Tätigkeitsbericht 2024

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

Das Jahr 2024 war durch die Revision des kantonalen Datenschutzgesetzes (KDSG) geprägt. Erfreulicherweise wurde nicht nur ein eigenständiger Entwurf für ein KDSG entwickelt, sondern der Gesetzgeber beschäftigte sich auch intensiv mit den Auswirkungen auf die Umsetzung. Die neuen Aufgaben der Aufsichtsbehörde erfordern zwingend eine entsprechende Anpassung ihrer Ressourcen. Insbesondere dem Datenschutzbeauftragten fehlt es noch an ausreichendem IT-Know-how. Zukünftig soll diesem wichtigen Aspekt jedoch mehr Aufmerksamkeit geschenkt werden. Es ist zu erwarten, dass neben juristischem Fachwissen künftig auch IT-Kompetenz aufgebaut wird, wozu die entsprechenden Experten benötigt werden.

Bisher war der Datenschutzbeauftragte auf die Unterstützung des Amts für Informatik angewiesen. In Zukunft wird er jedoch in der Lage sein, unabhängig und mit eigenem Personal die sich stellenden Fragen zu bearbeiten. Die Aufstockung des Personals stellt einen wesentlichen Fortschritt dar. Die datenschutzrechtlichen Vorgaben gelten bereits seit dem Inkrafttreten des revidierten Eidgenössischen Datenschutzgesetzes. Dennoch war es bisher nur unzureichend möglich, diese Vorgaben in vollem Umfang umzusetzen. Dies wird sich nun ändern.

Der Datenschutzbeauftragte hat vor allem eine beratende Funktion, die auch in Zukunft bestehen bleibt. Mit der Erhöhung des Personalbestands kann insbesondere die Unterstützung der Gemeinden verbessert werden. Gerade in Zeiten zunehmender Cyberkriminalität, von der auch öffentliche Institutionen betroffen sein können, ist es unerlässlich, dem Prinzip der Datensicherheit grösste Beachtung zu schenken. Die Gemeinden betreiben eine Vielzahl unterschiedlichster Programme, sind vernetzt und kommunizieren weitgehend elektronisch – sie sind somit anfällig für Angriffe. Dabei spielt es keine Rolle, ob es sich um eine Kleinstgemeinde oder die Stadt Chur handelt. Der Aspekt der Datensicherheit muss höchste Priorität geniessen. Hierzu dienen sowohl die neuen gesetzlichen Instrumente auf kantonaler und eidgenössischer Ebene als auch die persönliche Unterstützung durch Fachkräfte.

Abschliessend muss die Umsetzung der neuen Datenschutzverantwortlichkeiten kontrolliert werden. Kontrollen sind zwar nicht immer angenehm für die Betroffenen, tragen jedoch dazu bei, Schwachstellen zu identifizieren und Fehler aufzudecken – mit dem Ziel, die Datensicherheit zu verbessern. Der Fokus muss daher auf der konkreten Verbesserung der Sicherheitsmassnahmen liegen. Eine Kontrolle ist nicht Selbstzweck, sondern soll unbedingt zu klaren Erkenntnissen und den entsprechenden, wirksamen Massnahmen führen. Wir können also gespannt sein auf die Einführung einer eigenständigen kantonalen Datenschutzordnung im Kanton Graubünden.

Kantonaler Datenschutzbeauftragter:

Thomas Casanova

II. Bistum Chur – Anwendbares Datenschutzgesetz

(verfasst von MLaw Johannes Frings, RA)

Die römisch-katholische Kirche bildet im Kanton Graubünden die grösste Religionsgemeinschaft. Zusammen mit der evangelisch-reformierten Kirche ist sie öffentlichrechtlich anerkannt (Art. 98 Abs. 1 KV/GR). Die Organisation der römisch-katholischen Kirche weist in der Schweiz eine besondere Doppelstruktur auf. Im sog. dualen System besteht neben der demokratisch organisierten Landeskirche die hierarchisch organisierte Bischofskirche. Für die Regelung des Verhältnisses zwischen Kirche und Staat sind in der Schweiz die Kantone zuständig (Art. 72 Abs. 1 BV). Diese bestimmen die Rechtsstellung der Religionsgemeinschaften im staatlichen Recht. Die katholische Landeskirche ist im Kanton Graubünden als Körperschaft des öffentlichen Rechts anerkannt (Art. 98 Abs. 2 KV/GR). Die Kantonverfassung räumt den beiden Landeskirchen im Rahmen des kantonalen Rechts Autonomie ein (Art. 99 Abs. 1 KV/GR).

Die katholische Kirche kennt mit dem kanonischen Recht ihr eigenes Kirchenrecht. Sie ist territorial in Bistümer (Diözesen) untergliedert. Das Gebiet des Kantons Graubünden ist kirchenrechtlich Bestandteil des Bistums Chur. Die kirchliche Verwaltungsgliederung stimmt nicht notwendigerweise mit der staatlichen Organisationsstruktur überein. So umfasst das Bistum Chur gegenwärtig neben dem Kanton Graubünden auch die Kantone Schwyz, Uri, Glarus, Obwalden, Nidwalden und Zürich. Sitz des Diözesanbischofs ist der bischöfliche Hof in Chur, Bischofskirche die Churer Kathedrale St. Maria Himmelfahrt. Auch das bischöfliche Ordinariat befindet sich in Chur.

Die Schweiz verfügt über nicht weniger als 27 Datenschutzgesetze. Nebst dem eidgenössischen Datenschutzgesetz[1], welches kürzlich totalrevidiert worden ist, verfügt jeder Kanton über ein eigenes Datenschutzgesetz. Die katholische Kirche hat in der Schweiz – im Unterschied etwa zu Deutschland[2] – kein eigenes Datenschutzgesetz. Auf dem Territorium des Bistums Chur kommen damit sieben kantonale Datenschutzgesetze und das eidgenössische Datenschutzgesetz zur Anwendung. Vor diesem Hintergrund fragt es sich, welches Datenschutzgesetz auf das Bistum Chur in persönlicher Hinsicht anwendbar ist.

---

[1] *Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG) vom 25. September 2020 (SR 235.1).*

[2] *Gesetz über den Kirchlichen Datenschutz vom 20. November 2017 (KDG).*

Das eidgenössische Datenschutzgesetz bezweckt den Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen, über die Personendaten bearbeitet werden (Art. 1 DSG). Es regelt insbesondere Transparenz- und Informationspflichten, Datensicherheit und die Rechte der betroffenen Personen. Art. 2 DSG regelt den persönlichen und sachlichen Geltungsbereich des Datenschutzgesetzes und legt damit fest, wer sich an das eidgenössische Datenschutzrecht halten muss.[3] Es gilt gemäss Art. 2 Abs. 1 DSG für die Bearbeitung von Personendaten natürlicher Personen durch private Personen (Bst. a) sowie durch Bundesorgane (Bst. b).

Als private Personen werden alle Subjekte des Privatrechts, also alle natürlichen und juristischen Personen, verstanden (z.B. Unternehmen, Vereine, Stiftungen). Die Pflichten des Gesetzes richten sich aber auch an Personengesellschaften ohne Rechtspersönlichkeit, die prozessfähig sind.[4] Als Bundesorgan gelten alle Behörden oder Dienststellen des Bundes (z.B. Bundesämter) oder auch Personen, die mit öffentlichen Aufgaben des Bundes betraut sind (Art. 5 Bst. i DSG). Staatliche Organe untergeordneter Staatsebenen sind nicht vom Geltungsbereich des eidgenössischen Datenschutzgesetzes erfasst. Kantonale und kommunale Organe gelten selbst dann nicht als Bundesorgane, wenn sie Bundesaufgaben wahrnehmen.[5] Das eidgenössische Datenschutzgesetz ist damit nicht auf Kantone und Gemeinden anwendbar. Diese unterstehen den kantonalen Datenschutzgesetzen.[6]

Bei der römisch-katholischen Landeskirche Graubünden handelt es sich um eine staatskirchenrechtlich begründete Körperschaft des kantonalen öffentlichen Rechts. Sie kann damit weder als eine private Person noch als ein Bundesorgan qualifiziert werden. Die Landeskirche ist vom Anwendungsbereich des eidgenössischen Datenschutzgesetzes nicht erfasst. Hingegen untersteht die römisch-katholische Landeskirche Graubünden als öffentlich-rechtliche Körperschaft des Kantons ohne Weiteres nach Art. 1 Abs. 2 Bst. b KDSG[7] dem Anwendungsbereich des kantonalen Datenschutzgesetzes.

---

[3] Vgl. BSK DSG-Drechsler, Art. 2 N 1.

[4] So namentlich Kollektiv- und Kommanditgesellschaften (BSK DSG-Drechsler, Art. 2 N 7; DSG Komm.-Rosenthal/Jöhri, Art. 2 N 6).

[5] BSK DSG-Drechsler, Art. 2 N 12; Botschaft DSG 1988, 445.

