Botschaft der Regierung an den Grossen Rat

Heft Nr. 9 / 2024 – 2025

Inhalt

Seite

9. Totalrevision des Kantonalen Datenschutzgesetzes 495

9. Totalrevision des Kantonalen Datenschutzgesetzes

Das Wichtigste in Kürze 495
Il pli impurtant en furma concisa 496
L'essenziale in breve 496

I. Ausgangslage 497
1. Entwicklungen im Völker- und Bundesrecht 497
2. Revisionsbedarf 499

II. Vernehmlassungsverfahren 501
1. Allgemeine Beurteilung der Vorlage 501
2. Umgang mit den Anliegen 502
2.1 Berücksichtigte Anliegen 502
2.2 Nicht berücksichtigte Anliegen 510

III. Erläuterungen zu den einzelnen Bestimmungen 517
1. Kantonales Datenschutzgesetz 517
2. Fremdänderungen 543
2.1 Bürgerrechtsgesetz des Kantons Graubünden (KBüG; BR 130.100) 543
2.2 Gesetz über die Einwohnerregister und weitere Personen- und Objektregister (ERG; BR 171.200) 543
2.3 Einführungsgesetz zur Schweizerischen Zivilprozessordnung (EGzZPO; BR 320.100) 544
2.4 Einführungsgesetz zur Schweizerischen Strafprozessordnung (EGzStPO; BR 350.100) 545
2.5 Gesetz über die Finanzaufsicht (GFA; BR 710.300) 545

IV. Ausführungen zu den regierungsrätlichen Ausführungsverordnungen 545
1. Verordnung zum Kantonalen Datenschutzgesetz (VKDSG; BR 171.110) 546
2. Verordnung über die Bildüberwachung des öffentlichen und öffentlich zugänglichen Raums (VBÜ; BR 171.120) 549

V. Personelle und finanzielle Auswirkungen 550
1. Für den Kanton 550
2. Für die Regionen und Gemeinden 553

VI. Gute Gesetzgebung 554

VII. Inkrafttreten 554

VIII. Anträge 555

Abkürzungsverzeichnis / Abreviaziuns / Elenco delle abbreviazioni 556

Heft Nr. 9 / 2024 – 2025

Botschaft der Regierung an den Grossen Rat

9.

Totalrevision des Kantonalen Datenschutzgesetzes

Chur, den 24. Oktober 2024

Das Wichtigste in Kürze

Das Kantonale Datenschutzgesetz (KDSG; BR 171.100) wurde auf den 1. Mai 2002 in Kraft gesetzt. In den über 20 Jahren seither wurde es nur punktuell angepasst. In derselben Zeitspanne wurden jedoch grosse technologische Fortschritte erzielt. Zudem gewinnt die grenzüberschreitende Datenbearbeitung und -bekanntgabe an Bedeutung. Aus diesen Gründen wurden in den letzten Jahren auf europäischer Ebene diverse Datenschutzerlasse erlassen bzw. revidiert. Diese Erlasse sind auch für Bund und Kantone verbindlich und müssen im kantonalen Recht umgesetzt werden, damit die kantonalen Datenschutzbestimmungen auch künftig dem europäischen Standard genügen. Insbesondere für die Polizeiarbeit wird dadurch der Zugriff auf das Schengener Informationssystem (SIS) weiterhin sichergestellt. Das KDSG muss daher umfassend revidiert werden. Die Revision beschränkt sich dabei auf diejenigen Punkte, welche zur Umsetzung der völkerrechtlichen Vorgaben zwingend notwendig sind. Die dem Gesetz unterstellten öffentlichen Organe müssen einige neue Instrumente und Verpflichtungen befolgen, welche in erster Linie der Stärkung der Rechte der betroffenen Personen dienen, über welche Daten bearbeitet werden. Im Weiteren fordert das übergeordnete Recht eine Stärkung der Datenschutzaufsicht, welche im Kanton Graubünden durch die Datenschutzbeauftragte oder den Datenschutzbeauftragten wahrgenommen wird. Einerseits wird die Unabhängigkeit dieser Stelle gestärkt. Anderseits erhält sie mit der Gesetzesrevision neue Aufgaben und Befugnisse.

Il pli impurtant en furma concisa

La Lescha chantunala davart la protecziun da datas (LCPD; DG 171.100) è vegnida messa en vigur il 1. da matg 2002. En quests passa 20 onns è ella vegnida adattada mo en singuls puncts. En la medema perioda hai dentant dà gronds progress tecnologics. Ultra da quai daventa l'elavuraziun e la communicaziun transcunfinala da datas adina pli impurtanta. Per quests motivs èn vegnids decretads resp. revedids sin plaun europeic ils ultims onns differents relaschs davart la protecziun da datas. Quests relaschs èn liants er per la Confederaziun e per ils chantuns e ston vegnir realisads en il dretg chantunal, per che las disposiziuns chantunalas davart la protecziun da datas adempleschian er en l'avegnir il standard europeic. En spezial per la lavur da la polizia vegni uschia garantì, ch'ella haja vinavant access al sistem d'infurmaziun da Schengen (SIS). La LCPD sto perquai vegnir revedida cumplettamain. La revisiun sa restrenscha a quels puncts ch'èn absolutamain necessaris per realisar las prescripziuns dal dretg internaziunal. Ils organs publics ch'èn suttamess a la lescha duain observar in pèr novs instruments ed in pèr novas obligaziuns, che servan en emprima lingia a rinforzar ils dretgs da las persunas ch'èn pertutgadas d'ina elavuraziun da datas. Plinavant pretenda il dretg surordinà in rinforzament da la surveglianza da la protecziun da datas. Quella vegn ademplida en il chantun Grischun tras l'incumbensada u l'incumbensà per la protecziun da datas. D'ina vart vegn rinforzada l'independenza da quest post. Da l'autra vart survegn el – tras la revisiun da la lescha – novas incumbensas e cumpetenzas.

L'essenziale in breve

La legge cantonale sulla protezione dei dati (LCPD; CSC 171.100) è stata posta in vigore con effetto al 1° maggio 2002. In oltre venti anni, la legge è stata modificata soltanto in alcuni punti. Tuttavia, nello stesso arco di tempo la tecnologia ha fatto passi da gigante. Inoltre, il trattamento e la comunicazione transfrontalieri di dati acquisiscono un'importanza sempre maggiore. Per questi motivi, negli ultimi anni a livello europeo sono stati emanati o rivisti diversi atti normativi in materia di protezione dei dati. Questi atti normativi sono vincolanti anche per la Confederazione e i Cantoni e devono essere attuati nel diritto cantonale affinché le disposizioni cantonali sulla protezione dei dati soddisfino anche in futuro gli standard europei. In tal modo rimane garantito l'accesso al Sistema d'informazione Schengen (SIS), in particolare per il lavoro di polizia. La LCPD deve dunque essere sottoposta a revisione totale. La revisione si limita ai punti assolutamente necessari per attuare le disposizioni di diritto internazionale. Gli organi pubblici

soggetti alla legge sono tenuti a impiegare alcuni nuovi strumenti e a soddisfare alcuni nuovi obblighi concepiti principalmente per rafforzare i diritti delle persone i cui dati sono oggetto di trattamento. Inoltre, il diritto di rango superiore richiede un rafforzamento della vigilanza sulla protezione dei dati che nel Cantone dei Grigioni viene assunta dall'incaricato della protezione dei dati. La revisione legislativa da un lato rafforza l'indipendenza di quest'organo, dall'altro gli conferisce nuovi compiti e competenze.

Sehr geehrte Frau Standespräsidentin
Sehr geehrte Damen und Herren

Wir unterbreiten Ihnen nachstehend die Botschaft und den Antrag betreffend Totalrevision des Kantonalen Datenschutzgesetzes (KDSG; BR 171.100).

I. Ausgangslage

1. Entwicklungen im Völker- und Bundesrecht

Das Datenschutzrecht dient dem Persönlichkeitsschutz der Personen, deren Daten bearbeitet werden und damit der Gewährleistung der informationellen Selbstbestimmung im Sinne von Art. 13 Abs. 2 der Bundesverfassung der Schweizerischen Eidgenossenschaft (BV; SR 101). Gemäss dieser Bestimmung hat jede Person Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten. Auf Stufe Bund wird Art. 13 Abs. 2 BV in erster Linie im Bundesgesetz über den Datenschutz (DSG; SR 235.1) konkretisiert. Dieses Gesetz gilt für die Bearbeitungen von Personendaten durch Bundesbehörden sowie private Personen (Art. 1 DSG). Die Kantone müssen eigene Gesetze erlassen, welche die Datenbearbeitungen durch kantonale, regionale und kommunale öffentliche Organe regeln. Der Kanton Graubünden hat daher auf den 1. Mai 2002 ein Kantonales Datenschutzgesetz (KDSG; BR 171.100) in Kraft gesetzt. Das KDSG regelt als «formelles Datenschutzrecht» die Grundsätze und allgemeinen Vorgaben an die Datenbearbeitungen durch Behörden. Welche Daten in den jeweiligen Rechtsbereichen bearbeitet werden dürfen, ergibt sich aus den Datenbearbeitungsvorschriften im jeweiligen bereichsspezifischen Recht («materielles Datenschutzrecht»). Dabei kann es sich um kantonales oder eidgenössisches Recht handeln.

In den über zwanzig Jahren seit dem Inkrafttreten des KDSG wurden grosse technologische Fortschritte erzielt. So ist die Zahl der Geräte und Anwendungen, die Daten produzieren und verarbeiten, erheblich gestiegen.

Die sinkenden Preise für Speicherplatz sowie die steigende Verfügbarkeit immer schnellerer Internetanschlüsse eröffnen in grossem Mass die Möglichkeit, Daten über das Netz zu empfangen, zu versenden und zu speichern. Zudem gewinnen grenzüberschreitende Datenbearbeitungen und Datenbekanntgaben immer mehr an Bedeutung. Dies führte dazu, dass gewisse länderübergreifende Vorgaben an die Datenbearbeitung definiert wurden. Zu nennen sind etwa die im April 2016 durch das Europäische Parlament und den Rat der Europäischen Union verabschiedete Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutz-Grundverordnung, im Folgenden: DSGVO) und die Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Bearbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr (im Folgenden: RL 2016/680). Die DSGVO ist grundsätzlich auf alle Datenbearbeitungen anwendbar. Die RL 2016/680 regelt hingegen ausschliesslich die polizeiliche sowie die justizielle Zusammenarbeit. Während die RL 2016/680 als Teil des Schengen-Acquis von der Schweiz im innerstaatlichen Recht von Bund und Kantonen umzusetzen ist, handelt es sich bei der DSGVO nicht um eine Weiterentwicklung des Schengen-Besitzstands. Letztere muss daher nicht in das Landesrecht übernommen werden. Die DSGVO ist jedoch von Bedeutung, da die Schweiz für die EU datenschutzrechtlich als Drittstaat gilt. Hinsichtlich Drittstaaten entscheidet die Europäische Kommission periodisch gestützt auf die Vorgaben der DSGVO, ob diese ein angemessenes Datenschutzniveau einhalten. Dieser Angemessenheitsbeschluss führt dazu, dass der Datentransfer mit den Ländern der EU ohne zusätzliche Einschränkungen oder Vorkehrungen erfolgen kann. Datenschutzrechtliche Mindeststandards ergeben sich für die Schweiz zudem aus dem Europäischen Übereinkommen vom 28. Januar 1981 zum Schutz des Menschen bei der automatisierten Verarbeitung von personenbezogenen Daten (Übereinkommen SEV 108; SR 0.235.1) sowie dessen Zusatzprotokoll vom 8. November 2001 (SR 0.235.11). Dieses Übereinkommen wurde zeitgleich mit den oben genannten Regelungen durch den Europarat revidiert. Das revidierte Übereinkommen SEV 108 orientiert sich inhaltlich an der RL 2016/680. Es ist im Gegensatz zur RL 2016/680 aber auf alle Datenbearbeitungen anwendbar. Mit Bundesbeschluss vom 19. Juni 2020 ermächtigten die eidgenössischen Räte den Bundesrat zur Ratifizierung des revidierten Übereinkommens. Mit dessen Ratifizierung sind Bund und Kantone verpflichtet, in ihrem Datenschutzrecht die notwendigen Anpassungen vorzunehmen, um dem Minimalstandard des Übereinkommen SEV 108 gerecht zu werden.

Auf Bundesebene wurde aufgrund der völkerrechtlichen Vorgaben und der geänderten technologischen und gesellschaftlichen Rahmenbedingun-

gen das DSG totalrevidiert. Aus Zeitgründen wurde diese Vorlage aufgeteilt. Der hier interessierende Teil der Totalrevision des DSG wurde von den eidgenössischen Räten am 25. September 2020 verabschiedet. Das totalrevidierte DSG ist auf den 1. September 2023 in Kraft getreten.

2. Revisionsbedarf

Der Revisionsbedarf des Datenschutzrechts ist in erster Linie den technologischen Entwicklungen der letzten zwanzig Jahre geschuldet. Der sich daraus ergebende Änderungsbedarf für einen wirksamen Schutz der informationellen Selbstbestimmung wurde in den völkerrechtlichen Entwicklungen, welche nach dem oben Ausgeführten auch für die Schweiz von Bedeutung sind, erkannt und umgesetzt. Der Kanton Graubünden hat die entsprechenden Anpassungen aufgrund der RL 2016/680 und des Übereinkommen SEV 108 nachzuvollziehen. Die völkerrechtlichen Vorgaben enthalten neue Instrumente und Verpflichtungen, welche im kantonalen Recht umgesetzt werden müssen. Zudem wird vorgeschrieben, dass die Stellung und die Befugnisse der kantonalen Datenschutzaufsicht gestärkt werden müssen. Das auf den 1. September 2023 in Kraft getretene, totalrevidierte DSG des Bundes ist insofern relevant, als das bestehende KDSG mit einer Reihe von dynamischen Einzelverweisen (vgl. Art. 1 Abs. 4, Art. 2 Abs. 2 und 3, Art. 4 Abs. 2 und Art. 5 Abs. 3 KDSG) dieses Gesetz weitgehend für sinngemäss anwendbar erklärt. Mit dem Inkrafttreten der Totalrevision des DSG gelten die völkerrechtlich geforderten Instrumente und Verpflichtungen, welche im DSG neu eingeführt werden, also auch für den Kanton Graubünden als kantonales Recht und sind somit rechtlich bereits umgesetzt. Indes wurden im Rahmen der Totalrevision des DSG auch die Struktur des Erlasses und wichtige Begriffsdefinitionen geändert. Aus diesem Grund ist nicht mehr immer klar ersichtlich, auf welche Bestimmungen sich die einzelnen Verweise beziehen. Gerade dies stellt jedoch eine wichtige Voraussetzung für die Zulässigkeit von dynamischen Verweisen aus dem kantonalen Recht auf das Bundesrecht dar (vgl. BGE 134 | 179 E. 6.3). Es ist davon auszugehen, dass die Verweise im bestehenden KDSG nicht ausreichen, um alle notwendigen Änderungen genügend eindeutig in das kantonale Recht zu überführen. In gewissen Punkten geht das Bundesrecht zudem über die völkerrechtlichen Vorgaben hinaus. Sofern diese Bestimmungen aufgrund der bestehenden Verweise ohne Einschränkung übernommen werden, sind diese Verpflichtungen auch im Kanton Graubünden vollumfänglich umzusetzen. Der Kanton würde in diesen Fällen den ihm gewährten Gestaltungsspielraum nicht ausnützen und die Möglichkeit, eigenes, den kantonalen Eigenheiten angepasstes Recht zu setzen, aus der Hand geben. So sind z. B.

im DSG alle öffentlichen Organe zur Führung eines Verzeichnisses über die Bearbeitungstätigkeiten oder zur Bezeichnung einer Datenschutzberaterin/eines Datenschutzberaters verpflichtet (vgl. unten Art. 22 und 23). Im Kanton Graubünden würden diese Verpflichtungen somit auch für Gemeinden und Regionen gelten. Dies ist nicht gewollt. Im Weiteren regelt das KDSG die Stellung und die Befugnisse der Aufsichtsstelle bzw. der oder des Datenschutzbeauftragten in den Art. 7 bis 10 KDSG ohne Verweis auf das Bundesrecht. Die betreffenden Regelungen müssen ebenfalls angepasst werden, um den völkerrechtlichen Vorgaben zu entsprechen. Das bestehende KDSG erweist sich als revisionsbedürftig. Der Handlungsbedarf, welcher sich auf kantonaler Ebene durch die Vorgaben der RL 2016/680 und des Übereinkommens SEV 108 ergibt, wurde von der Konferenz der Kantonsregierungen (KdK) unter massgeblicher Mitwirkung von Vertretungen der kantonalen Datenschutz-Aufsichtsstellen in einem Leitfaden zusammengefasst (im Folgenden: KdK-Leitfaden). Dieser Leitfaden dient als Grundlage der Revision. Die Revision beschränkt sich weitgehend auf den in diesem Leitfaden ausgewiesenen Anpassungsbedarf, der zur Umsetzung des geänderten europäischen Datenschutzrechts zwingend notwendig ist. Lediglich bei der Vorabkonsultation gemäss Art. 21 KDSG, welche auch bereichsspezifisch für öffentliche Organe im Bereich der justiziellen und polizeilichen Zusammenarbeit hätte umgesetzt werden können, geht die Vorlage über das völkerrechtliche Minimum hinaus. Diese Vorgehensweise wurde auch in allen anderen Kantonen so gewählt. Sie führt für die öffentlichen Organe zu keinem Mehraufwand, da die in diesem Rahmen einzureichenden Angaben für die davon erfassten Bearbeitungstätigkeiten im Rahmen der durch alle öffentlichen Organe durchzuführenden DSFA sowieso erarbeitet werden müssen (vgl. die detaillierten Ausführungen unter II.2.2 und Art. 20).

