Tätigkeitsbericht 2021

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. Vorwort

Cybersicherheit

In der Schweiz wurden nach Angaben des Bundesamtes für Statistik im Jahre 2021 30'351 Fälle von Cyberkriminalität registriert. Die Dunkelziffer ist dabei nicht berücksichtigt. Die Anzahl dieser Delikte steigen jährlich mit zweistelligen prozentualen Wachstumsraten, z.B. vom Jahre 2020 zum Jahre 2021 um 24.4%, währenddem die Deliktszahl insgesamt (inkl. Cyber-Delikte) im gleichen Zeitraum nur um 8.5% zunahm. Bei den Betrugsfällen betraf der modus operandi der digitalen Kriminalität 76.3%, und bereits mehr als ein Drittel aller Straftaten haben einen digitalen Hintergrund. Die Zahlen sind alarmierend. Die digitale Kriminalität umfasst alle sogenannten «digitalen» Straftaten, die im Wesentlichen den Straftaten entsprechen, die in Telekommunikationsnetzen, insbesondere dem Internet, begangen werden.

Die Corona-Krise hat diese Tendenz noch verstärkt. Im Zuge von Homeoffice wurden vermehrt private IT-Geräte für dienstliche Zwecke eingesetzt. Diese vergrösserte IT-Umgebung ist nun oft weniger geschützt als beruflich genutzte IT-Geräte. Digitale Informationsangebote, soziale Medien, Streaming- und Cloud-Dienste, E-Mails und Telefon- bzw. Videokonferenzprogramme werden verstärkt genutzt. Die intensivere Nutzung des Internets und unerfahrene Nutzer bieten kriminellen Akteuren mehr Angriffsfläche. Es hat sich gezeigt, dass der Mensch nach wie vor das schwächste Glied im Bereich der IT-Sicherheit ist. Software mit Sicherheitslücken sowie veraltete Betriebssysteme (z.B. Windows 7), welche noch immer auf zahlreichen privaten Geräten laufen, bilden ideale Einstiegsmöglichkeiten. Verunsicherung, Neugierde und das Informationsbedürfnis des Menschen werden gezielt und professionell für kriminelle und heimtückische Aktivitäten ausgenutzt. Dabei passen die Cyberkriminellen ihre Taktik den veränderten Umständen an. Sie folgen ihren Opfern gleichsam nach Hause.

Nur langsam nimmt das Bewusstsein in der Bevölkerung zu, dass betrügerische E-Mails, Phishing-Versuche und Spam-Mails eine ernstzunehmende Bedrohung darstellen und es sich gegen Betrugsversuche zu wehren gilt. Angesichts der gesteigerten Cyber-Gefahren ist es wichtig, die Mitarbeitenden kontinuierlich für dieses Thema zu sensibilisieren und zu schulen. Es gehören aber auch geeignete Sicherheitsüberwachungen dazu, ohne dass dadurch eine nach Arbeitsgesetz verbotene digitale Überwachung der beruflichen Tätigkeit einhergeht.

Die Arbeitgeber, die Arbeitnehmenden, die IT-Industrie und die Strafverfolgungsbehörden sind gefordert, sich Tag für Tag zu verbessern. Bemühende, kostenintensive und zeitraubende Arbeiten sind unabdingbar, wenn wir den Wettbewerb gegen hochprofessionelle kriminelle Banden nicht verlieren wollen.

Kantonaler Datenschutzbeauftragter:

Thomas Casanova

II. Allgemeines

1. Homeoffice

Homeoffice war im Jahre 2021 eines der bestimmenden Themen. Unter dem Begriff Homeoffice wird jene Arbeit verstanden, die Arbeitnehmende ganz oder teilweise, regelmässig oder unregelmässig von zu Hause aus verrichten. Dabei ist der häusliche Arbeitsplatz normalerweise mit dem betrieblichen Arbeitsplatz durch elektronische Kommunikationsmittel verbunden.

Die Corona-Krise hat dem Homeoffice endgültig zum Durchbruch verholfen. Sowohl in der Privatwirtschaft als auch in der öffentlichen Verwaltung mussten innert kurzer Zeit Ressourcen geschaffen und technische Massnahmen ergriffen werden, um die Arbeitstätigkeit aufrechterhalten zu können. Auch wenn die Corona-Pandemie am abklingen ist und die Arbeitnehmenden wieder an ihre angestammten Arbeitsplätze zurückkehren, konnten die am Arbeitsmarkt Beteiligten Erfahrungen in dieser für viele immer noch neuen Arbeitsweise sammeln. Homeoffice wird sich in Zukunft im Arbeitsalltag etablieren. Es ist deshalb wichtig zu wissen, ob und allenfalls unter welchen Bedingungen die Arbeit von zu Hause aus möglich sein wird.

Die öffentlich-rechtlichen Personalgesetze kennen den Begriff «Homeoffice» nicht. Ebenfalls im Obligationenrecht finden sich dazu keine Bestimmungen (die Regeln zum Heimarbeitsvertrag sind nicht anwendbar). Es besteht kein gesetzlicher Anspruch auf Arbeit im Homeoffice. Folgerichtig bedarf es einer individuellen Vereinbarung zur Leistung von Arbeit an einem Ort ausserhalb des Arbeitsplatzes im Unternehmen bzw. der Dienststelle.

Gemäss den gesetzlichen Vorgaben hat im Regelfall der Arbeitgeber die Mitarbeitenden mit den Arbeitsgeräten und dem Material auszurüsten. Es ist jedoch möglich, abweichende Regelungen zu treffen und zu vereinbaren, dass die Mitarbeitenden die Arbeitsgeräte und das Material im Homeoffice selbst zur Verfügung stellen. Mit der Auslagerung der Arbeitstätigkeit in den privaten Wohnraum stellen sich mannigfaltige neue Rechtsfragen: Wie läuft der Informationsaustausch, welcher Zugang besteht zu betrieblichen Daten, wie funktioniert der betriebliche Support, welche Arbeitszeiten sind einzuhalten, welche Qualitätsstandards gelten, wie kann der Arbeitgeber die Arbeit kontrollieren, wer trägt die Kosten usw. Es versteht sich von selbst, dass die Arbeit im Homeoffice ein hohes Mass an Eigenverantwortung der Mitarbeitenden voraussetzt. Über-

wachungs- und Kontrollsysteme, die einzig den Zweck haben, die Mitarbeitenden bei ihrer Arbeit zu überwachen, sind generell und auch im Homeoffice unzulässig. Eine angemessene Überwachung der Sicherheit, die Kontrolle der Produktivität und Arbeitsqualität sowie des Informationsaustausches ist dagegen erlaubt. In der Praxis ist die Unterscheidung zwischen nicht erlaubten Überwachungsmassnahmen und legitimen Kontrolltätigkeiten nicht immer leicht zu ziehen, zumal bis anhin zumindest gerichtliche Leitentscheide weitgehend fehlen.

Die gesetzlichen Vorgaben wie Gesundheitsschutz oder Arbeits- und Ruhezeiten ändern sich bei der Arbeitstätigkeit von zu Hause aus nicht. Sie werden aber anspruchsvoller in der Um- und Durchsetzung. Es bedarf der aktiven Beteiligung der Arbeitnehmenden. Der Arbeitgeber ist verpflichtet, für die gesetzeskonforme Durchführung der Arbeit im Homeoffice Regelungen organisatorischer und technischer Art zu treffen. Ein Teil davon ist auch die Einhaltung der datenschutzrechtlichen Grundprinzipien. So hat er für die sichere Übermittlung zu sorgen, eine zuverlässige Authentifizierung einzurichten und insbesondere die Mitarbeitenden zu schulen und zu sensibilisieren. Art. 7 DSG hält explizit fest, dass Personendaten durch organisatorische und technische Massnahmen gegen unbefugtes Bearbeiten zu schützen sind. Währenddem der Arbeitgeber vorab durch technische Massnahmen seinen Verpflichtungen nachkommen kann, stellen sich bei den Mitarbeitenden vorwiegend konkrete praktische Probleme. Die Mitarbeitenden sind verpflichtet, die Geschäftsinformationen und Personendaten vor dem Zugriff Unberechtigter, auch vor Familienmitgliedern, zu schützen. Geschäftliche Daten auf dem privaten Computer sind sicher und getrennt von anderen Daten aufzubewahren, private und geschäftliche E-Mails sind zu trennen und Geschäftsunterlagen, wie Notizen, Entwürfe, Kopien oder Musterdokumente sind end-

Bekanntgabe von Impfdaten

Eine Behörde möchte die Mitarbeitenden über den Impfstatus ihrer Kollegen informieren. Es fragt sich, ob eine solche Mitteilung im Einklang mit den datenschutzrechtlichen Anforderungen steht.

