Tätigkeitsbericht 2023

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

Am 30. September 2023 ist das revidierte eidgenössische Datenschutzgesetz (nDSG) in Kraft getreten. Es kann festgestellt werden, dass mit dem neuen Gesetz die bis anhin geltenden Grundsätze nicht über Bord geworfen worden sind. Der technischen Entwicklung folgend und in Anpassung an das europäische Recht sind neue Instrumente eingeführt worden. Bei den Betroffenen am meisten Aufmerksamkeit haben indessen die im Gesetz integrierten Bussnormen gefunden. Auf Seiten des Datenschutzes konnte positiv konstatiert werden, dass sich die Betroffenen aktiv und intensiv mit dem neuen Gesetz auseinandergesetzt haben. An zahlreichen Tagungen und Vortragsabenden hatte der DSB Gelegenheit, die Grundsätze des Datenschutzes sowie die Änderungen und Neuerungen zu erläutern.

Das kantonale Datenschutzgesetz weist in Art. 2 Abs. 2 auf die sinngemässe Anwendung der Vorschriften des Bundesgesetzes für kantonale Behörden hin. Für den Kanton Graubünden stellte sich damit die Frage, ob das bestehende Rahmengesetz in dieser Form aufrechterhalten bleiben oder ob ein eigenständiges Gesetz erarbeitet werden sollte. Die bisherige Vorgehensweise des Kantons Graubünden hat sich bewährt, da jederzeit auf die eidgenössische Judikatur und Literatur zurückgegriffen werden konnte. Dennoch hat sich der Gesetzgeber dazu entschieden, eine unabhängige Lösung vorzubereiten. Dabei wurde darauf geachtet, dass die Begrifflichkeiten und die neuen Instrumente integral übernommen und nur dort Änderungen eingefügt werden, die von kantonaler Relevanz sind. Dadurch kann auch in Zukunft auf die umfangreichen Materialien zurückgegriffen werden. Derzeit durchläuft der Vorentwurf das Vernehmlassungsverfahren. Es bleibt abzuwarten, ob der Entwurf die erforderliche Akzeptanz bei den Betroffenen findet. Der DSB ist zuversichtlich und freut sich bereits heute, dass künftig auch in Bezug auf die Dotierung des Amtes Fortschritte erzielt werden.

Kantonaler Datenschutzbeauftragter:

Thomas Casanova

II. Allgemeines

1. Die Neuerungen im revidierten schweizerischen Datenschutzgesetz

I. Einleitung

Gemäss Art. 2 Abs. 2 des kantonalen Datenschutzgesetzes (KDSG) werden die Vorschriften des Bundesgesetzes für das Bearbeiten von Personendaten durch Bundesbehörden sinngemäss angewendet. Mit dem Inkrafttreten des revidierten Datenschutzgesetzes (nDSG) hat sich deshalb auch in Graubünden einiges geändert. Der integrale Verweis auf das nDSG ist jedoch auch mit Nachteilen verbunden. Daher hat sich der Kanton entschlossen, das kantonale Gesetz umfassend zu revidieren. Die im nDSG eingeführten Neuerungen werden im künftigen Gesetz fast ausnahmslos übernommen. Daher ist es gerechtfertigt, näher auf diese Anpassungen einzugehen.

Das bisherige Gesetz war bereits umfangreich, jedoch wurde eine Aktualisierung notwendig, um den neuen Herausforderungen im Bereich Datenschutz gerecht zu werden. Insbesondere die fortschreitende Digitalisierung und die verstärkte Nutzung von digitalen Diensten erforderten eine Anpassung der gesetzlichen Rahmenbedingungen.

II. Rechtliche Analyse der Neuerungen im DSG

Die Neuerungen im schweizerischen Datenschutzgesetz lassen sich in verschiedene Bereiche unterteilen, die im Folgenden näher betrachtet werden:

- Datenschutzprinzipien und -grundsätze
- Erweiterter Schutz personenbezogener Daten
- Regulierung des Datentransfers
- Verpflichtungen für Unternehmen und Organisationen
- Sanktionen und Strafen

1. Datenschutzprinzipien

- **Rechtmässigkeit, Fairness und Transparenz:** Personenbezogene Daten müssen auf rechtmässige Weise, fair und transparent bearbeitet werden. Dies bedeutet, dass die Datenverarbeitung auf einer rechtlichen Grundlage erfolgen muss, die Interessen der Betroffenen angemessen berücksichtigt und transparente Informationen über die Bearbeitung bereitgestellt werden müssen.

- **Zweckbindung:** Personenbezogene Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben und bearbeitet werden. Jede weitere Bearbeitung der Daten muss mit diesen Zwecken vereinbar sein.
- **Datenminimierung, Verhältnismässigkeit:** Die Bearbeitung personenbezogener Daten muss auf das erforderliche Mass beschränkt werden. Es dürfen nur die Daten bearbeitet werden, die für die Zwecke der Bearbeitung notwendig sind.
- **Richtigkeit der Daten:** Personenbezogene Daten müssen richtig und gegebenenfalls auf dem neuesten Stand gehalten werden. Massnahmen müssen ergriffen werden, um sicherzustellen, dass unrichtige oder unvollständige Daten berichtigt oder gelöscht werden.
- **Speicherbegrenzung:** Personenbezogene Daten dürfen nur so lange gespeichert werden, wie es für die Zwecke, für die sie erhoben wurden, erforderlich ist. Nach Ablauf dieser Frist müssen die Daten gelöscht oder anonymisiert werden.
- **Integrität und Vertraulichkeit:** Personenbezogene Daten müssen angemessen vor unbefugter oder unrechtmässiger Bearbeitung sowie vor unbeabsichtigtem Verlust, Zerstörung oder Schaden geschützt werden. Dies erfordert die Umsetzung geeigneter technischer und organisatorischer Massnahmen.
- **Rechenschaftspflicht und Nachweisbarkeit:** Verantwortliche und Auftragsverarbeiter müssen nachweisen können, dass sie die Anforderungen des Datenschutzgesetzes einhalten. Dies umfasst die Implementierung geeigneter Datenschutzmassnahmen, die Schulung von Mitarbeitenden und die Führung von Aufzeichnungen über die Datenbearbeitungstätigkeiten.

2. Erweiterter Schutz personenbezogener Daten

- **Stärkere Rechte der Betroffenen:** Das neue DSG stärkt die Rechte der Betroffenen bezüglich ihrer personenbezogenen Daten. Dazu gehören unter anderem das Recht auf Zugang zu den eigenen Daten, das Recht auf Berichtigung und Löschung von Daten sowie das Recht auf Datenübertragbarkeit.
- **Erhöhte Transparenz und Informationspflichten:** Behörden, Unternehmen und Organisationen sind gemäss dem neuen DSG verpflichtet, transparente Informationen über die Bearbeitung personenbezogener Daten bereitzustellen. Dies umfasst unter anderem die Offenlegung der

Zwecke der Datenbearbeitung, die Kategorien der bearbeiteten Daten, die Empfänger der Daten und die Dauer der Datenspeicherung.

- **Verbot der automatisierten Profilbildung:** Das neue DSG enthält Bestimmungen, die die automatisierte Profilbildung und Entscheidungsfindung einschränken. Personenbezogene Daten dürfen nicht für automatisierte Entscheidungen verwendet werden, die rechtliche Folgen für die Betroffenen haben oder sie in ähnlich erheblicher Weise beeinträchtigen.
- **Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Privacy by Design und Privacy by Default):** Das neue DSG fördert den Datenschutz durch Technikgestaltung und die Implementierung datenschutzfreundlicher Voreinstellungen. Behörden, Unternehmen und Organisationen sind verpflichtet, bereits bei der Entwicklung von Produkten, Dienstleistungen oder Verarbeitungssystemen Datenschutzprinzipien zu berücksichtigen und Datenschutzmassnahmen zu implementieren, um den Schutz personenbezogener Daten von vornherein sicherzustellen.
- **Meldung von Datenschutzverletzungen:** Das neue DSG führt eine Pflicht zur Meldung von Datenschutzverletzungen ein. Behörden, Unternehmen und Organisationen sind verpflichtet, Datenschutzverletzungen den zuständigen Datenschutzbehörden und gegebenenfalls den betroffenen Personen zu melden.

3. Regulierung des Datentransfers

- **Anforderungen an den Datentransfer in Drittländer:** Das neue DSG legt Anforderungen an den Datentransfer personenbezogener Daten in Drittländer. Unternehmen und Organisationen müssen sicherstellen, dass der Datentransfer in Drittländer nur stattfindet, wenn das Datenschutzniveau im Zielland angemessen ist oder angemessene Sicherheitsmassnahmen getroffen wurden, um den Schutz der Daten zu gewährleisten.
- **Angemessenheitsbeschluss:** Wenn die Europäische Kommission einen Angemessenheitsbeschluss für ein Drittland erlässt, der besagt, dass das Datenschutzniveau in diesem Land angemessen ist, können Daten ohne zusätzliche Massnahmen in dieses Land übertragen werden. Das neue DSG nimmt Bezug auf solche Angemessenheitsbeschlüsse und erleichtert damit den Datentransfer in Länder mit einem angemessenen Datenschutzniveau.