II. Vernehmlassungsverfahren

Die Vernehmlassungsvorlage wurde von einer Arbeitsgruppe unter der Leitung des Departements für Justiz, Sicherheit und Gesundheit (DJSG) gemeinsam mit dem Datenschutzbeauftragten des Kantons Graubünden erarbeitet. Mit Beschluss vom 23. Januar 2024 gab die Regierung den Entwurf zur Totalrevision des KDSG zur Vernehmlassung frei und ermächtigte das DJSG, ein Vernehmlassungsverfahren durchzuführen (Prot. Nr. 42/2024). Vom 25. Januar bis zum 24. April 2024 konnten sich alle interessierten Personen und Gruppierungen zur Vernehmlassungsvorlage äussern. Insgesamt gingen 50 Stellungnahmen ein. Es äusserten sich sieben Parteien, 18 Gemeinden, drei Regionen, sieben kantonale Departemente und Dienststellen sowie das Verwaltungsgericht. Weitere Stellungnahmen gingen ein von der Gebäudeversicherung Graubünden, der Sozialversicherungsanstalt des Kantons Graubünden, den Psychiatrischen Diensten Graubünden, der Pädagogischen Hochschule und der Fachhochschule Graubünden, dem Kantonsspital Graubünden, der Graubündner Kantonalbank und Evangelisch-reformierten Landeskirche Graubünden. Als Interessensverbände äusserten sich zudem der Bündner Anwaltsverband und der Bündner Spital- und Heimverband sowie die Digitale Gesellschaft Schweiz.

1. Allgemeine Beurteilung der Vorlage

Die Vernehmlassungsvorlage stiess weitgehend auf Zustimmung. Der Revisionsbedarf des über zwanzig Jahre alten KDSG wurde aufgrund der veränderten technologischen Gegebenheiten und der neuen völkerrechtlichen Verpflichtungen als gegeben erachtet. Es wurde weitgehend als richtig erachtet, dass die bisherigen dynamischen Verweise durch eine eigenständige Regelung ersetzt werden. Die dynamischen Verweise hatten insbesondere für Gemeinden im Zusammenhang mit der Totalrevision des DSG eher für Unsicherheit gesorgt, als zu einer Klärung der Rechtslage beigetragen. Der Grundsatz sich bei der Umsetzung der entsprechenden völkerrechtlichen Vorgaben auf das notwendige Minimum zu beschränken und keine darüber hinausgehenden Verpflichtungen vorzusehen, wurde ebenfalls begrüsst. Als wichtig wurde insbesondere von den Gemeinden erachtet, dass die entsprechenden Verpflichtungen für sie ohne grossen personellen und finanziellen Mehraufwand umsetzbar sind. Im Übrigen gingen zahlreiche wertvolle Verbesserungsvorschläge, vorab redaktioneller Natur ein, die im Botschaftsentwurf grossmehrheitlich berücksichtigt wurden.

2. Umgang mit den Anliegen

2.1 Berücksichtigte Anliegen

Aufsicht über privatrechtlich handelnde, öffentliche Organe (Art. 2 Abs. 2 KDSG)

Gemäss Art. 2 Abs. 2 KDSG werden öffentliche Organe vom Anwendungsbereich des Gesetzes ausgenommen, wenn sie am wirtschaftlichen Wettbewerb teilnehmen und dabei nicht hoheitlich handeln. Da die entsprechenden Organe dabei jedoch nur privatrechtlich handeln und nicht zu Privatpersonen werden, unterstehen sie weiterhin der Aufsicht durch die kantonale Aufsichtsstelle. Diese Bestimmung wurde im Rahmen der Vernehmlassung von der Graubündner Kantonalbank (GKB) kritisiert. Die GKB brachte vor, dass die Auswirkungen dieser Bestimmung auf Institute wie sie unklar seien. Sie gehen davon aus, dass sie sich in ihren Datenbearbeitungen weiterhin nur an den Bestimmungen des DSG des Bundes auszurichten haben. Im Weiteren erachten sie sich durch das geltende Recht der Aufsicht des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) unterstellt. Eine zusätzliche Aufsicht durch die kantonale Aufsichtsstelle und die Einreichung von Dokumenten auch an diese würde für die GKB zu einem Zusatzaufwand führen. Für die betroffenen Personen sei dagegen kein Mehrwert ersichtlich.

Es gilt darauf hinzuweisen, dass die betroffenen, öffentlichen Organe hinsichtlich der Bearbeitung die Regeln für Privatpersonen gemäss dem DSG zu beachten haben. Dies bedeutet, dass sie gegenüber der zuständigen Aufsichtsstelle die für Private geltenden Ausnahmebestimmungen und Privilegierungen geltend machen können (z.B. Verzicht auf Vorabkonsultation, wenn die Datenschutzberaterin oder der Datenschutzberater konsultiert wurde, Art. 23 Abs. 4 DSG). Die Regelung wurde in die Vernehmlassungsvorlage eingefügt, da bisher die Aufsicht über privatrechtlich handelnde, öffentliche Organe nicht klar geregelt war. Die Lehre geht mehrheitlich davon aus, dass der EDÖB grundsätzlich nur die Aufsicht über Bundesorgane und Privatpersonen wahrnimmt. Kantonale und kommunale Organe unterstehen nicht seiner Aufsicht (vgl. René Huber in Blechta/Vasella, Basler Kommentar Datenschutzgesetz, 4. Aufl., Art. 4, N. 80). Dies dürfte auch dann zu gelten haben, wenn sie privatrechtlich handeln. Da es keinen aufsichtsfreien Raum geben kann, hat die Zuständigkeit bei der kantonalen Aufsichtsstelle zu verbleiben. Es macht Sinn, dass ein öffentliches Organ, welches nur teilweise privatrechtlich handelt, nicht je nach Tätigkeitsfeld einer anderen Aufsicht unterstellt ist. Diese Konstellation kommt dort an ihre Grenzen, wo ein öffentliches Organ ausschliesslich im Wettbewerb steht und nicht hoheitlich handelt. Dies ist insbesondere bei den Kantonalbanken der Fall. Gegenüber

Kantonalbanken hat der EDÖB in der Vergangenheit auch bereits Aufsichtsaufgaben wahrgenommen und namentlich Empfehlungen formuliert.[1] Es erscheint daher schlüssig, die betroffenen öffentlichen Organe von der Aufsicht der kantonalen Aufsichtsstelle auszunehmen und ebenfalls einer einheitlichen Aufsicht durch den EDÖB zu unterstellen. Art. 2 Abs. 2 wurde entsprechend ergänzt.

Schutz von Personendaten juristischer Personen (Art. 3 Abs. 2 KDSG)

In Art. 3 Abs. 2 wird vorgesehen, dass als Personendaten im Sinne dieses Gesetzes alle Angaben gelten, die sich auf eine bestimmte oder bestimmbare natürliche oder juristische Person beziehen. Im Gegensatz zum DSG des Bundes schützt das KDSG somit weiterhin auch die Personendaten juristischer Personen. Diese Abweichung vom Bundesrecht wird im Rahmen der Vernehmlassung nicht grundsätzlich bestritten. Lediglich eine Vernehmlassungsteilnehmende erachtet die datenschutzrechtliche Gleichstellung von juristischen und natürlichen Personen als fraglich. Sie gibt zu bedenken, dass der Gesetzestext im revidierten DSG und somit auch im KDSG auf natürliche Personen ausgelegt sei. Einige Gesetzesbestimmungen lassen sich nicht ohne Weiteres von natürlichen auf juristische Personendaten übertragen, weil den juristischen Personen gewisse Eigenschaften sachgemäss nicht zukommen könnten (vgl. Damian George: «Juristische Personen als Subjekte der Datenschutzgesetzgebung», Jusletter vom 5. September 2016).

Es trifft zu, dass das KDSG in erster Linie auf den Schutz natürlicher Personendaten ausgerichtet ist. Die Übertragung gewisser Konzepte auf juristische Personen kann zu Auslegungsschwierigkeiten führen. Es ist zu beachten, dass diese Probleme auch bei einer eigenständigen Regelung (wie im DSG) nicht vollständig behoben werden können. Vielmehr würde eine solche Regelung zu einer nicht anwenderfreundlichen, parallelen Gesetzgebung führen (vgl. die Ausführungen zu Art. 3 KDSG). Es ist der Stellungnahme insofern zuzustimmen, dass gewisse Kategorien von Personendaten nicht sinnvoll auf juristische Personen angewandt werden können. Dies wird adressiert, indem namentlich das Persönlichkeitsprofil und das Profiling sich nur auf natürliche Personen beziehen können. Die entsprechenden Bestimmungen werden daher angepasst (vgl. Art. 3 Abs. 4 und 5 KDSG).

[1] vgl. Empfehlung des EDÖB betreffend Übermittlung von Mitarbeiterdaten (inklusive ehemalige Mitarbeitende und externe Dritte) durch die Basler Kantonalbank (BKB) an US-Behörden von 15. Oktober 2012.

Nachweis der Einhaltung der Datenschutzbestimmungen (Art. 4 Abs. 3 KDSG)

Art. 4 Abs. 3 KDSG regelt, dass das verantwortliche öffentliche Organ gegenüber der Aufsichtsstelle nachweisen können muss, dass es die Datenschutzbestimmungen einhält. In der Vernehmlassung wurde von verschiedenen Teilnehmenden kritisiert, dass nicht geklärt sei, wie dieser Nachweis der Einhaltung der Datenschutzbestimmungen erfolgen solle und mit welchem Mehraufwand diese neue Verpflichtung einhergehe. Durch die offene Formulierung der Bestimmung lasse es sich für die Betroffenen schwierig abschätzen, ob diese Verpflichtung einen personellen und finanziellen Mehraufwand bedeute. Zudem sei nicht geregelt, ob das verantwortliche öffentliche Organ von sich aus oder nur auf Verlangen der Aufsichtsstelle die Einhaltung der Datenschutzbestimmungen nachweisen muss.

Den Vernehmlassungsteilnehmenden ist zuzustimmen, dass die Bestimmung die Art und Weise des Nachweises offenlässt. Dies ist insofern gewollt, als es sich dabei um eine unter Umständen rasch ändernde, technische Materie handelt. Aktuell taugliche Massnahmen zum Nachweis können in einigen Jahren überholt sein. Daher wird auf Verordnungsstufe ausgeführt, wie der Nachweis erbracht werden kann. Der Nachweis der Einhaltung der Datenschutzbestimmungen soll die öffentlichen Organe nicht zu fest zusätzlich belasten, aber dennoch ein gewisses Mass an Dokumentation der Massnahmen zur Einhaltung des Datenschutzes sicherstellen. Die Verordnung soll daher vorsehen, dass der Nachweis durch eine Vielzahl an verschiedenen Dokumenten geführt werden kann. Dabei kann es sich auch um Dokumente handeln, welche von den Behörden bereits jetzt oder spätestens nach neuem Recht zwingend zu erarbeiten sind (z.B. Geschäftsordnungen, Weisungen zu Datenbearbeitungen oder Informationssicherheits- und Datenschutzkonzepte; vgl. unten IV.1.). Es wird im Gegensatz zu anderen Kantonen darauf verzichtet, die Einführung eines Datenschutzmanagementsystems oder eine Zertifizierung nach ISO-Standards zu verlangen. Ein entsprechendes Vorgehen wäre gerade für kleine Gemeinwesen mit einem kaum stemmbaren Mehraufwand verbunden. Aufgrund der Rückmeldungen in der Vernehmlassung wird im Gesetzestext neu klargestellt, dass der Nachweis gegenüber der Aufsichtsstelle lediglich auf Anfrage hin erbracht werden muss. Aufgrund der Übergangsbestimmung in Art. 41 KDSG haben die öffentlichen Organe zudem zwei Jahre Zeit, bis dieser Nachweis eingefordert werden kann.

Mittelbare gesetzliche Grundlage für Datenbearbeitungen (Art. 7 KDSG)

Art. 7 KDSG regelt, unter welchen Voraussetzungen Personendaten bearbeitet werden können. Die Bestimmung statuiert, dass grundsätzlich eine gesetzliche Grundlage benötigt wird. Dieses Erfordernis ergibt sich aus dem

Legalitätsprinzip und bestand bereits vor der Revision des DSG. Es wird im Rahmen der Vernehmlassung nicht grundsätzlich in Frage gestellt. Eine Vernehmlassungsteilnehmende weist darauf hin, dass es ausreichend sein solle, wenn eine Datenbearbeitung in einem sachlichen Zusammenhang mit der gesetzlichen Aufgabe der betreffenden Behörde stehe. Es wird dabei auf die Datenschutzgesetze anderer Kantone verwiesen. In diesen wird statuiert, dass es anstelle einer expliziten gesetzlichen Grundlage auch ausreiche, wenn eine Datenbearbeitung zur Erfüllung einer gesetzlichen Aufgabe unentbehrlich sei. Gerade Gemeinden würden bisher oft nur die öffentliche Aufgabe gesetzlich regeln, zu deren Erfüllung die Datenbearbeitung erforderlich ist und nicht zwingend die Datenbekanntgabe selbst. Diese Möglichkeit solle beibehalten werden.

Bisher wurde es im Bundesrecht und somit aufgrund des Verweises auch im KDSG für die Bearbeitung von Personendaten als ausreichend erachtet, wenn das Gesetz dem öffentlichen Organ eine Aufgabe zuweist, die dieses nur mit der Bearbeitung der betreffenden Daten erfüllen kann (Art. 17 Abs. 2 lit. a aDSG). Diese so genannte mittelbare gesetzliche Grundlage steht im Gegensatz zur unmittelbaren gesetzlichen Grundlage, bei welcher die Datenbearbeitung explizit im Gesetz geregelt ist. Durch die angepasste Formulierung in Art. 34 Abs. 2 – 4 KDSG wird neu das Verhältnis der einzelnen Absätze untereinander im Vergleich zu Art. 17 aDSG klarer geregelt. Die Mehrheit der Lehre geht davon aus, dass die Verwendung mittelbarer gesetzlicher Grundlagen dadurch eingeschränkt werde (vgl. Claudia Mund in: Baeriswyl/Pärli/Blonski [Hrsg.], Stämpflis Handkommentar zum DSG, 2. Aufl., Art. 34, N. 10). Es wird im Hinblick auf die Bestimmung vertreten, dass mittelbare gesetzliche Grundlagen insbesondere auf kantonaler Stufe verbreitet seien und beim Bundesrecht die Ausnahme darstellen. Daher rechtfertige sich im Bundesrecht eine entsprechende Privilegierung im Bundesrecht nicht mehr. Die Mehrheit der Kantone sieht es demgegenüber für die Bearbeitung von Personendaten als ausreichend an, dass diese zur Erfüllung einer gesetzlich vorgeschriebenen Aufgabe unentbehrlich oder erforderlich ist. Dies normieren sie entsprechend im Datenschutzgesetz. Da grundsätzlich durch die Revision keine bestehenden Datenbearbeitungen verunmöglicht werden sollen, wird es als zielführend erachtet, an dieser Stelle Datenbearbeitungen auch aufgrund mittelbarer gesetzlicher Grundlagen zu erlauben. Die entsprechende Abweichung vom Wortlaut des DSG erscheint gerechtfertigt.

