgende
GesG	kantonales Gesundheitsgesetz
GPK	Geschäftsprüfungskommission
GR	Graubünden
Hrsg.	Herausgeber
KDSG	Kantonales Datenschutzgesetz
KESB	Kindes- und Erwachsenenschutzbehörde
KV	Kantonsverfassung
lit.	litera
N	Note
RB	Rechtsbuch
Rz	Randziffer
S	Seite
SR	Sammlung der eidgenössischen Gesetze und systematische Sammlung des Bundesrechts (Systematische Rechtssammlung)
TB	Tätigkeitsbericht
usw.	und so weiter
vgl.	vergleiche
VOz-GesG	Verordnung zum kantonalen Gesundheitsgesetz
z.B.	zum Beispiel
ZGB	Schweizerisches Zivilgesetzbuch
Ziff.	Ziffer