- **Standardvertragsklauseln und verbindliche interne Datenschutzvorschriften:** Wenn kein Angemessenheitsbeschluss vorliegt, können Unternehmen und Organisationen auf Standardvertragsklauseln zurückgreifen, um den Datentransfer zu sichern. Alternativ können sie auch verbindliche interne Datenschutzvorschriften (Binding Corporate Rules) einführen, um den Datentransfer innerhalb eines Unternehmens oder einer Organisation zu regeln.
- **Genehmigungspflicht für bestimmte Datentransfers:** In einigen Fällen kann der Datentransfer in Drittländer einer vorherigen Genehmigung durch die zuständige Datenschutzbehörde unterliegen. Dies gilt insbesondere dann, wenn besondere Risiken für die Datenschutzrechte der Betroffenen bestehen oder keine anderen geeigneten Schutzmassnahmen ergriffen werden können.
- **Dokumentationspflichten und Nachweisführung:** Unternehmen und Organisationen sind verpflichtet, den Datentransfer in Drittländer zu dokumentieren und nachzuweisen, dass angemessene Schutzmassnahmen getroffen wurden, um den Schutz der Daten zu gewährleisten. Dies umfasst die Aufzeichnung von Verträgen, Standardvertragsklauseln oder anderen Sicherheitsmassnahmen, die im Rahmen des Datentransfers implementiert wurden.

4. Verpflichtungen für Behörden

- **Einrichtung von Datenschutzmassnahmen:** Behörden, Unternehmen und Organisationen sind verpflichtet, angemessene technische und organisatorische Massnahmen zum Schutz personenbezogener Daten zu implementieren. Dies umfasst Massnahmen wie Zugangskontrollen, Verschlüsselung, regelmässige Sicherheitsüberprüfungen und Schulungen der Mitarbeitenden.
- **Benennung eines Datenschutzberater:** Behörden, Unternehmen und Organisationen, die besonders sensible Daten verarbeiten oder bestimmte Schwellenwerte überschreiten, sind verpflichtet, einen Datenschutzberater zu benennen. Der Datenschutzberater überwacht die Einhaltung des Datenschutzgesetzes, berät das Unternehmen oder die Organisation in Datenschutzfragen und dient als Ansprechpartner für die Datenschutzbehörde und die Betroffenen.
- **Durchführung von Datenschutz-Folgenabschätzungen:** Behörden, Unternehmen und Organisationen müssen Datenschutz-Folgenabschätzungen durchführen, bevor sie bestimmte Datenverarbeitungstätigkeiten durchführen, die voraussichtlich ein hohes Risiko für die Da-

tenschutzrechte der Betroffenen darstellen. Diese Folgenabschätzungen sollen die Risiken der Datenbearbeitung identifizieren und geeignete Schutzmassnahmen empfehlen.

- **Dokumentationspflichten:** Behörden, Unternehmen und Organisationen sind verpflichtet, Aufzeichnungen über ihre Datenbearbeitungstätigkeiten zu führen. Dies umfasst Angaben über die Art der verarbeiteten Daten, die Zwecke der Datenbearbeitung, die Kategorien der betroffenen Personen, die Empfänger der Daten und die Speicherdauer der Daten.
- **Meldung von Datenschutzverletzungen:** Behörden, Unternehmen und Organisationen sind verpflichtet, Datenschutzverletzungen den zuständigen Datenschutzbehörden und gegebenenfalls den betroffenen Personen zu melden. Die Meldung muss innerhalb einer angemessenen Frist erfolgen und bestimmte Informationen über die Datenschutzverletzung enthalten.

5. Sanktionen und Strafen

- **Bussgelder:** Das neue DSG sieht die Möglichkeit vor, Geldbussen gegen Unternehmen und Organisationen zu verhängen, die gegen die Datenschutzbestimmungen verstossen. Die Höhe der Bussgelder kann je nach Schwere des Verstosses und anderen Faktoren variieren.
- **Verwaltungsstrafen:** Neben Geldbussen können Unternehmen und Organisationen auch mit Verwaltungsstrafen belegt werden. Diese können verschiedene Formen annehmen, wie beispielsweise die Verhängung von Auflagen oder die Anordnung von Massnahmen zur Verbesserung des Datenschutzes.
- **Strafrechtliche Sanktionen:** In schwerwiegenden Fällen von Datenschutzverstössen können strafrechtliche Sanktionen verhängt werden. Dies kann zur Einleitung von Strafverfahren führen.
- **Berichtigung oder Löschung von Daten:** Die zuständige Datenschutzbehörde kann Unternehmen und Organisationen anweisen, unzulässig verarbeitete personenbezogene Daten zu berichtigen oder zu löschen.
- **Unterlassungsanordnungen:** Bei anhaltenden oder schwerwiegenden Datenschutzverstössen kann die zuständige Datenschutzbehörde Unterlassungsanordnungen gegen Unternehmen und Organisationen erlassen.

III. Stärkung der Verbraucherrechte

Das neue eidgenössische Datenschutzgesetz stärkt die Verbraucherrechte im Zusammenhang mit dem Datenschutz und trägt dazu bei, das Ver-

trauen der Verbraucherinnen und Verbraucher in den Umgang mit ihren Daten zu stärken. Hier sind einige Aspekte aufgeführt, die die Beziehung zwischen Datenschutz und Verbraucherrechten im Rahmen des neuen DSG charakterisieren:

- **Informationspflichten:** Unternehmen und Organisationen sind gemäss dem neuen DSG verpflichtet, transparente Informationen über die Verarbeitung personenbezogener Daten bereitzustellen. Dies umfasst die Offenlegung der Zwecke der Datenverarbeitung, die Kategorien der verarbeiteten Daten, die Empfänger der Daten und die Dauer der Datenspeicherung.
- **Einwilligung der Verbraucher:** Wenn die Bearbeitung personenbezogener Daten auf der Einwilligung der betroffenen Personen basiert, müssen Unternehmen und Organisationen sicherstellen, dass die Einwilligung freiwillig, informiert, spezifisch und eindeutig ist. Die Verbraucherinnen und Verbraucher müssen über die Zwecke der Datenbearbeitung, die Kategorien der bearbeiteten Daten und ihre Rechte umfassend informiert werden. Dies gibt den Verbrauchern mehr Kontrolle über ihre Daten und ermöglicht es ihnen, informierte Entscheidungen über die Verwendung ihrer Daten zu treffen.
- **Recht auf Zugang und Berichtigung:** Das neue DSG stärkt das Recht der Verbraucherinnen und Verbraucher auf Zugang zu ihren eigenen Daten sowie das Recht auf Berichtigung von unrichtigen oder unvollständigen Daten. Dies ermöglicht es den Verbrauchern, ihre Daten zu überprüfen, Fehler zu korrigieren und sicherzustellen, dass ihre Daten korrekt und aktuell sind.

IV. Anpassungen für Behörden und Unternehmen

Das neue eidgenössische Datenschutzgesetz erfordert von Unternehmen und Organisationen verschiedene Anpassungen an ihre internen Datenschutzrichtlinien und -verfahren, um die Einhaltung der neuen Datenschutzbestimmungen sicherzustellen. Hier sind einige notwendige Anpassungen, die Unternehmen und Organisationen vornehmen sollten:

- **Aktualisierung der Datenschutzrichtlinien**: Unternehmen und Organisationen sollten ihre Datenschutzrichtlinien überarbeiten und aktualisieren, um sicherzustellen, dass sie die Anforderungen des neuen DSG widerspiegeln. Die aktualisierten Richtlinien sollten die neuen Datenschutzprinzipien, Rechte der Betroffenen und Verpflichtungen des Unternehmens gemäss dem neuen Gesetz klar und umfassend darlegen.

- **Überprüfung und Anpassung von Bearbeitungsaktivitäten**: Unternehmen und Organisationen sollten ihre Datenberarbeitungsaktivitäten überprüfen und anpassen, um sicherzustellen, dass sie den Anforderungen des neuen DSG entsprechen. Dies kann die Identifizierung und Dokumentation aller personenbezogenen Daten umfassen, die bearbeitet werden, sowie die Überprüfung der Rechtmässigkeit, Zweckbindung und Transparenz der Datenbearbeitung.
- **Einrichtung von Datenschutzmassnahmen**: Unternehmen und Organisationen sollten angemessene technische und organisatorische Massnahmen zum Schutz personenbezogener Daten implementieren. Dazu gehören Massnahmen wie Zugangskontrollen, Verschlüsselung, regelmässige Sicherheitsüberprüfungen und Schulungen der Mitarbeiter. Diese Massnahmen sollten den Anforderungen des neuen DSG entsprechen und den Schutz der Daten gewährleisten.
- **Benennung eines Datenschutzberaters**: Unternehmen und Organisationen, die besonders sensible Daten verarbeiten oder bestimmte Schwellenwerte überschreiten, sollten einen Datenschutzberater benennen. Der Datenschutzberater überwacht die Einhaltung des Datenschutzgesetzes, berät das Unternehmen oder die Organisation in Datenschutzfragen und dient als Ansprechpartner für die Datenschutzbehörde und die Betroffenen.
- **Schulung der Mitarbeitenden**: Unternehmen und Organisationen sollten ihre Mitarbeitenden über die neuen Datenschutzbestimmungen informieren und Schulungen zur Einhaltung des Datenschutzgesetzes durchführen. Die Mitarbeitenden sollten darüber informiert werden, welche Daten verarbeitet werden dürfen, wie diese Daten geschützt werden müssen und welche Verpflichtungen das Unternehmen oder die Organisation gemäss dem neuen DSG hat.