Bildüberwachung des öffentlichen und öffentlich zugänglichen Raums (Art. 14 KDSG)

Art. 14 KDSG regelt die Bildüberwachung des öffentlichen und öffentlich zugänglichen Raums. Die Bestimmung wurde weitgehend aus dem bestehen-

den Recht übernommen (Art. 3a und 3b des bestehenden KDSG), zumal sie sich bisher für die öffentlichen Organe in ihrer Handhabung grundsätzlich bewährt hat. Für drei Parteien, den kantonalen Datenschutzbeauftragen und eine weitere Vernehmlassungsteilnehmende geht die Bestimmung in gewissen Aspekten zu weit. Teilweise werden die entsprechenden Möglichkeiten insgesamt abgelehnt, da sie schwerwiegende Eingriffe in die Grundrechte nach sich ziehen. Zudem wird die Bildüberwachung als Türöffner zur automatisierten Überwachung der Bevölkerung gesehen. Die Notwendigkeit entsprechender Massnahmen in Einzelfällen wird von den meisten Teilnehmenden nicht grundsätzlich in Frage gestellt. Sie bringen jedoch vor, dass die Bestimmung den Behörden in verschiedener Hinsicht zu viel Spielraum lasse. Namentlich müsse nur in geeigneter Weise auf die Videoüberwachung hingewiesen werden. Dies lasse zu, dass eine Überwachung für die Überwachten nicht unbedingt erkennbar sein müsse. Gerade dies stelle für die Betroffenen eine wesentliche Voraussetzung dar, um die Auswirkungen auf ihre Privatsphäre einschätzen zu können. Im Weiteren können die durch eine Bildüberwachung gespeicherten Daten grundsätzlich 90 Tage aufbewahrt werden, was teilweise als zu lange erachtet wird. Auch nach diesen 90 Tagen müssen sie nicht gelöscht werden, wenn sie in einem Strafverfahren oder zur Gefahrenabwehr benötigt werden. Hierbei wird der Begriff der Gefahrenabwehr als zu weitgehend erachtet. Auf diese Weise würde eine längere bzw. dauerhafte Speicherung von Personendaten erlaubt, welche im Unterschied zu Strafverfahren unabhängig von einem klaren und richterlichen Beschluss möglich wäre. Dies widerspräche dem Grundsatz von Art. 5 Abs. 4 KDSG, wonach Daten «vernichtet oder anonymisiert (werden), sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind.»

Vor dem Hintergrund, dass mit der Revision die Rechte der Betroffenen stärker geschützt werden sollen, erscheinen diese Vorbringen durchaus berechtigt. Während ein gänzlicher Verzicht auf dieses Instrument nicht zielführend ist, kann der monierte, weite Spielraum der öffentlichen Organe teilweise begrenzt werden. Hinsichtlich der Erkennbarkeit der Bildüberwachungen finden sich einschränkendere Formulierungen auch in den Bestimmungen anderer Kantone zur Bildüberwachung. Zumindest für kantonale Organe ist im geltenden Recht in der Verordnung über die Bildüberwachung des öffentlichen und öffentlich zugänglichen Raums (VBÜ; BR 171.120) normiert, dass die Videoüberwachung mit Piktogrammen signalisiert werden muss. Eine entsprechende Mindestanforderung soll auch für andere Organe gelten. Neu wird daher im Gesetz vorgesehen, dass der Hinweis auf die Bildüberwachung sowohl geeignet als auch erkennbar sein muss.

Art. 14 KDSG wurde dahingehend konkretisiert, dass nun ersichtlich ist, dass es sich bei der Speicherungsdauer von 90 Tagen um eine Maximalfrist handelt. Bei der Ausarbeitung der Allgemeinverfügung, auf welcher die

konkrete Überwachung basiert, ist das datenschutzrechtliche Verhältnismässigkeitsprinzip zu beachten und die Daten nur so lange wie notwendig zu speichern. Ein interkantonaler Rechtsvergleich zeigt, dass eine neunzigtägige Maximalfrist die Regel ist und nur in wenigen Kantonen kürzere oder längere Fristen vorgesehen werden. Aufgrund der Rückmeldungen aus der Vernehmlassung wird es als vertretbar erachtet, dass eine über die 90 Tage hinausgehende Speicherung der Aufnahmen alleine zu Zwecken der Gefahrenabwehr nicht mehr möglich sein wird.

Umfang der Datenschutz-Folgenabschätzung (Art. 19 KDSG)

Mit Art. 19 KDSG wird die Datenschutz-Folgenabschätzung (DSFA) als neues Instrument eingeführt. Eine DSFA ist gestützt auf die völkerrechtlichen Vorgaben durchzuführen, wenn eine Bearbeitungstätigkeit ein hohes Risiko für die Grundrechte der betroffenen Person mit sich bringen kann. Die Bestimmung wurde nicht wortgemäss aus Art. 22 DSG übernommen, da dieser auch Ausführungen zur Ausgestaltung der DSFA für private Verantwortliche enthält. Diese sind vom KDSG grundsätzlich nicht umfasst. Somit wurde auch Art. 22 Abs. 2 DSG nicht übernommen, welcher definiert, wann ein hohes Risiko vorliegt. Der Begriff sollte ursprünglich auf Verordnungsstufe definiert werden, auch weil er der technischen Entwicklung unterworfen ist. Die Definition sollte sich jedoch an Art. 22 Abs. 2 DSG orientieren. Verschiedene Vernehmlassungsteilnehmende führten aus, es sei angezeigt, die Regelung aufgrund ihrer Relevanz ins Gesetz zu übernehmen. Es wurde auch vorgebracht, dass nicht zu hohe Anforderungen an die DSFA gestellt werden sollen, da dieses neue Instrument eine zusätzliche Belastung für die öffentlichen Organe darstelle.

Aufgrund der Rückmeldungen erscheint es angezeigt, die Definition des hohen Risikos analog zu Art. 22 Abs. 2 DSG auf Gesetzesstufe vorzunehmen. Welche Sachverhalte konkret darunterfallen, kann aufgrund des stetigen technologischen Fortschritts und der Tatsache, dass eine aktuell neue Technologie sich in fünf Jahren vielleicht bereits etabliert hat, nicht auf Gesetzesstufe festgelegt werden. Ob im konkreten Fall ein hohes Risiko vorliegt, kann für die öffentlichen Organe der Kantonalen Verwaltung im Rahmen der bestehenden Schutzbedarfsanalyse bestimmt werden, welche für jedes neue Informatikvorhaben durchzuführen ist. Für die weiteren öffentlichen Organe bietet sich ein ähnliches Vorgehen an. Hierzu können allenfalls Hilfsdokumente durch die kantonale Aufsichtsstelle bereitgestellt werden, wie dies in anderen Kantonen der Fall ist.

Einschränkung des Auskunftsrechts bei querulatorischen und unbegründeten Anfragen (Art. 25 und 28 KDSG)

Art. 24 KDSG regelt das Auskunftsrecht der betroffenen Personen. Er sieht vor, dass diese vom verantwortlichen öffentlichen Organ Auskunft darüber verlangen können, ob Personendaten über sie bearbeitet werden. Das Auskunftsrecht kann unter den in Art. 25 statuierten Voraussetzungen eingeschränkt werden. Die Gründe, welche eine Einschränkung ermöglichen, wurden weitgehend aus dem Bundesrecht übernommen. Nicht übernommen wurde die Möglichkeit zur Einschränkung, wenn ein Auskunftsgesuch offensichtlich unbegründet oder querulatorisch ist. Verschiedene Vernehmlassungsteilnehmende erachten den Verzicht auf diese Einschränkung als nicht dienlich. Sie befürchten, dass dadurch staatskritische Personen (wie etwa Staatverweigerernde oder «Reichsbürger») eine weitere Möglichkeit hätten, die staatlichen Institutionen auf allen Ebenen zu beschäftigen und zu überlasten.

Die Regelung wurde ursprünglich nicht übernommen, da sie sich nicht aus dem Völkerrecht ergibt. Im Rahmen der Botschaft zum DSG wird sogar in Frage gestellt, ob sie sich mit den völkerrechtlichen Vorgaben gemäss dem Übereinkommen SEV 108 vereinbaren lässt (vgl. BBl 2017 6941, 707). Dennoch sieht die Mehrheit der Kantone entweder vor, dass das Auskunftsrecht in entsprechenden Fällen eingeschränkt werden kann oder zumindest Kosten erhoben werden können. Aufgrund der oben ausgeführten Rückmeldungen erscheint eine solche Regelung auch im Kanton Graubünden angebracht. Es wird als für die Betroffenenrechte dienlicher erachtet, dass dabei nicht die oder der Verantwortliche von sich aus entscheiden kann, ob sie oder er das Auskunftsrecht einschränkt (wie etwa Art. 26 DSG). Stattdessen soll sie oder er dessen Gewährung mit der Überbindung der daraus entstehenden Kosten verbinden können. Die Entscheidung, ob am Auskunftsbegehren festgehalten wird, kann somit bei der oder dem Betroffenen verbleiben.

Unvereinbarkeiten (Art. 33 KDSG)

Art. 33 KDSG regelt, welche Tätigkeiten inskünftig mit dem Amt der oder des Datenschutzbeauftragten und der Stellvertretung unvereinbar sind. Namentlich dürfen sie kein anderes öffentliches Amt und keine leitende Funktion in einer politischen Partei ausüben. Bei einem Vollpensum darf zudem keine andere Erwerbstätigkeit ausgeübt werden, wobei die Regierung Ausnahmen bewilligen kann. Versehen sie das Amt in einem Teilpensum, ist eine Nebentätigkeit ebenfalls durch die Regierung zu bewilligen. Eine Bewilligung kann nur verweigert werden, wenn dadurch die Ausübung der Funktion sowie Unabhängigkeit und Ansehen beeinträchtigt werden. Diese Regelung wurde von einer Partei und weiteren Vernehmlassungsteilnehmenden in verschiedener Hinsicht als problematisch erachtet. Einerseits wurde

vorgebracht, dass auch bei einem Teilzeitpensum die Nebenerwerbstätigkeit die Unabhängigkeit, Glaubwürdigkeit und das Ansehen dieser Stelle massiv beeinträchtigen könne (z.B. bei der anwaltlichen Vertretung von natürlichen Personen in Verfahren gegen die datenschutzrechtlich verantwortlichen öffentlichen Organe). Im Weiteren erschliesse sich aus den Ausführungen nicht, warum die leitende Funktion in einer Partei nicht vereinbar mit der Tätigkeit als Datenschutzbeauftragte oder Datenschutzbeauftragter sei. Kritisiert wurde zudem, dass nicht klar sei nach welchen Kriterien entsprechende Ausnahmen genehmigt werden können.

Den Vernehmlassungsteilnehmenden ist insofern zuzustimmen, als die Unabhängigkeit und die Glaubwürdigkeit der Aufsichtsstelle dadurch gestärkt werden muss, dass sie keine mit dem Amt nicht vereinbaren Tätigkeiten wahrnimmt. Aufgrund des weiten Wirkungskreises der Aufsichtsstelle wird deren parteipolitische Unabhängigkeit von Bedeutung sein. Das Amt soll insbesondere nicht als politisch wahrgenommen werden, da eine Politisierung der Wahl und der Aufsichtsstelle keine guten Voraussetzungen für deren Akzeptanz schafft. Indes wäre es nicht verhältnismässig, einer Bewerberin oder einem Bewerber jegliches politisches Engagement zu verbieten, daher soll eine Beschränkung auf leitende Funktionen (z.B. Parteipräsidien oder Vorstandsämter) vorgenommen werden. Sinn und Zweck der Unvereinbarkeitsbestimmung ist zudem, dass geeignete Personen weiterhin Tätigkeiten nachgehen können, welche mit der Aufsichtstätigkeit nicht in Interessenskonflikt stehen (z.B. künstlerische Tätigkeit, Lehrauftrag, Vereinstätigkeit). Die entsprechenden Bindungen sollen jedoch offengelegt werden müssen, damit die Regierung befinden kann, ob die Unabhängigkeit dadurch beeinträchtigt wird. Wie in anderen Kantonen ist der Bewilligungsbehörde ein gewisser Ermessensspielraum zuzugestehen. Oberste Maxime ist allerdings die Unabhängigkeit des Amts. Daher wird Art. 33 Abs. 1 dahingehend angepasst, dass die Regierung die Erteilung entsprechender Bewilligungen (wie in Abs. 2 bereits vorgesehen) daran zu messen hat, ob die Ausübung der Funktion sowie Unabhängigkeit und das Ansehen der Stelle beeinträchtigt werden.

Koordination von datenschutzrechtlichen Gesuchen an das öffentliche Organ und Meldungen an die Aufsichtsstelle (Art. 36 KDSG)

Gemäss Art. 35 Abs. 1 lit. g KDSG behandelt die Aufsichtsstelle Meldungen von Betroffenen betreffend die Missachtung von Vorschriften dieses Gesetzes. Mit dieser Bestimmung wird die völkerrechtliche Verpflichtung zu einem «Recht auf Beschwerde» bei der Aufsichtsstelle umgesetzt. Eine Vernehmlassungsteilnehmende wies darauf hin, dass das Verhältnis zum Verfahren aus datenschutzrechtlichen Ansprüchen gegen das verantwortliche öffentliche Organ nach Art. 28 KDSG nicht geklärt sei. In der jetzigen

Fassung sei die Meldung nicht subsidiär zu weiteren Rechtsmitteln. Es sei zu verhindern, dass ein Sachverhalt durch den Datenschutzbeauftragten untersucht werde, wenn dieser Sachverhalt bereits in einem Verfahren rechtshängig sei. Damit soll vermieden werden, dass der Datenschutzbeauftragte eine Meldung bearbeiten muss, über welche demnächst eine Rechtsmittelinstanz (Departement oder Gericht) entscheide.

Gemäss den völkerrechtlichen Vorgaben darf das «Recht auf Beschwerde» gerade nicht subsidiär zu anderen Rechtsmitteln sein. Der Datenschutzbeauftragte muss sich mit der Meldung befassen. Als Ergebnis kann er Untersuchungen anstellen, welche etwa in der Formulierung konkreter Empfehlungen (Art. 36 KDSG) münden können, aber nicht müssen. Im Mindesten muss er die Person über die Ergebnisse seiner Untersuchung informieren. Im Rahmen seiner Untersuchungen wird der DSB nicht umhinkommen, das öffentliche Organ zur Stellungnahme einzuladen. Auf diese Weise würde er auch von einem allfälligen Verfahren nach Art. 28 KDSG Kenntnis erhalten und kann seine Empfehlungen etwa hinsichtlich dieses Verfahrens formulieren. Er kann jedoch auch auf ein weiteres Tätigwerden verzichten, wenn aus seiner Sicht die Rechte der Person durch das entsprechende Verfahren gewahrt werden. Um das Verhältnis zwischen dem Handeln der Aufsichtsstelle gestützt auf Art. 35 KDSG und allfälligen Verfahren nach Art. 28 KDSG zu verdeutlichen, wird in Art. 36 Abs. 1 KDSG eine Koordinationsnorm eingefügt werden. Diese besagt, dass bei einem Tätigwerden der Aufsichtsstelle auf Meldung der Betroffenen dem verantwortlichen öffentlichen Organ von dieser Meldung Kenntnis zu geben und ihm Gelegenheit zur Stellungnahme zu geben ist.