Bei Impfdaten handelt es sich um Gesundheitsdaten. Diese Daten werden als besonders schützenswert qualifiziert (Art. 3 lit. c Ziff. 2 DSG). Gesundheitsdaten sind entsprechend zu bearbeiten. Hinzuweisen ist insbesondere auf Art. 17 Abs. 2 DSG, wonach besonders schützenswerte Personendaten nur bearbeitet werden dürfen, wenn ein Gesetz im formellen Sinn es ausdrücklich vorsieht oder die Bearbeitung für eine im Gesetz klar umschriebene Aufgabe unentbehrlich ist. Beim Bearbeiten von Personendaten ist zudem der Grundsatz der Verhältnismässigkeit zu beachten. Ausfluss dieses Grundsatzes ist, dass nur diejenigen Daten bekannt gegeben werden dürfen, die für die Erfüllung einer Aufgabe erforderlich sind. Die Mitteilung an alle Mitarbeiter, wer welchen Impfstatus hat, ist nun klarerweise für die Mitarbeitenden nicht erforderlich, um deren Aufgaben erfüllen zu können. Die Mitteilung des Impfstatus an alle Mitarbeitenden ist offensichtlich nicht datenschutzkonform.

gültig zu vernichten. Entscheidend für die datenschutzkonforme Umsetzung der Arbeit zu Hause sind die räumlichen und familiären Verhältnisse. In räumlicher Hinsicht muss gewährleistet sein, dass getrennt von anderen Familienmitgliedern gearbeitet werden kann. Homeoffice am Mittagstisch kann weder aus datenschutz- noch arbeitsrechtlicher Sicht durchgeführt werden. Homeoffice kann nur gestattet werden, wenn dessen einwandfreie Umsetzung gewährleistet werden kann. Dies kann dazu führen, dass für Arbeiten, die grundsätzlich von zu Hause aus erledigt werden könnten, keine Erlaubnis erteilt werden kann. Die Mitarbeitenden sind gegenüber dem Arbeitgeber verpflichtet, den Nachweis zu erbringen, dass auf Grund der räumlichen und familiären Situation ein Arbeiten im Homeoffice möglich ist. Dabei ist ein strenger Massstab anzulegen.

Da sich Berufliches und Privates nirgends so sehr vermischt wie im Homeoffice, ist es wichtig, klar festzuhalten, was bei Vertragsende mit den dem Arbeitnehmenden überlassenen, allenfalls auch privat genutzten Geräten, den Geschäftsunterlagen und den auf privaten Datenträgern gespeicherten Betriebsdaten zu geschehen hat. Ideal wäre die strikte Trennung zwischen privatem und geschäftlichem Gebrauch. Denn oft geht vergessen, dass moderne Peripheriegeräte wie Drucker, Scanner oder Kopierer über lokale Festplatten mit Datenspeicher verfügen können, so dass - unter Berücksichtigung des Datenschutzes - theoretisch nur durch eine professionelle Löschung der lokalen Daten ein sauberes Ende gefunden werden kann.

Der Arbeitnehmende unterliegt im Homeoffice denselben Geheimhaltungs- und Datenschutzpflichten wie an seinem gewöhnlichen Arbeitsort. Aus Sicherheitsgründen und mit Blick auf die Haftung ist zu regeln, welche Aufgaben überhaupt ausserhalb der Büroräumlichkeiten erledigt werden dürfen und wie mit sensiblen Daten (Datenspeicherung) und Unterlagen (digital und auf Papier) umzugehen ist.

Soll die Arbeit im Homeoffice permanent zugelassen werden, empfiehlt es sich, ein entsprechendes Reglement oder eine entsprechende Weisung zu erlassen. Dieses Reglement sollte insbesondere Aussagen über folgende Punkte enthalten:

1. Umfang der Arbeit im Homeoffice
2. zeitliche Rahmenbedingungen
3. fachliche und räumliche Voraussetzungen
4. Vorgaben betreffend Einrichtung des Arbeitsplatzes
5. Ausrüstung des Arbeitsplatzes
6. Überwachungs- und Kontrollmassnahmen
7. Verhalten bei Störungen
8. Geheimhaltungspflichten
9. Beendigungsmodalitäten

Moderne Arbeitsformen können in der Verwaltung durchaus umgesetzt werden. Voraussetzung dafür ist ein verantwortungsvolles und konzeptionelles Verhalten von Arbeitgebern und Arbeitnehmenden. Homeoffice setzt einerseits Disziplin, Motivation, gute Selbstorganisation und effektives Zeitmanagement voraus, andererseits aber auch die erforderliche Infrastruktur am Arbeitsplatz zu Hause.

2. Grossraumbüro und Datenschutz

Eine Vielzahl von kantonalen Angestellten ist in den Neubau an der Ringstrasse in Chur gezogen und hat sich an das Arbeiten in einem Grossraumbüro gewöhnt. Kann aus datenschutzrechtlicher Warte uneingeschränkt in einem Grossraumbüro gearbeitet werden? Allein die Tatsache, dass zahlreiche Personen in einem Raum arbeiten, führt nicht zwangsläufig zu rechtlichen Problemen. Indessen sind auf gewisse Faktoren ein besonderes Augenmerk zu legen. Rein exemplarisch werden die wichtigsten Aspekte beispielhaft aufgeführt:

- Es ist durch technische und organisatorische Massnahmen sicherzustellen, dass keine Telefongespräche von aussenstehenden Dritten mitgehört werden können (z.B. Telefonkabinen, Telefon mit Unterdrückung von Hintergrundgeräuschen etc.).

- Besprechungen mit Drittpersonen dürfen nicht im Mehrpersonenbüro durchgeführt werden. Für diesen Zweck müssen genügend Besprechungszimmer zur Verfügung stehen.

- Es ist danach zu trachten, dass persönliche Gespräche mit Mitarbeitenden auf «neutralem» Boden erfolgen.

- Der eigene Arbeitsplatz ist vor Arbeitsschluss oder einer Abwesenheit aufzuräumen und Akten mit Personenbezug sind adäquat zu sichern.

- Der einzelne Arbeitsplatz ist so zu gestalten, dass genügend Abstand eingehalten wird und akustisch keine Störungen auftreten.

- Der Qualität der zu bearbeitenden Personendaten ist gebührend Aufmerksamkeit zu schenken; je sensibler die Daten sind, desto grösser müssen die Sicherheitsvorkehrungen sein. Beim Umgang mit besonders schützenswerten Personendaten kann dies situativ dazu führen, dass die Bearbeitung in abgetrennten Räumen zu erfolgen hat.

Offene Bürolandschaften können mit zusätzlichen baulichen Massnahmen (z.B. Telefonkabinen, Rückzugsräume, genügend Besprechungszimmer etc.) und vor allem durch die persönliche Aufmerksamkeit der Mitarbeitenden durchaus datenschutzkonform betrieben werden. Es ist Aufgabe der Vorgesetzten, die datenschutzrechtlichen Vorgaben in ihrem Wirkungskreis durchzusetzen.

III. Fälle aus der Praxis

1. Maskenpflicht

Gemäss Art. 36 Personalverordnung (PVO) der Gemeinde A achtet die Gemeinde A die Persönlichkeit der Angestellten und Lehrpersonen und schützt diese. Sie nimmt auf die Gesundheit der Angestellten und Lehrpersonen gebührend Rücksicht. Die Gemeinde ist verpflichtet, die zum Schutze der Gesundheit erforderlichen Massnahmen zu treffen. Sie sorgt im Weiteren insbesondere dafür, dass keine Angestellten auf Grund von Persönlichkeitsmerkmalen wie Geschlecht, Herkunft, politische Gesinnung, Sprache, Religion, geschlechtlicher Orientierung, Behinderung oder vergleichbaren Persönlichkeitsmerkmalen, diskriminiert werden. Es stellt sich primär die Frage, was unter dem Begriff Diskriminierung zu verstehen ist. Gemäss bundesgerichtlicher Rechtsprechung (vgl. statt vieler BGer 1D_6/2018 vom 3. Mai 2019) darf niemand diskriminiert werden, namentlich wegen der Herkunft, der Rasse, des Geschlechts, des Alters, der Sprache, der sozialen Stellung, der Lebensform, der religiösen, weltanschaulichen oder politischen Überzeugung oder wegen einer körperlichen, geistigen oder psychischen Behinderung. Die Diskriminierung stellt eine qualifizierte Ungleichbehandlung von Personen in vergleichbaren Situationen dar, in dem sie eine Benachteiligung von Menschen bewirkt, die als Herabwürdigung oder Ausgrenzung derselben einzustufen ist. Eine Diskriminierung liegt somit bei einer nachteiligen Behandlung vor, die sich auf eine unrechtmässige Grundlage abstützt und bei welcher eine angebrachte und objektive Rechtfertigung fehlt. Liegt der Handlung ein legitimes Ziel zu Grunde, wie zum Beispiel der Schutz der Gesundheit und ist die Handlung verhältnismässig, so fehlt ihr das diskriminierende Element. Vereinfacht gesagt liegt also eine Diskriminierung immer dann vor, wenn identitätsbildende und mit einem gewissen Stigmatisierungspotential versehene Eigenschaften, welche nur schwer abänderbar und deren Veränderung unzumutbar sind, zu Unrecht entweder als unmittelbarer oder mittelbarer Anknüpfungspunkt einer Handlung herangezogen oder anlässlich einer Handlung unterdrückt werden. Folgerichtig ist zunächst zu prüfen, ob die massgebenden tatsächlichen Merkmale als Differenzierungskriterien herangezogen werden können und ob diese Merkmale zu den konstituierenden Elementen der Wertschätzung eines Menschen als Person gehören oder nicht. Nicht jede Ungleichbehandlung führt zu einer Diskriminierung.