V. Schlussfolgerung und Ausblick

Das neue Datenschutzgesetz legt den Grundstein für einen modernen und effektiven Datenschutz in der Schweiz, der den aktuellen und zukünftigen Herausforderungen im Bereich Datenschutz gerecht wird. Es ist jedoch wichtig zu beachten, dass der Datenschutz ein dynamisches Feld ist, das sich ständig weiterentwickelt. Behörden, Unternehmen und Organisationen sollten sich daher kontinuierlich über neue Entwicklungen und Best Practices im Datenschutz informieren und ihre Datenschutzpraktiken entsprechend anpassen.

Insgesamt bietet das neue Datenschutzgesetz eine solide Grundlage für einen verbesserten Datenschutz in der Schweiz und trägt dazu bei, das Vertrauen der Betroffenen in den Umgang mit ihren Daten zu stärken. Es ist ein wichtiger Schritt zur Förderung von Datenschutz und Privatsphäre in der digitalen Welt und wird voraussichtlich zu einer zunehmenden Sensibilisierung für Datenschutzfragen und einem verantwortungsvolleren Umgang mit personenbezogenen Daten führen.

2. Einführung von Microsoft 365 in der kantonalen Verwaltung 2.0

Bekanntlich hat die Regierung des Kantons Graubünden am 7. März 2023 die Rahmenbedingungen für den Einsatz von Microsoft 365 Cloud-Services festgelegt sowie Kenntnis von den Risiken und Restrisiken genommen. Im Tätigkeitsbericht 2022 ist auf die Einführung von Microsoft 365 in der kantonalen Verwaltung ausführlich eingegangen und auf die Risiken hingewiesen worden.

Im Kanton Zürich wird bereits länger über die Einführung diskutiert. Im Zuge dessen haben Prof. Dr. Markus Schefer und Dr. Philip Glass, Universität Basel, ein Gutachten zum grundrechtskonformen Einsatz von Microsoft 365 durch die Gemeinden im Kanton Zürich verfasst[1]. Dieses Gutachten hat Signalwirkung für die Anwendung von Microsoft 365 in Graubünden. David Rosenthal veröffentlichte gegen Ende Jahr Anmerkungen zum vorgenannten Gutachten. Schliesslich tauschten sich Mitglieder von privatim mit den beiden Gutachtern aus.

Vorab beschäftigt sich das Gutachten mit der Anerkennung des Rechtes auf informationelle Selbstbestimmung. Nach konstanter Rechtsprechung bildet dieses Recht einen Teilgehalt von Art. 13 Abs. 2 BV sowie Art. 8 EMRK und schützt im Einzelnen vor Beeinträchtigungen, die durch die staatliche Bearbeitung der persönlichen Daten entstehen. Als Rechtsgrundlage der Beeinträchtigung, und damit Teil des Schutzbereiches der informationellen Selbstbestimmung, anerkannte das Gericht verschiedene Grundrechte, insbesondere die persönliche Freiheit bzw. die Entfaltung elementarer Aspekte der Persönlichkeit und den Schutz der Geheim- und Privatsphäre. Die gerichtliche Rechtsprechung geht dabei von einem sehr weiten Schutzbereich aus, wonach grundsätzlich ohne Rücksicht darauf, wie sensibel die fraglichen Informationen tatsächlich sind, jede Person gegenüber fremder, staatlicher oder privater Bearbeitung von sie betreffenden Informationen bestimmen können muss, ob und zu welchem Zweck diese Informationen über sie bearbeitet werden. Aus dem Missbrauchsverbot gestützt auf Art. 13 Abs. 2 BV folgt, dass jeder staatliche Umgang mit persönlichen Daten gewissen Minimalerfordernissen unterworfen ist. Bei der eigentlichen Prüfung der im Zusammenhang mit einer Cloud-Auslagerung identifizierten Eingriffsmomente und damit dem Kern der Fragestellung stellen sich die Gutachter auf den Standpunkt, dass mit der Auslagerung ein rechtlicher und faktischer Kontrollverlust verbunden ist. Dieser Kontrollverlust führt zum Schluss, dass die bestehenden gesetzlichen Grund-

[1] *https://rosenthal.ch/downloads/Gutachten-Schefer-Glass-M365.pdf*

lagen nicht genügen. Indessen kann ein Kontrollverlust durch sichernde Massnahmen kompensiert werden, indem in der Rechtsbeziehung zwischen öffentlichem Organ und Cloud-Anbieterin die Eingriffsmomente der Übertragung der faktischen und rechtlichen Datenherrschaft durch die in verschiedenen Merkblättern und Leitbildern ausgeführten vertraglichen und technischen Massnahmen gemildert und entsprechend grundrechtverträglicher ausgestaltet werden.

Festgestellt wird auch, dass die Speicherung von Personendaten in der Cloud, und damit unfreiwillig "auf Vorrat" zu Handen von US-Behörden, welche diese mittels CLOUD Act/SCA unter Umständen beschaffen könnten, ein spezifisches Eingriffsmoment darstelle, das gemäss Art. 36 BV zu rechtfertigen ist. Im Einzelfall muss durch Risikoanalyse ermittelt werden, ob grundsätzlich von einem schweren Gefährdungseingriff auszugehen ist.

David Rosenthal widerspricht in seinen Anmerkungen zum Gutachten[2] der Aussage, wonach Daten in der Cloud einem wesentlichen Kontrollverlust gegenüber U.S. Behörden unterliegen. Es könne nicht davon ausgegangen werden, dass U.S. Behörden sich ungehindert an in der Cloud gespeicherten Daten bedienen könnten. Vielmehr treffe das Gegenteil zu, jedenfalls, wenn wie bei Microsoft 365 üblich, entsprechende Abwehrmassnahmen getroffen werden. Die Schlussfolgerungen der Gutachter würden auf verschiedenen unzutreffenden Annahmen beruhen, weshalb sie nicht haltbar seien. Schliesslich setzt Rosenthal den seiner Ansicht nach minimalen Kontrollverlust im Bereich von U.S. Behördenzugriffen einem deutlich höheren Kontrollgewinn beim Schutz vor Hackern und anderen Gefahren gegenüber.

In Übereinstimmung mit den Gutachtern kann jedoch der Schluss gezogen werden, dass die öffentlichen Organe den Verhältnismässigkeitsgrundsatz einzuhalten und die sich in diesem Zusammenhang stellenden Fragen zu beantworten haben. Der Kontrollverlust muss möglichst minimiert werden und die Eingriffsintensität muss für die Einzelnen zumutbar bleiben. Das öffentliche Organ muss die Frage beantworten, welche Funktionen von Microsoft 365 für die Aufgabenerfüllung wirklich notwendig sind, zu welchem Zweck die Bearbeitung stattfindet und was die Alternativen

---

[2] *https://www.rosenthal.ch/downloads/Rosenthal_Cloud-Gutachten-Replik.pdf*

sind. Die Einhaltung des Verhältnismässigkeitsgrundsatzes verlangt potentiell die Einschränkung der Bequemlichkeit. In der Konsequenz führt die Einführung von Microsoft 365 zu einer Präzisierung der gesetzlichen Vorgaben, insbesondere wenn besonders schützenswerte Personendaten über cloudbasierte Dienste übertragen werden sollen. Es bietet sich dabei das Gesetz über die digitale Verwaltung (BR 177.100) an.

3. Akteneinsichtsrecht in das Personaldossier

Es stellt sich immer wieder die Frage, was Inhalt eines Personaldossiers bildet. Anhand eines konkreten Falles ist dieser Frage nachgegangen worden.

Das Auskunftsrecht ist das zentrale Instrument des Datenschutzgesetzes und ermöglicht es dem Betroffenen häufig überhaupt erst, seine übrigen datenschutzrechtlichen Ansprüche durchzusetzen (Botschaft DSG, BBl 1988 II 452). Das Auskunftsrecht erstreckt sich auf alle über den Arbeitnehmer bzw. Arbeitnehmerin vorhandenen Daten. Die Summe dieser Daten wird oft als Personaldossier oder Personalakte bezeichnet, wobei beides keine gesetzlichen Begriffe sind. Es ist jedoch unerheblich, ob ein zentrales Personaldossier geführt wird oder die Daten an unterschiedlichen Orten aufbewahrt werden. Gestützt auf Art. 8 DSG haben Arbeitnehmende grundsätzlich ein umfassendes Auskunftsrecht hinsichtlich der über sie vom Arbeitgeber bearbeiteten bzw. gesammelten Daten. Vor diesem Hintergrund sind Rechtsbegehren zu prüfen.