2.2 Nicht berücksichtigte Anliegen

Bekanntgabe von Stammdaten (Art. 10 Abs. 3)

Art. 10 Abs. 3 sieht vor, dass gewisse grundsätzlich wenig sensitive Personendaten (Name, Vorname, Adresse und Geburtsdatum) auch dann bekannt gegeben werden dürfen, wenn keine gesetzliche Grundlage besteht und auch die Voraussetzungen für eine Bekanntgabe im Einzelfall nicht erfüllt sind. Zwei Parteien und weitere Vernehmlassungsteilnehmende sehen im Erläuternden Bericht nicht schlüssig begründet, wieso diese Stammdaten von Behörden, die nicht mit der Einwohnerkontrolle betraut sind, an Dritte weitergegeben werden dürfen. Daher wird beantragt, die Bestimmung zu streichen oder zumindest auf Behörden zu beschränken, welche mit der Einwohnerkontrolle betraut sind.

Es gilt zu beachten, dass die fragliche Bestimmung aus dem geltenden Recht übernommen wurde. Auch im DSG des Bundes existiert sie weiter-

hin. Sie erlaubt öffentlichen Organen die Bekanntgabe dieser «ungefährlichen» Daten. Diese Ausnahme wurde gemäss den Tätigkeitsberichten des Datenschutzbeauftragten[2] in verschiedenen Situationen angerufen. Der Gesetzgeber ging bei der Einführung der Bestimmung davon aus, dass diese Daten weitgehend öffentlich sind bzw. auf andere Weise leicht beschafft werden können. Sie können aber dazu dienen, eine Person, über welche weitere Daten bereits bekannt sind, zweifelsfrei zu identifizieren, ohne dazu auf weitere und sensiblere Daten (wie die AHV-Nummer) zurückgreifen zu müssen. Es wird in der Lehre vertreten, dass die Bekanntgabe der Stammdaten an Private nur mit Zurückhaltung praktiziert werden soll, um bei einem anderen öffentlichen Organ hinterlegte Widersprüche (vgl. Art. 26 KDSG) nicht zu unterlaufen. Was die Verwendung der Stammdaten im behördeninternen Verkehr angeht, gilt zu beachten, dass diese Bekanntgabe in der Regel bereits durch Art. 10 Abs. 2 Bst. a KDSG gedeckt ist. Dieser lässt eine Bekanntgabe zu, wenn sie für die Erfüllung einer öffentlichen Aufgabe notwendig ist (vgl. sinngemäss Claudia Mund in: Baeriswyl/Pärli/Blonski [Hrsg.], Stämpflis Handkommentar zum DSG, 2. Aufl., Art. 36, N. 35). Dennoch soll den öffentlichen Organen diese bestehende Möglichkeit nicht ohne zwingenden Grund vorenthalten werden. Es gilt zu beachten, dass auch bei der Bekanntgabe dieser Daten gemäss Art. 10 Abs. 3 KDSG eine Interessensabwägung gemäss Art. 10 Abs. 4 KDSG durchgeführt werden muss.

Archivierung und Vernichtung (Art. 16 KDSG)

Art. 16 regelt die Archivierung und die Vernichtung von Personendaten, die nicht mehr benötigt werden. In Abs. 3 wird vorgesehen, dass die Regierung weitere Vorschriften, namentlich Löschfristen und Massnahmen zur regelmässigen Überprüfung der Notwendigkeit von Personendatenbeständen, erlassen kann. Zwei Parteien und eine weitere Vernehmlassungsteilnehmende bringen vor, dass die Löschfristen aufgrund ihrer Wichtigkeit und damit sie nicht beliebig angepasst werden können, auf Gesetzesstufe geregelt werden müssen.

Auch wenn in der Praxis durchaus eine gewisse Unsicherheit hinsichtlich der Festlegung von Aufbewahrungs- bzw. Löschfristen festgestellt werden kann, kennt soweit ersichtlich nur der Kanton Zürich eine allgemeine Aufbewahrungsfrist von zehn Jahren in der Datenschutzgesetzgebung. Die Mehrheit der Kantone belässt es den jeweils sachkundigen Behörden, die Aufbewahrungsfristen je nach Dokument zu bestimmen. Auch im Kanton Graubünden sieht das Gesetz über die Aktenführung und Archivierung (GAA; BR 490.000) vor, dass die diesem Gesetz unterstellten Behörden Auf-

[2] Vgl. etwa Tätigkeitsbericht 2013 des Datenschutzbeauftragten des Kantons Graubünden, S. 11; Tätigkeitsbericht 2019 des Datenschutzbeauftragten des Kantons Graubünden, S. 22.

bewahrungsregeln und -fristen definieren müssen (Art. 6 Abs. 1 GAA). Die Festlegung einer allgemeinen Frist auf Gesetzesstufe wäre eine Abkehr von der bisherigen und bewährten Praxis. Zudem dürfte es schwierig sein, diese Frist allgemeingültig festzulegen, da es immer Ausnahmen gibt, welche eine längere oder kürzere Aufbewahrung verlangen. Es ist daher zu befürchten, dass das Versprechen einer höheren Rechtssicherheit durch eine allgemeine Löschfrist nicht erfüllt werden könnte. Zudem statuierte Art. 16 KDSG, dass die Regierung weitere Vorschriften zur regelmässigen Überprüfung der Notwendigkeit von Personendaten vorsehen kann. Für die dem GAA unterstellten Organe ergibt sich die Definierung von Aufbewahrungsfristen als wichtigste solcher Massnahmen bereits aus dem Gesetz und ist daher an dieser Stelle nicht zu wiederholen. Daher wird Art. 16 Abs. 3 KDSG gestrichen.

Streichung der Vorabkonsultation (Art. 20 KDSG)

Art. 20 KDSG sieht vor, dass geplante Datenbearbeitungen, bei denen trotz der im Rahmen der DSFA (Art. 19 KDSG) vorgesehenen Massnahmen ein hohes Risiko für die Grundrechte der betroffenen Personen verbleibt, der Aufsichtsstelle zur Stellungnahme zuzustellen sind. Auf diese Weise soll die Aufsichtsstelle bei sensitiven Datenbearbeitungen in einem möglichst frühen Zeitpunkt miteinbezogen werden. Dadurch kann etwa verhindert werden, dass die Aufsichtsstelle erst zu einem späteren Zeitpunkt in Form von Empfehlungen oder Verfügungen gegen eine datenschutzrechtswidrige Bearbeitungstätigkeit vorgehen muss und diese kostenintensiv angepasst werden muss. Verschiedene Gemeinden verweisen darauf, dass die Verpflichtung zur Vorabkonsultation nur für den Bereich der justiziellen und polizeilichen Zusammenarbeit bestehe. Es wird daher beantragt, die Vorabkonsultation auf diese Organe zu beschränken, um den ohnehin schon erheblichen Zusatzaufwand der Gemeinden aufgrund des neuen Datenschutzgesetzes zu reduzieren.

Es trifft zu, dass die Vorabkonsultation nur in der RL 2016/680 vorgesehen ist und somit nur für die davon erfassten Behörden umgesetzt werden könnte. Es ist indes kein anderer Kanton bekannt, welcher die Vorabkonsultation nur in diesem Bereich vorsieht. Es gilt zu beachten, dass die Vorabkonsultation nur bei neuen oder wesentlich geänderten Datenbearbeitungsvorgängen durchgeführt werden muss, bei welchen nach der Durchführung der DSFA ein hohes Risiko für die Grundrechte der betroffenen Personen verbleibt. Hiermit weicht man von den meisten anderen Kantonen ab, welche eine Vorabkontrolle grundsätzlich bei jeder Bearbeitung vorsehen, die eine DSFA benötigen und nicht nur, wenn nach dieser ein hohes Risiko verbleibt. Dadurch ist ihr Anwendungsbereich bereits begrenzt. Zudem dürfte es im Rahmen der Vorabkonsultation in der Regel (wie dies auch in anderen Kantonen vorgesehen ist) ausreichen, wenn das öffentliche Organ der Auf-

sichtsstelle die im Rahmen der DSFA erarbeitete Dokumentation zukommen lässt. Diese sind aufgrund der völkerrechtlichen Vorgaben bei jeder Bearbeitung mit hohem Risiko (auch ausserhalb des Anwendungsbereichs der RL 2016/680) zu erstellen. Daher dürfte der sich für die öffentlichen Organe aus der Vorabkonsultation ergebende Zusatzaufwand entsprechend gering sein. Dieses Instrument soll daher für alle öffentlichen Organe beibehalten werden.

Erweiterung der Verpflichtungen zur Erstellung eines Verzeichnisses über die Datenbearbeitung und die Ernennung einer Datenschutzberaterin oder eines Datenschutzberaters (Art. 22 und 23 KDSG)

Art. 22 und Art. 23 KDSG führen das Verzeichnis über die Datenbearbeitungstätigkeiten und die Datenschutzberaterin oder den Datenschutzberater als neue Verpflichtungen ein. Diese ergeben sich aus der RL 2016/680 und sollen im Kanton Graubünden ausschliesslich für die dadurch verpflichteten Organe umgesetzt werden. Zwei Parteien und eine weitere Vernehmlassungsteilnehmende beantragen, alle öffentlichen Organe zur Einführung dieser Instrumente zu verpflichten. Dies wird einerseits damit begründet, dass gerade das Verzeichnis der Bearbeitungstätigkeiten als wichtiger Nachweis zur Einhaltung der Datenschutzbestimmungen genannt wird. Anderseits wird es für die Umsetzung in der Praxis als wichtig erachtet, dass es eine für die Datenschutzberatung zuständige Person in den Organisationen gibt. Teilweise wird auch angeführt, dass die Umsetzung der neuen Verpflichtungen sowie der Ansprüche der betroffenen Personen nur sichergestellt werden könne, wenn eine Datenschutzberatung beim verantwortlichen öffentlichen Organ existiere. Daher würden Gemeinwesen trotz mangelnder gesetzlicher Verpflichtung nicht umhinkommen, eine solche Person zu bezeichnen oder zu mandatieren. Um diesen finanziellen Mehraufwänden entgegenzuwirken, sei eine Grundlage zu schaffen, damit sich der Kanton am Zusatzaufwand der Gemeinden (namentlich für die Ernennung oder den externen Beizug einer Datenschutzberaterin oder eines Datenschutzberaters) finanziell beteilige.

Ein überwiegender Anteil der sich in dieser Sache äussernden Vernehmlassungsteilnehmenden (insbesondere die Gemeinden) begrüsst hingegen die Einschränkung der Instrumente auf die von der RL 2016/680 erfassten Organe. In praktischer Hinsicht wird der Nutzen der Instrumente für andere Organe durchaus gesehen. Daher sollen die Möglichkeiten allen öffentlichen Organen offenstehen. Im Zusammenhang mit dem Verzeichnis der Datenbearbeitungstätigkeiten weisen die Erfahrungen aus anderen Kantonen darauf hin, dass dessen Führung nicht alleine bereits als Nachweis ausreicht und andere Nachweismöglichkeiten gegebenenfalls aussagekräftiger sind (vgl. unten IV). Dies spricht dafür, die Führung des Verzeichnisses nicht

verpflichtend auszugestalten. Hinsichtlich der Ernennung eines oder einer Datenschutzbeauftragten ist darauf hinzuweisen, dass die Gemeinden insbesondere aufgrund der höheren Dotierung der Aufsichtsstelle vermehrt von deren Beratungstätigkeit profitieren können. Es wird daher nicht damit gerechnet, dass die neuen Verpflichtungen und Instrumente die Benennung eines oder einer Datenschutzbeauftragten für Organe ausserhalb des Anwendungsbereichs der RL 2016/680 (was die Gemeinden und Regionen mit der Ausnahme der Stadtpolizei Chur sind) faktisch zur Pflicht machen. Insofern eine Kostenbeteiligung für die Umsetzung allfälliger Massnahmen des neuen Datenschutzgesetzes (namentlich für die Anstellung oder den Beizug einer Datenschutzberaterin oder eines Datenschutzberaters) gefordert wird, ist festzuhalten, dass für den Datenschutz dasjenige Organ verantwortlich ist, welches über den Zweck und die Mittel der Bearbeitung entscheidet (vgl. Art. 4 KDSG). Dies bedeutet, dass die Gemeinden in ihrem Bereich für die jeweiligen Datenbearbeitungen und Verpflichtungen verantwortlich sind. Der Kanton ist grundsätzlich nur für seine eigenen Datenbearbeitungen verantwortlich. Eine gesetzliche Grundlage, dass sich der Kanton an dem Mehraufwand der Gemeinden für die Datenschutzberaterin oder den Datenschutzberater beteiligen kann, widerspräche der verfassungsmässigen Ordnung. Zudem ist festzuhalten, dass kein anderer Kanton entsprechende Regelungen vorsieht. Dies obwohl dort teilweise gar die Gemeinden eigene Aufsichtsstellen vorsehen müssen.

Verzicht auf Verfügungsbefugnis der Aufsichtsstelle (Art. 37 KDSG)

Gemäss Art. 36 KDSG kann die Aufsichtsstelle den öffentlichen Organen Empfehlungen zur Bearbeitung von Personendaten geben. Sofern ein öffentliches Organ erklärt, der Empfehlung der Aufsichtsstelle nicht folgen zu wollen oder ihr tatsächlich nicht folgt, kann die Aufsichtsstelle die Empfehlung oder Teile davon gestützt auf Art. 37 KDSG in der Form eines anfechtbaren Entscheids erlassen. Es wird von einigen Vernehmlassungsteilnehmenden beantragt, diese Verfügungsbefugnis zu streichen. Namentlich sei sie nicht zielführend und wird als Misstrauensvotum gegenüber den öffentlichen Organen verstanden. Zudem wird es als sachfremd und in der bündnerischen Rechtsordnung bisher unbekannt empfunden, wenn diese Entscheide beim Obergericht angefochten werden können und somit Gerichtsprozess zweier kantonaler öffentlicher Organe möglich sind.

Gemäss den völkerrechtlichen Vorgaben muss die Aufsichtsstelle die Möglichkeit haben, Entscheide auszustellen (Art. 15 Abs. 2 lit. c Übereinkommen SEV 108) bzw. die Verantwortlichen anzuweisen, Verarbeitungsvorgänge, gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums, mit den nach dieser Richtlinie erlassenen Vorschriften in Einklang zu bringen (Art. 47 RL 2016/680). Aufgrund des Wortlauts der entsprechenden Be-

stimmungen muss dieses Recht zwingend der Aufsichtsstelle zustehen. Eine Weisung durch die Regierung auf Antrag der Aufsichtsstelle, wie bisher in Art. 6 Abs. 3 des bestehenden KDSG vorgesehen, erfüllt diese Vorgaben nicht. Auch in anderen Kantonen wird das Völkerrecht dadurch umgesetzt, dass die Aufsichtsstelle gegenüber den betroffenen Organen als ultima ratio verfügen oder auf ähnliche Weise verbindliche Anordnungen treffen kann. Ebenfalls zwingend vorzusehen ist eine Anfechtungsmöglichkeit der Verfügungen vor einer gerichtlichen Behörde (Art. 53 RL 2016/680, Art. 15 Übereinkommen SEV 108). Auch wenn Gerichtsprozesse zwischen kantonalen Verwaltungsbehörden im kantonalen Recht nicht Usus sind, empfiehlt der KdK-Leitfaden das kantonale Verwaltungs- bzw. Obergericht als Beschwerdeinstanz. Alternativ könnte die Regierung als Beschwerdeinstanz vorgesehen werden. Da deren Entscheide an das Obergericht weitergezogen werden könnten, wären die Vorgaben des Völkerrechts ebenfalls erfüllt. Gegen eine solche Lösung sprechen Unabhängigkeitsüberlegungen (vgl. Beat Rudin, Bruno Baeriswyl, Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Basel-Stadt, § 47, N. 9). Daher wird im Kanton Graubünden – wie in der Mehrheit der Kantone – grundsätzlich der Rechtsweg zum kantonalen Obergericht vorgesehen.[3] Insofern das Obergericht Adressat von Entscheiden der Aufsichtsstelle ist (vgl. aber Art. 30 Abs. 2), kann es über diese Entscheide nicht auch noch als Rechtsmittelinstanz befinden. Daher soll bei Entscheiden der Aufsichtsstelle, welche das Obergericht betreffen, das Justizgericht (vgl. Art. 63 ff. Gesetz über die Verwaltungsrechtspflege [VRG; BR 370.100]) zuständig sein.