[6] Für den Kanton Graubünden vgl. Art. 1 Abs. 2 KDSG.

[7] Kantonales Datenschutzgesetz (KDSG) vom 10. Juni 2001 (BR 171.100).

Um die Anwendbarkeit des eidgenössischen oder eines kantonalen Datenschutzgesetzes auf das Bistum Chur beurteilen zu können, ist zunächst dessen Rechtsnatur zu qualifizieren. Es könnte sich bei diesem namentlich um eine öffentlich-rechtliche Körperschaft des Kantons Graubünden, ein interkantonales Organ, eine juristische Person des Privatrechts oder eine Personengesellschaft ohne Rechtspersönlichkeit handeln.

Das Bistum Chur ist nach kanonischem Recht als Diözese eine Teilkirche der einen und einzigen römisch-katholischen Kirche.[8] Es handelt sich bei diesem damit grundsätzlich um eine Rechtsperson kirchlichen Rechts. Das Bistum Chur wurde allerdings durch die Schweiz staatsvertraglich als Rechtsperson anerkannt.[9] Aus Sicht des eidgenössischen Datenschutzgesetzes handelt es sich folglich um eine private (juristische) Person im Sinne von Art. 2 Abs. 1 Bst. a DSG. Das Bistum Chur ist vom persönlichen Anwendungsbereich des eidgenössischen Datenschutzgesetzes erfasst.

Weiter ist zu prüfen, welche Bedeutung den kantonalen Datenschutzgesetzen im Zusammenhang mit dem Bistum Chur zukommt. Das Gebiet des Bistums Chur erstreckt sich über sieben Kantone mit je eigenem Datenschutzgesetz.[10] Da sich der Bischofssitz in Chur und damit im Kanton Graubünden befindet, rechtfertigt es sich, zunächst auf das Datenschutzgesetz des Kantons Graubünden einzugehen.

Gemäss Art. 1 Abs. 1 KDSG dient das Datenschutzgesetz dem Schutz von Personen vor widerrechtlichem Bearbeiten von Personendaten durch Behörden. Der persönliche Anwendungsbereich des Gesetzes wird in Art. 1 Abs. 2 KDSG festgelegt. Als Behörden im Sinne des KDSG gelten Behörden und Amtsstellen des Kantons, der Regionen, Gemeinden und Gemeindeverbindungen (Bst. a), öffentlich-rechtliche Anstalten, Stiftungen und Körperschaften des Kantons, der Regionen und Gemeinden (Bst. b) sowie Private, soweit ihnen öffentliche Aufgaben übertragen sind (Bst. c).

---

[8] Vgl. Canon 368 f. Codex Iuris Canonici (CIC).

[9] Vgl. zum Ganzen BGer 2C_955/2016, 2C_190/2018 vom 17. Dezember 2018 E. 1.4.

[10] Schwyz: Gesetz über die Öffentlichkeit der Verwaltung und den Datenschutz (ÖDSG) vom 23. Mai 2007 (SRSZ 140.410); Glarus: Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (IDAG) vom 05. September 2021 (GS IF/1); Uri: Gesetz über den Schutz von Personendaten (Kantonales Datenschutzgesetz, KDSG) vom 22. Oktober 2023 (RB 2.2511); Obwalden: Gesetz über den Datenschutz (Datenschutzgesetz, kDSG) vom 25. Januar 2008 (GDB 137.1); Nidwalden: Gesetz über den Datenschutz (Kantonales Datenschutzgesetz, kDSG) vom 20. Februar 2008 (NG 232.1); Zürich: Gesetz über die Information und den Datenschutz (IDG) vom 12. Februar 2007 (LS 170.4).

Beim Bistum Chur handelt es sich – wie gezeigt – um eine Rechtsperson kirchlichen Rechts bzw. um eine private juristische Person. Es kann daher weder als kantonale Behörde noch als öffentlich-rechtliche Körperschaft des Kantons angesehen werden. Eine Anwendung des KDSG auf das Bistum Chur kommt daher nur ausnahmsweise in Betracht. Wenn das Bistum als Privater öffentliche Aufgaben wahrnimmt, welche ihm übertragen wurden, gilt es als Behörde im Sinne des KDSG. Sinngemäss gilt das Gesagte auch für die anderen kantonalen Datenschutzgesetze, welche auf dem Gebiet des Bistums in Kraft stehen.

Zusammenfassend kann damit festgehalten werden, dass hinsichtlich der römisch-katholischen Kirche datenschutzrechtlich zu differenzieren ist. Sie verfügt in der Schweiz über kein eigenes Datenschutzgesetz. Die römisch-katholische Landeskirche Graubünden untersteht als öffentlich-rechtliche Körperschaft dem Anwendungsbereich des kantonalen Datenschutzgesetzes. Auf das Bistum Chur ist als private juristische Person primär das eidgenössische Datenschutzgesetz anwendbar. Das revidierte DSG (in Kraft seit dem 1. September 2023) gilt für alle privaten Organisationen, auch für kirchliche Einrichtungen wie das Bistum Chur. Die Einordnung des Bistums Chur als private Organisation im datenschutzrechtlichen Sinne ergibt sich aus der rechtlichen Stellung der katholischen Kirche im Schweizer Rechtssystem. Das Bistum ist befugt, sich eigene interne Datenschutzrichtlinien zu geben. Diese dürfen das übergeordnete DSG jedoch nicht unterlaufen. Je nach der konkreten Datenverarbeitungstätigkeit können auf das Bistum Chur ausnahmsweise auch kantonale Datenschutzgesetze anwendbar sein. Namentlich wenn es um die Zusammenarbeit mit öffentlichen Stellen wie beispielsweise Schulen oder Behörden geht und das Bistum dabei öffentliche Aufgaben übernimmt, ist es an die Bestimmungen des jeweils betroffenen kantonalen Datenschutzgesetzes gebunden.

Telefonverkehr in der Strafanstalt

In einer Strafanstalt ist zwischen Telefongesprächen aus dem eigentlichen Strafvollzug und jenen aus dem Bereich des Sozialdienstes zu unterscheiden.

Die Aufzeichnung und Protokollierung von Telefongesprächen, die direkt aus dem Bereich des Strafvollzugs geführt werden, ist gestützt auf Art. 36 Abs. 3 des Gesetzes über den Justizvollzug in Verbindung mit Art. 35 Abs. 1 der Verordnung über die Vollzugseinrichtungen rechtlich zulässig. Die Strafanstalt ist somit befugt, solche Gespräche aufzuzeichnen.

Anders verhält es sich bei der Nutzung der Telefone im Bereich des Sozialdienstes. Dort erfolgt keine Aufzeichnung der Telefongespräche. Allerdings wird bei diesen Anrufen die Absendernummer standardmässig unterdrückt, was dazu führt, dass viele der angerufenen Personen die Gespräche aus Misstrauen nicht entgegennehmen.

Dieser Umstand wurde dem Amt für Justizvollzug zur Kenntnis gebracht. Das Amt ist sich der Problematik bewusst und hat entsprechend reagiert. Es wurde verfügt, dass bei einem definierten Telefonanschluss die Absendernummer angezeigt wird. Dieses Telefon wird konkret und eindeutig bezeichnet.

Damit wird künftig sichergestellt, dass aus dem Sozialdienst heraus Telefonate mit sichtbarer Rufnummer und ohne Aufzeichnung möglich sind. Durch diese Massnahme wird dem berechtigten Schutz der Persönlichkeitsrechte der betroffenen Personen in angemessener Weise Rechnung getragen.

III. Merkblätter

Ein Merkblatt ist ein kurzes, informatives Dokument, das wichtige Informationen, Hinweise oder Anweisungen zu einem bestimmten Thema übersichtlich zusammenfasst. Es hat das Ziel, den Leser schnell und verständlich über relevante Aspekte zu informieren. Dabei ist es entscheidend, dass das Merkblatt den Anwender erreicht und seine Zielgruppe effektiv anspricht.

Angesichts der begrenzten Kommunikationsmöglichkeiten des Datenschutzbeauftragten werden die auf der Webseite des Kantons Graubünden (https://www.gr.ch/DE/institutionen/verwaltung/staka/themen/dienstleistungen/Seiten/datenschutz.aspx) veröffentlichten Merkblätter in diesem Tätigkeitsbericht aufgeführt. Diese Merkblätter enthalten wichtige Informationen zu den Vorgehensweisen bei Datenschutzverletzungen sowie zu Vorabkonsultationen.

1. Merkblatt Vorabkonsultation

1. Definition

Eine Vorabkonsultation ist eine vorgängige Prüfung einer geplanten Bearbeitung von Personendaten (Art. 20 E-KDSG).

2. Wann ist eine Vorabkonsultation erforderlich?

a) Allgemeines
Wenn eine geplante Bearbeitung von Daten trotz den vorgesehenen Massnahmen dennoch ein hohes Risiko für die Grundrechte der betroffenen Person zur Folge hat, so muss vorgängig (vorab) eine Stellungnahme des Datenschutzbeauftragen eingeholt werden. Mit der Datenschutz-Folgeabschätzung (DSFA) wird evaluiert, ob ein hohes Risiko für die Grundrechte der betroffenen Personen verbleibt.