Die Gemeinde ist als Arbeitgeberin verpflichtet, die erforderlichen Massnahmen zum Schutze der Gesundheit ihrer Angestellten und Lehrpersonen zu treffen. Die in Art. 36 PVO legiferierten Grundsätze korrespondieren mit den Schutzpflichten eines Arbeitgebers gemäss Art. 328 OR. Danach hat der Arbeitgeber zum Schutze der Gesundheit der Arbeitnehmer diejenigen Massnahmen zu treffen, die nach der Erfahrung notwendig, nach dem Stand der Technik anwendbar und den Verhältnissen des Betriebes angemessen sind. Dazu gehört auch die Pflicht der Arbeitgeberin, die Gesundheit des einzelnen Arbeitnehmenden vor Beeinträchtigung durch Dritte wie auch Mitarbeiter zu schützen, wozu auch der Schutz vor einer Ansteckung durch potentiell erkrankte Arbeitskollegen oder andere Personen, mit denen der Arbeitnehmende im Rahmen seiner Arbeitstätigkeit in direktem Kontakt steht, zählt.

Im Bereich des Arbeitsrechts werden die allgemeinen Bestimmungen des Datenschutzgesetzes durch Sonderbestimmungen punktuell ergänzt. Hinzuweisen ist namentlich auf Art. 328b OR. Vor diesem Hintergrund erachtet die Lehre es als grundsätzlich zulässig, Daten über den Gesundheitszustand eines Arbeitnehmers zu bearbeiten, um andere Mitarbeiter sowie Drittpersonen vor ansteckenden Krankheiten zu schützen, sofern auf Grund der Arbeitstätigkeit ein erhöhtes Ansteckungsrisiko besteht.

Ein Unternehmen und auch eine Kommune sind gesetzlich verpflichtet, ihre Mitarbeitenden davor zu schützen, dass sie sich im Unternehmen mit einer Krankheit anstecken, wobei der Umfang der Schutzpflichten von den konkreten Umständen abhängt. Zweck der Schutzvorkehrung ist es also, zu verhindern, dass Mitarbeitende, von denen eine Covid-19-Ansteckungsgefahr ausgeht, sich am Arbeitsplatz aufhalten und dort Arbeitskollegen einem Ansteckungsrisiko aussetzen. Zumindest die potentiell gefährdeten Arbeitnehmenden sind mit geeigneten Massnahmen zu schützen. Ein adäquates Mittel dazu besteht im Tragen einer Schutzmaske. Es kann also festgestellt werden, dass der Arbeitgeber befugt ist, eine Schutzmaskenpflicht anzuordnen, wenn die erhöhte Gefahr einer Ansteckung besteht. Aktuell ist bekannt, dass genesene oder geimpfte Personen über eine geraume Zeit vor einer Übertragung des Virus geschützt sind. Aus epidemiologischer Sicht ist es demnach möglich, Geimpfte bzw. Genesene und Nicht-Geimpfte unterschiedlich zu behandeln. Wenn folgerichtig die Gemeinde das Maskentragen in einem gemeinsam genutzten Fahrzeug lediglich dann verlangt, wenn eine Person nicht geimpft oder nicht genesen ist, handelt es sich nicht um eine Diskriminierung im rechtlichen Sinn. Es stellt sich lediglich die Frage, ob

die Anordnung des Tragens einer Maske verhältnismässig ist. Wenn eine Person, bei welcher der Gesundheitszustand nicht eindeutig festgestellt werden kann, sich in einem engen Raum mit anderen Personen aufhalten muss, müssen Schutzmassnahmen getroffen werden. Eine adäquate Massnahme besteht im Tragen einer Schutzmaske. Diese Massnahme kann als geringer Eingriff in die Persönlichkeit qualifiziert werden. Sie führt nicht zu einer Stigmatisierung der betroffenen Person. Die Vorschrift, eine Maske zu tragen, ist den Verhältnissen angepasst und sachgerecht. Der Gesundheitsschutz ist für alle beteiligten Personen höher zu gewichten, als die marginale Einschränkung der betroffenen Person bzw. die Offenlegung des Umstandes, dass keine Impfung gegen oder Genesung einer durchlittenen Krankheit vorliegt. In Anwendung von Art. 36 PVO ist die Gemeinde berechtigt, eine Maskentragpflicht anzuordnen, sofern eine Person kein Covid-Zertifikat vorweisen kann.

2. *Auslagerung von Gesundheitsdaten*

Ist beim Outsourcing von Aufgaben eines Spitals eine Zustimmung der Patienten erforderlich?

Ein Bearbeiten im Auftrag liegt vor, wenn ein öffentliches Organ oder eine Organisation mit einem Leistungsauftrag Informationen, d.h. Sach-, Personen- oder besondere Personendaten durch Private oder andere öffentliche Organe bearbeiten lässt. Das konkrete Auslagern der Pseudonymisierung bedeutet mithin eine Datenbearbeitung im Auftrag.

Dem Bearbeiten im Auftrag dürfen keine rechtlichen Bestimmungen entgegenstehen, wie beispielsweise das Amts- oder Berufsgeheimnis. Werden die Daten verschlüsselt und verbleibt der Schlüssel bzw. das Schlüsselmanagement beim Auftraggeber, kann auch bei umfassenden Geheimnispflichten ausgelagert werden. Ob das Berufsgeheimnis auch für die Auftragnehmer gilt, ist umstritten. Deshalb sind bei solchen Bearbeitungen im Auftrag spezifische Massnahmen zum Schutze der Daten umzusetzen.

Bekanntlich bleibt der Auftraggeber für die ausgelagerten Daten und Datenbearbeitungen verantwortlich. Dieser Umstand ist im zu beurteilenden Sachverhalt massgebend. Der Auftraggeber muss in der Lage sein, die Pflichten zum Schutz der Informationen wahrzunehmen. Eine sorgfältige Auswahl des Vertragspartners ist deshalb unabdingbar. Eine Zertifizierung nach anerkannten Standards und die dieser zu Grunde liegende Qualitätssicherung sowie Auditberichte können bei der Auswahl behilflich sein. Erforderlich ist bei der Auswahl des Vertragspartners eine seriöse und sorgfältige Risikoanalyse. Für den Auftragnehmer bedeutet die Auslagerung, dass er die Daten nur insoweit bearbeiten darf, als es der Auftraggeber tun dürfte und dass er dieselben Sicherheitsanforderungen in Bezug auf die Gewährleistung von Vertraulichkeit, Verfügbarkeit und Integrität erfüllen muss. Der Auftraggeber muss die Risiken in Bezug auf die vorgenannten Aspekte analysieren, die Informationen einer Schutzstufe zuordnen und die Informationssicherheitsmassnahmen definieren. Die Informationen dürfen unberechtigten Dritten nicht zugänglich sein, verloren gehen oder unbefugt abgeändert werden können. Aus diesen Beurteilungen resultieren die geforderten Massnahmen. Je sensitiver die Daten sind, desto umfangreicher haben die Massnahmen zu sein. Die Umsetzung der im Vertrag festgehaltenen Massnahmen muss vom Auftraggeber periodisch kontrolliert werden. Es können dafür auch Auditberichte von unabhängigen Prüfstellen in Anspruch genommen werden.

Bei der Auslagerung von Daten zur Bearbeitung im Interesse des Auftraggebers handelt es sich nicht um eine Bekanntgabe von Personendaten im Sinne von Art. 19 DSG. Die Verantwortung verbleibt beim Auftraggeber. Er bleibt Datenherr. Der Auftragsdatenbearbeiter ist gleichsam Hilfsperson des Auftraggebers. Folgerichtig bedarf die Auslagerung der Pseudonymisierung von Patientendaten keiner Zustimmung der betroffenen Personen.