Die Mitarbeitende machte geltend, sie habe bei der Behörde um Zustellung ihres Personaldossiers ersucht. Gleichentags habe sie eine E-Mail mit einer PDF-Datei und dem Hinweis, dass es sich dabei um ihr Personaldossier handle, erhalten. Später ersuchte die Mitarbeitende um Bestätigung, wonach die ihr zugestellten Unterlagen vollständig und richtig seien. Die Weiterleitung des gesamten Dossiers, so wie es in der Personalabteilung abgelegt und vorhanden sei, wurde ihr bestätigt. Daraufhin teilte die Mitarbeitende mit, dass im Personaldossier keine Informationen zur Kompetenzüberschreitung vermerkt seien. Ebenso fehle ihre Stellungnahme dazu, obwohl sie darum gebeten habe. Die Behörde antwortete gleichentags per E-Mail: "*Die "fehlenden Dokumente" wie z.B. auch dieses E-Mail, die du erwähnt hast, werden von mir erst nach Abschluss der laufenden Diskussionen und Stellungnahmen abgelegt.*" Nach einer Besprechung wurde der Mitarbeitenden ordentlich gekündigt und das rechtliche Gehör gewährt. In ihrer Stellungnahme wies sie darauf hin, dass verschiedene Dokumente nicht übermittelt worden waren. Im daran anschliessenden Beschwerdeverfahren ersuchte sie erneut um Zustellung von Dokumenten. Hierauf wurden weitere Dokumente übermittelt. Die Mitarbeitende machte geltend, dass die Zustellung des vollständigen Personaldossiers damit aber immer noch unterblieben sei, so würden insbesondere "*die Kopien der unterzeichneten Mitarbeiterbeurteilungen, weitere Korrespondenzen usw.*" fehlen. Im Beschwerdeentscheid wird ausgeführt, es sei das gesamte Personaldossier in Kopie abgegeben worden. Noch nicht enthalten darin seien, aufgrund der ständigen Praxis der Arbeitgeberin, Akten zum laufenden

Verfahren. Nicht oder noch nicht im Personaldossier abgelegt seien Unterlagen, die im Rahmen der Willensbildung im Hinblick auf aktuell oder absehbar zu fällende personalrechtliche Entscheide anfallen würden, wie interne Anträge, Entwürfe und Notizen sowie Mitberichte Korrespondenz und Unterlagen aus internen oder externen Untersuchungen.

Die Mitarbeitende sieht in den Handlungen der Behörde einen Verstoss gegen Art. 8 DSG und Art. 328b OR. Eine Möglichkeit zur Einschränkung des Auskunftsrechts gemäss Art. 9 DSG sei nicht ersichtlich.

Der Kern der Auseinandersetzung besteht einerseits darin, dass sich die Parteien uneinig darüber sind, ob die Mitarbeitende nur Einblick in die Akten haben wollte, die Gegenstand des zentralen Personaldossiers sind, oder in sämtliche Akten, über die die Behörde in Bezug auf die Mitarbeitende verfügte. Sollte sie Einsicht in sämtliche Akten gewollt haben, stellt sich zudem die Frage, ob die Behörde dies angesichts der Korrespondenzen hätte erkennen können und müssen, und schliesslich, ob sie alle vorhandenen Daten zum Zeitpunkt des ersten Einsichtsgesuches hätte aushändigen müssen.

In ihrer Replik hat die Mitarbeitende ihren ersten Antrag leicht präzisiert. Sie beantragte "*Einsicht in sämtliche über sie vorhandene Daten bzw. das komplette (physische und elektronische, sortierte und nummerierte) Personaldossier*". Damit war mindestens zu diesem Zeitpunkt offensichtlich, dass die Mitarbeitende sämtliche über sie verfügbare Akten einsehen wollte.

Da die Behörde mitgeteilt hat, dass die entsprechende E-Mail erst nach dem Verfahrensabschluss im Personaldossier abgelegt werde, ist davon auszugehen, dass auch die Behörde davon ausging, die besagte E-Mail bilde Bestandteil des Personaldossiers. Ob solche Akten trotz Art. 60a Abs. 4 PV zwingend im Personaldossier abgelegt werden müssen, kann daher an dieser Stelle offenbleiben.

Es ist darauf hinzuweisen, dass es sich beim zentralen Personaldossier i.S. des Personalgesetzes des Kantons Graubünden und der zitierten Verordnung, nicht um die vollständige Sammlung aller Daten eines Datenherrn im Sinne des Datenschutzgesetzes handelt. In der Botschaft zur Änderung des Personalgesetzes vom 16. Mai 2016 wird der Sinn und Zweck des zentralen Personaldossiers erläutert. Demnach wird mit Art. 60a Abs. 2 PG neu die gesetzliche Grundlage dafür geschaffen, dass den Mitarbeitenden und Vorgesetzten Personalakten in einem elektronischen, automatisier-

ten Abrufverfahren zugänglich gemacht werden können. Dieser Zugang ist auf solche Personalangaben beschränkt, bezüglich deren aufgrund der allgemeinen Regeln ein Zugangsrecht besteht, mithin für den Mitarbeitenden auf seine persönlichen Daten und für die vorgesetzte Person auf jene Mitarbeitenden-Daten, die sie für die Ausübung ihrer Vorgesetztenfunktion benötigt (Botschaft zur Teilrevision des Personalgesetzes, Heft Nr. 2/2016-2017, S. 41). Für die Bearbeitung von Personendaten, inkl. dem Auskunftsrecht, ist aber das kantonale Datenschutzgesetz massgebend (vgl. auch Art. 60 PG i.V.m. Art. 60c PV). Somit ist irrelevant, ob die entsprechenden Daten Bestandteil des zentralen Personaldossiers bilden, da die Einschränkung eines Auskunftsbegehrens nach datenschutzrechtlichen Vorgaben zu beurteilen ist.

Die Behörde wendet dazu ein, es gäbe weder einen Anspruch darauf, dass das Personaldossier zu jedem Zeitpunkt vollständig geführt werde, noch auf Bestätigung der Vollständigkeit und Richtigkeit des Dossiers. Der HR-Verantwortliche habe lediglich bestätigt, das Personaldossier so kopiert zu haben, wie es in der Personalabteilung abgelegt gewesen sei.

Der Behörde ist insoweit zuzustimmen, als das Dossier resp. die Aktensammlung nicht zu jedem Zeitpunkt vollständig sein muss. Wenn jedoch eine Person um Einsicht in die eigenen Daten ersucht, ist das Dossier zu vervollständigen und anschliessend zur Einsicht zuzustellen. Der Behörde kommt diesbezüglich eine Vorbildfunktion zu. Sie agiert überspitzt formalistisch, wenn sie sich darauf beruft, dass der HR-Verantwortliche zu Recht bestätigt habe, alle im Personaldossier enthaltenen Akten seien kopiert worden. Dadurch wurde der Eindruck erweckt, dass alle vorhandenen Akten an die Mitarbeitende zugestellt worden sind.

Die Argumentation der Behörde, wonach die fehlenden Unterlagen von der Mitarbeitenden selbst eingereicht worden seien und somit der Zweck, aufgrund dessen sie Einsicht in das Personaldossier verlangte, nicht vereitelt werde, überzeugt nicht. Obwohl eine Verletzung des Datenschutzrechts unter diesem Gesichtspunkt nicht so schwerwiegend erscheint, stellt die unvollständige Herausgabe von Akten einen Verstoss gegen das Recht auf Akteneinsicht dar. Es ist daher festzuhalten, dass die Mitarbeitende Einsicht in sämtliche Akten wünschte, die die Behörde über sie verfügt. Dieser Anspruch musste für die Behörde erkennbar sein, und es ist grundsätzlich irrelevant, ob Teile der Akten von der Mitarbeitenden selbst verfasst worden sind.

Es bleibt zu prüfen, ob die Behörde berechtigt war, Teile der Akten zurückzuhalten, da es sich um Akten eines laufenden Prozesses handelt. Die Zulässigkeit der Einschränkung der Akteneinsicht wird, wie bereits oben ausgeführt, durch das kantonale Datenschutzgesetz in Verbindung mit dem Bundesgesetz über den Datenschutz bestimmt. Gemäss Art. 2 Abs. 2 KDSG finden die Vorschriften des Bundesgesetzes für das Bearbeiten von Personendaten durch Bundesorgane sinngemäss Anwendung. Soweit das kantonale Datenschutzgesetz keine abweichenden oder ergänzenden Bestimmungen enthält, gelten die Definitionen des Bundesgesetzes über den Datenschutz sinngemäss (Art. 2 Abs. 3 KDSG). Das KDSG sieht keine Bestimmungen für die Einschränkung des Auskunftsrechts vor, weshalb auf die Bestimmungen des DSG abgestellt wird.