Erklärung Schutzbedarfsanalyse

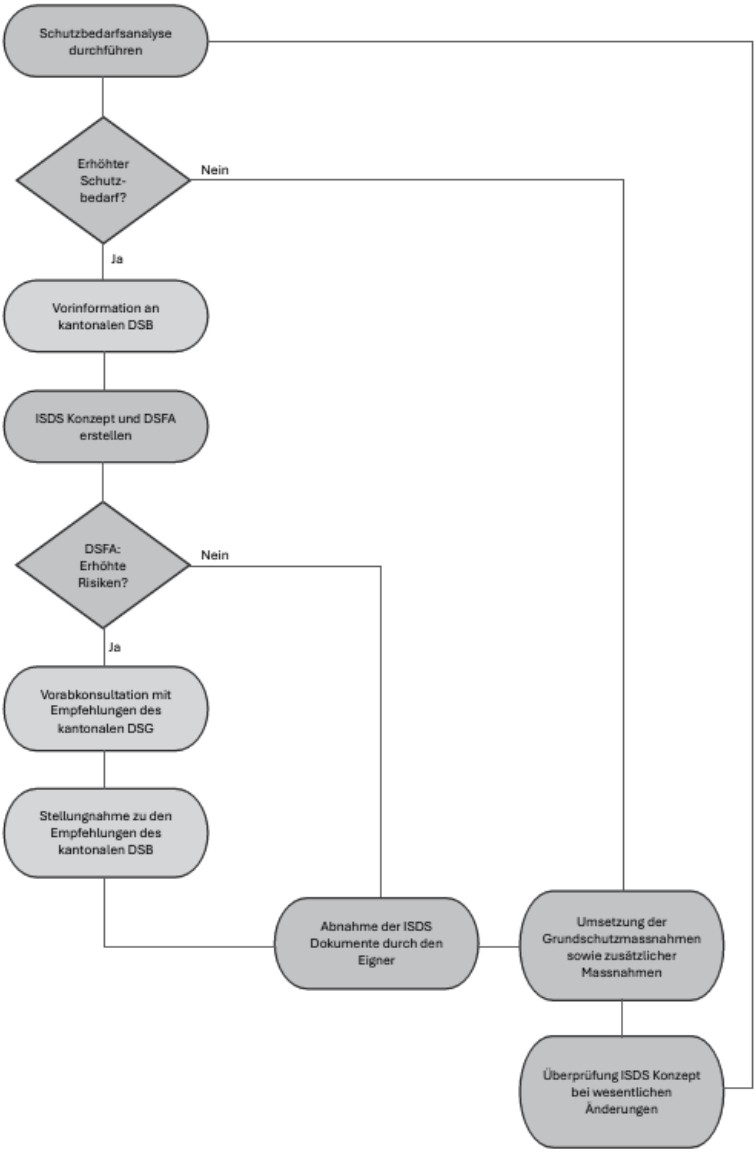
Mit einer Schutzbedarfsanalyse wird der Schutzbedarf einer Fachanwendung in Bezug auf die Datensicherheit und den Datenschutz bestimmt. Weitere Informationen siehe Ziffer 7 Links.

Erklärung ISDS-Konzept

In einem ISDS-Konzept werden Risiken in den Bereichen Datensicherheit und Datenschutz beurteilt und Massnahmen definiert. Weitere Informationen siehe Ziffer 7 Links.

Erklärung DSFA

Eine DSFA enthält eine Beschreibung der geplanten Bearbeitung, eine Bewertung der Risiken sowie die erforderlichen Schutzmassnahmen. Vgl. Formular DSFA siehe Ziffer 7 Links.


Schutzbedarfsanalyse durchführen
Erhöhter Schutz-bedarf?
Nein
Ja
Vorinformation an kantonalen DSB
ISDS Konzept und DSFA erstellen
DSFA: Erhöhte Risiken?
Nein
Ja
Vorabkonsultation mit Empfehlungen des kantonalen DSG
Stellungnahme zu den Empfehlungen des kantonalen DSB
Abnahme der ISDS Dokumente durch den Eigner
Umsetzung der Grundschutzmassnahmen sowie zusätzlicher Massnahmen
Überprüfung ISDS Konzept bei wesentlichen Änderungen

b) Risiken
Besondere Risiken umfassen in der Regel:

- Das Abrufverfahren
- Die Sammlung einer Vielzahl besonderer schützenswerter Personendaten
- Der Einsatz neuer Technologien
- Die gemeinsame Bearbeitung von Daten durch verschiedene öffentliche Organe
- Eine grosse Anzahl von betroffenen Personen

Weitere besondere Risiken sind:

- Automatisierte Einzelentscheidungen
- Systematische Überwachung
- Zusammenführen bzw. Kombinieren von Personendaten, die durch unterschiedliche Prozesse gewonnen werden
- Scoring oder Profiling

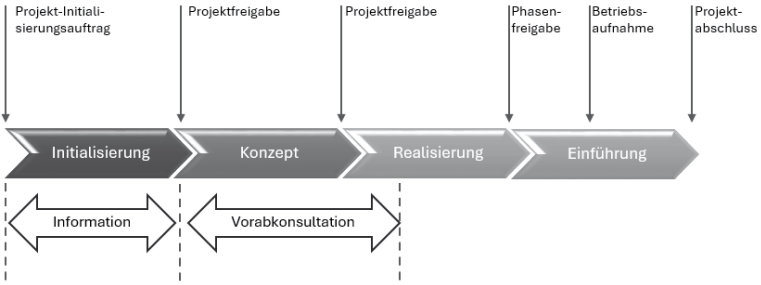
c) Zeitpunkt
Der Datenschutzbeauftragte ist frühzeitig über eine beabsichtigte Bearbeitung von Personendaten zu informieren oder in ein solches Vorhaben einzubeziehen. Die Vorabkonsultation findet in der Konzeptphase statt. Der Datenschutzbeauftragte sollte schon in der Initialisierungsphase über die bevorstehende Vorabkonsultation informiert werden.

3. Wann ist keine Vorabkonsultation erforderlich?

Wenn die geplante Bearbeitung zu keinem grossen Eingriff in die Grundrechte einer betroffenen Person führt oder das eingesetzte Programm mit Bezug auf Datenschutz und Informationssicherheit von einer staatlichen Stelle umfassend geprüft wurde, kann auf eine Vorabkonsultation verzichtet werden.

4. Was muss das öffentliche Organ tun?

Sind die Kriterien für eine Vorabkonsultation erfüllt, muss das öffentliche Organ die unter Ziffer 5 aufgelisteten Unterlagen dem Datenschutzbeauftragten zur Stellungnahme vorlegen. Auf der untenstehenden Zeitachse wird ersichtlich, in welchem Zeitabschnitt die Unterlagen vorgelegt werden müssen. Wichtig ist in jedem Fall eine frühzeitige Information der Fachstelle über das geplante Vorhaben.



5. Welche Unterlagen müssen eingereicht werden?

a) Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept)
b) Datenschutz-Folgenabschätzung mit einer detaillierten Beschreibung der Bearbeitung von Personendaten
c) Rechtsgrundlagenanalyse
d) Risikoanalyse und -bewertung
e) Massnahmenplan
f) Rollen- und Berechtigungskonzept
g) Verträge

6. Abschluss der Vorabkonsultation

Der Datenschutzbeauftragte prüft die rechtlichen, organisatorischen und technischen Rahmenbedingungen der beabsichtigten Datenbearbeitung. Die Aufsichtsstelle teilt dem öffentlichen Organ seine Einwände gegen die geplante Bearbeitung sowie seine Empfehlungen mit und schlägt geeignete Massnahmen vor. Das Resultat der Vorabkonsultation wird in einem schriftlichen Bericht festgehalten und dem öffentlichen Organ zugestellt. Das öffentliche Organ nimmt dazu Stellung. Es trägt die Verantwortung für die Restrisiken.

7. Links

- Erklärung Schutzbedarfsanalyse gemäss Hermes: Schutzbedarfsanalyse erarbeiten (admin.ch)
- Erklärung ISDS-Konzept gemäss Hermes: ISDS-Konzept erarbeiten (admin.ch)
- Vorlagen des Bundes
  - Beurteilung des Schutzbedarfs (admin.ch)
  - Erhöhter Schutz (admin.ch)

2. Merkblatt Meldepflicht bei Verletzungen der Datensicherheit

Was ist eine Verletzung der Datensicherheit?

Der Schutz von personenbezogenen Daten wird verletzt, wenn

- sie unwiederbringlich vernichtet werden oder verloren gehen,
- unbeabsichtigt oder unrechtmässig verändert oder offenbart werden oder
- Unbefugte Zugang zu solchen Personendaten erhalten.
  (im Folgenden: Datenschutzvorfall)

Wann besteht die Pflicht zur Meldung eines Datenschutzvorfalls?