3. Kontrolle Urinabgabe

In einer verkehrsmedizinischen Praxis müssen die Probanden Urinproben unter Aufsicht einer Medizinalperson abgeben, um damit Manipulationsversuche zu unterbinden. Die Sichtkontrolle wird von der Schweizerischen Gesellschaft für Rechtsmedizin gefordert und ist auch in anderen forensischen Settings obligatorisch. Die Urinabgabe unter Sicht wird von den Probanden als invasiv und erniedrigend erlebt und ist auch für die Untersuchenden nicht angenehm. Im Rahmen von baulichen Massnahmen soll nun geprüft werden, ob die direkte Sichtkontrolle durch eine Kamera ersetzt werden könnte und welche Voraussetzungen dafür erfüllt werden müssen. Dabei sind drei Szenarien zu prüfen. Nach Szenario A würde eine Videokamera eingesetzt, deren Aufnahmen durch die Medizinalperson unmittelbar gesichtet würden und keine Aufzeichnung vornimmt. Es wäre gleichsam die bisherige Sichtkontrolle per Video. Gemäss Szenario B würde eine Kamera die Urinabgabe für einige Stunden aufzeichnen. Damit könnte man die Aufzeichnung nur bei Verdacht auf Manipulation sichten oder den Zeitpunkt der Sichtung freier wählen. Nach Szenario C würde die Toilette angepasst, welche die Sichtkontrolle direkt oder mit Spiegel ermöglichen würde.

Eine Übertragung von Daten ohne Aufzeichnung fällt m.E. nicht unter die Normen der Videoüberwachung. Vielmehr handelt es sich um ein technisches Hilfsmittel, das die physische Anwesenheit ersetzt. Gewisse Datenschutzbeauftragte und der Grossteil der Literatur vertreten jedoch eine andere Meinung. Bis anhin wurden «Direktübertragungen» in Graubünden nicht als Videoüberwachung abgehandelt und dementsprechend zugelassen (vgl. Stadtpolizei Chur). An dieser Praxis ist festzuhalten. Folgerichtig kann Szenario A aus datenschutzrechtlicher Sicht realisiert werden. Die Probanden sind selbstverständlich darauf hinzuweisen, dass keine Aufzeichnung erfolgt und wenn eine Person den Einsatz von Kameras ablehnt, muss das bisher übliche Vorgehen gewählt werden.

Problematischer präsentiert sich Szenario B. Videoaufzeichnungen im Gesundheitswesen sind datenschutzrechtlich heikel. Wenn medizinische Daten mittels Videoaufzeichnung gespeichert werden, bedarf dies grundsätzlich immer einer ausdrücklichen Einwilligung der Probanden. Diese Einwilligung muss freiwillig erfolgen. Die Erhebung von Gesundheitsdaten stellt einen Eingriff in die Persönlichkeitsrechte des Probanden dar. Dieser bedarf eines Rechtfertigungsgrundes, der regelmässig nur in der Einwilligung des Patienten zu finden ist. Selbst wenn für die Abnahme einer Urinprobe eine gesetzliche Grundlage besteht, kann aus diesem Umstand nicht die Zulässigkeit der bildmässigen Speicherung des Abnahmeprozederes abgeleitet werden. Das Vorgehen nach Szenario B

ist mithin nur bei Vorliegen einer ausdrücklichen Zustimmung des Probanden möglich. Wird diese verweigert, verbleibt zwangsläufig nur die Abgabe der Urinprobe unter Aufsicht einer Medizinalperson.

Das Szenario C entspricht faktisch dem Ist-Zustand und kann durchgeführt werden.

4. Bekanntgabe der Adressdaten von Schülerinnen und Schülern

Hat die Gemeinde Anspruch auf Bekanntgabe der Adressdaten von Schülerinnen und Schülern, die in einem Spital unterrichtet werden?

Im Zusammenhang mit der Schulung und Förderung von erkrankten oder verunfallten Schülerinnen und Schülern in Spitälern und Kliniken ist im Rahmen der Revision des Schulgesetzes eine Änderung eingetreten. Vorübergehend erkrankte oder verunfallte Schülerinnen und Schüler der Regelklasse können nicht mehr als Schülerinnen oder Schüler der Sonderschülerschaft betrachtet werden und gelten deshalb als Regelschüler. Folgerichtig sind die Schulträgerschaften für diese Schüler zuständig.

Es stellt sich zunächst die Frage, wer für die Kosten des Schulangebotes in Kliniken und Spitälern aufzukommen hat. Der ehemalige Regierungsrat Martin Jäger empfahl in einem Schreiben vom 12. Februar 2018 zu Handen des Schulbehördenverbandes Graubünden unter anderem folgendes Vorgehen:

- Die Schulträgerschaften sollen die Beschulung der hospitalisierten Kinder an die Spitalschule delegieren.
- Die Rechnungen der Spitalschule sollen durch die Schulträgerschaft bezahlt werden, sofern nicht die zuständige Spitalregion die Aufwände pauschal übernimmt.
- Eine Kostengutsprache durch die Schulträgerschaft ist nicht notwendig.

Es stellt sich nun die Frage, ob der Gemeinde zu Kontrollzwecken die Namen der durch die Spitäler und Kliniken beschulten Kinder bekannt gegeben werden müssen. Nach Vorschlag der Regierung sollen die Vollkosten nach Massgabe der auf sie entfallenden Schultage des Vorjahres den zwölf Spitalregionen in Rechnung gestellt werden. Zur Aufteilung der Rechnung auf die einzelnen Gemeinden bzw. Schulträgerschaften soll auf den gleichen Verteilschlüssel wie für die übrigen Spitalleistungen abgestellt werden. Wenn nach dieser Abrechnungsmethode vorgegangen wird, ist die Gemeinde nicht auf die Namen der Kinder, welche sich stationär in einem Spital oder einer Klinik aufgehalten haben, angewiesen. Die Kostentragung richtet sich nach einer abstrakten Methode und stellt nicht auf die erbrachten Leistungen für betroffenen Kinder ab.

Wird jedoch konkret aufgeteilt auf die jeweilige Schulträgerschaft eine Abrechnung vorgenommen, muss die Gemeinde in die Lage versetzt werden, ihren Kontrollaufgaben nachkommen zu können. Dies kann nur geschehen, wenn der Gemeinde bzw. der Schulträgerschaft Name und Adresse eines betroffenen Kindes bekannt gegeben werden. In diesem Zusammenhang stellt sich die Frage, ob nicht besonders schützenswerte Personendaten ausgetauscht werden. Als Gesundheitsdaten im Sinne des Datenschutzgesetzes werden alle möglichen Informationen definiert, die auf welche Art auch immer, Rückschlüsse auf den körperlichen oder geistigen Gesundheitszustand einer Person erlauben. Es handelt sich mithin um Daten, die im weitesten Sinne einen medizinischen Befund darstellen und sich für die Betroffenen negativ auswirken können. Als medizinischer Befund wird das Ergebnis medizinischer Untersuchung, wie etwa einer körperlichen Untersuchung, einer psychischen Exploration oder einer labor- und gerätemedizinischen Untersuchung bezeichnet. Adressdaten für sich alleine betrachtet stellen somit keine besonders schützenswerten Personendaten dar. Selbstverständlich muss diese Aussage in einen Kontext gestellt werden. Auf Grund der Bekanntgabe der Adressdaten durch das Spital oder Klinik kann gefolgert werden, dass ein Kind in einer dieser Institutionen behandelt worden ist. Diese Information dürfte einer Schulträgerschaft aber ohnehin schon bekannt sein, fehlt doch ein stationär behandeltes Kind im Regelunterricht. Seitens der Erziehungsberechtigten muss der Schule bekannt gegeben werden, weshalb ein Kind am Schulunterricht nicht teilnehmen kann (Art. 10 Abs. 2, Art. 54 Abs. lit. a und insb. Art. 68 Schulgesetz). Mit der Bekanntgabe durch das Spital oder die Klinik wird die Schulträgerschaft lediglich in die Lage versetzt, eine konkrete Prüfung des ihr bekannten Sachverhaltes vorzunehmen. Die Bekanntgabe der Adressdaten von Kindern an die Schulträgerschaft, welche stationär in einem Spital oder einer Klinik behandelt worden sind, ist aus datenschutzrechtlicher Sicht im vorgenannten Fall nicht zu beanstanden.

5. IPads in der Schule

In einer Schule werden iPads an die Schülerinnen und Schüler abgegeben. Gemäss einer Vereinbarung mit den Schülern und Eltern sind die iPads nur für schulische Angelegenheiten zu gebrauchen und die Lehrer haben jederzeit das Recht, die iPads zu kontrollieren. Dürfen mit Blick auf den Datenschutz uneingeschränkt Kontrollen durchgeführt werden?