Ausweitung der Strafbestimmungen (Art. 40 KDSG)

Art. 40 KDSG sieht vor, dass gewisse Verstösse gegen die Regelungen dieses Gesetzes mit Busse bestraft werden können. Die Bestimmung konkretisiert die bis anhin sehr unbestimmt gehaltene Strafbestimmung in Art. 10a des bestehenden KDSG. Sie orientiert sich an Regelungen anderer Kantone. Gewissen Vernehmlassungsteilnehmenden gehen diese Straftatbestände zu wenig weit. Sie erachten es als fragwürdig, dass die öffentlichen Organe neu von der Geltung dieser Strafbestimmung ausgenommen seien.

Die Strafbestimmung in Art. 40 KDSG soll es ermöglichen, Verstösse gegen das Datenschutzrecht zu sanktionieren. Insofern auf die bestehende Strafbestimmung verwiesen wird, ist fraglich, ob diese Formulierung dem Legalitätsprinzip genügt. Mit dem bestehenden Wortlaut ist es für die Be-

[3] Im Kanton Graubünden wird das fachlich zuständige, kantonale Verwaltungsgericht im Rahmen der Justizreform 3 auf den 1. Januar 2025 mit dem Kantonsgericht zu einem einzigen Obergericht fusionieren. Innerhalb des Obergerichts wird diejenige Abteilung für die betreffenden Fälle zuständig sein, welche mit der Bearbeitung der verwaltungsrechtlichen Fälle betraut ist.

troffenen kaum absehbar, welches Verhalten unter Strafe steht. Auch wenn die neue Bestimmung nur noch konkrete Verhaltensweisen sanktionieren wird, bedeutet dies nicht, dass andere Fehlverhalten für das öffentliche Organ oder die handelnde Person folgenlos bleiben. Einerseits kann die Aufsichtsstelle bei Verletzungen von Bestimmungen des Datenschutzes gegenüber den Verwaltungseinheiten Änderungen an der Datenbearbeitung oder deren Abbruch empfehlen bzw. verfügen. Anderseits können die entsprechenden Fehlverhalten (z.B. bei einer Verletzung des Amtsgeheimnisses) personalrechtlich oder strafrechtlich bereits nach dem geltenden Recht wirksam anderweitig geahndet werden. Es wird daher in den meisten Kantonen davon abgesehen, eine zusätzliche Möglichkeit zur Sanktionierung der öffentlichen Organe oder Mitarbeitenden zu statuieren. Dies wird auch damit begründet, dass Bussen innerhalb der Verwaltung, d.h. innerhalb desselben Budgets, nur begrenzt Sinn machen.

Verbot der biometrischen Überwachung

Zwei Teilnehmende bringen vor, dass die Verwendung biometrischer Erkennungssystemen (z.B. Gesichtserkennungssoftware) immer häufiger werde. Der Einsatz solcher Systeme im öffentlich zugänglichen Raum ermögliche eine biometrische Massenüberwachung. Dabei bestehe nur wenig Transparenz darüber, wo und von wem biometrische Erkennungssysteme eingesetzt werden. Das KDSG definiere biometrische Daten neu als besonders schützenswert, wenn sie eine natürliche Person eindeutig identifizieren. Über die mit dieser Kategorisierung verbundenen Konsequenzen (z.B. betreffend Anforderungen an die rechtliche Grundlage) hinausgehende Vorgaben an die biometrische Überwachung statuiere das Gesetz nicht. Bei der biometrischen Überwachung handle es sich um nicht verhältnismässige Eingriffe in die Grund- und Menschenrechte. Es wird daher bedauert, dass mit der Totalrevision des KDSG die Gelegenheit nicht genutzt wird, um biometrische Überwachung (konkret Gesichtserkennung) zu regulieren und biometrische Erkennungssysteme im öffentlich zugänglichen Raum zu verbieten.

Es wird grundsätzlich anerkannt, dass die biometrische Überwachung (namentlich im Zusammenhang mit der automatisierten Gesichtserkennung) für die Betroffenen einen schweren Eingriff in ihre Privatsphäre darstellen kann. Bisher wurden in verschiedenen Kantonen sowie beim Bund parlamentarische Anfragen zum Verbot der biometrischen Überwachung lanciert. Die damit beauftragten Kantonsregierungen bzw. der Bundesrat führten zu deren Beantwortung namentlich aus, dass eine biometrische Überwachung mit den bestehenden Rechtsgrundlagen nicht zulässig sei. Aufgrund der Klassifizierung als besonders schützenswerte Personendaten müsste für die Einführung entsprechender Überwachungsmassnahmen eine Grundlage in einem Gesetz geschaffen werden, an deren Konkretisierung zudem

in Anlehnung an die aktuelle Rechtsprechung des Bundesgerichts zur automatischen Fahrzeugfahndung hohe Anforderungen gestellt werden müssten (vgl. BGE 146 I 11). Ausserdem muss der Eingriff in die Grundrechte mittels biometrischer Überwachung durch ein hinreichendes öffentliches Interesse gerechtfertigt und verhältnismässig sein. Auch in der Lehre wird ein explizites, gesetzliches Verbot des staatlichen Einsatzes von maschineller Gesichtserkennung als nicht notwendig erachtet (vgl. Braun Binder/Kunz/Obrecht, Maschinelle Gesichtserkennung im öffentlichen Raum, in: sui generis 2022, Rz. 36). Zudem würde ein allgemeines Verbot nicht zu mehr Rechtssicherheit führen, da spezialgesetzliche Ausnahmen nach den strengen, hiervor genannten Anforderungen weiterhin möglich wären. Basierend auf die entsprechenden Ausführungen wurden die entsprechenden parlamentarischen Anfragen in der Regel abgelehnt, weil kein Rechtssetzungsbedarf erkannt wurde.[4] Die in anderen Kantonen vorgebrachte Begründung erscheint überzeugend, weswegen im Kanton Graubünden auf ein entsprechendes Verbot im Rahmen der Datenschutzgesetzgebung verzichtet werden soll.

III. Erläuterungen zu den einzelnen Bestimmungen

1. Kantonales Datenschutzgesetz

Art. 1 Zweck

Wie bis anhin bereits in Art. 1 des geltenden KDSG festgelegt, dient das Gesetz dem Schutz von (natürlichen und juristischen) Personen vor widerrechtlichem Bearbeiten von Personendaten durch öffentliche Organe. Die Zweckbestimmung erfährt gegenüber dem geltenden Recht nur redaktionelle Änderungen.

Art. 2 Geltungsbereich

Dieser Artikel regelt den Geltungsbereich des KDSG. Das Gesetz gilt wie bis anhin für die Bearbeitung von Personendaten durch öffentliche Organe. Beibehalten werden soll die Ausnahme vom Geltungsbereich, sofern öffentliche Organe am wirtschaftlichen Wettbewerb teilnehmen und dabei nicht hoheitlich handeln. In diesen Fällen haben sich die öffentlichen Organe bei ihren Datenbearbeitungen nach den Vorgaben für Private gemäss dem DSG des Bundes zu richten. Die öffentlichen Organe werden dadurch

[4] Lediglich im Kanton Basel-Landschaft wurde eine Motion (Verbot von biometrischer Überwachung im Kanton Basel-Landschaft, Nr. 2023/205) angenommen, welche vom Regierungsrat den Erlass eines Verbots von biometrischer Überwachung und die Vornahme der dafür notwendigen Gesetzesanpassungen fordert. Ein allfälliges daraus ergebendes Gesetzgebungsprojekt ist aber im jetzigen Zeitpunkt noch nicht vorliegend.

jedoch nicht zu Privatpersonen. Um eine einheitliche Aufsicht zu gewährleisten, sollen diese Organe grundsätzlich auch im privatrechtlichen Tätigkeitsbereich umfassend durch die Aufsichtsstelle beaufsichtigt werden. Eine Ausnahme gilt für diejenigen Organe, welche ausschliesslich am wirtschaftlichen Wettbewerb teilnehmen und dabei privatrechtlich handeln (vgl. oben II.2.1). Die nach altem Recht in Art. 1 Abs. 5 lit. b des geltenden KDSG statuierte Ausnahme für Personendaten, welche in einem öffentlichen Archiv archiviert sind, wird nicht mehr benötigt. Hier gehen die einschlägigen Bestimmungen des inzwischen erlassenen GAA als materielles Datenschutzrecht vor (vgl. Art. 2 Abs. 4 GAA). Weitere Ausschlussgründe galten bisher aufgrund des Verweises auf das Bundesrecht (Art. 1 Abs. 4 des bestehenden KDSG). Die auf diese Weise übernommenen Ausschlussgründe in Art. 2 Abs. 2 DSG (privater Gebrauch, institutionelle Begünstigte) sind im Zusammenhang mit der Bearbeitung durch öffentliche Organe nur zum Teil einschlägig und werden im Rahmen der Revision nicht übernommen. Gemäss Völkerrecht dürfen keine generellen Ausnahmen vom Geltungsbereich des Datenschutzgesetzes mehr für Verfahren der Zivil-, der Straf- und der gerichtlichen Verwaltungsrechtspflege sowie Rechtshilfeverfahren vorgesehen werden. Dies bedeutet nicht, dass die Prozessordnungen nicht mehr gelten. Die entsprechenden Regelungen in diesen Gesetzen z.B. der Schweizerischen Strafprozessordnung [StPO; SR 312.0]) behalten als bereichsspezifisches Datenschutzrecht Geltung und gehen dem KDSG vor. Die Grundsätze des Datenschutzgesetzes gelten jedoch subsidiär. Art. 2 Abs. 3 KDSG übernimmt die Formulierung des Bundesgesetzes (Art. 2 Abs. 3 DSG) weitgehend. Zusätzlich zur Regelung auf Bundesebene müssen im KDSG die Verfahren der Verwaltungsrechtspflege erwähnt werden, in denen sich die Rechte nach dem VRG richten. Für erstinstanzliche Verwaltungsverfahren richtet sich davon abweichend die Datenbearbeitung wie bis anhin nur nach den Regeln des KDSG.

Art. 3 Begriffe

Durch den Verzicht auf die dynamischen Verweise ist neu auch im KDSG eine Bestimmung mit den wichtigsten Legaldefinitionen einzufügen. Diese orientiert sich weitestgehend an der Bestimmung im Bundesrecht (Art. 5 DSG). Folgende Definitionen sind abweichend vom Bundesrecht gewählt:

– In Abs. 1 wird definiert, was unter einem öffentlichen Organ zu verstehen ist. Dadurch wird der sachliche Geltungsbereich des Gesetzes umschrieben. Dieser wird von den Begrifflichkeiten her an das Gesetz über das Öffentlichkeitsprinzip (KGÖ; BR 171.000) angeglichen. Daraus ergibt sich keine Änderung der Rechtslage. Wie nach geltendem Recht richtet sich das Gesetz an die Behörden des Kantons, der Regionen und der Gemeinden sowie deren Anstalten, Stiftungen und Körperschaften.

Darunter sind beispielsweise auch die Bürgergemeinden und die Kirchgemeinden zu verstehen. Ebenfalls gilt das Gesetz für Private, welche ihnen übertragene öffentliche Aufgaben erfüllen.

– Abs. 2 definiert den Begriff der Personendaten. Er weicht vom Bundesrecht ab, indem das KDSG weiterhin sowohl die Daten natürlicher als auch juristischer Personen schützen wird. Eine Aufhebung der Anwendbarkeit des KDSG auf die Daten juristischer Personen hätte aufgrund des Legalitätsprinzips zur Folge, dass sämtliche Regelungen des materiellen Datenschutzrechts, die Daten juristischer Personen nicht mehr umfassen. Um diese Daten weiterhin bearbeiten zu können, müssten neue gesetzliche Grundlagen geschaffen werden. Dies hat beim Bund und bei anderen Kantonen zur Schaffung neuer Gesetzesgrundlagen (z.B. im Regierungs- und Verwaltungsorganisationsgesetz [RVOG; SR 172.010]) geführt, welche allerdings weitgehend mit den Regelungen des Datenschutzgesetzes übereinstimmen. Die daraus entstehende parallele Gesetzgebung ist nicht anwenderfreundlich und trägt nicht zum Schutz der juristischen Personendaten bei. Daher soll das KDSG weiterhin auch die Daten juristischer Personen schützen. Der Schutz juristischer Personendaten wurde auch in anderen Kantonen beibehalten.
– Abs. 9 definiert die Auftragsbearbeiterin oder den Auftragsbearbeiter. Diese Regelung wird grundsätzlich aus dem Bundesrecht übernommen, welches Private oder Bundesorgane als Auftragsbearbeitende vorsieht. Im kantonalen Recht würde eine Einschränkung auf öffentliche Organe (gemäss der Definition in Art. 3 Abs. 1) bedeuten, dass Bundesorgane als Auftragnehmende nicht in Frage kommen. Es sind indes Konstellationen denkbar, in denen ein kantonales öffentliches Organ eine Datenbearbeitung an ein Bundesorgan auslagert. Auch hierbei sind die Vorgaben von Art. 9 KDSG zu erfüllen. Daher sollen als Auftragsbearbeitende grundsätzlich Dritte verstanden werden, welche Daten im Auftrag einer oder eines Verantwortlichen bearbeiten. Bei den Dritten kann es sich dabei sowohl um Private als auch um öffentliche Organe (des Bundes, des Kantons, einer Gemeinde) handeln.

Im Weiteren wird der Katalog der besonders schützenswerten Personendaten an das Bundesrecht bzw. die völkerrechtlichen Vorgaben angeglichen und umfasst neu auch genetische Daten und biometrische Daten, welche eine Person eindeutig identifizieren. Im Vergleich zum alten Recht muss zusätzlich das «Profiling» geregelt werden. Im Gegensatz zum Bundesrecht wird der Begriff des Persönlichkeitsprofils (Art. 3 lit. d aDSG) vorliegend beibehalten. Der Grund hierfür ist, dass der Begriff in Fachgesetzen verwendet wird und dort nicht eins zu eins durch das Profiling ersetzt werden kann (vgl. etwa Art. 24 Bürgerrechtsgesetz des Kantons Graubünden [KBüG; BR 130.100]).

Art. 4 Verantwortlichkeit

Die Zuweisung der datenschutzrechtlichen Verantwortlichkeit ist ein zentraler Pfeiler des Datenschutzrechts. Gemäss Abs. 1 ist für den Datenschutz dasjenige öffentliche Organ verantwortlich, welches allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung entscheidet. Hiermit wird die Definition der oder des Verantwortlichen aus dem Bundesrecht (Art. 5 lit. j DSG) übernommen. Bei der gemeinsamen Bearbeitung durch mehrere Organe ist die Verantwortlichkeit unter diesen zu regeln. Aufgrund der Vorgaben des übergeordneten Rechts muss das öffentliche Organ künftig auf Verlangen die Einhaltung der Datenschutzbestimmungen gegenüber der Aufsichtsstelle nachweisen können. Auf welche Weise dies erbracht werden kann, wird auf Verordnungsstufe definiert (vgl. unten IV.).

Art. 5 Grundsätze

Art. 5 hält die wichtigen Grundsätze der Datenbearbeitung fest. Bisher statuiert Art. 2 Abs. 1 des geltenden KDSG, dass das Bearbeiten von Personendaten die Grundsätze der Rechtmässigkeit, der Verhältnismässigkeit, der Zweckmässigkeit, der Zweckgebundenheit, der Richtigkeit und der Datensicherheit zu beachten hat. Die Konkretisierung der genannten Grundsätze sowie die Übernahme allfälliger weiterer Prinzipien erfolgt aufgrund des Verweises in Art. 2 Abs. 2 des bestehenden KDSG durch das Bundesrecht. Mit dem Wegfall des Verweises werden die Grundsätze neu eigenständig im Gesetz verankert. Die Umschreibung der Grundsätze wird aus Art. 6 DSG übernommen. Allfällige Anpassungen gegenüber dem aDSG sind terminologischer Natur und führen nicht zu einer Änderung der Rechtslage.