Führt ein Datenschutzvorfall zu einem hohen Risiko für die Grundrechte der Betroffenen muss er gemeldet werden. Bestehen Zweifel, ob durch einen Vorfall in schwerer Weise Grundrechte gefährdet sind, ist ebenfalls Meldung zu erstatten.

Wie wird bestimmt, ob ein hohes Risiko für die Grundrechte der Betroffenen vorliegt?

Die Risikobeurteilung obliegt dem öffentlichen Organ. Es berücksichtigt sowohl die möglichen Auswirkungen eines Datenschutzvorfalls auf die Betroffenen als auch die Wahrscheinlichkeit, dass ein solcher Vorfall eintritt. Um die Schwere der möglichen Folgen bestimmen zu können, müssen der konkrete Datenschutzvorfall (z.B. unbefugte Bekanntgabe, Löschung, etc.) sowie weitere Kriterien (z.B. Art und Sensibilität der Personendaten, Umfang der betroffenen Daten, Anzahl Betroffener, Identifizierbarkeit der Betroffenen) bei der Beurteilung des Risikos berücksichtigt werden.

Bei der Beurteilung des Risikos muss stets der Einzelfall betrachtet und gewürdigt werden. Das Vorliegen gleicher Kriterien und der gleichen Folgen bedeutet nicht zwingend, dass das gleiche Risiko besteht.

Information

Müssen die vom Datenschutzvorfall betroffenen Personen informiert werden?

Die betroffenen Personen sind über den Datenschutzvorfall zu informieren, wenn es zu ihrem Schutz erforderlich ist oder die Aufsichtsstelle es verlangt. Dies ist insbesondere dann der Fall, wenn die betroffenen Personen Massnahmen zu ihrem Schutz ergreifen müssen. Solche Vorkehrungen können nicht nur unmittelbare Schutzmassnahmen wie das Zurücksetzen eines Passworts umfassen, sondern auch weitere Massnahmen, die der betroffenen Person helfen, den Vorfall zu bewältigen, wie beispielsweise die Inanspruchnahme von Hilfe, wenn ein Geheimnis offenbart wurde.

Die Information an die betroffenen Personen umfasst die Art der Verletzung, die möglichen Folgen des Vorfalls, die getroffenen oder geplanten Massnahmen sowie die Kontaktdaten des kantonalen Datenschutzbeauftragten.

Die Information an die betroffenen Personen kann eingeschränkt oder aufgeschoben werden oder es kann auf sie verzichtet werden, wenn

- dies aufgrund überwiegender Interessen Dritter erforderlich ist;
- dies insbesondere aufgrund überwiegender öffentlicher Interessen erforderlich ist;
- die Mitteilung der Information eine Ermittlung, eine Untersuchung oder ein behördliches oder gerichtliches Verfahren gefährden kann;
- eine gesetzliche Geheimhaltungspflicht dies verbietet;
- die Information unmöglich ist oder einen unverhältnismässigen Aufwand erfordert;
- die Information der betroffenen Person durch eine öffentliche Bekanntmachung in vergleichbarer Weise sichergestellt ist.

Meldung prüfen

Wer muss den Datenschutzvorfall melden?

Das für die Datenbearbeitung verantwortliche öffentliche Organ muss den Datenschutzvorfall melden.

Ist ein Auftragsdatenbearbeiter involviert, muss dieser das meldepflichtige öffentliche Organ unverzüglich über den Vorfall informieren. Die Meldung an den Datenschutzbeauftragten erfolgt auch in diesem Fall durch das verantwortliche öffentliche Organ.

Wem ist der Datenschutzvorfall zu melden?

Ein Datenschutzvorfall ist dem kantonalen Datenschutzbeauftragten zu melden (dsb@staka.gr.ch, Tel: 081 256 55 58).

Ist erkennbar, dass der Datenschutzvorfall Auswirkungen in mehreren Kantonen haben könnte, ist dies bei der Meldung zu vermerken.

In welcher Form muss ein Datenschutzvorfall gemeldet werden?

Die Form der Meldung ist nicht vorgeschrieben. Eine schriftliche Meldung mittels des bereitgestellten Meldeformulars wird jedoch empfohlen.

Innerhalb welcher Frist muss ein Datenschutzvorfall gemeldet werden?

Der Datenschutzvorfall ist so rasch als möglich nach Feststellung zu melden.

Die Meldung über einen Datenschutzvorfall darf nicht unbillig verzögert werden. Zum Zeitpunkt der Meldung müssen noch nicht alle Angaben vorliegen. Zusätzliche Informationen zum Vorfall können später nachgereicht werden.

Welche Ursachen bzw. Schwachstellen können zu einem Datenschutzvorfall führen?

Die Ursachen bzw. Schwachstellen, die zu einem Datenschutzvorfall führten, sind ausschlaggebend um wirksame Massnahmen bestimmen zu können. Daher sollte – abgesehen von Sofortmassnahmen – vor der Bestimmung von Massnahmen stets evaluiert werden, weshalb es zu einem konkreten Datenschutzvorfall kommen konnte. Oft weisen die Ursachen bzw. Schwachstellen auf die erforderlichen Massnahmen hin.

Wie können Massnahmen zur Bewältigung von Datenschutzvorfällen aussehen?

Der kantonale Datenschutzbeauftragte beurteilt den Datenschutzvorfall und empfiehlt je nach Fall und Auswirkungen des Vorfalls Massnahmen, die das öffentliche Organ umzusetzen hat. Diese Massnahmen sollen dazu dienen, die Folgen des Datenschutzvorfalls zu reduzieren und zu beseitigen, sowie zukünftig vergleichbare Vorfälle zu vermeiden.

Im Folgenden sind beispielhaft Massnahmen aufgelistet. Es obliegt jedoch dem öffentlichen Organ sowie dem kantonalen Datenschutzbeauftragten die passenden Massnahmen festzulegen und umzusetzen.

- Mitarbeitende des öffentlichen Organs sind in Schulungen zu sensibilisieren und auf ihre Pflicht hinzuweisen. Die zuständige interne Stelle ist zu festzulegen.
- Es ist zu prüfen, welche technischen Vorkehrungen getroffen werden können, um die Übermittlung von (besonders schützenswerten) Personendaten auf gesicherte Kanäle zu beschränken.
- Durchführung von regelmässigen Systemupdates (Aufspielen/Installation von neuer Korrekturauslieferung für Software "Patches") und Protokollierung (Logging) dieser Updates.
- Strenge Massnahme: Es ist zu prüfen, ob die Eintrittswahrscheinlichkeit im Geschäftsprozess durch ein Vier-Augen-Prinzip (Segregation of duty) signifikant gesenkt werden kann. Hierbei kann aber die Effizienz und Wirtschaftlichkeit als Gegenargument angeführt werden.

Müssen die Tatsachen der Verletzung aufbewahrt werden?

Das verantwortliche Organ dokumentiert die Verletzungen. Die Dokumentation hat die mit den Vorfällen zusammenhängenden Tatsachen, deren Auswirkungen und die ergriffenen Massnahmen zu enthalten. Die Dokumentation ist zwei Jahre aufzubewahren.

IV. Fälle aus der Praxis

1. Auskunftsrecht in einem Verfahren vor KESB

A. Sachverhalt

Im Rahmen eines Verfahrens vor der Kindes- und Erwachsenenschutzbehörde (KESB) wurde eine Aktennotiz zwischen der KESB und einem Schulleiter erstellt. Diese Aktennotiz wurde dem Schulleiter in indirekter Form zur Kenntnis gebracht. Der Schulleiter war der Ansicht, dass seine Aussagen nicht korrekt wiedergegeben worden seien. Aus diesem Grund stellte er bei der KESB den Antrag, ihm eine Kopie der Aussagen zur Verfügung zu stellen, um die seiner Meinung nach fehlerhaften Aussagen korrigieren zu können. Die KESB verweigerte jedoch die Herausgabe der Aktennotiz, da sie der Auffassung war, dass der Schulleiter nicht als Verfahrensbeteiligter anzusehen sei.

B. Begründung

a) Akteneinsichtsrecht im Erwachsenenschutzrecht
Das Akteneinsichtsrecht wird im Erwachsenenschutzrecht durch Art. 449b ZGB geregelt. Danach hat eine am Verfahren beteiligte Person Anspruch auf Akteneinsicht, soweit nicht überwiegende Interessen entgegenstehen. Zunächst ist zu klären, ob eine Person, welche der KESB Auskunft erteilt hat, unter den Begriff der "am Verfahren beteiligte Person" fällt. Am Verfahren beteiligt ist in erster Linie die von einer Anordnung der KESB direkt betroffene Person, also die schutzbefohlene, hilfsbedürftige Person. Ebenso gehören dazu alle Personen, die sich im erstinstanzlichen Verfahren vor der KESB tatsächlich beteiligt haben, oder denen mindestens ein Entscheid der KESB zugestellt wurde. (DANIEL STECK in: Peter Breitschmid/Alexandra Rumo-Jungo (Hrsg.), Handkommentar zum Schweizer Privatrecht, 2. Auflage, Art. 450, Note 17 f.). Darunter fallen ferner eine nahestehende Person sowie die Vertrauensperson und der Beistand oder die Beiständin (DANIEL STECK, a.a.O., Artikel 445, Note 4).