Es lässt sich praktisch nicht verhindern, dass die zur Verfügung gestellten iPads auch privat genutzt werden. Allein schon die Kontrolle einer Recherche, ob nun z.B. eine Homepage aus privaten oder schulischen Gründen aufgerufen wurde, gestaltet sich als schwierig. Die Unterscheidung zwischen schulischem und privatem Zweck ist fliessend. Es wird deshalb empfohlen, eine private Nutzung nicht gänzlich zu verbieten. Dabei ist wesentlich, dass eine Unterscheidung zwischen beiden Nutzungsarten erreicht werden kann. Im Mailverkehr ist dies einfach möglich, indem ein Ordner als privat deklariert wird oder Daten auf dem iPad ausdrücklich unter privat abgelegt werden. Es sollte eine technische Lösung angestrebt werden in dem Sinne, welche die erwähnte Unterscheidung ermöglicht. Dies hat den Vorteil, dass alles was schulischer Art ist, eingesehen werden kann und alles was privat konsumiert oder gespeichert wird, nicht kontrolliert wird.

Schultestung

Bekanntlich beruht die Testung von Kindern in der Schule auf Freiwilligkeit. Wenn nun Eltern die Zustimmungserklärung nicht zurücksenden, liegt keine Zustimmung vor. Folgerichtig kann dieses Kind nicht getestet werden. Ein passives Verhalten der Eltern ist als Verweigerung der Zustimmung zu werten, unabhängig davon, ob nun die Erklärung versehen mit einem Nein zurückgesendet wurde oder die Eltern überhaupt nicht reagiert haben. Wie ist nun vorzugehen, wenn eine Pooltestung einer Schulklasse positiv ausgefallen ist?

Mit Bezug auf die Weitergabe von Daten aller betroffenen Kinder ist das Epidemiengesetz (EpG) massgebend. In den Art. 30 ff. EpG werden die möglichen Massnahmen gegenüber einzelnen Personen aufgeführt. Für die Durchsetzung der Massnahmen sind die Kantone zuständig. Gemäss Art. 33 EpG kann eine Person, die krank, krankheitsverdächtig, angesteckt oder ansteckungsverdächtig ist oder Krankheitserreger ausscheidet, identifiziert und benachrichtigt werden. Der Kanton kann für diese Person Massnahmen wie Quarantäne, Absonderung, ärztliche Untersuchung oder ärztliche Behandlung anordnen und durchsetzen. Wenn also in einer Klasse ein Fall ermittelt wird, kann das Gesundheitsamt die Daten sämtlicher Kinder der Klasse verlangen, da alle Kinder dieser Klasse krankheitsverdächtig sind, unabhängig davon, ob die Kinder am freiwilligen Test teilgenommen haben oder nicht. Personen dürfen indessen nicht prophylaktisch in eine Datenbank aufgenommen werden. Eine rechtliche Grundlage für die Identifizierung der Person besteht erst, wenn die vorgenannten Voraussetzungen erfüllt sind. Den Behörden sind diejenigen Daten auszuhändigen, welche erforderlich sind, um eine Identifizierung und Kontaktnahme vorzunehmen. Grundsätzlich sollte es genügen, wenn Name, Adresse, Geburtsdatum und Telefonnummer bekanntgegeben werden.

Privates bleibt privat. Das Schulorgan ist somit nicht berechtigt, Einsicht in die privaten Daten zu nehmen. Ergeben sich Verdachtsmomente ist das Vorgehen mit den Erziehungsberechtigten abzusprechen und deren Einverständnis einzuholen oder in Extremfällen sind die Strafverfolgungsbehörden zu informieren. Die Schule könnte sich natürlich auf den Standpunkt stellen, alle gespeicherten Informationen seien schulischer Natur, da nur schulisch relevante Daten bearbeitet werden dürfen.

Diese Sichtweise trägt jedoch der gelebten Wirklichkeit nicht Rechnung und ist deshalb theoretischer Natur, auch wenn entsprechende Vorgaben gemacht werden. Mit einer Unterscheidung von privater und schulischer Sphäre wird den Schülern auch eine gewisse Verantwortung übertragen. Es liegt sodann an den Schülerinnen und Schülern Disziplin zu wahren. Wenn also Daten nicht ausdrücklich als privat deklariert werden, sind sie schulischer Natur und können eingesehen werden. Eine entsprechende Unterscheidung erleichtert damit auch dem Lehrkörper die Arbeit.

Zusammenfassend ist die Schulträgerschaft nicht berechtigt, Einsicht in private Daten zu nehmen. Eine Kontrolle muss also so aufgegleist werden, dass nur schulisch relevante Daten kontrolliert werden. Eine Kontrolle sollte im Beisein der betroffenen Schülerin oder des betroffenen Schülers erfolgen. Damit wird auch auf die Bedeutung der persönlichen Daten und des Datenschutzes hingewiesen und dem Prinzip der Transparenz nachgelebt.

6. *Mitteilung der Erziehungsbeistandschaft an die Schuldirektion*

Ein Beistand wollte im Zusammenhang mit einer Erziehungsbeistandschaft Kontakt mit einer Schulbehörde aufnehmen. Es fragt sich, ob die damit verbundene Preisgabe von Informationen unter dem Gesichtswinkel des Datenschutzes zulässig ist.

Die Erziehungsbeistandschaft zeichnet sich dadurch aus, dass sie auf die individuellen Verhältnisse und Bedürfnisse ausgerichtet ist und das Kindswohl in jedem Fall im Vordergrund steht. In Art. 307 ZGB wird ausdrücklich auf das Erfordernis der Eignung der zu treffenden Massnahmen hingewiesen. Es gilt das Prinzip der Beschränkung auf den geringstmöglichen Eingriff. Ausfluss des Prinzips der Verhältnismässigkeit ist die präzise Festlegung des Inhalts des Auftrages. Der Auftrag limitiert die Handlungsbefugnis des Beistandes. Aus diesem Grund kann keine allgemein gültige Antwort auf die Fragestellung gegeben werden. Der Auftrag eines Beistandes kann durchaus schulische Belange umfassen. Wenn sich ein Berufsbeistand um schulische Aufgaben zu kümmern hat, ist der Einbezug der Lehrkraft oder der Schuldirektion denkbar und opportun. In einem solchem Fall kann der Bestand einer Erziehungsbeistandschaft den Schulbehörden zur Kenntnis gebracht werden.

Es kann also festgestellt werden, dass Informationen von Dritten im Einzelfall für die Ausübung der Erziehungsbeistandschaft erforderlich sind. Diese Informationen können nur eingeholt werden, wenn die Erziehungsbeistandschaft bekannt gegeben wird. Es muss in jedem Fall eine Interessenabwägung zwischen dem Kindswohl, als zentralem Element der Erziehungsbeistandschaft, und der Bekanntgabe der fraglichen Personendaten vorgenommen werden. Einer Schuldirektion kann der Bestand einer Erziehungsbeistandschaft jedoch mitgeteilt werden, wenn Informationen der Schule für die richtige Erfüllung des Auftrags erforderlich sind.

7. Einsicht in die Unterlagen eines Schülers

Ein Schüler der Gemeinde A besucht die Schule in der Gemeinde B. Nach Ablauf des Schuljahres muss die Schulkommission der Gemeinde A entscheiden, ob der Schüler wieder in der eigenen Gemeinde oder weiterhin in der Nachbargemeinde die Schule besuchen soll. Um einen sachgerechten Entscheid fällen zu können, möchte die Schulkommission Einsicht in das «Personaldossier» des Schülers, das bei der Schulleitung der Gemeinde B liegt, nehmen. Die Schulleitung verweigert die Einsichtnahme aus Gründen des Datenschutzes. Es stellt sich die Frage, ob die Schulkommission Einsicht in die Akten nehmen darf.

Gemäss Art. 17 Abs. 1 DSG darf die Schulleitung Personendaten bekannt geben, wenn dafür eine gesetzliche Grundlage besteht. Art. 17 Abs. 2 DSG hält fest, dass besonders schützenswerte Personendaten nur bearbeitet werden dürfen, wenn ein Gesetz im formellen Sinn es ausdrücklich vorsieht oder, wenn es ausnahmsweise für ein Gesetz im formellen Sinn klar umschriebene Aufgabe unentbehrlich ist.

Gemäss Art. 10 des Schulgesetzes der Gemeinde A obliegen der Schulkommission die Leitung und die Beaufsichtigung der Schule. Sie vollzieht die Gesetzgebung im Schulwesen, soweit auf Grund der kantonalen und kommunalen Gesetzgebung nicht ein anderes Organ dafür zuständig ist. Sie vertritt die Schule gegen aussen. Gestützt auf Art. 7 Abs. 2 des Schulgesetzes entscheidet die Schulkommission über die Aufnahme von auswärtigen Kindern. Die Schulkommission erstellt zu Handen des Gemeindevorstandes das Budget und sorgt für dessen Einhaltung. Dem gegenüber ist die Schul-

Daten von Musikschülern

Hat der Kanton das Recht, von den Schulen flächendeckend Listen mit den betroffenen Musikschülern einzuverlangen, für welche Kantonsbeiträge geleistet werden?