Art. 6 Datensicherheit

Es obliegt dem verantwortlichen öffentlichen Organ bzw. den Auftragsbearbeitenden, durch geeignete technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit zu gewährleisten. Die entsprechende Bestimmung wurde weitgehend aus dem Bundesrecht übernommen (Art. 2 Abs. 2 des geltenden KDSG i.V.m. Art. 8 DSG). Abs. 2 bestimmt, dass das Ziel der Massnahmen die Vermeidung von Verletzungen der Datensicherheit sein muss. Woraus die technischen und organisatorischen Massnahmen im jeweiligen Einsatzbereich bestehen, basiert wie im Bundesrecht auf einem risikobasierten Ansatz. Je grösser das Risiko einer Verletzung der Datensicherheit ist, umso höher sind die Anforderungen an die zu treffenden Massnahmen. In Abs. 3 wird die Regierung ermächtigt, die Mindestanforderung auf Verordnungsstufe zu konkretisieren. Bisher galten gestützt auf die dynamischen Verweise die einschlägigen Bestimmungen in

der Verordnung über den Datenschutz des Bundes (DSV; SR 235.11).[5] Die DSV sieht in diesem Zusammenhang gewisse Vorgaben vor, welche nicht vom Völkerrecht vorgeschrieben sind und für die öffentlichen Organe einen beträchtlichen Mehraufwand bedeuten können (z.B. Führung eines Bearbeitungsreglements, umfassende Vorgaben an die Protokollierung). Diese Vorgaben wurden bisher nicht in dieser Weise umgesetzt und erweisen sich für die öffentlichen Organe im Kanton Graubünden nicht in jedem Fall als zweckmässig. Nach dem soeben Ausgeführten und basierend auf den Regelungen in anderen Kantonen können die völkerrechtlichen Vorgaben auch auf andere als in der DSV vorgesehen Weise erfüllt werden. Auf Verordnungsstufe wird indes wie in anderen Kantonen vorgesehen, dass die öffentlichen Organe zur Sicherstellung der Datensicherheit dem Schutzbedarf der bearbeiteten Daten, der Einschätzung der möglichen Risiken für die betroffenen Personen sowie dem Stand der Technik und den Implementierungskosten angemessene technische und organisatorische Massnahmen treffen müssen (weitere Ausführungen weiter unten, IV.).

Art. 7 Bearbeitung von Personendaten

Die Bearbeitung von Personendaten durch öffentliche Organe ist wie bisher in erster Linie gestützt auf eine Rechtsgrundlage zulässig. Dabei wird die einschlägige Bestimmung des DSG weitgehend übernommen (Art. 34 DSG). Das Bündner Recht kennt jedoch die dort verwendeten Begriffe des Gesetzes im formellen und materiellen Sinn nicht. Daher soll im KDSG von Gesetz (formell) resp. Verordnung (materiell) gesprochen werden, sodass die Einheit der Rechtsordnung des Kantons gewährleistet wird. Die Rechtsgrundlage kann einerseits als ausdrückliche Verpflichtung oder Ermächtigung zu einer bestimmten Datenbearbeitung vorliegen (sog. unmittelbare gesetzliche Grundlage, vgl. etwa Art. 24 KBüG, welcher die zuständigen Behörden explizit zur Bearbeitung von Daten bemächtigt). Im Vergleich zur Formulierung von Art. 34 DSG soll klargestellt werden, dass für eine Datenbearbeitung grundsätzlich auch ausreichen kann, wenn die Bearbeitung zur Erfüllung einer in einem Gesetz festgeschriebenen Aufgabe unentbehrlich ist (sog. mittelbare gesetzliche Grundlage, vgl. etwa Art. 130a des Steuergesetzes für den Kanton Graubünden [StG; BR 720.000]). Entsprechende mittelbare gesetzliche Grundlagen sind auf Kantons- und Gemeindeebene relevanter und verbreiteter als im Bundesrecht. Durch die explizite Nennung soll diese Möglichkeit im Gesetz deutlicher hervorgehoben werden. Abs. 2 regelt, in welchen Fällen aufgrund des Schutzbedarfs der betroffenen Daten zwingend eine Grundlage in einem Gesetz notwendig ist. In Ausnahme von

[5] Bzw. bis zum 1. September 2023 in der Verordnung zum Bundesgesetz über den Datenschutz vom 14. Juni 1993 (VDSG; SR 235.11).

Abs. 2 soll eine Grundlage auf Verordnungsstufe genügen, wenn die in Abs. 3 statuierten Voraussetzungen kumulativ erfüllt sind. Aufgrund der expliziten Verankerung der mittelbaren gesetzlichen Grundlage in Abs. 1 (vgl. oben II.2.1) musste Abs. 3 gegenüber der Vernehmlassungsvorlage angepasst werden. Eine Abweichung von Abs. 2 erfordert daher, dass die Aufgabe, auf welche sich die Bearbeitung stützt, im Gesetz ausdrücklich umschrieben sein muss und der Bearbeitungszweck für die Grundrechte keine besonderen Risiken birgt. Verzichtet wird künftig darauf, dass die Regierung eine Datenbearbeitung ohne Gesetzesgrundlage bewilligen kann, wenn sie die Rechte der betroffenen Person für nicht gefährdet hält. Diese Ausnahme wurde soweit ersichtlich bisher nie angewendet. Abs. 4 sieht vor, dass auf eine gesetzliche Grundlage verzichtet werden kann, wenn die betroffene Person im Einzelfall ihre rechtmässige Einwilligung (vgl. Art. 5 Abs. 6 und 7) gibt, oder wenn sie ihre Personendaten allgemein zugänglich gemacht und die Bearbeitung nicht ausdrücklich untersagt hat. Neu wird in Übereinstimmung mit dem internationalen Recht eine Ausnahme vorgesehen, wenn die Bearbeitung notwendig ist, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen und es nicht möglich ist, die Einwilligung der Person innert angemessener Frist einzuholen. Es gilt zu beachten, dass diese Ausnahmen nur für den Einzelfall gelten und keine andauernde Datenbearbeitung ohne Gesetzesgrundlage rechtfertigen.

In Bezug auf das alte Recht ergeben sich einzelne Änderungen und Konkretisierungen. Da neu das Profiling (vgl. oben Art. 3) als besonders schützenswerte Art der Datenbearbeitung geregelt wird, erfordert es eine Grundlage in einem Gesetz. Zudem wird in Übereinstimmung mit der Regelung des Bundes ein Auffangtatbestand für Datenbearbeitungen geschaffen, welche weder ein Profiling noch ein Persönlichkeitsprofil sind, aber aufgrund des Bearbeitungszwecks oder der Art und Weise dennoch zu einem schwerwiegenden Eingriff in die Grundrechte der betroffenen Person führen können.

Art. 8 Automatisierte Datenbearbeitung im Rahmen von Pilotversuchen

Bereits nach geltendem Recht kann gestützt auf Art. 35 DSG die automatisierte Datenbearbeitung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen im Rahmen von Pilotversuchen von gewissen Erleichterungen insbesondere hinsichtlich der gesetzlichen Grundlagen profitieren. Die Bestimmung ermöglicht es, gewisse Bearbeitungstätigkeiten vor Erlass einer formellen gesetzlichen Grundlage zu erproben. So kann die Zweckmässigkeit und Notwendigkeit der Bearbeitungstätigkeit und der Regelungsbedarf bestimmt werden. Dies trägt dem Umstand Rechnung, dass der Gesetzgebungsprozess in der Regel zwei Jahre dauert. Somit kann es vorkommen, dass ein Regelungsentwurf aufgrund technischer Entwick-

lungen bereits veraltet ist und den effektiven Bedürfnissen nicht mehr entspricht. Gerade im Hinblick auf die Intensivierung der Digitalisierung der Verwaltung soll diese Möglichkeit beibehalten werden. Die Bestimmung in Art. 35 DSG wird dabei sinngemäss übernommen. Auf Verordnungsstufe wird definiert, wann ein solcher Pilotversuch unentbehrlich ist und weitere Ausführungen zum Verfahren gemacht.

Art. 9 Bearbeitung durch Auftragsbearbeiterin oder Auftragsbearbeiter

Art. 9 regelt die Bearbeitung durch eine Auftragsbearbeiterin oder einen Auftragsbearbeiter. Das sogenannte «Outsourcing» ist in der Praxis von grosser Wichtigkeit, da z.B. bereits das Speichern von Daten auf einem Clouddienst als Datenbearbeitung gilt (vgl. Art. 3 Ziff. 6 KDSG). Im geltenden Recht wird im Wesentlichen auf die Regelungen des Bundes verwiesen (Art. 9 DSG). In Art. 3 Abs. 2 des bestehenden KDSG ist zusätzlich vorgesehen, dass wer Personendaten im Auftrag einer Behörde bearbeitet, zu deren Bekanntgabe an Dritte der ausdrücklichen Zustimmung der Auftraggebenden bedarf. Durch diese Bestimmung wird die völkerrechtliche Vorgabe, dass bei der Übertragung der Bearbeitung der Auftragsbearbeiterin oder des Auftragsbearbeiters an Dritte (sog. «Subcontracting») eine vorgängige Genehmigung notwendig ist, bereits erfüllt. Das geltende Recht wird daher im Wesentlichen übernommen. Dementsprechend kann die Bearbeitung von Personendaten vertraglich oder durch Gesetz einer Auftragsbearbeiterin oder einem Auftragsbearbeiter übertragen werden, wenn die Daten so bearbeitet werden, wie das verantwortliche öffentliche Organ selbst es tun dürfte und keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet.

An dieser Stelle soll noch auf das Verhältnis von Art. 9 KDSG zu Art. 7 des Gesetzes über die digitale Verwaltung (DVG; BR 177.100) hingewiesen werden. Diese Bestimmung statuiert Vorgaben an die Auslagerung von Datenbearbeitungen und die Verwaltung von Informatiklösungen durch Dritte. Art. 7 DVG muss als Mindestvorgabe für alle Auslagerungen durch Kantonale Verwaltungsbehörden erfüllt werden. Art. 9 KDSG gilt hingegen für alle öffentlichen Organe gemäss den Vorgaben dieses Gesetzes. Er ist in seinem Geltungsbereich jedoch enger, da er nur dann einschlägig ist, wenn Personendaten bearbeitet werden. Art. 7 Abs. 1 lit. a DVG verweist auf die Regelungen der Datenschutzgesetzgebung, welche bei der Auslagerung zu beachten sind. Die konkreten Vorgaben an den Datenschutz ergeben sich dann aus Art. 9 KDSG. Sowohl Art. 7 DVG als auch Art. 9 KDSG verlangen eine Grundlage für die Bearbeitung (z.B. in der Form einer gesetzlichen Regelung oder eines Vertrags). Was diese Grundlage beinhalten muss, wird auf Verordnungsstufe konkretisiert (vgl. bereits Art. 2 Verordnung zum Gesetz über die digitale Verwaltung [VDVG; BR 177.110]). Es wird davon aus-

gegangen, dass aufgrund der bestehenden datenschutzrechtlichen Vorgaben die von den öffentlichen Organen abgeschlossenen Verträge ein genügendes Schutzniveau sicherstellen und kein unmittelbarer Handlungsbedarf zu deren Anpassung besteht. Daher erscheint es sachgerecht, dass bestehende Vereinbarungen nicht sofort mit dem Inkrafttreten angepasst werden müssen. In der Verordnung wird eine entsprechende Bestimmung vorgesehen (analog zu Art. 24 VDVG).

Art. 10 Bekanntgabe von Personendaten 1. Allgemeine Vorgaben

Art. 10 regelt die allgemeinen Voraussetzungen unter welchen öffentliche Organe Personendaten bekannt geben dürfen. Es wird das Bundesrecht (Art. 36 DSG) weitgehend übernommen, wodurch sich nur geringe Änderungen zur alten Rechtslage ergeben. Wie bis anhin ist für die Bekanntgabe von Personendaten in erster Linie eine Rechtsgrundlage notwendig. An diese sind dieselben Anforderungen zu stellen wie hinsichtlich der Bearbeitung (vgl. oben Art. 7). Dies bedeutet auch, dass je nach Art und Weise der Bekanntgabe eine Grundlage in einem Gesetz vorzusehen ist. Die Ausnahmen vom Erfordernis einer Rechtsgrundlage im Einzelfall sind in Abs. 2 abschliessend geregelt und übernehmen den Ausnahmenkatalog des DSG. Neu ist eine Ausnahme vorgesehen, wenn die Bearbeitung notwendig ist, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen (vgl. bereits Art. 7).

Die Möglichkeit der öffentlichen Organe gewisse Stammdaten auf Anfrage an Dritte bekannt zu geben, soll beibehalten werden (vgl. oben 2.2.). Abs. 4 vermerkt, dass bei der Bekanntgabe von Personendaten aus Gründen der Verhältnismässigkeit in jedem Fall eine Interessensabwägung durchzuführen ist. Die Bekanntgabe ist abzulehnen, einzuschränken oder mit Auflagen zu verbinden, wenn wesentliche öffentliche Interessen oder offensichtlich schutzwürdige Interessen der betroffenen Person bzw. eine gesetzliche Geheimhaltungspflicht oder besondere Datenschutzvorschrift es verlangt. Dies gilt auch für die Stammdaten, welche je nach Sachverhalt durchaus sensible Informationen über eine Person beinhalten. In Übereinstimmung mit dem Bundesrecht werden keine spezifischen Vorgaben mehr an die Bekanntgabe durch Abrufverfahren gemacht (Art. 19 Abs. 3 aDSG). Diese Bestimmung erscheint im digitalen Zeitalter überholt. Auch bei Abrufverfahren sind weiterhin die Vorgaben an die Rechtsgrundlage zu erfüllen. Dies bedeutet, dass wenn ein Abrufverfahren (z.B. aufgrund der Art und Weise der Datenbearbeitung) zu einem schwerwiegenden Eingriff führt, eine Grundlage in einem Gesetz notwendig ist. Die bereichsspezifischen Datenschutzbestimmungen, welche ein Abrufverfahren vorsehen, können bestehen bleiben und als Gesetzesgrundlage für entsprechende Bekanntgaben dienen (vgl. etwa Art. 27a Polizeigesetz des Kantons Graubünden [PolG; BR 613.000]).

Art. 11 2. Bekanntgabe von Personendaten im Rahmen der behördlichen Informationstätigkeit

Art. 11 befasst sich mit der Bekanntgabe von Daten im Rahmen der aktiven behördlichen Informationstätigkeit. Verschiedene Kantone regeln diesen Aspekt vertieft in ihren Informations- und Datenschutzerlassen oder sogar in einem separaten Gesetz. Der Kanton Graubünden hat sich im Rahmen des Erlasses des KGÖ gegen einen solchen Ansatz entschieden. Das KGÖ umfasst lediglich die behördliche Information auf Anfrage (passive Informationstätigkeit). Da auch im Rahmen der aktiven behördlichen Informationstätigkeit Personendaten bekannt gegeben werden können (z.B. Namen von Ansprechpersonen in der Verwaltung oder Kommissionsmitgliedern), soll dieser Aspekt im vorliegenden Gesetz geregelt werden. Dabei wird die bestehende Regelung aus Art. 36 Abs. 3 und Abs. 5 DSG übernommen. Sie wird aus Gründen der Übersichtlichkeit in einem eigenen Artikel überführt werden. Materiell werden die bisherigen Bestimmungen beibehalten. Die Bekanntgabe von Personendaten im Rahmen der aktiven behördlichen Informationstätigkeit ist zulässig, wenn die Daten im Zusammenhang mit der Erfüllung öffentlicher Aufgaben stehen und an der Bekanntgabe ein überwiegendes öffentliches Interesse besteht. Gemäss Abs. 2 dürfen die Daten über automatisierte Informations- und Kommunikationsdienste (z.B. Internet oder soziale Medien) nach Abs. 1 oder gestützt auf eine eigene Rechtsgrundlage allgemein zugänglich gemacht werden. Die Daten sind zu löschen, wenn daran kein öffentliches Interesse mehr besteht. Der Schutz von Personendaten im Rahmen von Verfahren der passiven Informationstätigkeit (auf Anfrage) ist in Art. 10 ff. KGÖ geregelt. Im Gegensatz zum Bundesgesetz über die Öffentlichkeit (BGÖ; SR 152.3) wird im KGÖ nicht auf das anwendbare Datenschutzrecht verwiesen. Die Privatsphäre der betroffenen Personen wird im Gesuchverfahren jedoch durch Art. 11 KGÖ sichergestellt. Die dortige Bestimmung regelt die Behandlung entsprechender Gesuche abschliessend und hat sich bisher in der Praxis bewährt. Um die Koordination mit Verfahren nach dem KGÖ sicherzustellen wird in Art. 11 Abs. 3 DSG künftig explizit auf die Anwendbarkeit der entsprechenden Bestimmungen hingewiesen.