Gemäss Art. 9 DSG kann der Inhaber einer Datensammlung die Auskunft einschränken, soweit ein Gesetz im formellen Sinn dies vorsieht und es wegen überwiegender Interessen Dritter erforderlich ist. Zudem kann ein Bundesorgan (resp. in casu eine kantonale Behörde) die Auskunft einschränken, soweit es wegen überwiegender öffentlicher Interessen, insbesondere der inneren oder äusseren Sicherheit der Eidgenossenschaft erforderlich ist oder die Auskunft den Zweck einer Strafuntersuchung oder eines anderen Untersuchungsverfahrens in Frage stellt.

Offensichtlich kann vorliegend keine Einschränkung aufgrund öffentlicher Interessen oder eines Untersuchungsverfahrens festgestellt werden. Demnach ist zu prüfen, ob ein Gesetz im formellen Sinn die Einschränkung vorsieht und die Einschränkung wegen überwiegender Drittinteressen erforderlich ist.

Die Behörde stützt sich für die Einschränkung des Akteneinsichtsrechts auf Art. 60a Abs. 4 PV. Die Verordnung ist kein Gesetz im formellen Sinne, weshalb allein deshalb eine Einschränkung unzulässig erscheint. Wie bereits ausgeführt, wird aber in Art. 60a Abs. 4 PV nicht die Einschränkung des Akteneinsichtsrechts geregelt, sondern lediglich die Führung eines zentralen Personaldossiers, zu welchem sowohl die betroffenen Mitarbeitenden und die vorgesetzten Personen Zugriff haben sollen. Ob die Behörde, neben der regulären Datensammlung auch solche zentrale Personaldossiers führt und welche Daten sie darin ablegt, ist vorliegend irrelevant. In jedem Fall vermag sich die Behörde für eine Beschränkung des Auskunftsrechts nicht auf Art. 60a Abs. 4 PV zu stützen. Eine andere gesetzliche Grundlage für die Einschränkung des Auskunftsrechts wird nicht geltend gemacht und ist im Übrigen auch nicht ersichtlich.

Weiter kommen auch keine überwiegenden Interessen Dritter für die Einschränkung des Akteneinsichtsrecht in Frage. Die Behörde ist im vorliegenden Verfahren Beteiligte und nicht Dritte (vgl. Epiney/Fasnacht; in: Belser/Epiney/Waldmann, Datenschutzrecht, § 11 N 53). Schützenswerte und überwiegende Interessen Dritter werden von der Behörde weder geltend gemacht, noch sind sie ersichtlich. Die Einschränkung des Auskunftsrechts findet daher keine Rechtfertigung.

Demnach kann festgehalten werden, dass die Behörde zu Unrecht ihrer Mitarbeitenden auf ihr erstes Begehren hin nicht sämtliche Daten zur Einsicht zustellte.

Meldescheine

Vor beinahe 10 Jahren hat der Kanton Graubünden die Meldepflicht für Schweizer Hotelgäste abgeschafft. Einzelne Gemeinden, insbesondere Tourismusgemeinden, haben für die Abrechnung der kommunalen Gästetaxen oder den Erhalt von Gästekarten in ihren Tourismusgesetzen kommunale Regelungen festgelegt. Für die Erhebung von gewissen Daten besteht somit in der Regel eine gesetzliche Grundlage. Wenn nun eine Gemeinde für die Abrechnung und Kontrolle der richtigen Abrechnung Name und Wohnort eines Schweizer Gastes verlangt, wird dem Prinzip der Verhältnismässigkeit nachgelebt. In der Konsequenz ist der Gast jedoch nicht verpflichtet, einen offiziellen Meldeschein, der eine Vielzahl anderer Angaben enthält, auszufüllen. Der Hotelier muss lediglich Name und Wohnort weiterleiten und den Gast um Auskunft ersuchen. Andere Daten sind nicht erforderlich und dürfen folgerichtig auch nicht verlangt werden.

III. Fälle

1. Betrieb einer App bei der Spitex

Wenn bei einem Spitex Klient festgestellt wird, dass eine psychiatrische Pflegeleistung angezeigt ist, zieht die Spitex externe Fachpersonen zu. Die Spitex hat dazu mit den Psychatrischen Diensten Graubünden (PDGR) einen Vertrag abgeschlossen. Die PDGR Fachpersonen handeln in diesem Fall im Auftrag der Spitex und werden dafür auch von dieser Organisation bezahlt. Seitens der Spitex Organisation wird eine Klientendatenbank über App betrieben. Der Zugriff über diese App ermöglicht den Zugriff auf alle in der App verwalteten Personen. Derzeit ist es softwaremässig nicht möglich, die Berechtigung auf einen bestimmten Personenkreis einzuschränken. In der Konsequenz haben alle Personen, welche die App nutzen auf alle Klientendaten Zugriff.

Ein tragendes Prinzip im Datenschutz bildet der Grundsatz der Verhältnismässigkeit (vgl. Art. 2 Abs. 1 KDSG). Allgemein besagt der Grundsatz der Verhältnismässigkeit, dass eine staatliche Massnahme geeignet und erforderlich sein muss, um den verfolgten Zweck herbeizuführen. Daten dürfen nur dann und nur insoweit bearbeitet werden, wenn sie zur Erfüllung des Zweckes objektiv notwendig sind, wobei diese Frage sowohl im Bezug auf den Umfang der bearbeiteten Daten als auch auf die Intensität der Bearbeitungsvorgänge zu beantworten ist. Aus dem allgemein geltenden Verhältnismässigkeitsgrundsatz lässt sich für die Datenbearbeitung ableiten, dass ein Datenbearbeiter nur diejenigen Daten beschaffen und bearbeiten darf, die er für einen bestimmten Zweck objektiv tatsächlich benötigt. Ausfluss dieses Prinzips ist der Umstand, dass der Datenbearbeiter nur auf diejenigen Daten zugreifen kann, welche für die Auftragserfüllung erforderlich sind. Aus datenschutzrechtlicher Sicht ist es deshalb unhaltbar, wenn über eine mobile App durch jeden Mitarbeitenden der Spitex Organisation auf alle Klientendaten zugegriffen werden kann.

Vorliegend ist weiter der Umstand zu berücksichtigen, dass besonders schützenswerte Personendaten (vgl. Art. 3 lit. c Ziff. 2 DSG) bearbeitet werden. Gesundheitsdaten sind hoch sensibel. In diesem Bereich müssen somit die gesetzlichen Vorgaben in jedem Fall berücksichtigt werden.

2. Weiterleitung Austritts- und Operationsbericht an die Spitex

Es geht um die Frage, ob ein Austrittsbericht des Spitals einer Spitex-Organisation abgegeben werden darf. Der Austrittsbericht fasst den Spital- oder Heimaufenthalt eines Patienten/einer Patientin zusammen. Grundsätzlich umfasst er alle Diagnosen und enthält Kommentare oder wenn nötig eine Diskussion sowie die Behandlung nach der Spitalentlassung. Der primäre Zweck eines Austrittsberichtes liegt damit in der Information des nachbehandelnden Arztes. Grundsätzlich dient somit der Austrittsbericht der künftigen Behandlung des Patienten/der Patientin.

Für das behandelnde Spital stellt sich die Frage, ob der Austrittsbericht an Dritte weitergegeben werden darf. Unbestreitbar werden im Zusammenhang mit der Erstellung eines Austrittsberichtes besonders schützenswerte Personendaten bearbeitet. Gemäss Art. 17 Abs. 2 DSG dürfen besonders schützenswerte Personendaten nur weitergegeben werden, wenn ein Gesetz im formellen Sinne es ausdrücklich vorsieht, wenn sie ausnahmsweise für eine im Gesetz im formellen Sinn klar umschriebene Aufgabe unentbehrlich sind oder die betroffene Person im Einzelfall eingewilligt hat. Was die Anforderungen an die formell-gesetzliche Grundlage betrifft, hat der EDÖB schon sehr früh erläutert. Danach sind insbesondere der "Zweck und Umfang der Datenbearbeitung, allenfalls die dabei verwendeten Mittel sowie die zur Bearbeitung befugten Behörden" mit hinreichender Bestimmtheit zu beschreiben (Sarah Ballenberger in: Maurer-Lambrou/Blechta, Basler Kommentar, Datenschutzgesetz/Öffentlichkeitsgesetz, Art. 17 Note 22). Aus dem Gesundheitsgesetz und den dazugehörigen Nebenerlassen lassen sich die Aufgaben der Spitex-Organisation nicht mit hinreichender Bestimmtheit beschreiben. Die ausnahmsweise Überlassung von Daten für eine klar umschriebene Aufgabe setzt voraus, dass der Spitex-Organisation die Erfüllung ihrer im Gesetz umschriebenen Aufgaben ansonsten nicht möglich wäre. Alleine der Umstand, dass eine Aufgabe durch die Verwendung von sensitiven Daten noch besser erfüllt werden kann, rechtfertigt die Bearbeitung solcher Daten nicht. Gestützt auf die gesetzlichen Vorgaben besteht keine genügende Grundlage, um den Austrittsbericht direkt an die Spitex-Organisation weiterzuleiten.