Gemäss bundesgerichtlicher Rechtsprechung müssen drei Voraussetzungen erfüllt sein, damit eine Person als nahestehend gilt:

1. Die Person muss glaubhaft machen können, dass sie unmittelbare Kenntnis der Persönlichkeit der betroffenen Person hat;
2. Die Beziehung muss von Verantwortung für das Wohl der betroffenen Person geprägt sein;
3. Die Beziehung muss von der betroffenen Person anerkannt werden.

Diese Kriterien beruhen auf den tatsächlichen Verhältnissen (LUCA MARANTA in: Geiser/Fountoulakis (Hrsg.), Basler Kommentar zum ZGB, 6. Auflage, Vorbemerkungen zu Art. 443 – 450g, Note 24 f.).

Daher lässt sich feststellen, dass eine Drittperson, die lediglich auf Anfrage Auskunft erteilt hat, sich nicht auf Art. 449b ZGB berufen kann.

b) Abgrenzung zum datenschutzrechtlichen Auskunftsrecht

Das verfahrensrechtliche Akteneinsichtsrecht ist vom datenschutzrechtlichen Auskunftsrecht zu unterscheiden. Beide Rechte sind selbständige Ansprüche, die hinsichtlich Umfang und Voraussetzungen nicht deckungsgleich sind (vgl. BGE 125 II 473; KURT PÄRLI/NATHALIE FLÜCK in: Baeriswyl/Pärli/Blonski (Hrsg.), Handkommentar zum DSG, 2. Auflage, Art. 25, Note 7). Das datenschutzrechtliche Auskunftsrecht kann angerufen werden, wenn eine Person beabsichtigt, weitere datenschutzrechtliche Ansprüche geltend zu machen, wie zum Beispiel eine Berichtigung (LUCA MARANTA, a.a.O., Art. 449b, Note 39). Dieses Recht geht insoweit über das verfahrensrechtliche Akteneinsichtsrecht hinaus, als es ohne jeglichen Interessennachweis auch ausserhalb eines Verwaltungsverfahrens geltend gemacht werden kann. Andererseits ist das Auskunftsrecht auf die eigenen Daten beschränkt. Gemäss Art. 25 DSG erstreckt sich das Auskunftsrecht auf alle über eine Person in einer

Bekanntgabe von Personendaten im Zusammenhang mit der Anfechtung von Volksabstimmungen

Rechtsgrundlage für die Veröffentlichung von Personendaten durch Behörden bildet Art. 36 DSG. Danach dürfen Behörden im Rahmen ihrer Informationsaufgaben Personendaten von Amtes wegen bekannt geben, sofern diese Daten im Zusammenhang mit der Erfüllung öffentlicher Aufgaben stehen und ein überwiegendes öffentliches Interesse an der Bekanntgabe besteht (Art. 36 Abs. 3 DSG). Ob eine solche Bekanntgabe zulässig ist, muss im konkreten Einzelfall durch eine Interessen- und Güterabwägung beurteilt werden. Die Prüfung orientiert sich insbesondere an der Art der betroffenen Daten, der Funktion bzw. öffentlichen Stellung der betroffenen Person, einem allfälligen besonderen Informationsinteresse der Öffentlichkeit, der gesellschaftlichen Bedeutung des Sachverhalts sowie den möglichen Konsequenzen einer Veröffentlichung (vgl. CLAUDIA MUND, in: Baeriswyl/Pärli/Blonski (Hrsg.), Stämpflis Handkommentar zum DSG, 2. Auflage, Art. 36 N. 29).

Im Zusammenhang mit gerichtlichen Verfahren zur Anfechtung von Volksabstimmungen besteht grundsätzlich ein öffentliches Interesse an der Bekanntgabe des Ausgangs des Verfahrens und der rechtlichen Würdigung durch das Gericht. Dieses Interesse dient der Transparenz demokratischer Prozesse und der Nachvollziehbarkeit von Behördenentscheiden. Demgegenüber ist das Interesse der Öffentlichkeit an der Identität der beschwerdeführenden Person als gering einzustufen. Die Möglichkeit, einen Entscheid der Gemeinde gerichtlich überprüfen zu lassen, ist ein verfassungsmässig garantiertes Recht, das allen Einwohnerinnen und Einwohnern offensteht. Die gerichtliche Beurteilung erfolgt dabei unabhängig von der Identität der beschwerdeführenden Person und konzentriert sich ausschliesslich auf die rechtlichen Fragen. Da das Urteil des Gerichts in der Sache nicht von der konkreten Person abhängig ist, welche die Beschwerde eingereicht hat, besteht aus datenschutzrechtlicher Sicht kein überwiegendes öffentliches Interesse an der Offenlegung ihrer Identität. In der vorliegenden Konstellation überwiegt das Interesse am Schutz der Privatsphäre gegenüber dem allgemeinen Informationsinteresse. Hinzuweisen ist jedoch auf den bestehenden Ermessensspielraum der Gemeindebehörde. Diese verfügt bei der Beurteilung, ob und in welchem Umfang eine Bekanntgabe zulässig ist, über einen gewissen Beurteilungsspielraum, wobei stets die verfassungsrechtlichen Vorgaben des Datenschutzes und der Transparenz zu beachten sind.

Datensammlung vorhandenen Daten, d.h. auf alle Angaben, die sich auf diese Person beziehen. Die Ausnahmen zum Auskunftsrecht sind in Art. 26 DSG abschliessend normiert.

Das datenschutzrechtliche Auskunftsrecht ist das zentrale Instrument, um die Rechtmässigkeit der Datenbearbeitung zu überprüfen und allenfalls eine Berichtigung oder Löschung der Daten zu verlangen. Das Auskunftsrecht konkretisiert das Grundrecht auf informationelle Selbstbestimmung (Art. 13 Abs. 2 BV). Es ist darüber hinaus Voraussetzung für die Verwirklichung des Schutzes der Privatsphäre nach Art. 8 EMRK. Der grosse Stellenwert des Auskunftsrechtes für die Verwirklichung des Grund- und Menschenrechtsschutzes ist bei der Auslegung von Art. 25 DSG zu berücksichtigen (KURT PÄRLI/NATHALIE FLÜCK, a.a.O., Art. 25, Note 5 f.).

Jede Person ist Trägerin des Auskunftsrechts bezüglich der über sie bearbeiteten Personendaten. Das Auskunftsrecht steht der betroffenen Person voraussetzungslos zu (RALPH GRAMIGNA in: Blechta/Vasella (Hrsg.), Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz, 4. Auflage, Art. 25, Note 6). Die Ansprüche der betroffenen Person gegenüber einer Behörde richten sich nach Art. 41 DSG. Diese kann insbesondere die Berichtigung, Löschung oder Vernichtung verlangen. Diese Ansprüche können jedoch nur geltend gemacht werden, wenn Kenntnis von den bearbeiteten Personendaten erlangt wird.

C. Zusammenfassung

Zusammenfassend kann festgestellt werden, dass zwischen dem verfahrensrechtlichen Akteneinsichtsrecht und dem datenschutzrechtlichen Auskunftsrecht unterschieden werden muss. Diese beiden Rechtsinstitute bestehen nebeneinander und folgen unterschiedlichen Ansprüchen und Rechtsfolgen. Eine Drittperson kann sich in einem Verfahren der KESB nicht auf Art. 449b ZGB berufen. Ihr steht aber das datenschutzrechtliche Auskunftsrecht offen.

Auskunftsrecht im Zusammenhang mit einem Notruf

Ein Auskunftsbegehren wurde an das Gesundheitsamt gerichtet, betreffend den Inhalt eines Notrufs, den ein Betroffener an die Nummer 144 weitergeleitet hat. Die Auskunft wurde gemäss Art. 34 Abs. 3 der Verordnung zum kantonalen Krankenpflegegesetz (VOzKPG) verweigert, da diese Vorschrift nur eine eingeschränkte Zugriffsberechtigung vorsieht. Art. 34 VOzKPG regelt die Abwicklung im Bereich des Rettungswesens und stellt klar, dass der Zugang zu diesen Informationen intern beschränkt ist.

Die im Gesetz genannte Einschränkung bezieht sich jedoch nur auf den internen Ablauf innerhalb der betroffenen Institutionen und dient dem Schutz der internen Prozesse und der Vertraulichkeit von Daten. Sie betrifft nicht das Auskunftsrecht des Betroffenen auf seine eigenen Daten. Das Zugriffsrecht gemäss Art. 34 VOzKPG ist daher auf die behördliche Bearbeitung und interne Nutzung beschränkt. Es stellt sicher, dass nur befugte Personen oder Stellen auf die relevanten Daten zugreifen können, um die Integrität und Vertraulichkeit dieser Informationen zu gewährleisten.