Art. 12 3. Grenzüberschreitende Bekanntgabe von Personendaten

Die grenzüberschreitende Bekanntgabe von Personendaten ist mit zusätzlichen Gefahren verbunden, weil nicht garantiert ist, dass die Daten im Empfängerstaat gleichwertigen Schutz geniessen. Art. 12 KDSG regelt die grenzüberschreitende Bekanntgabe von Personendaten in Orientierung an Art. 16 ff. DSG. Eine grenzüberschreitende Bekanntgabe ist nur zulässig, wenn die Gesetzgebung des betreffenden Staates oder das internationale Organ einen angemessenen Schutz gewährleistet. Auf Bundesebene obliegt

der Entscheid über ein angemessenes Datenschutzniveau dem Bundesrat (Art. 16 Abs. 1 DSG). Es erscheint sinnvoll, dass der Kanton Graubünden keine eigenen Einschätzungen vornimmt. Stattdessen wird er sich auf Verordnungsstufe den Regeln des Bundesrats anschliessen, welche in den Ausführungsbestimmungen zum DSG statuiert sind (vgl. Art. 8 ff. DSV). Sofern die Gesetzgebung eines Staates kein angemessenes Datenschutzniveau gewährleistet, muss der Schutz der Personendaten auf andere Weise gewährleistet werden können. Hierzu zählen z.B. völkerrechtliche Verträge oder Datenschutzklauseln in einem Vertrag zwischen den Vertragsparteien. Über das Vorliegen entsprechender Garantien hat das öffentliche Organ den Datenschutzbeauftragten zu informieren. Anderseits ist eine Bekanntgabe einzelfallbezogen bei Vorliegen der Vorgaben gemäss Art. 12 Abs. 2 lit. b bis g KDSG zulässig. Der entsprechende Katalog wurde aus dem Bundesrecht übernommen und entspricht bis auf sprachliche Klarstellungen der Rechtslage nach dem aDSG. Auf Verordnungsstufe wird (wie in anderen Kantonen) klargestellt, dass die Veröffentlichung von Personendaten im Rahmen der behördlichen Informationstätigkeit (vgl. Art. 11) nicht als Bekanntgabe ins Ausland gilt, auch wenn die entsprechenden Daten vom Ausland zugänglich sind.

Art. 13 Datenbearbeitung für nicht personenbezogene Zwecke

Art. 13 regelt unter welchen Voraussetzungen die Datenbearbeitung und -bekanntgabe zu nicht personenbezogenen Zwecken erleichtert werden kann. Die Bestimmung übernimmt Art. 39 DSG sinngemäss und sieht gegenüber dem alten Recht keine Neuerungen vor.

Art. 14 und 15 Bildüberwachung des öffentlichen und öffentlich zugänglichen Raums

Mit der Revision des PolG wurden 2018 im KDSG in Art. 3a und 3b Regelungen zur Bildüberwachung des öffentlichen Raums eingefügt. Die entsprechenden Regelungen haben sich in der Praxis grundsätzlich bewährt und sollen daher an dieser Stelle beibehalten werden. Zu beachten ist, dass es mit der bestehenden Formulierung möglich und unbestritten ist, Aufnahmen in einem Strafverfahren zu benutzten. Dieselben Aufnahmen könnten jedoch nicht benutzt werden, wenn sich aus derselben zugrundeliegenden Straftat zivilrechtliche Ansprüche ergeben (z.B. wenn diese gemäss Art. 126 Abs. 2 StPO auf den Zivilweg verwiesen werden). Es entspricht dem Schutzzweck der Norm und wird in anderen Kantonen ebenfalls vorgesehen, dass die Nutzung entsprechender Aufzeichnungen auch in diesem Fall über die Frist von 90 Tagen hinaus ermöglicht wird. Aufgrund der Rückmeldungen aus dem Vernehmlassungsverfahren werden darüber hinausgehend einige Anpassungen am Wortlaut vorgenommen, welche insbesondere den Schutz der Privat-

sphäre der betroffenen Personen verbessern sollen (vgl. oben 2.1). Zudem wird die Bestimmung an die neue Terminologie angepasst (z.B. öffentliches Organ statt Behörde).

Art. 16 Archivierung und Vernichtung

Die Vorgaben zur Archivierung und Vernichtung von Personendaten ergeben sich aktuell gestützt auf den dynamischen Verweis aus dem Bundesrecht. Art. 38 DSG wird sinngemäss angewendet. Gemäss dieser Bestimmung müssen öffentliche Organe dem Staatsarchiv die nicht mehr benötigten Personendaten anbieten. Vom Staatsarchiv als nicht archivwürdig bezeichnete Daten sind zu vernichten, es sei denn, diese werden anonymisiert oder müssen zu Beweis- oder Sicherheitszwecken oder zur Wahrung der schutzwürdigen Interessen der betroffenen Person aufbewahrt werden. Diese Regelung führt bei wortgemässer Umsetzung zu Rechtsunsicherheit. Einerseits besteht das Problem, dass es im Kanton nicht nur ein einziges Archiv gibt. Neben dem kantonalen Staatsarchiv führen die Regionen und Gemeinden eigene Archive mit eigenen Zuständigkeiten (vgl. Art. 12 GAA). Zudem sind Gesundheitsinstitutionen und Landeskirchen vom GAA nicht umfasst, so dass die entsprechenden Regelungen des KDSG für diese Institutionen ins Leere laufen. Diese Institutionen haben ebenfalls eigene Archivierungsregeln aufgestellt. Der Wortlaut von Art. 16 weicht aus diesen Gründen vom DSG ab. Demgemäss sind Personendaten, die nicht mehr benötigt werden, nach den dafür geltenden Vorschriften dem zuständigen Archiv anzubieten. Abs. 1 dient als Koordinationsnorm mit den jeweiligen Archivierungsregeln (z.B. im GAA). Abs. 2 regelt das Schicksal der als nicht archivwürdig befundenen Personendaten und übernimmt die Regelung des Bundes, wonach Daten aufbewahrt werden können, wenn sie anonymisiert sind oder zu Beweis- und Sicherheitszwecken bzw. zur Wahrung der Interessen der betroffenen Person aufbewahrt werden müssen.

Art. 17 Informationspflicht bei der Beschaffung von Personendaten

Art. 17 übernimmt im Wesentlichen den geltenden Art. 19 DSG. Die Bestimmung fordert, dass die betroffene Person grundsätzlich über die Beschaffung von Personendaten informiert werden muss. Die entsprechende Mitteilung muss die betroffene Person in die Lage versetzen, ihre Rechte nach dem Gesetz geltend zu machen und eine transparente Datenbearbeitung gewährleisten können. Die dazu mitzuteilenden Informationen sind in Abs. 2 geregelt. Zusätzlich zu den im Bundesrecht aufgelisteten Informationen, soll die betroffene Person explizit auf ihre Rechte hingewiesen werden (vgl. KdK-Leitfaden, S. 11). Die Form der entsprechenden Information wird auf Verordnungsstufe konkretisiert (vgl. unten IV.1).

Art. 18 Ausnahmen von der Informationspflicht und Einschränkungen

Art. 18 regelt, in welchen Fällen die Informationspflicht entfallen kann. Die Bestimmung übernimmt die Vorgaben von Art. 20 DSG, sofern sich diese nicht ausschliesslich an Private richten. Für öffentliche Organe kann die Informationspflicht entfallen, wenn die betroffene Person bereits über die entsprechenden Informationen verfügt oder die Bearbeitung gesetzlich vorgesehen ist. Letzteres ist aufgrund der Vorgabe von Art. 7 Abs. 1 KDSG bei staatlichem Handeln häufig der Fall. In denjenigen Fällen von Art. 7, wo die Datenbearbeitung nicht auf einer gesetzlichen Grundlage basiert, namentlich bei der Einwilligung in die Datenbearbeitung, ist die Person nach den Vorgaben von Art. 17 KDSG zu informieren. Sofern die Personendaten nicht bei der betroffenen Person beschafft werden, kann die Information zudem entfallen, wenn sie nicht möglich ist oder einen unverhältnismässigen Aufwand erfordert. Diese Ausnahme ist in Übereinstimmung mit dem Bundesrecht eng auszulegen. Im Weiteren kann das verantwortliche öffentliche Organ unter gewissen Voraussetzungen auf die Mitteilung von Informationen verzichten, diese einschränken oder aufschieben. Im Gegensatz zu Abs. 1 hat in diesen Konstellationen eine Interessenabwägung zu erfolgen. Die Einschränkung, der Aufschub oder der Verzicht kann nur soweit gehen, als dies durch die entgegenstehenden Interessen gerechtfertigt ist. Die Gründe für diese Einschränkung entsprechen denjenigen für die Einschränkung des Auskunftsrechts nach Art. 25 KDSG. Daher wird der Übersicht halber auf diese Bestimmung verwiesen.

Art. 19 Datenschutz-Folgenabschätzung

Art. 19 sieht vor, dass bei gewissen Datenbearbeitungsvorgängen vor der geplanten Bearbeitung eine Datenschutz-Folgenabschätzung (DSFA) zu erstellen ist. Diese Pflicht wurde im Bundesrecht neu mit Art. 22 DSG eingeführt. Das Instrument dient dazu, bereits in frühen Projektphasen Risiken für die betroffenen Personen zu erkennen und Massnahmen zu deren Bewältigung definieren zu können. Dies führt letztendlich dazu, dass der Datenschutz präventiv eingehalten werden kann und nicht zu einem späteren Zeitpunkt kostspielig nachgebessert werden muss. Eine DSFA ist immer dann vorzunehmen, wenn die vorgesehene Datenbearbeitung (basierend auf eine Vorabprognose des verantwortlichen öffentlichen Organs) voraussichtlich zu einem hohen Risiko für die Grundrechte der betroffenen Personen führt. Aufgrund der Rückmeldungen aus der Vernehmlassung soll das hohe Risiko neu auf Gesetzesstufe definiert werden. Die Definition wird dabei aus dem Bundesrecht (Art. 22 Abs. 2 DSG) übernommen. Ein hohes Risiko ergibt sich dabei, insbesondere bei der Verwendung neuer Technologien, aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung. Es liegt namentlich dann vor, wenn umfangreich besonders schützenswerte Perso-

nendaten bearbeitet werden oder wenn systematisch umfangreiche öffentliche Bereiche überwacht werden. Die öffentlichen Organe sollen sich bei der Beurteilung eines hohen Risikos insbesondere auf bestehende (z.B. des Bundes) oder noch durch die Aufsichtsstelle zu erarbeitende Risikoprüfungstools stützen können. Die Bestimmung regelt zudem den Mindestinhalt der Datenschutzfolgenabschätzung in Übereinstimmung mit dem Bundesrecht. Die Befassung mit Datenschutzaspekten im Frühstadium eines Projekts ist zumindest für Behörden der Kantonalen Verwaltung nicht vollständig neu. Gestützt auf die Weisung «IKT-Sicherheit in der Kantonalen Verwaltung Graubünden» (Weisung AFI-1083) müssen Dienststellen und Departemente bei der Einführung neuer Datenbearbeitungen eine Schutzbedarfsanalyse durchführen. Ergibt diese einen erhöhten Schutzbedarf, ist ein Informationssicherheits- und Datenschutz-Konzept (ISDS-Konzept) zu erstellen. Dieses beinhaltet insbesondere eine Risikoanalyse und allfällige zusätzliche Sicherheitsmassnahmen oder Restrisiken. Die entsprechenden Dokumente können der DSFA zugrunde gelegt werden und zudem dem Nachweis der Einhaltung der Datenschutzbestimmungen (vgl. Art. 4) dienen.

Art. 20 Vorabkonsultation

Die völkerrechtlichen Vorgaben verlangen, dass gewisse Bearbeitungsvorhaben vorab der Aufsichtsstelle zur Vorabkonsultation unterbreitet werden. Diese Verpflichtung ergibt sich aus der RL 2016/680 und könnte daher auch ausschliesslich für den Bereich der justiziellen und polizeilichen Zusammenarbeit umgesetzt werden. Jedoch haben – soweit ersichtlich – alle Kantone die Vorabkonsultation für das gesamte kantonale Verwaltungsrecht vorgesehen. Dies soll aufgrund des geringen Mehraufwands gegenüber der für alle Organe obligatorischen DSFA (vgl. oben 2.2) auch im Kanton Graubünden so gehandhabt werden. Das DSG des Bundes sieht die Vorabkonsultation in Art. 23 DSG vor. Diese Bestimmung wird weitgehend übernommen. Eine Vorabkonsultation ist durchzuführen, wenn die geplante Bearbeitung trotz der vom verantwortlichen öffentlichen Organ vorgesehenen Massnahmen ein hohes Risiko für die Grundrechte der betroffenen Person zur Folge hat. Durch die Vorabkonsultation soll sich die Aufsichtsstelle bereits vor der Einführung der in Frage stehenden Datenbearbeitung mit der datenschutzrechtlichen Problematik eines Projekts auseinandersetzen können. Grundsätzlich macht es Sinn, die oder den Datenschutzbeauftragten möglichst früh in den Prozess einzubeziehen. Daher wird auf Verordnungsstufe statuiert, dass auf eine Vorabkontrolle verzichtet werden kann, wenn die Aufsichtsstelle sich auf andere Weise (z.B. durch Mitwirkung in der Projektorganisation) zu den datenschutzrechtlichen Fragen äussern kann. Die Verpflichtung nach Art. 20 KDSG kann erfüllt werden, indem der oder dem Datenschutzbeauftragten zur Vorabkonsultation die Ergebnisse der DSFA

oder andere gleichwertige Dokumente vorzulegen sind. Nicht als zweckdienlich wird die im Bundesrecht vorgesehene gesetzliche Fixierung einer Bearbeitungsfrist erachtet. Kleine Vorabkonsultationen können durchaus rascher erledigt werden, während bei grossen Projekten eine Vorabkonsultation in verschiedenen Projektphasen gestaffelt stattfinden dürfte. Die Bearbeitung durch die Aufsichtsstelle hat aber «innert angemessener Frist» zu erfolgen, wobei die oder der Beauftragte sich bei der Bearbeitung an der im Bund und anderen Kantonen statuierten Frist von zwei Monaten orientieren soll.

Art. 21 Meldung von Verletzungen der Datensicherheit

Im Bundesrecht wurde mit der Revision aufgrund der Vorgaben des internationalen Rechts die Pflicht zur Meldung von Verletzungen der Datensicherheit eingeführt (Art. 24 DSG). Diese Bestimmung wird in Art. 21 übernommen. Das verantwortliche öffentliche Organ muss der Aufsichtsstelle so rasch als möglich jede Verletzung der Datensicherheit melden, die voraussichtlich zu einem hohen Risiko für die Grundrechte der betroffenen Person führt. Als Datenschutzverletzung gilt dabei eine Verletzung der Sicherheit, die dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden (vgl. Art. 3 Abs. 8). Auch die Angaben zum Mindestinhalt der Meldepflicht sowie das weitere Vorgehen werden aus dem Bundesrecht übernommen. Die Betroffenen sind zu informieren, wenn dies zu ihrem Schutz erforderlich ist oder wenn die Aufsichtsstelle dies verlangt. Von einer Meldung an die Betroffenen kann unter den in Abs. 5 genannten Voraussetzungen abgesehen werden. Im Gegensatz zum Bundesrecht wurde aus Gründen der Übersichtlichkeit auf eine Verweisung auf andere Bestimmungen verzichtet. Die Ausschlussgründe bleiben aber dieselben (insbesondere überwiegende öffentliche Interessen, Unmöglichkeit der Information, bestehende Geheimhaltungspflichten).