Indessen sieht Art. 17 Abs. 2 lit. c DSG die Möglichkeit vor, bei der betroffenen Person die Einwilligung für die Abgabe des Austrittsberichts an die Spitex vorzusehen. Grundsätzlich ist die Einwilligung nicht an eine bestimmte Form gebunden. Wenn jedoch besonders schützenswerte

Daten bearbeitet werden, ist eine explizite Einwilligung, die sich auf den bestimmten Einzelfall bezieht, vorausgesetzt. Nur diese auf den Einzelfall bezogene Einwilligung erlaubt es, von einer Zustimmung in Kenntnis der Konsequenzen ausgehen zu können. In der Rahmenvereinbarung zwischen der Spitex und einer Patientin/einem Patienten wird ausdrücklich auf die Entbindung von der Schweigepflicht hingewiesen. Es wird der Spitex-Organisation empfohlen, die Rahmenvereinbarung mit einem Zusatz betreffend die Einwilligung zu ergänzen, wonach die Patientin/der Patient ausdrücklich die Einwilligung gibt, bei behandelnden Ärzten, Spitälern und Heimen die Krankengeschichte anzufordern. Mit dieser Massnahme wird den strengen Anforderungen des Datenschutzgesetzes nachgelebt und die Spitex-Organisation in die Lage versetzt, allenfalls bei behandelnden Ärzten oder Spitälern weitergehende Unterlagen anzufordern. Hingewiesen sei in diesem Zusammenhang auf die Anwendung des Prinzips der Verhältnismässigkeit. Selbst wenn eine Zustimmung für den Beizug von Patientendaten gegeben ist, dürfen nur jene Dokumente angefordert werden, die notwendig und erforderlich sind für die Ausübung des gesetzlichen Auftrages.

3. Akteneinsicht in einen abgeschlossenen Fall

Eine Person möchte Akteneinsicht in einen abgeschlossen Fall der KESB. Die Behörde stellt sich auf den Standpunkt, dass für abgeschlossene Fälle kein Akteneinsichtsrecht mehr bestehe.

Vorab stellt sich die Frage, welches Recht zur Anwendung gelangt. Steck (Daniel Steck, Erwachsenenschutz, ZGB Art. 449b, N. 10) stellt sich auf den Standpunkt, dass das Akteneinsichtsrecht gemäss Art. 449b ZGB nicht nur für laufende, sondern grundsätzlich auch für abgeschlossene Verfahren gelte. Es bedürfe dafür eines Interessennachweises der gesuchstellenden Person. Demgegenüber kann im Basler Kommentar (Geiser/Fountoulakis in: Maurer-Lambrou/Blechta, Basler Kommentar, ZGB Art. 449b, N. 31ff) nachgelesen werden: "Ist ein Verfahren abgeschlossen, so können die seinerzeit am Verfahren Beteiligten ihr Begehren auf Einsicht in die (nunmehr abgeschlossenen) Akten nicht mehr auf Art. 449b stützen." Den Verfahrensbeteiligten komme aber gestützt auf Art. 29 Abs. 2 BV ein Einsichtsrecht zu, sofern sie dafür ein schutzwürdiges Interesse glaubhaft machen könnten. Darüber hinaus kann gestützt auf das datenschutzrechtliche Auskunftsrecht Einsicht verlangt werden. Das Obergericht des Kantons Zürich (PQ 170082, 05.02.2018) hat sich ebenfalls dahingehend geäussert.

Gemäss Art. 25 Abs. 1 nDSG kann jede Person vom Verantwortlichen (vorliegend die KESB) Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden. Die Einschränkungen des Auskunftsrechtes werden in Art. 26 nDSG behandelt. Aus folgenden Gründen kann die Auskunft verweigert, eingeschränkt oder aufgeschoben werden:

- Wenn ein Gesetz dies vorsieht;
- wenn überwiegende Interessen Dritter vorliegen;
- wenn das Auskunftsrecht offensichtlich unbegründet ist;
- wenn überwiegende öffentliche Interessen dagegen sprechen oder
- wenn eine Mitteilung eine Ermittlung, eine Untersuchung oder ein behördliches oder gerichtliches Verfahren gefährden.

Die Behörde muss angeben, worauf sich die Verweigerung bezieht.

Es kann also festgehalten werden, dass bei einem laufenden Verfahren die am Verfahren beteiligten Personen grundsätzlich vorbehaltlos und ohne einen besonderen Interessennachweis ein Akteneinsichtsrecht besitzen.

Nach Abschluss des Verfahrens richtet sich das Akteneinsichtsrecht nach dem kantonalen Datenschutzrecht. Die betroffene Person kann ohne jeglichen Interessennachweis dieses Recht geltend machen (Geiser/Fountoulakis, a.a.O., Art. 449b, N. 39). Die Auskunft kann verweigert oder eingeschränkt werden, wenn obgenannte Gründe vorliegen. Andere am Verfahren Beteiligte haben ein besonders schützenswertes Interesse glaubhaft zu machen (vgl. BGE 129 I 253; Daniel Steck, a.a.O., Art. 449b, N. 10).

Krebsvorsorge

Eine Person hat eine Einladung von der Darmkrebsvorsorge Graubünden erhalten. Auf Anfrage wurde ihr mitgeteilt, dass die persönlichen Daten (Name, Adresse, Geschlecht und Geburtsdatum) vom Amt für Gesundheit übermittelt worden sind. Nach dessen Angabe wurden die Daten bewusst für eine Präventionskampagne weitergegeben. Als Begründung hat das Gesundheitsamt angegeben, einen Leistungsauftrag zu haben.

Es ist richtig, dass das Gesundheitsamt Graubünden mit Bezug auf die Darmkrebsvorsorge Graubünden die erforderlichen Daten an die Krebsliga mitteilt, analog zum Donna-Programm betreffend die Brustkrebsvorsorge. Vor dieser Mitteilung wurden umfangreiche Abklärungen seitens der Kantone getroffen, welche bis ins Jahr 2020 zurückreichen. Das Programm läuft schweizweit.

Da das Gesundheitsamt die Abwicklung dieses Präventionsprogramms nicht selbstständig durchführt, sondern auf das Know-How der Krebsliga zurückgreift, wurde eine umfassende Leistungsvereinbarung abgeschlossen. Die Krebsliga ist somit im Auftrag des Kantons tätig. Die Daten werden ausschliesslich entsprechend den gültigen Sicherheitsvorschriften bearbeitet. Mitgeteilt werden lediglich die Adressdaten. Adressdaten weisen gemäss Art. 19 Abs. 2 DSG keinen hohen Schutzgehalt auf.

Die Teilnahme am Programm ist freiwillig. Wird im Rahmen der Vorsorgeuntersuchung eine Krebserkrankung diagnostiziert, findet das Bundesgesetz über die Registrierung von Krebserkrankungen (KRG, SR 818.33) Anwendung. Danach sind Ärzte und Ärztinnen, Spitäler und andere private oder öffentliche Institutionen des Gesundheitswesens, die eine Krebserkrankung diagnostizieren oder behandeln, verpflichtet, die Daten an das zuständige Krebsregister zu melden (Art 3 KRG). Dieses Register wird in einzelnen Kantonen von der Krebsliga geführt.

Schliesslich ist darauf hinzuweisen, dass eine Datenbearbeitung durch Dritte (Outsourcing) datenschutzrechtlich zulässig ist. Behörden dürfen somit Daten an Dritte weitergeben, sofern dies zur Bewältigung einer eigenen Aufgabe erforderlich ist.

4. Anfrage beim Sozialamt betreffend Aufenthalt einer Person

Für eine Aufenthaltsabklärung eines Einwohnerdienstes im Zusammenhang mit einer suchtabhängigen Person stellte sich das kantonale Sozialamt auf den Standpunkt, es erteile aufgrund der in Art. 13 Sozialhilfegesetz (SHG; BR 546.100) statuierten Geheimhaltungspflicht und aufgrund des DSG keinerlei Auskünfte über den Aufenthaltsort der besagten Person.