Im vorliegenden Fall möchte jedoch der Betroffene Einsicht in die eigenen Daten nehmen. Das Auskunftsbegehren richtet sich daher nach dem DSG. Gemäss Art. 25 DSG hat jede Person das Recht, von der zuständigen Behörde Auskunft darüber zu verlangen, ob und in welchem Umfang Personendaten über sie bearbeitet werden. Grundsätzlich ist einem Auskunftsbegehren stattzugeben, es sei denn, es liegen spezifische Gründe für eine Einschränkung vor, wie sie in Art. 26 DSG geregelt sind.

Das Auskunftsrecht stellt eine zentrale Säule des Datenschutzes dar. Es ermöglicht es dem Betroffenen, die Rechtmässigkeit der Datenbearbeitung zu überprüfen und gegebenenfalls eine Berichtigung oder Löschung der Daten zu verlangen. Dieses Recht ist eine wesentliche Ausprägung des Grundrechts auf informationelle Selbstbestimmung und bildet die Grundlage für den Schutz der Privatsphäre. Der hohe Stellenwert des Auskunftsrechts für den Schutz grundlegender Menschenrechte muss bei der Auslegung von Art. 25 DSG berücksichtigt werden (vgl. KURT PÄRLI/NATHALIE FLÜCK, in: Baeriswyl/Pärli/Blonski, Handkommentar zum Datenschutzgesetz, 2. Auflage, Art. 25, Note 6).

Da Art. 34 VOzKPG keine explizite gesetzliche Grundlage für eine Einschränkung des Auskunftsrechts bietet, muss das Auskunftsbegehren grundsätzlich positiv beschieden werden, es sei denn, es lägen spezifische Ausschlussgründe gemäss Art. 26 DSG vor.

2. Einführung einer Videoüberwachung

Die Einführung einer Videoüberwachung durch ein öffentliches Organ – etwa eine Behörde oder eine öffentlich-rechtliche Institution – kann aus verschiedenen Gründen erfolgen. Wichtig ist dabei stets, dass sie auf einer gesetzlichen Grundlage basiert, verhältnismässig ist und dem Schutz öffentlicher Interessen dient. Sie kann dem Schutz von Personen und Sachen dienen, zur Wahrung der öffentlichen Ordnung und Sicherheit erforderlich sein oder kritische Infrastruktur sichern. Für die Einführung einer Videoüberwachung soll die nachfolgende Checkliste dienen:

Checkliste für die Einführung einer Videoüberwachung

1. Ausgangslage und Schutzbedürfnis
2. Rechtliche Grundlage
   - 2.1 Zuständigkeit
   - 2.2 Rechtsgrundlage
   - 2.3 Zulässigkeit des Eingriffs (Verhältnismässigkeit)
3. Zweck
4. Betriebsbedingungen/technische Massnahmen
   - 4.1 Allgemeines
   - 4.2 Umfang, Art der Videoüberwachung und Örtlichkeiten
     - Aufnahmepunkte
     - Kamerawinkel
     - Aufnahmebereich
     - Aufzeichnungsdauer
   - 4.3 Hinweistafel
   - 4.4 Verantwortung
   - 4.5 Einsichtnahme/Wartung und Kontrolle
   - 4.6 Zugriffsberechtigung und Protokollierung
   - 4.7 Weiterverwendung
   - 4.8 Sicherheitsmassnahmen
   - 4.9 Aufbewahrung und Datenlöschung
5. Dauer des Projekts
6. Rechte der betroffenen Personen
7. Änderung des Reglements
8. Verfahren
   - Allgemeinverfügung
   - Rechtsmittelbelehrung
   - Mitteilung
9. Anhänge
   - Pläne
   - Abbildungen

3. Erstellung eines audiovisuellen Archivs der Debatten des Grossen Rates Graubünden

A. Ausgangslage

Die Präsidentenkonferenz des Grossen Rats (PK) beantragt dem Grossen Rat mittels Direktbeschluss ein audiovisuelles Archiv der Grossratsdebatten einzuführen. Bevorzugt wird eine Variante, die eine ganztägige Aufzeichnung ermöglicht, wobei die Benutzer über Abspiel- und Spultasten die Debatten navigieren können. Das Videoarchiv soll online zugänglich sein. Mittels Klick kann direkt zum Startpunkt der Beratung des jeweiligen Geschäfts eingesprungen werden. Es wird davon ausgegangen, dass Dritte die Möglichkeit besitzen, Kopien der Videoaufzeichnungen zu speichern.

Die Videoaufnahmen dokumentieren die Debatten im Grossen Rat. Es werden somit Personendaten bearbeitet. Das kantonale Datenschutzgesetz kommt zur Anwendung.

B. Gesetzliche Grundlage

Gemäss Art. 1 Abs. 2 DSG müssen Personendaten rechtmässig bearbeitet werden. Die Verletzung der Bearbeitungsgrundsätze (Art. 6 DSG) führt zur Verletzung der Persönlichkeit der betroffenen Person (Art. 30 Abs. 2 lit. a DSG). Bei Behörden stimmt der Grundsatz der Rechtmässigkeit mit dem Legalitätsprinzip überein (LUKAS BÜHLMANN/MICHAEL REINLE, in: Blechta/Vasella (Hrsg.), Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz, 4. Auflage, Art. 6, N. 34).

Das Legalitätsprinzip im schweizerischen Recht umfasst zwei zentrale Anforderungen: Erstens die «hinreichende Dichte einer Bestimmung» und zweitens die «Verwendung der richtigen Normstufe». Das «Erfordernis des Rechtssatzes» besagt, dass eine Norm so präzise formuliert sein muss, dass der Bürger sein Verhalten entsprechend anpassen und die Folgen seines Verhaltens mit einem hinreichenden Grad an Gewissheit vorhersagen kann (vgl. BGE 109 Ia 273). Gesetze müssen für Bürgerinnen und Bürger vorhersehbar sein, und eine hinreichende Bestimmtheit ist auch ein Gebot der Rechtssicherheit. Das Erfordernis des Rechtssatzes kommt auf alle Normen zur Anwendung und erfüllt wesentliche rechtsstaatliche Anliegen. (FELIX UHLMANN/FLORIAN FLEISCHMANN, Das Legalitätsprinzip – Überlegungen aus dem Blickwinkel der Wissenschaft S. 8, in: Das Legalitätsprinzip in Verwaltungsrecht und Rechtsetzungslehre).

Art. 5, 36 und 164 BV sind die wichtigsten Bestimmungen, welche das Legalitätsprinzip aufnehmen, wobei sich für das Erfordernis des Rechtssatzes auf Verfassungsstufe keine präzisierenden Bestimmungen finden. Das Bundesgericht hat sich mit Bezug darauf folgendermassen geäussert (BGE 131 II 13 ff.): "Der Grad der erforderlichen Bestimmtheit lässt sich nicht abstrakt festlegen. Der Bestimmtheitsgrad hängt unter anderem von der Vielfalt der zu ordnenden Sachverhalte, von der Komplexität und der Vorhersehbarkeit der im Einzelfall erforderlichen Entscheidung, von den Normadressaten, von der Schwere des Eingriffs in Verfassungsrechte und von der erst bei der Konkretisierung im Einzelfall möglichen und sachgerechten Entscheidung ab […]. Für den Bestimmtheitsgrad sind auch die Flexibilitätsbedürfnisse zu beachten." Folgerichtig muss eine einzelne Gesetzesbestimmung hinreichend bestimmt sein, damit sich staatliches Handeln im Anwendungsfall auf diese Grundlage stützen kann. Ist die gesetzliche Grundlage zu offen, zu unbestimmt, verstösst sie gegen das Legalitätsprinzip. Das Legalitätsprinzip stellt mit anderen Worten nicht nur Anforderungen an das staatliche Handeln im Einzelfall, sondern auch an das Gesetz selbst. Massstab der Prüfung ist das Erfordernis des Rechtssatzes (FELIX UHLMANN/FLORIAN FLEISCHMANN, a.a.O.; S. 14). Das Legalitätsprinzip bedeutet somit, dass jede staatliche Massnahme eine gesetzliche Grundlage, eine ausreichende Bestimmtheit und eine demokratische Legitimation haben muss.