Im Kulturförderungsgesetz (KFG) werden die gesetzlichen Vorgaben für Sing- und Musikschulen festgelegt. In der entsprechenden Verordnung (KFV) ist festgehalten, welche Unterlagen dem Kanton zur Verfügung gestellt werden müssen. Gemäss Art. 18 Abs. 1 KFV sind die Gemeinden verpflichtet, dem Departement die Schülerzahl, die anspruchsberechtigten Unterrichtseinheiten sowie die Jahresbeiträge der Gemeinden und anderer öffentlich-rechtlicher Körperschaften mitzuteilen. Aus dieser Bestimmung geht hervor, dass keine Namensliste eingereicht werden muss. Art. 19 Abs. 2 KFG hält fest, dass ein Kantonsbeitrag für Kinder und junge Erwachsene bis zum vollendeten 20. Altersjahr ausgerichtet wird. Insofern kann der Kanton den Nachweis dafür verlangen. Konsequenterweise muss es genügen, wenn die Gemeinde bzw. die Sing- und Musikschule eine Tabelle abgeben, aus der hervorgeht, wie viele Kinder und junge Erwachsene in welchem Alter unterrichtet werden.

Der Kanton darf gestützt auf das KFG im Einzelfall eingehende Kontrollen durchführen. In einem solchen Einzelfall ist der Kanton möglicherweise auf detailliertere Angaben angewiesen. Es ist also vorstellbar, dass im Zusammenhang mit einer konkreten Prüfung der Anspruchsberechtigung die Personendaten der Kinder und jungen Erwachsenen einverlangt werden können. Zusammenfassend kann festgestellt werden, dass es an einer gesetzlichen Grundlage mangelt für das Einverlangen einer flächendeckenden Liste, welche die Schülerinnen und Schüler namentlich ausweist. Im Einzelfall darf zu Kontrollzwecken indes eine detaillierte Liste, welche auch die Namen der Schülerschaft umfasst, angefordert werden.

leitung für die operative Führung im Bereich Pädagogik und Sonderpädagogik, Personal, Organisation, Administration und Finanzen der Gemeindeschule verantwortlich.

Einschlägig ist Art. 6 kantonale Verordnung zum Schulgesetz. Danach sind in den Wechsel der Schulträgerschaft die Erziehungsberechtigten und die beiden betroffenen Schulräte bzw. Schulkommissionen involviert. Ein Schulwechsel kann nur erfolgen, wenn die Schulkommission ihr Einverständnis gibt. Um nun einen sachgerechten Entscheid fällen zu können, ist die Schulträgerschaft auf die relevanten Unterlagen das jeweilige Kind betreffend angewiesen. Die Schulträgerschaft ist in Anwendung von Art. 6 kantonale Schulverordnung berechtigt, ihr Einverständnis zurückzunehmen, wenn sich die Verhältnisse geändert haben und das Kind wieder in der Wohnortsgemeinde die Schule besuchen kann. Auch in diesem Fall ist die Schulkommission darauf angewiesen, die erforderlichen Unterlagen einzusehen, um einen adäquaten Entscheid fällen zu können. Folgerichtig sind der Schulkommission die relevanten Dokumente auszuhändigen.

Listenauskunft

Ein Verein hat bei einer Gemeinde die Adressdaten von Einwohnern, welche über 65 sind, angefragt. Es fragt sich, ob die Auskunft aus datenschutzrechtlicher Sicht zu erteilen ist.

Für die Listenauskunft ist Art. 32 Abs. 1 Einwohnerregistergesetz (ERG) massgebend. Danach kann eine Gemeinde Auskunft über Jahrgang, Name und Adresse listenmässig erteilen, wenn ein ideeller Zweck verfolgt wird. Weder in der Botschaft zum ERG noch in der parlamentarischen Debatte findet sich ein Hinweis auf die Definition des Begriffs ideell.

Im Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Basel-Stadt kann auf Seite 441 Folgendes nachgelesen werden: «Die Daten dürfen ausschliesslich für schützenswerte ideelle Zwecke bekannt gegeben werden. Als ideeller Zweck wird ein nicht materieller Beweggrund verstanden. Die Nutzung der Daten darf also nicht der Erwirtschaftung eines finanziellen Gewinns dienen, sondern muss -höhere- Ziele verfolgen.» Als Beispiele werden die Mitgliederwerbung für politische Parteien oder Kultur- und Sportvereine genannt. Auch darunter fallen Spendenaufrufe des Schweizerischen Roten Kreuzes oder Pro Infirmis. Ähnliche Beispiele führt der DSB des Kantons Basel-Landschaft auf. Massgabe für die Definition ist grundsätzlich das Fehlen der Gewinnstrebigkeit. Wie den Beispielen entnommen werden kann, wird nach Ansicht der Kommentatoren auch ein Spendenaufruf als nicht kommerzieller Zweck beurteilt, wenn die Institution als solche nicht Gewinnerzielung anstrebt. Aus datenschutzrechtlicher Sicht kann die Gemeinde einem Verein die Adressdaten von Einwohnern, die über 65 Jahre sind, aushändigen, wenn diese Organisation keinen Gewinn anstrebt, sondern vielmehr einen ideellen Zweck verfolgt und die Daten nur für den bekannt gegebenen Zweck gebraucht. Es liegt auf der Hand, dass sich ausnahmsweise Einwohnerinnen oder Einwohner von einem allfälligen Besuch gestört fühlen. Diesem Umstand könnte aber nur begegnet werden, wenn vorab die Einwilligung der Betroffenen eingeholt würde. Er ist grundsätzlich hinzunehmen.

8. Einsicht in Protokolle des Gemeindevorstandes

Kann eine Bürgerin/ein Bürger Einsicht in die Protokolle des Gemeindevorstandes verlangen, die seine eigene Person bzw. die von ihm beherrschten Gesellschaften betreffen?

Das Auskunftsrecht wird in den Art. 8 und 9 DSG geregelt. Danach kann jede Person vom Inhaber einer Datensammlung Auskunft darüber verlangen, ob Daten über sie bearbeitet werden (Art. 8 Abs. 1 DSG). Das Auskunftsrecht gilt als Institut zur Durchsetzung des Persönlichkeitsschutzes (BGE 138 III 431) und ist das bedeutendste Prinzip des Datenschutzgesetzes. Beim Auskunftsrecht handelt es sich um den Kern des Rechts an den eigenen Daten. Das Auskunftsrecht ergänzt und unterstützt die in der Bundesverfassung niedergelegten Grundrechte und insbesondere das Recht auf informationelle Selbstbestimmung (Art. 10 BV). Vor diesem Hintergrund ist ein Auskunftsbegehren zu prüfen.

In Art. 9 DSG werden die Einschränkungen der Informationspflicht aufgeführt. Es werden als Voraussetzung für Einschränkungen eine gesetzliche Grundlage, ein überwiegendes Interesse Dritter oder ein überwiegendes öffentliches Interesse genannt. Das Vorliegen solcher Voraussetzungen kann zu einer rechtmässigen Verweigerung, Einschränkung oder Aufschub der Einsichtnahme führen.

Gemäss Art. 12 Abs. 2 Gemeindegesetz (GG) wird, ohne anderslautendes kommunales Recht, die Einsicht in die Protokolle des Gemeindevorstandes und der übrigen Gemeindebehörden nur gestattet, wenn schutzwürdige Interessen geltend gemacht werden. Vorab ist also zu prüfen, ob auf kommunaler Ebene eine weitergehende Einschränkung oder eine grosszügigere Handhabung der Einsichtnahme in solche Protokolle legiferiert worden sind. Sollte dies nicht der Fall sein (was der Regel entspricht) ist Art. 12 Abs. 2 GG anwendbar. Die einsichtbegehrende Partei hat somit bekanntzugeben, weshalb sie Einsicht in die Protokolldaten haben will. An die Schutzwürdigkeit dürfen jedoch nicht allzu hohe Ansprüche gestellt werden, zumal bei Anfragen, welche die eigene Persönlichkeit betreffen, ein Interesse zu vermuten ist.

Daneben hat die Gemeinde eine Abwägung zwischen dem Anspruch des Auskunftersuchenden und den entgegengesetzten, berechtigten Interessen des Dateninhabers vorzunehmen. Dabei gilt, je schützenswerter die Personendaten sind und je grösser das Interesse des Auskunftsersuchenden an einer vollständigen Auskunft ist, desto klarer müssen die Interessen an der Einschränkung überwiegen. Die Auskunft darf nur insoweit beschränkt werden, als dies zwingend geboten ist. Jede Verweige-

rung oder Einschränkung ist gemäss Art. 9 Abs. 5 DSG zu begründen und zwar in Form einer anfechtbaren Verfügung. Nur bei offensichtlich überwiegenden entgegenstehenden Interessen der Gemeinde oder Dritter darf eine Einsichtnahme folglich verwehrt werden.