Gemäss Art. 34 Abs. 1 nDSG darf eine Behörde Personendaten nur bearbeiten, wenn dafür eine gesetzliche Grundlage besteht. In Art. 5 Einwohnerregistergesetz (ERG) wird festgehalten, dass die Gemeinde bzw. das Einwohneramt ein Einwohnerregister über sämtliche Personen mit Niederlassung oder Aufenthalt in der Gemeinde mit den vorgeschriebenen Merkmalen führt. Es besteht also grundsätzlich eine gesetzliche Grundlage für die Erhebung der Personendaten gemäss den Attributen von Art. 5 Abs. 1 lit. a ERG. Es ist davon auszugehen, dass nur die gesetzlichen Merkmale beim Sozialamt angefragt worden sind. Gemäss Art. 36 Abs. 2 lit. a nDSG ist eine Bekanntgabe möglich, wenn die Daten für die anfragende Behörde unentbehrlich sind und sie anderweitig nicht beschafft werden können. Bei Art. 36 Abs 2 nDSG handelt es sich um einen Ausnahmetatbestand und dieser kann nur im Einzelfall angerufen werden. Es muss also keine eigenständige Rechtsgrundlage vorliegen. Die Daten müssen aber für den Empfänger zur Erfüllung einer gesetzlichen Aufgabe unentbehrlich sein. Unentbehrlich bedeutet, dass ohne die Datenbekanntgabe die gesetzliche Aufgabe überhaupt nicht erfüllt werden kann. Eine bloss verbesserte oder effizientere Aufgabenerfüllung genügt nicht als Rechtfertigung. Als ultima ratio kann somit auch das Sozialamt um eine Bekanntgabe von Aufenthaltsdaten angefragt werden.

Wenn ein Einwohnerdienst das Sozialamt kontaktiert, muss es offensichtlich darüber informiert sein, dass ein entsprechender Fall bei der Sozialbehörde hängig ist. Es können nur Informationen zum Aufenthalt angefragt werden. Diese können im Kontext der Bearbeitung durch das Sozialamt von besonderer Bedeutung sein. Wenn die Einwohnerdienste jedoch bereits über die Bearbeitung des Falls informiert sind, entfällt die Sensibilität. Das Einwohneramt darf nicht erfragen, ob eine bestimmte Person unter Betreuung steht. Allerdings kann es den Aufenthaltsort erfragen, wenn es Kenntnis von der Fallbehandlung hat.

Der Datenbeauftragte des Kantons Zürich hat beispielsweise die Bekanntgabe des Aufenthaltsortes eines Inhaftierten an das Betreibungsamt für zulässig erachtet (vgl. Claudia Mund, in: Baeriswyl, Pärli, Blonski, Handkommentar zum DSG, 2. Auflage, Art. 36, N 12). Vor dem Hintergrund der gesetzlichen Aufgabe der Einwohnerdienste und der offenkundig fehlenden Sensibilität der angefragten Daten kann auch unter Einbezug einer Interessenabwägung und dem Verhältnismässigkeitsprinzip gestützt auf Art. 36 Abs. 2 lit. a nDSG der Aufenthaltsort bekannt gegeben werden.

Einsicht in Arbeitsverträge

In einem Gemeindevorstand hat sich die Frage gestellt, ob einzelne Vorstandsmitglieder berechtigt sind, Kopien der Arbeitsverträge von Gemeindeangestellten, die ihnen nicht direkt unterstellt sind, zu erhalten (im konkreten Fall ging es um den Vertrag des Gemeindeschreibers).

Im Bereich Datenschutz gilt als tragende Säule das Prinzip der Verhältnismässigkeit. Ein Verhalten entspricht dann dem Verhältnismässigkeitsprinzip, wenn die Massnahme folgende Elemente erfüllt: Geeignetheit, d.h. sie ist geeignet, das angestrebte Ziel zu erreichen; Erforderlichkeit, also diejenige Massnahme, welche die privaten Interessen am meisten schont und die Zumutbarkeit. Es soll ein vernünftiges Verhältnis zwischen dem Zweck der Bearbeitung und der damit verbundenen Beeinträchtigung der Persönlichkeit bestehen.

Gemäss Aussage der Gemeindepräsidentin ist der Gemeindevorstand für die Anstellung der Mitarbeitenden zuständig. Diese Kompetenz impliziert grundsätzlich auch die Einsichtnahme in die entsprechenden Verträge. Es stellt sich einzig die Frage, ob nach Durchlaufen des Bewerbungs- und Anstellungsverfahrens ein Gemeindevorstandsmitglied weiterhin berechtigt ist, in die konkreten Verträge Einsicht zu nehmen. Als oberste Führungsebene ist der Gemeindevorstand grundsätzlich befugt, Unterlagen einzusehen, wenn sie im direkten Zusammenhang mit der Ausübung des politischen Amtes stehen. Wenn also der Arbeitsvertrag des Gemeindeschreibers erforderlich ist, um einen Entscheid in personalrechtlicher Hinsicht zu fällen, kann der Arbeitsvertrag herangezogen werden. Wenn indessen kein Zusammenhang zu einem aktuellen Entscheid besteht, wird der Schutz der Persönlichkeit der betroffenen Person höher gewichtet als das Interesse auf Einsichtnahme, dies als Ausfluss der Anwendung des Prinzips der Verhältnismässigkeit.

5. Videoüberwachung aufgrund einer aktuellen Gefährdung

Eine Gemeinde fragt an, ob sie während eines bestimmten Zeitraumes zur Gefahrenabwehr und Intervention Bildüberwachungsmassnahmen anordnen darf. Gemäss Art. 3a Abs. 1 lit. a KDSG kann der öffentliche und öffentlich zugängliche Raum mit Bildübermittlungs- und Bildaufzeichnungsgeräten zur Personenidentifikation überwacht werden, sofern die öffentliche Sicherheit und Ordnung konkret gefährdet ist. Eine solche konkrete Gefahrenlage gilt als erstellt, wenn eine sicherheitspolizeiliche Lagebeurteilung die Annahme rechtfertigt, dass am zu überwachenden Ort die öffentliche Ordnung verletzt werden könnte. In Art. 3b KDSG wird unterschieden zwischen anlassbezogenen Bildüberwachungen und Bildüberwachungen zum Schutze öffentlicher Gebäude. Die anlassbezogene Bildüberwachung bezieht sich auf Vorfälle im öffentlichen Raum, für welche keine permanente Bildüberwachung installiert wird. Darunter werden Bildüberwachungsanlagen verstanden, die für einen längeren Zeitraum Bildaufzeichnungen vornehmen. Soll jedoch eine Bildüberwachung von Beginn weg über drei Monate dauern, ist das "ordentliche Verfahren" durchzuführen. Zur Abwendung von aktuellen Gefahren wurde in Art. 3b Abs. 4 KDSG bewusst eine einfache Lösung getroffen, im Wissen, dass dadurch der vorgängige Rechtsschutz nicht gewährt werden kann.

Wenn nun die Gemeinde aufgrund der aktuellen Gefahr für Leib und Leben im Zusammenhang mit einem vorhersehbaren Bergsturz eine Videoüberwachung betreibt und nicht vorgesehen ist, diese länger als drei Monate aufrechtzuerhalten, handelt sie rechtmässig. Mit Art. 3b Abs. 4 KDSG sind Sachverhalte dieser Art abgedeckt, obschon in den Materialien nicht expressis verbis darauf eingegangen wird. Ein weiterer Hinweis auf die Rechtmässigkeit ergibt sich aus der Tatsache, dass die Art. 3a und 3b KDSG im Zusammenhang mit der Revision des Polizeigesetzes eingeführt worden sind. Dabei ging es u.a. um die Anordnung von Massnahmen im Zusammenhang mit der konkreten Gefährdung der öffentlichen Sicherheit und Ordnung. Es kann wohl kaum ernsthaft bestritten werden, dass in der Gemeinde aufgrund der akuten Gefahr eines Bergsturzes aktuell die öffentliche Sicherheit und Ordnung nicht tangiert ist. Folgerichtig dienen die Überwachungsmassnahmen sicherheitspolizeilichen Zwecken. Sie sind polizeilicher Natur.

Gestützt auf Art. 3b Abs. 4 KDSG ist die Gemeinde befugt, Bildüberwachungsmassnahmen im Zusammenhang mit der aktuellen Gefahrenlage in der Gemeinde ohne vorgängigen Rechtsschutz anzuordnen.

6. Weitergabe von Daten des Gemeindevorstandes an die GPK

Es stellt sich die Frage, ob die Daten eines Audits im Zusammenhang mit personellen Problemen in der Gemeindeverwaltung an die GPK weitergeleitet werden müssen. Die Aufgabe der GPK ergibt sich aus der Verfassung. In der gültigen Verfassung wird ähnlich wie bei anderen Gemeinden die Aufgabe der GPK erläutert. Sie kann alle Unterlagen, welche für die Aufgabenerfüllung erforderlich sind, bei allen Behörden verlangen. Die spezifischen Aufgaben ergeben sich aus Gesetz. Daraus wird ersichtlich, dass die GPK vornehmlich die Finanzen zu prüfen hat, aber nicht nur. Sie ist auch befugt, die richtige Anwendung der Gesetzgebung im Zusammenhang mit der Übereinstimmung mit den Rechnungsprüfungsstandards zu überwachen. Selbst hier zeigt sich der Konnex mit finanziellen Auswirkungen. In diesem Gesetz wird indessen auch ausgeführt, die Prüfung der Gesamtverwaltung und der politischen, administrativen und finanziellen Führung der Gemeinde bilde Aufgabe des Gemeindevorstandes. Die Kernfrage, die sich somit stellt, ist die Frage, ob der Audit-Bericht zur Prüfung der Verwaltung erforderlich ist, oder ob es sich nicht vielmehr um ein internes Arbeitspapier des Vorstandes handelt, das nicht weitergegeben werden muss. Dieser Fragenkomplex ist grundsätzlich nicht datenschutzrechtlicher Natur. Es handelt sich hier um Fragen der Anwendung des Verwaltungsrechtes.