Vorliegend stützt sich die PK in ihrem Bericht auf Art. 29 der Kantonsverfassung (KV), Art. 44 des Gesetzes über den Grossen Rat (GRG) und Art. 47 der Geschäftsordnung des Grossen Rates (GGO). Art. 29 KV besagt, dass "die Sitzungen des Grossen Rates in der Regel öffentlich" sind. In Art. 44 GRG wird festgehalten, dass der Grosse Rat ausnahmsweise beschliessen kann, die Verhandlung unter Ausschluss der Öffentlichkeit zu führen, und in Art. 47 GGO werden Verhaltensweisen des Publikums und der Medien konkretisiert. Diese Bestimmungen bilden jedoch keine Grundlage für die Einführung eines audiovisuellen Archivs. Allein aufgrund der Tatsache, dass die Sitzungen des Grossen Rates öffentlich sind, reicht nicht aus, um auf dieser Basis ein digitales, audiovisuelles Archiv zu schaffen. In Anbetracht der Tatsache, dass mit Bezug auf die Protokollierung in Art. 36 GGO eine präzisierende gesetzliche Grundlage auf Stufe Verordnung geschaffen wurde, hätte erwartet werden können, dass für die Einführung eines audiovisuellen Archivs zumindest auf Verordnungsebene gleich vorgegangen worden wäre.

Ein audiovisuelles Archiv, das die Sitzungen des Grossen Rates integral abbildet, stellt einen erheblichen Eingriff in die Persönlichkeit eines Ratsmitglieds dar. Wie dem entsprechenden Antrag zu Recht entnommen werden kann, sind Liveaufzeichnungen der Debatten um einiges lebendiger als schriftliche Protokolle. Damit einher geht ein qualitativ grösserer Eingriff in die Persönlichkeit. Grammatikalische Fehler, welche in den Protokollen korrigiert werden, treten in Videoaufzeichnungen unmittelbar zu Tage, Emotionen in der Debatte werden manifest und mögliche Zwischenrufe oder Störungen bleiben ersichtlich. Bilder können auf die Meinungsbildung grossen Einfluss ausüben. Dennoch soll auf eine gesetzliche Regelung verzichtet werden, währenddem für das Wortlautprotokoll eine Bestimmung geschaffen wurde.

Abschliessend ist auf Art. 50 GRG (Antrag auf Direktbeschluss) hinzuweisen. Mit einem Antrag auf Direktbeschluss kann verlangt werden, dass der Grosse Rat im Bereich seiner eigenen Zuständigkeit einen Beschluss fasst. Die Debatten im Grossen Rat umfassen jedoch nicht nur die eigene Zuständigkeit. Es werden beispielsweise Wahlgeschäfte (Richterwahlen) abgewickelt, Debatten über Personen geführt (z.B. Fall Quadroni) und die Sitzungen sind öffentlich. Art. 50 GRG genügt nicht als gesetzliche Grundlage.

Die Entscheidung, ein audiovisuelles Archiv zu schaffen, liegt beim Grossen Rat. Ihm sind die damit verbundenen Gefahren und das Missbrauchspotential bekannt. Der Grosse Rat kann das Interesse der Öffentlichkeit auf eine umfassende, audiovisuell unterstützte Information höher gewichten als die persönlichen Interessen der einzelnen Mitglieder. Indessen bedarf die Einführung eines audiovisuellen Archivs einer klaren gesetzlichen Grundlage.

Aushändigung einer Liste der Bürger

Ein Einwohner hat angefragt, ob die Bürgergemeinde verpflichtet ist, eine Liste der Bürger der Gemeinde herauszugeben. Diese Anfrage wurde aus Datenschutzgründen abgelehnt. Zur Beantwortung der Frage ist auf das Gesetz über die Einwohnerregister sowie weitere Personen- und Objekteregister (ERG) hinzuweisen. Die Bestimmungen dieses Gesetzes können zur Klärung des Sachverhalts herangezogen werden.

Gemäss Art. 32 Abs. 1 ERG ist die Gemeinde verpflichtet, Auskunft über den Namen, das Geburtsjahr und die Adresse von Personen zu erteilen, die im Einwohnerregister geführt werden. Diese Daten dürfen jedoch nur dann listenmässig veröffentlicht werden, wenn sie ausschliesslich für ideelle Zwecke genutzt und nicht an Dritte weitergegeben werden. Es ist daher grundsätzlich möglich, eine Vielzahl von Daten in Listenform zu übermitteln.

Im vorliegenden Fall stellt sich die Frage, ob das Anliegen des Einwohners, die Bürger kennenzulernen, als "ideeller Zweck" im Sinne des Gesetzes qualifiziert werden kann. Persönliche Motive wie etwa das Kennenlernen von Mitbürgern lassen keinen klaren ideellen Zweck erkennen.

Es ist zudem zu beachten, dass den Behörden bei der Feststellung eines «ideellen Zwecks» ein erheblicher Ermessensspielraum zukommt. In Anbetracht dieser Ermessensfreiheit und aus datenschutzrechtlicher Sicht erscheint es daher nachvollziehbar, dass die Aushändigung der Liste aller Bürger verweigert wurde.

4. Auskunftsbegehren bei einem Verein

A. Ausgangslage

Ein Mitarbeitender eines Vereins, der öffentliche Aufgaben erfüllt, verlangt im Zusammenhang mit einer arbeitsrechtlichen Auseinandersetzung Einsicht in die Vorstandsprotokolle sowie weitere ihn betreffende Unterlagen. Er beruft sich dabei auf das Öffentlichkeits- und Datenschutzgesetz.

B. Anwendung des Öffentlichkeitsgesetz (BR 171.000; KGÖ)

Zunächst ist zu klären, ob der betroffene Verein dem Geltungsbereich des KGÖ unterstellt ist. Der Verein ist privatrechtlich organisiert, erfüllt jedoch auf Grundlage einer Leistungsvereinbarung mit dem Kanton Graubünden mutmasslich kantonale öffentliche Aufgaben. Ob tatsächlich eine Unterstellung vorliegt, bedarf einer vertieften Prüfung Diese Frage kann aus nachfolgender Begründung offenbleiben.

Gemäss Art. 2 Abs. 2 lit. c KGÖ gilt das KGÖ für juristische Personen des Privatrechts, soweit sie ihnen übertragene kantonale öffentliche Aufgaben erfüllen. Das KGÖ ist somit grundsätzlich anwendbar. Zu beachten ist der sachliche Geltungsbereich gemäss Art. 4 KGÖ. Art. 4 Abs. 1 lit. a KGÖ schliesst insbesondere Verfahren zivilrechtlicher Natur aus, sofern ein entsprechendes Sonderverfahren zur Anwendung gelangt. Da im vorliegenden Fall (noch) kein Zivilverfahren hängig ist, steht dem öffentlichkeitsrechtlichen Zugang grundsätzlich nichts entgegen. Art. 4 Abs. 2 KGÖ bestimmt allerdings, dass der Zugang zu amtlichen Dokumenten, welche Personendaten des Gesuchstellers enthalten, durch das Datenschutzgesetz geregelt wird. Da der Mitarbei-

Grenzgängerabkommen und Datenschutz

Im Zusammenhang mit dem neuen Grenzgängerabkommen zwischen der Schweiz und der Republik Italien, das am 23. Dezember 2020 unterzeichnet wurde und am 17. Juli 2023 in Kraft trat, stellt sich die Frage, ob das Datenschutzgesetz des Kantons Graubünden den im Abkommen vorgesehenen automatischen Informationsaustausch zwischen Italien und dem Kanton Graubünden zulässt.

Das Grenzgängerabkommen sieht ab dem Jahr 2024 einen automatischen Informationsaustausch zwischen dem Kanton Graubünden (sowie den Kantonen Wallis und Tessin) und Italien vor, der sich auf Arbeitnehmer bezieht, deren in der Schweiz erzielte Einkünfte aus unselbstständiger Erwerbstätigkeit auch in Italien besteuert werden.

Gemäß Art. 34 Abs. 1 DSG dürfen Bundesorgane und damit auch kantonale Organe Personendaten nur dann bearbeiten, wenn eine gesetzliche Grundlage vorliegt. Als «Gesetz im formellen Sinn» gelten diejenigen Erlassbestimmungen, die im Rahmen des ordentlichen Gesetzgebungsverfahrens vom Parlament verabschiedet werden (vgl. Andreas Stöckli/Christoph Grüninger, in: Blechta/Vasella (Hrsg.), Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz, Art. 34, Note 7). Zu den möglichen Rechtsgrundlagen für die Bearbeitung von Personendaten zählen auch völkerrechtliche Verträge (vgl. Claudia Mund, in: Baeriswyl/Pärli/Blonski (Hrsg.), Handkommentar zum DSG, 2. Auflage, Art. 34, Note 6).

Im vorliegenden Fall wurde der Staatsvertrag zwischen der Schweiz und Italien am 18. März 2022 von der Bundesversammlung genehmigt. Dieser Vertrag hat Gesetzescharakter. Art. 7 des Abkommens listet die zu übermittelnden Daten auf, und der Vertrag bietet eine ausreichende gesetzliche Grundlage für den Informationsaustausch.

Aus datenschutzrechtlicher Sicht ist für den Kanton Graubünden daher kein weiterer Handlungsbedarf gegeben, da der Staatsvertrag eine hinreichende Grundlage für den automatischen Informationsaustausch darstellt.

tende Informationen zu seiner eigenen Person verlangt, kommt nicht das KGÖ, sondern das kantonale Datenschutzgesetz zur Anwendung.