9. Einrichtung Videoüberwachung im Gerichtssaal

Ein Regionalgericht möchte für Notfälle eine Videoüberwachung im Gerichtssaal installieren.

Gestützt auf Art. 1 Abs. 4 KDSG gelten die Ausschlussgründe des DSG für den Geltungsbereich sinngemäss. Das Datenschutzgesetz ist nicht anwendbar auf hängige Zivilprozesse (Art. 2 Abs. 2 lit. c DSG). Damit stellt sich die Frage, ob das DSG vorliegend überhaupt zur Anwendung gelangt. Die Meinungen dazu gehen auseinander, wobei insbesondere Uneinigkeit besteht, welche Bereiche des Zivilprozesses in zeitlicher, sachlicher und persönlicher Hinsicht von der Anwendung des DSG ausgenommen sind. Eine allgemeine unabhängig von einem Prozess und nicht auf prozessuale Handlungen bezogene Videoüberwachung unterliegt m.E. grundsätzlich nicht der Zwecksetzung von Art. 2 Abs. 2 lit. c DSG. Aus den Gesetzesmaterialien ergibt sich jedoch, dass der Gesetzgeber sowohl das Verhältnis zwischen Parteien und Gericht als auch das Verhältnis zwischen den Parteien untereinander und zu beteiligten Dritten vom Anwendungsbereich des Datenschutzgesetzes ausnehmen wollte. Die Materialien sprechen somit eher gegen die Anwendung des DSG. Die Lehrmeinungen gehen auseinander. Diese Frage muss vorliegend jedoch nicht abschliessend erörtert werden.

Datenschutzvereinbarung

In Graubünden besteht kein Mustervertrag für eine Datenschutzvereinbarung bzw. einen Auftragsbearbeitungsvertrag. Welchen Mindestinhalt muss eine entsprechende Vereinbarung haben?:

1. Einleitung und Allgemeines
2. Gegenstand und Dauer der Vereinbarung
3. Art, Zweck und Betroffene der Datenbearbeitung (was, warum, von wem)
4. Pflichten Auftragnehmer (Art der Bearbeitung, Geheimhaltung, Weitergabe, Vernichtung etc.)
5. Sicherung der Bearbeitung
6. Regelung zur Berichtigung, Löschung und Sperrung von Daten
7. Rechte und Pflichten Auftraggeber (Kontrolle)
8. Weisungsrecht
9. Beendigung (Vernichtung)

Das Gerichtsorganisationsgesetz (GOG) regelt u.a. die Organisation der richterlichen Behörden. Unter dem Titel Öffentlichkeit werden in Art. 15 GOG Vorschriften über die Gerichtsverhandlungen festgehalten. Art. 15 Abs. 4 GOG bestimmt, dass Bild- und Tonaufnahmen der Gerichtsverhandlungen untersagt sind. Obwohl diese Bestimmung unter dem Titel Öffentlichkeit geführt wird, ist die Aussage klar und nicht auslegungsbedürftig. An Gerichtsverhandlungen Teilnehmende können sich darauf verlassen, dass während der Verhandlung keine Bild- und Tonaufnahmen erfolgen.

Schliesslich spricht auch die Berücksichtigung des Grundsatzes der Verhältnismässigkeit gegen die Installation einer Videoüberwachung. Vorgesehen sind die Filmaufnahmen vorliegend ohnehin nur für Notfälle. Nur in ganz seltenen Fällen sind Gerichtsverhandlungen mit einem Gefahrenpotential für die Teilnehmenden behaftet. Es ist Aufgabe des Gerichts bereits im Vorfeld anhand einer Risikoanalyse dieses Potential abzuschätzen und die erforderlichen Massnahmen zu treffen, sei dies in dem zum Beispiel Eintrittskontrollen durchgeführt werden oder allenfalls polizeiliche Hilfe angefordert wird.

Es kann festgestellt werden, dass eine Videoüberwachung bereits von Gesetzes wegen nicht installiert werden kann. Aber auch vor dem Hintergrund des Datenschutzes ist eine Videoüberwachung im Gerichtssaal abzulehnen.

10. Öffentlich zugängliches Grabregister

Eine Gemeinde möchte das Grabregister webbasiert auf ihrer Homepage aufschalten.

Massgebend für die Beurteilung dieses Problems ist das Gesetz über das Bestattungs- und Friedhofwesen der Gemeinde (BestG). Gemäss Art. 9 BestG soll ein Friedhof ein Ort der Besinnung und Ruhestätte Verstorbener sein. Alle Personen werden zu besonderer Rücksichtnahme und Sorgfalt verpflichtet. In dieser Bestimmung wird der Sinngehalt der Friedhofordnung verständlich wiedergegeben. Tatsächlich ist der Tod eine höchst intime, die Persönlichkeit unmittelbar betreffende Angelegenheit. Allein schon deshalb ist eine gewisse Zurückhaltung bei der Veröffentlichung entsprechender Informationen angezeigt. Zurecht wird im Gesetz auf die Besinnlichkeit und die besondere Rücksichtnahme gegenüber der Totenehre hingewiesen.

Gemäss Art. 19 Abs. 1 DSG dürfen Personendaten in der Regel nur bekanntgegeben werden, wenn dafür eine gesetzliche Grundlage besteht. Das Datenschutzgesetz verlangt grundsätzlich eine eigenständige Rechtsgrundlage. Diese muss sich explizit und spezifisch auf die Datenbekanntgabe beziehen und eine Verpflichtung oder zumindest eine Ermächtigung zur Datenbekanntgabe enthalten. Eine allgemeine Kompetenz zur Datenbearbeitung, welcher eine mittelbare Grundlage für die Datenbekanntgabe immanent sein kann, genügt in der Regel nicht. In Art. 16 BestG wird lediglich der Gemeinde die Kompetenz eingeräumt, ein Grabregister zu führen. Gewisse persönliche Daten bilden Inhalt dieses Registers. Die Gemeinde ist für das Bestattungswesen zuständig und muss allein gestützt auf ihren Auftrag auf bestimmte Daten zugreifen können. Aus der Formulierung von Art. 16 BestG kann jedoch nicht abgeleitet werden, dass der Gemeinde eine Kompetenz zur Veröffentlichung der erhobenen Daten zukäme. Art. 16 BestG genügt somit nicht als gesetzliche Grundlage für die öffentliche Zugänglichmachung der persönlichen Daten Verstorbener.

Das Erfordernis einer besonderen gesetzlichen Grundlage gilt indessen nicht absolut. Die Ausnahmetatbestände werden in Art. 19 Abs. 1 lit. a – d DSG konkretisiert. Gemäss Art. 19 Abs. 1 lit. c DSG können Daten bekannt gegeben werden, welche die betroffene Person allgemein zugänglich gemacht hat. Vorliegend sind bestimmte Daten auf dem Friedhof präsent und damit zugänglich. Der Gesetzgeber definiert das allgemeine Zugänglichmachen als eine besondere Art der Einwilligung.

Die Bekanntgabe der Daten auf dem Friedhof kann nun jedoch nicht als Zustimmung zu einer gleichsam weltweiten Veröffentlichung verstanden werden. Um die spezifischen Daten einer verstorbenen Person zu erfahren, muss der Friedhof besucht und die betreffende Grabstätte gesucht werden. Demgegenüber kann weltweit und jederzeit auf das Internet und damit auf die dort veröffentlichten persönlichen Daten zugegriffen werden. Darüber hinaus stellt sich die Frage, ob die Daten auf einem Grabstein das Kriterium der allgemeinen Zugänglichkeit tatsächlich erfüllen. Somit fehlt für die internetmässige Aufschaltung der Daten aus dem Grabregister die gesetzliche Grundlage. Diese ist damit unzulässig.

11. Fotofallen / Wildkameras

Beim Aufstellen von privaten Wildkameras stellt sich die grundsätzliche Frage, ob diese aus datenschutzrechtlichen Gründen überhaupt und wenn ja in welchem Umfange zulässig ist.

Für die Beantwortung dieser Frage ist der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDOEB) zuständig. Das eidgenössische Datenschutzgesetz gilt gemäss Art. 2 Abs. 1 lit. a DSG für das Bearbeiten von Daten durch private Personen. Da die Jagd im Kanton Graubünden einen hohen Stellenwert besitzt und Fragen dazu regelmässig an den Datenschutzbeauftragten gerichtet werden, wird auf diese Thematik eingegangen, zumal dazu ein parlamentarischer Vorstoss im kantonalen Parlament eingereicht worden ist.