Gemäss Art. 34 Abs. 1 nDSG dürfen Personendaten nur bekannt gegeben werden, wenn dafür eine gesetzliche Grundlage besteht. Vorliegend stellt sich somit die Frage, ob die Formulierung in der Verfassung und dem Gesetz genügt bzw. ob die Daten, die angefordert werden, zur Erfüllung der Aufgabe der GPK von Bedeutung sind. Das Audit ist vom Gemeindevorstand in Auftrag gegeben worden im Zusammenhang mit Problemen innerhalb der Verwaltung. Das abgegebene Dokument dient als Arbeitshilfe für den Gemeindevorstand, um die zwischenmenschlichen Probleme einzelner Mitarbeitenden zu benennen und Lösungsvarianten zu erarbeiten. Der Gemeindevorstand stellt sich somit auf den Standpunkt, es handle sich um ein internes Arbeitspapier des Gemeindevorstandes, das nicht zur Aufgabenerfüllung der GPK dient. Diese Auffassung hat durchaus etwas für sich.

Nicht völlig unberücksichtigt darf der Umstand bleiben, dass in diesem Papier besonders schützenswerte Personendaten bearbeitet werden. Gera-

de in einer kleinen Gemeinschaft kann die Weiterverbreitung von solchen Daten einschneidende Folgen für die Betroffenen haben. In Art. 34 Abs. 2 nDSG wird darauf Bezug genommen. Er lautet:

Eine Grundlage in einem Gesetz im formellen Sinn ist in folgenden Fällen erforderlich:

a. Es handelt sich um die Bearbeitung von besonders schützenswerten Personendaten.
b. Es handelt sich um ein Profiling.
c. Der Bearbeitungszweck oder die Art und Weise der Datenbearbeitung können zu einem schwerwiegenden Eingriff in die Grundrechte der betroffenen Person führen.

Vor dem Hintergrund, dass sensible Daten bearbeitet worden sind, ist die Zurückhaltung in der Weitergabe von Daten verständlich.

7 . Weitergabe von Daten an aussenstehende Dritte

Die Schulleiterin hat eine E-Mail einer Mutter erhalten. Dieses Mail hat keine Namen enthalten. Aufgrund des Absenders konnte jedoch auf Personen geschlossen werden. Das Mail wurde an eine Person ausserhalb des Schulbetriebs weitergeleitet. Durch eine Indiskretion hat die Mutter von der Weiterleitung des Mails erfahren.

Vorab stellt sich die Frage, ob datenschutzrechtlich relevante Daten weitergeleitet wurden. Gemäss Art. 5 lit. a nDSG (Art. 3 lit. a DSG) werden alle Daten, die sich auf eine bestimmte oder bestimmbare Person beziehen, als Personendaten qualifiziert. Das Gesetz bezweckt den Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen, über die Personendaten bearbeitet werden (Art. 1 nDSG; Art. 1 DSG). Es kann festgestellt werden, dass das weitergeleitete Mail eine Adresse beinhaltete. Folgerichtig war erkennbar, wer das Mail geschrieben hatte. Ebenso konnte der Inhalt des Mails zwangsläufig den betroffenen Personen zugeordnet werden. Das Datenschutzgesetz kommt zur Anwendung.

Offenkundig wurden diese Personendaten an eine Drittperson weitergeleitet. Aus datenschutzrechtlicher Sicht stellt sich die Frage, ob die dafür notwendigen Voraussetzungen erfüllt waren. Die Bekanntgabe von Personendaten ist in Art. 36 nDSG (Art. 19 DSG) geregelt. Eine Bekanntgabe ist möglich, wenn eine gesetzliche Grundlage besteht. Vorliegend ist dies nicht der Fall. Wenn eine gesetzliche Grundlage fehlt, ist dennoch eine Weitergabe aus datenschutzrechtlicher Sicht möglich, wenn eine der folgenden Voraussetzungen erfüllt ist:

- Die Bekanntgabe ist für den Empfänger zur Erfüllung einer gesetzlichen Pflicht unentbehrlich,
- Die betroffene Person hat eingewilligt,
- Die Bekanntgabe ist notwendig, um das Leben oder die körperliche Unversehrtheit einer Person zu schützen,
- Die Daten hat die betroffene Person allgemein zugänglich gemacht,
- Es liegt eine unberechtigte Verweigerung der betroffenen Person vor.

Im vorliegenden Fall kann festgestellt werden, dass keine dieser Voraussetzungen erfüllt ist und somit ist gegen datenschutzrechtliche Bestimmungen verstossen worden.

Die Angelegenheit hat sich im Juni 2023 zugetragen. Damals galt noch das am 1.9.2023 abgelöste Datenschutzgesetz. Gemäss Art. 35 Abs. 1 DSG wird auf Antrag mit Busse bestraft, wer vorsätzlich geheime, besonders schützenswerte Personendaten oder Persönlichkeitsprofile unbefugt bekannt gibt, von denen er bei der Ausübung seines Berufes, der die Kenntnis solcher Daten erfordert, erfahren hat. Vorliegend kann nicht beurteilt werden, ob besonders schützenswerte Personendaten (vgl. Art. 5 lit. c nDSG; Art. 3 lit. c DSG) bekannt gegeben worden sind. Der Strafnorm liegt der Gedanke zugrunde, dass nur qualifizierte Privatdaten strafrechtlich schützenswert sind. Wurden also keine besonders schützenswerten Personendaten weitergeleitet, entfällt eine strafrechtliche Verfolgung. Hinzuweisen ist auf den Umstand, dass es sich um ein Antragsdelikt handelt. Es muss also eine Anzeige bei der Polizei oder der Staatsanwaltschaft erfolgen.

Weiterleitung von Dokumenten

Eltern wenden sich mit Vorwürfen an die Schulleitung, welche den Schulalltag betreffen. In diesem Zusammenhang stellt sich die Frage, an wen die Schulleitung die entsprechenden Akten weiterleiten darf.

Die Schulleitung hat die Aufgabe, den Schulbetrieb innerhalb eines Schulhauses zu organisieren und zu koordinieren. Darüber hinaus hat sie sich auch mit Problemen zwischen Eltern und Lehrpersonen zu beschäftigen. Wenn also Reklamationen von Eltern an die Schulleitung herangetragen werden, ist die Schulleitung verpflichtet, einen entsprechenden Fall zu eröffnen. Die involvierten Personen haben ein Akteneinsichtsrecht. Es ist also möglich, die betreffende Lehrperson zu benachrichtigen. Die Offenlegung aller Akten richtet sich nach Art. 26 nDSG. Danach kann eine Auskunft verweigert, eingeschränkt oder aufgeschoben werden, wenn eine gesetzliche Grundlage besteht oder überwiegende Interessen Dritter dies erfordern.

IV. Statistik

Wer \ Was	Kurzanfragen	Berichte	Empfehlungen	Kontrollen	Vernehmlassungen	Referate	Kurse	Weiterbildung/Verbände
Kantonale Dienste								
Allgemeine Verwaltung	1							
DVS	5		1			1		
DJSG	10					1		
EKUD	11		1					
DFG	3				1			
DIEM								
öff. rechtliche Anstalten	12		1					
Gerichte								
Regionen								
Gemeindeverbände								
Gemeinden	46					1		
Bürgergemeinden								
Juristische Personen	1		2					
Private Personen	66		6					
Andere	1				1	10	2	3
Total	156	0	11	0	2	13	2	3

VI. Abkürzungsverzeichnis

a.a.O.	am angeführten Ort
Abs.	Absatz
AFI	Kantonales Amt für Informatik
AGB	Allgemeine Geschäftsbedingungen
a.M.	anderer Meinung
Art.	Artikel
B	Botschaft
BBl	Bundesblatt
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
ERG	Gesetz über die Einwohnerregister und weitere Personen- und Objektregister
etc.	et cetera
f./ff.	folgend/folgende
GPK	Geschäftsprüfungskommission
GPR	Gesetz über die politischen Rechte
GR	Graubünden
Hrsg.	Herausgeber
i.V.m.	in Verbindung mit
KDSG	Kantonales Datenschutzgesetz
KESB	Kindes- und Erwachsenenschutzbehörde
KRG	BG über die Registrierung von Krebserkankungen
KV	Kantonsverfassung
lit.	litera
N	Note
nDSG	neues Datenschutzgesetz
OR	Obligationenrecht
PDGR	Psychiatrische Dienste Graubünden
PG	Personalgesetz
PV	Personalverordnung
RB	Rechtsbuch
Rz	Randziffer
S	Seite
SHG	Sozialhilfegesetz
SR	Sammlung der eidgenössischen Gesetze und systematische Sammlung des Bundesrechts (Systematische Rechtssammlung)
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