Hinzuweisen ist noch auf Art. 9 Abs. 1 KGÖ. Danach sind amtliche Dokumente der Öffentlichkeit und dem Recht auf Zugang zeitweilig entzogen, wenn die Dokumente Grundlage für einen politischen oder administrativen Entscheid bilden. Der Aufschub des Zugangs zu grundsätzlich "zugangspflichtigen" Dokumenten ist ohne weitere Interessenabwägung zulässig, sofern diese eine Entscheidungsgrundlage bildet (vgl. Botschaft zum KGÖ, Seite 32). Die Äusserungen im Vorstand sind sicherlich für die Entscheidfindung im vorliegenden Verfahren von Belang und können Einfluss auf die Begründung der arbeitsrechtlichen Massnahme und die Haltung des Vorstandes haben. Auch gestützt auf Art. 9 Abs. 1 KGÖ können die Vorstandsprotokolle dem Antragsteller vorenthalten werden.

C. Datenschutzgesetz

Ausgehend davon, dass der Verein öffentliche Aufgaben wahrnimmt, ist gestützt auf Art. 1 Abs. 2 lit. c KDSG das kantonale Datenschutzgesetz anwendbar. Das KDSG verweist in Art. 2 Abs. 2 KDSG auf die sinngemässe Anwendung der Vorschriften des DSG für das Bearbeiten von Personendaten.

Der Gesuchsteller verlangt Einsicht in Protokolle, in denen sein Arbeitsverhältnis thematisiert wurde. Gemäss Art. 25 DSG hat jede Person Anspruch darauf, vom Verantwortlichen Auskunft darüber zu verlangen, ob Personendaten über sie bearbeitet werden. Die Einschränkungen des Auskunftsrechtes finden sich in Art. 26 DSG. Das Auskunftsrecht konkretisiert das Grundrecht auf informationelle Selbstbestimmung. Dieser grosse Stellenwert ist bei der Auslegung von Art. 25 DSG zu berücksichtigen.

Wird das Auskunftsrecht im Vorfeld eines Prozesses zweckwidrig zur Beweismittelbeschaffung geltend gemacht, kann die Auskunft nach Art. 26 Abs. 1 lit. c DSG eingeschränkt werden. Das Auskunftsrecht dient der Durchsetzung des Persönlichkeitsschutzes und nicht der Abklärung von Prozesschancen. Dies bringt gemäss Bundesgericht bereits die Formulierung von Art. 25 Abs. 2 DSG zum Ausdruck, wonach die betroffene Person diejenigen Informationen erhält, die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist. Das Bundesgericht hat in seiner bisherigen Praxis aber hohe Anforderungen an die rechtsmissbräuchliche Anrufung des Auskunftsrechts gestellt (vgl. KURT PÄRLI/NATHALIE FLÜCK,

in: Baeriswyl/Pärli/Blonski (Hrsg.), Stämpflis Handkommentar zum DSG, 2. Auflage, Art. 25, Note 8). Wenn der Arbeitnehmer ein Auskunftsbegehren zum Beispiel im gleichen Schreiben mit der Einsprache wegen missbräuchlicher Kündigung stellt, kann der Verdacht auf ein zweckwidriges Auskunftsbegehren aufkommen.

Die Einschränkungen des Auskunftsrechtes werden im Art. 26 DSG angeführt. Vorliegend interessiert insbesondere Art. 26 Abs. 1 lit. b DSG. Diese Bestimmung trägt dem Umstand Rechnung, dass Akten nicht immer nur die Personendaten einer einzelnen Person enthalten bzw. dass viele Informationen über eine bestimmte Person auch Auskunft über eine andere Person geben können, z.B. Aussagen, die Dritte über eine Person machen, geben immer auch Auskunft über das Verhältnis, in welchen der Informant und die fragliche Person zueinander stehen. Werden Drittdaten in diesem Sinne Gegenstand des Auskunftsrechts, so ist eine Interessenabwägung im Einzelfall vorzunehmen. Die Auskunft darf nicht automatisch verweigert werden. Vielmehr müssen die Drittinteressen an der Nicht-Nennung überwiegen (vgl. SANDRA HUSI-STÄMPFLI, a.a.O., Art. 26, Note16). Eine Einschränkung oder Verweigerung der Auskunft muss darüber hinaus mitgeteilt werden. Selbstverständlich können bei einem einzelnen Dokument Teilbereiche geschwärzt werden, oder es wird ein Auszug erstellt, sofern Angaben erfolgen, die keinen Zusammenhang mit der Auskunftserteilung haben.

Die Entscheidfindung im Einzelfall ist anspruchsvoll und nicht immer einfach, zumal eine Interessenabwägung vorgenommen und die sich entgegenstehenden Interessen gegeneinander abgewogen werden müssen. Vorliegend sind somit die Aussagen der einzelnen Vorstandsmitglieder innerhalb eines Gremiums mit den Anliegen des Betroffenen auf Auskunft gegeneinander abzuwägen. Ein Gremium wie ein Vereinsvorstand ist auf Vertraulichkeit angewiesen, um effektiv arbeiten zu können. Die Mitglieder müssen sich darauf verlassen können, dass ihre Äusserungen innerhalb des Gremiums nicht ohne Weiteres offengelegt werden. Die Offenlegung könnte zu einer Einschränkung der Diskussionskultur und zur Beeinträchtigung der Funktionsfähigkeit des Organs führen. Ein Vorstandsmitglied muss darin geschützt werden, dass seine Äusserungen innerhalb des Gremiums diskret behandelt werden. Dennoch überwiegt das Auskunftsinteresse der betroffenen Person, sofern der Schutz Dritter gewahrt bleibt – z. B. durch Anonymisierung.

D. Schlussfolgerung

Dem Mitarbeitenden steht grundsätzlich ein datenschutzrechtlicher Anspruch auf Auskunft über die ihn betreffenden Personendaten zu. Die Einsicht in Vorstandsprotokolle kann jedoch nur unter Wahrung des Schutzes Dritter erfolgen. Eine vollständige Offenlegung ist nicht angezeigt; vielmehr ist die Auskunft in geeigneter Form zu erteilen, etwa durch:

- Schwärzung sensibler Inhalte (z. B. Namen der Votanten),
- Herausgabe eines selektiven Auszugs,
- oder durch eine zusammenfassende Darstellung der ihn betreffenden Aussagen.

Das Begehren ist unter Berücksichtigung der datenschutzrechtlichen Schranken zu prüfen. Eine ausgewogene Interessenabwägung zwischen dem Schutz der Persönlichkeit des Gesuchstellers und dem Schutz der Vertraulichkeit innerhalb des Gremiums ist zentral.

V. Statistik

Was

Wer

Kantonale Dienste	Kurzanfragen	Berichte	Empfehlungen	Kontrollen	Vernehmlassungen	Referate	Kurse	Weiterbildung/Verbände
Allgemeine Verwaltung							1	
DVS	2							
DJSG	11		1		4	1		
EKUD	3		1					
DFG	4		2			1		
DIEM	2		1					
öff. rechtliche Anstalten	10		5					
Gerichte								
Regionen								
Gemeindeverbände								
Gemeinden	29					0		
Bürgergemeinden								
Juristische Personen	2	1						
Private Personen	58	1						
Andere	1					7		2
Total	122	2	10	0	4	9	1	2

VI. Abkürzungsverzeichnis

a.a.O.	am angeführten Ort
Abs.	Absatz
AFI	Kantonales Amt für Informatik
a.M.	anderer Meinung
Art.	Artikel
B	Botschaft
BBl	Bundesblatt
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
DSFA	Datenschutz-Folgenabschätzung
DVS	Departement für Volkswirtschaft und Soziales
EDOEB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EKUD	Erziehungs-, Kultur- und Umweltschutzdepartement
EMRK	Europäische Menschenrechtskonvention
ERG	Gesetz über die Einwohnerregister und weitere Personen- und Objektregister
etc.	et cetera
f./ff.	folgend/folgende
GGO	Geschäftsordnung des Grossen Rats
GRG	Gesetz über den Grossen Rat
GR	Graubünden
Hrsg.	Herausgeber
ISDS	Informationssicherheit und Datenschutz
KDSG	Kantonales Datenschutzgesetz
KESB	Kindes- und Erwachsenenschutzbehörde
KGÖ	kantonales Öffentlichkeitsgesetz
KV	Kantonsverfassung
lit.	litera
N	Note
PK	Präsidentenkonferenz
RB	Rechtsbuch
Rz	Randziffer
S	Seite
SR	Sammlung der eidgenössischen Gesetze und systematische Sammlung des Bundesrechts (Systematische Rechtssammlung)
TB	Tätigkeitsbericht
usw.	und so weiter
VOzKPG	Verordnung zum kantonalen Krankenpflegegesetz
vgl.	vergleiche
z.B.	zum Beispiel
ZGB	Schweizerisches Zivilgesetzbuch
Ziff.	Ziffer