Wer Personendaten beschafft, aufbewahrt und bearbeitet, greift in die Privatsphäre der betroffenen Person ein. In den letzten Jahren hat sich der Einsatz von Wildkameras durch private Personen stark ausgeweitet. Dies führte im Bundesparlament zu einer Anfrage an den Bundesrat. In seiner Antwort äusserte sich der Bundesrat am Rande zum Einsatz von Wildkameras durch private Personen wie folgt: «Es besteht auch kein Überblick über den Einsatz von Fotofallen durch Private. Insbesondere die rasante Entwicklung beim Einsatz von Fotofallen in Jägerkreisen bereitet den zuständigen Behörden Sorgen, denn hier besteht keine Kontrollmöglichkeit, ob die Fotofallen rechtskonform eingesetzt werden. Bei nächster Gelegenheit soll deshalb in Art. 2 der Jagdverordnung der Einsatz von Fotofallen zu jagdlichen Zwecken verboten werden.» Die Antwort des Bundesrates datiert vom 12. Februar 2014. Bis anhin wurde indessen Art. 2 Jagdverordnung nicht angepasst.

Herausgabe einer Verfügung an Dritte

Der Eigentümer A verlangt eine Auskunft betreffend eine Parzelle X im Eigentum von B. Ein kantonales Amt hat für diese Parzelle eine Verfügung erlassen. Danach sind gewisse Handlungen auf der Parzelle X vorzunehmen. Es stellt sich die Frage, ob die betroffene Gemeinde diese Verfügung an Eigentümer A herausgeben kann.

Grundsätzlich kann ein Eigentümer nur Auskunft über die eigene Parzelle verlangen. Nur Daten, die öffentlich zugänglich sind (z.B. Kanalisationspläne etc.), können eingesehen werden. Vorliegend hat das Amt eine Verfügung erlassen, die Handlungen auf der Parzelle X beinhalten. Folgerichtig ist das Amt für die mögliche Weitergabe dieser Daten an Dritte zuständig. Die Gemeinde darf ohne Zustimmung des Amtes die Verfügung nicht Dritten zur Verfügung stellen, sofern keine gesetzliche Grundlage besteht. Wenn Eigentümer B Anordnungen des Amtes missachtet hat, kann Eigentümer A eine Anzeige an das Amt machen, selbst wenn er nicht genau weiss, worin die Missachtung besteht. Auf alle Fälle ist die Gemeinde nicht direkter Ansprechpartner betreffend die fragliche Verfügung. Die Gemeinde kann das Anliegen von Eigentümer A jedoch an das Amt zur weiteren Bearbeitung weiterleiten. Damit ist sie ihren Pflichten nachgekommen.

Wildkameras sind vergleichbar mit Webcams und gemäss Datenschutzgesetz in der Regel nicht zulässig. Privatpersonen dürfen auf öffentlichem Grund keine Video- oder Fotoüberwachung betreiben. Ausnah-

men sind grundsätzlich nur in einem sehr engen Rahmen möglich, wenn nämlich die Wildkamera so aufgestellt werden kann, dass keine Personen erkennbar sein können. In der Regel ist diese Umsetzung kaum möglich. Jedoch ist auch bei dieser Vorgehensweise eine Interessenabwägung vorzunehmen. Der Wald ist öffentliches Gut und kann von jedermann betreten werden. Dies gilt selbst für Privatwald. Wenn nun eine Person auf Grund einer bestimmten Anzahl von Wildkameras befürchten muss, jederzeit aufgenommen zu werden (z.B. beim Pilzsammeln) ist diese Person in der Ausübung ihrer Persönlichkeitsrechte eingeschränkt, selbst wenn eine Kamera so aufgestellt wird, dass keine Person erkennbar bleibt. Die beiden sich entgegenstehenden Interessen sind zu Gunsten des unbeschränkten Betretens des Waldes auszulegen. Dementsprechend ist das Aufstellen von Wildkameras durch Privtpersonen im Wald aus datenschutzrechtlichen Überlegungen nicht statthaft.

Die Auslegung der Nutzung von Wildkameras sind kantonal unterschiedlich. Dies hängt wesentlich mit den unterschiedlichen Jagdgesetzen und Jagdarten zusammen. Der Kanton Zürich beispielsweise, der die Revierjagd kennt, überträgt den Jägern eine grössere Verantwortung hinsichtlich Hege und Pflege, in dem auf den gesetzlichen Auftrag der Jägerschaft hingewiesen wird, wonach diese Wildtierbestände zu erheben oder Standorte bestimmter Wildarten festzustellen haben. Im Kanton Graubünden werden diese Aufgaben von den Wildhütern übernommen. Es verbleibt damit kein Raum für die Nutzung von Wildkameras im Zusammenhang mit der Umsetzung des Jagdgesetzes für die Jäger und Jägerinnen.

IV. Statistik

Was Wer	Kurzanfragen	Berichte	Empfehlungen	Kontrollen	Vernehmlassungen	Referate	Kurse	Weiterbildung/Verbände
Kantonale Dienste								
Allgemeine Verwaltung	2		1				2	
DVS	3		1					
DJSG	7		5		3			
EKUD	6		2					
DFG	6		1					
DIEM	1		1					
öff. rechtliche Anstalten	17		1		1			
Gerichte	1							
Kreise								
Gemeindeverbände	2							
Gemeinden	37		2					
Bürgergemeinden								
Juristische Personen	1					1		
Private Personen	84		3			2		
Andere	1							
Total	168	0	17	0	4	3	2	0

V. Literaturverzeichnis

Für die Abfassung des Tätigkeitsberichts wurde auf folgende Literatur zurückgegriffen:

- BRUNO BAERISWYL
  Datenschutz in der (Corona)-Krise, in:
  Zeitschrift für Europarecht (EuZ), 2020, S. 168 ff.
- EVA MARIA BELSER / ASTRID EPINEY / BERNHARD WALDMANN
  Datenschutzrecht, Bern 2011
- DOMINIKA BLONSKI
  Leitfaden Bearbeiten im Auftrag
  abrufbar unter *https://docs.datenschutz.ch/u/d/publikationen/leitfaeden/leitfaden_bearbeiten_im_auftrag.pdf*
- DANIEL KETTIGER
  Videoüberwachung im medizinischen und paramedizinischen Bereich
  abrufbar unter *https://www.kettiger.ch/publikationen/datenschutzpraxis/*
- ANELA LUCIC
  Homeoffice und Arbeitsrecht, in: Recht relevant. für
  Verwaltungsräte, Heft 1, 2022, S.8 ff.
- URS MAURER-LAMBROU / GABOR-PAUL BLECHTA (Hrsg.)
  Datenschutzgesetz (DSG) / Öffentlichkeitsgesetz (BGÖ), Basler Kommentar,
  3. Auflage, Basel 2014
- MARKUS NÄF / MICHEL VERDE,
  § 12 Datenschutz und IT-Recht, in: Covid-19, Basel 2020
- NICOLAS PASSADELIS / DAVID ROSENTHAL / HANSPETER THÜR (Hrsg.)
  Datenschutzrecht, Basel 2015
- DAVID ROSENTHAL / YVONNE JÖHRI
  Handkommentar zum Datenschutzgesetz, 2. Auflage, Zürich 2021
- BERNHARD WALDMANN
  Das Diskriminierungsverbot von Art. 8 Abs. 2 BV als besonderer
  Gleichheitssatz, Bern 2003
- ROLF H. WEBER / DOMINIC OERTLY
  Datenschutzrechtliche Problemfelder von zivilen Drohneneinsätzen,
  in: Jusletter vom 26.10.2015, S. 1 ff.

VI. Abkürzungsverzeichnis

a.a.O.	am angeführten Ort
Abs.	Absatz
a.M.	anderer Meinung
Art.	Artikel
B	Botschaft
BestG	kommunales Bestattungsgesetz
BG	Bundesgesetz
BGE	Bundesgerichtsentscheid
BGer	Bundesgericht
Bl	Blatt
BR	Bündner Rechtsbuch
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
EpG	Bundesgesetz über die Bekämpfung übertragbarer Krankheiten des Menschen
ERG	Gesetz über die Einwohnerregister und weitere Personen- und Objektregister
etc.	et cetera
f./ff.	folgend/folgende
GG	Gemeindegesetz des Kantons Graubünden
GOG	Gerichtsorganisationsgesetz
GR	Graubünden
Hrsg.	Herausgeber
i.V.m.	in Verbindung mit
KDSG	Kantonales Datenschutzgesetz
KFG	Gesetz über die Förderung der Kultur
KV	Kantonsverfassung
lit.	litera
m.E	meines Erachtens
N	Note
OR	Obligationenrecht
POV	kommunale Personalverordnung
RB	Rechtsbuch
Rz	Randziffer
S	Seite
TB	Tätigkeitsbericht
u.a.	unter anderem
usw.	und so weiter
VDSG	Verordnung zum Bundesgesetz über den Datenschutz
vgl.	vergleiche
z.B.	zum Beispiel
ZGB	Schweizerisches Zivilgesetzbuch
Ziff.	Ziffer