Art. 22 Verzeichnis der Bearbeitungstätigkeiten

Nach geltendem Recht ist die Aufsichtsstelle verpflichtet, ein öffentliches Register über die Datensammlungen zu führen. Zu diesem Zweck müssen die Behörden ihre Datensammlung der Aufsichtsstelle melden (Art. 4 Abs. 1 des bestehenden KDSG). Dieses Register wurde bisher nur rudimentär bewirtschaftet und aktuell gehalten, so dass seine Aussagekraft gering ist. Zumal die Betroffenenrechte bisher ohne das Register gewahrt werden können, wird die Verpflichtung zur Führung des Registers gestrichen. Die RL 2016/680 verlangt jedoch die Führung eines Verzeichnisses über die Datenbearbeitungstätigkeiten. Aufgrund des Geltungsbereichs der RL 2016/680 reicht es aus, wenn dieses Verzeichnis im Bereich der justiziellen und polizeilichen

Datenbearbeitung umgesetzt wird. Im Gegensatz zum Bund (Art. 12 DSG) wird der Kanton Graubünden diese Pflicht daher nicht für alle dem Gesetz unterstellten öffentlichen Organe vorsehen. Es soll der Regierung obliegen, die der RL 2016/680 unterstellten und somit zur Führung des Verzeichnisses verpflichteten öffentlichen Organe (namentlich die Strafverfolgungs- und die Justizvollzugbehörden) im Rahmen der Verordnung zu benennen. Für die Strafgerichte (gemäss Einführungsgesetz zur Schweizerischen Strafprozessordnung [EGzStPO; BR 350.100]) reicht eine Regelung auf Verordnungsstufe nicht aus. Daher werden diese auf Gesetzesstufe benannt.

Gemäss den oben getätigten Ausführungen kann der Nachweis über die Einhaltung der Datenschutzbestimmungen mit einer Vielzahl an Dokumenten geführt werden. Aufgrund der bisherigen Erfahrungen aus anderen Kantonen wird bezweifelt, dass das Verzeichnis in der vom Völkerecht verlangten Form alleine ausreicht, um diesen Nachweis zu erbringen. Weitere kantonale Verwaltungsbehörden und insbesondere die Gemeinden sollen daher nicht zur Führung dieses Verzeichnisses verpflichtet sein. Es ist ihnen aber gleichwohl möglich, ein entsprechendes Verzeichnis zu erstellen, zumal es dennoch der eigenen Dokumentation und dem Nachweis nach Art. 4 KDSG dienen kann. Abs. 2 und Abs. 3 regeln den erforderlichen Inhalt in Anlehnung an Art. 12 DSG. Das öffentliche Organ hat das Verzeichnis der Aufsichtsstelle zu melden und laufend zu aktualisieren. Aus praktischer Sicht hat sich gezeigt, dass die in Art. 12 Abs. 2 lit. g DSG vorgesehene Pflicht zur Angabe der konkreten Staaten, in welche Daten bekannt gegeben werden, aufgrund der abstrakten Natur des Verzeichnisses keinen Mehrwert bringt. Daher reicht es aus, wenn angegeben wird, ob Daten ins Ausland bekannt gegeben werden und welche Garantien für die Angemessenheit des Datenschutzniveaus im Empfängerstaat vorhanden sind (z.B. Länderliste des Bundes, Verträge).

Art. 23 Datenschutzberaterin oder -berater

Die RL 2016/680 verlangt, dass die Behörden im Bereich der justiziellen und polizeilichen Datenbearbeitung eine für die Datenschutzberatung zuständige Person vorsehen (Datenschutzberaterin oder Datenschutzberater). Diese Person berät und unterstützt die Mitarbeitenden bei der Bearbeitung von Personendaten, sorgt für die Vornahme der DSFA durch die Verantwortliche oder den Verantwortlichen (vgl. Art. 19 KDSG) und ist Ansprechperson der Aufsichtsstelle. Der Bund verpflichtet alle seine Behörden zur Benennung einer Datenschutzberaterin oder eines Datenschutzberaters (vgl. Art. 27 DSV). Hingegen beschränken die meisten Kantone die Verpflichtung auf die Behörden im Anwendungsbereich der RL 2016/680. Dies soll auch im Kanton Graubünden so gehandhabt werden. Wie beim Verzeichnis der Bearbeitungstätigkeiten wird die Pflicht der Strafgerichte im KDSG statuiert. Die der RL 2016/680 unterstehenden öffentlichen Organe werden auf

Verordnungsstufe zur Benennung einer oder mehrerer entsprechender Personen verpflichtet. Es kann sich um eine interne oder externe Person handeln und sie kann auch für mehrere Verwaltungseinheiten gemeinsam benannt werden, wobei jede Lösung verschiedene Vor- und Nachteile hat, die es im Einzelfall abzuwägen gilt. Auf Verordnungsstufe werden zudem die Voraussetzungen an und die Kompetenzen dieser Person geregelt. Es gilt zu beachten, dass es sich bei der Datenschutzberaterin oder dem Datenschutzberater nicht um eine neue Stelle oder Funktion handeln muss. Es kann auch ein Mitglied des vorhandenen Personals diese Aufgabe wahrnehmen, welches Kenntnisse auf dem Gebiet Datenschutz vorweisen kann oder sich entsprechend schulen lässt.

Art. 24 Auskunftsrecht

Das Recht jeder Person, Auskunft darüber zu erhalten, ob und welche Daten über sie von einem öffentlichen Organ bearbeitet werden, ist einer der Kernpunkte des Datenschutzrechts. Es ist der Ausgangspunkt für die Geltendmachung weiterer Rechte und Ansprüche der betroffenen Person. Das Auskunftsrecht wird bereits im geltenden Recht gestützt auf Art. 5 Abs. 1 KDSG gewährt. Diese Bestimmung wird aufgrund des dynamischen Verweises durch Art. 25 DSG konkretisiert. Die Regelung in Art. 24 wird sich weiterhin an dieser Norm im DSG orientieren. Im Vergleich zum alten Bundesrecht findet somit lediglich dahingehend eine Konkretisierung statt, dass der Person alle Informationen mitgeteilt werden müssen, die erforderlich sind, um die Rechte nach jenem Gesetz geltend zu machen und eine transparente Datenbearbeitung zu gewährleisten. Namentlich sind der Person die Angaben zu machen, welche auch im Rahmen der Informationspflicht nach Art. 17 Abs. 2 anzugeben sind. Daher kann an dieser Stelle auf die entsprechende Bestimmung verwiesen werden. Zusätzlich müssen in Übereinstimmung mit dem Bundesrecht Angaben zur Aufbewahrungsdauer und zur Herkunft der Personendaten gemacht werden können. Die Modalitäten des Auskunftsrechts werden in der Verordnung konkretisiert (vgl. die Ausführungen unter IV.1).

Art. 25 Einschränkungen des Auskunftsrechts

Wie bisher (vgl. Art. 5 Abs. 1 des geltenden KDSG i.V.m. Art. 26 DSG) muss das Auskunftsrecht Einschränkungen zugänglich sein. Die Gründe, welche eine Einschränkung ermöglichen, wurden weitgehend aus dem alten Bundesrecht übernommen. Die Auskunft kann eingeschränkt werden, wenn und soweit eine besondere gesetzliche Geheimhaltungspflicht dies vorsieht oder es zum Schutz überwiegender öffentlicher oder privater Interessen Dritter (z.B. weiterer Personen) erforderlich ist, sowie wenn damit eine Ermittlung, Untersuchung oder ein behördliches oder gerichtliches Verfahren

gefährdet würde. Nicht aus dem Bundesrecht übernommen wird die Möglichkeit, dass die Auskunft eingeschränkt werden kann, wenn das Auskunftsgesuch offensichtlich unbegründet oder querulatorisch ist (Art. 26 Abs. 1 lit. c DSG). Aufgrund der Rückmeldungen aus der Vernehmlassung wird den öffentlichen Organen indes eine Handhabung gegen entsprechende Gesuche gegeben werden. Aus den weiter oben skizzierten Vorbehalten gegen die Vereinbarkeit mit dem Völkerrecht, soll die Auskunft in diesen Fällen allerdings nicht ganz verunmöglicht werden. Es soll den öffentlichen Organen aber ermöglicht werden, in diesen Fällen eine angemessene Gebühr zu verlangen (vgl. oben II.2.1 und unten Art. 28).

Art. 26 Widerspruch gegen die Bekanntgabe von Personendaten

Der betroffenen Person muss es unter gewissen Voraussetzungen möglich sein, dem öffentlichen Organ die Weitergabe von Personendaten zu untersagen. Dies ist vor allem relevant, wo Personendaten oder zumindest gewisse Stammdaten (vgl. Art. 10 Abs. 3 KDSG) ohne weitere Vorgaben weitergegeben werden können. Dieses Recht stand der betroffenen Person bereits gestützt auf dem alten Recht unter dem Begriff «Sperrung» (Art. 20 aDSG) zu. In Anlehnung an das europäische Recht wird in Art. 37 DSG neu der Begriff des Widerspruchs gegen die Bekanntgabe verwendet. Die Materialien gehen allerdings davon aus, dass sich dadurch der materielle Gehalt der Bestimmung nicht ändert (vgl. BBl 2017, 7083). Es obliegt der betroffenen Person, den Widerspruch beim jeweiligen öffentlichen Organ geltend zu machen. Dies kann jederzeit und nicht nur im Rahmen einer konkreten Datenbekanntgabe gemacht werden. Die betroffene Person muss zudem ein schutzwürdiges Interesse am Widerspruch gegen die Bekanntgabe geltend machen (z.B. die Verhinderung möglicher Belästigungen oder Schikanen). Das Begehren um Widerspruch kann abgelehnt bzw. durchbrochen werden, wenn eine Rechtspflicht zur Bekanntgabe besteht oder die Erfüllung der Aufgabe des öffentlichen Organs dadurch gefährdet ist. Da die Datenbekanntgabe zwischen öffentlichen Organen in der Regel an eine gesetzliche Grundlage geknüpft ist (vgl. Art. 9 KDSG), greift der Widerspruch in erster Linie für die Bekanntgabe an Private oder ausländische Behörden. Aus Art. 10 Abs. 2 lit. d KDSG ergibt sich zudem, dass ein Widerspruch abgelehnt werden kann, wenn die Empfängerin oder der Empfänger glaubhaft macht, dass die gesuchstellende Person rechtsmissbräuchlich vom Widerspruchsrecht Gebrauch macht (z.B. um die Durchsetzung von Rechtsansprüchen zu verhindern).

Art. 27 Weitere Ansprüche

Das KDSG muss den betroffenen Personen die Möglichkeit geben, sich gegen eine nicht gesetzeskonforme Bearbeitung zur Wehr zu setzen, etwa wenn eine Bearbeitung ohne genügende rechtliche Grundlage erfolgt. Hierzu

kann die betroffene Person verschiedene Ansprüche geltend machen, welche in Art. 27 KDSG geregelt sind. Diese Rechte umfassen den Anspruch auf Unterlassung, Beseitigung und Feststellung der widerrechtlichen Bearbeitung sowie der Berichtigung unrichtiger Daten. Sie sind bereits nach geltendem Recht in Art. 5 KDSG i.V.m. Art. 41 DSG vorgesehen. Im Bundesrecht regelt Art. 41 Abs. 3 DSG die Einschränkung der Bearbeitung als weniger einschneidende Alternative zur Löschung. Diese Bestimmung sieht vor, dass in den vom Gesetz genannten Fällen die Daten weiterbearbeitet werden dürfen, jedoch nur zu bestimmten Zwecken. Da ein entsprechendes Instrument in keinem anderen Kanton bekannt ist, wird vorliegend auf dessen Übernahme verzichtet. Wie bisher bringt das öffentliche Organ statt der Berichtigung eines Personendatums ein Bestreitungsvermerk an, wenn weder die Richtigkeit noch die Unrichtigkeit der betreffenden Personendaten festgestellt werden kann. Nicht aus dem Bundesrecht übernommen wird die Regelung betreffend Beständen öffentlicher Gedächtnisinstitutionen (z.B. Archive oder Museen). Sofern diese die Archive betrifft, gehen gestützt auf Art. 2 Abs. 4 KDSG die spezialrechtlichen Regelungen im GAA vor. Diese sehen in Art. 11 Abs. 1 GAA abweichend vom Bundesrecht die Möglichkeit eines Bestreitungsvermerks ebenfalls vor, womit kein Grund zur Übernahme dieser Bestimmung besteht. Betreffend anderer Gedächtnisinstitutionen wäre allenfalls eine separate Regelung denkbar. Dies wurde (soweit ersichtlich) in keinem anderen Kanton so gehandhabt und kann daher auch im Kanton Graubünden unterbleiben.

Art. 28 Verfahren

Den betroffenen Personen muss der Rechtsweg offenstehen, wenn die ihnen nach diesem Gesetz gewährten Rechte verletzt werden. Daher hat das öffentliche Organ über die Abweisung von Begehren nach diesem Gesetz einen begründeten Entscheid zu erlassen. Nach geltendem Recht ist dies in Art. 6 geregelt. Die Bestimmung überzeugt in verschiedener Hinsicht nicht. Art. 6 Abs. 1 und Abs. 3 des bestehenden KDSG weichen nicht von der im VRG statuierten Zuständigkeitsordnung (vgl. Art. 28 VRG) ab. Sie müssen daher nicht wiederholt werden. Auch der bisherige Art. 6 Abs. 2 KDSG kann gestrichen werden, da bei Privaten, welchen öffentliche Aufgaben übertragen werden, die Verfügungsbefugnis grundsätzlich nur dann übergeht, wenn dies spezialgesetzlich vorgesehen ist. Daher ist auch der Beschwerdeweg in der Regel bereichsspezifisch geregelt. Gemäss Art. 6 Abs. 4 des geltenden KDSG hat die Aufsichtsstelle zudem die Möglichkeit, Entscheide der Behörden beim vorgesetzten Departement anzufechten. Bisher hat die Aufsichtsstelle von diesem Beschwerderecht nie Gebrauch gemacht. Im Rahmen der Stärkung der Aufsichtsstelle muss der Aufsichtsstelle neu im Einklang mit den völkerrechtlichen Vorgaben ermöglicht werden, anfechtbare Entscheide

zu erlassen (vgl. Art. 37 KDSG). Daher besteht keine Notwendigkeit, der Aufsichtsstelle weiterhin eine separate Beschwerdelegitimation einzuräumen. Neu sieht Art. 28 Abs. 1 KDSG dementsprechend lediglich noch vor, dass die öffentlichen Organe einen Entscheid zu erlassen haben, wenn sie einem Begehren nach diesem Gesetz nicht entsprechen. Im Weiteren richtet sich das Verfahren nach dem VRG.

Gestützt auf die völkerrechtlichen Vorgaben ist das Auskunftsrecht als wichtigstes Instrument der betroffenen Personen und als Ausgangspunkt für die Geltendmachung der weiteren Rechte und Ansprüche grundsätzlich kostenlos zu gewähren. Selbiges gilt für das Gesuch um Berichtigung unrichtiger Personendaten. Das Gesuch um Widerspruch gegen die Bekanntgabe der Personendaten ist zwar praktisch weniger relevant, aber erfahrungsgemäss mit einem geringen Aufwand verbunden und soll daher ebenfalls kostenlos gewährt werden. Von diesem Grundsatz der Kostenlosigkeit soll einerseits abgewichen und eine angemessene Gebühr verlangt werden können, wenn ein Gesuch mit einem unverhältnismässigen Aufwand verbunden ist. Wann ein unverhältnismässiger Aufwand vorliegt, wird dabei auf Verordnungsstufe konkretisiert (vgl. unten IV. 1). Anderseits wird dem öffentlichen Organ die Möglichkeit gegeben, Gebühren zu erheben, wenn ein Gesuch offensichtlich unbegründet oder querulatorisch ist. Damit soll ihm eine Handhabung gegen datenschutzwidrige Gesuche (z.B. zur Beweismittelausforschung) oder querulatorische und wiederholte Anfragen gegeben werden (vgl. oben II.2.1). Die Beurteilung der weiteren datenschutzrechtlichen Ansprüche ist hingegen tendenziell aufwändiger. Daher wird für diese (in Übereinstimmung mit den meisten anderen Kantonen) von einer Kostenbefreiung abgesehen. Die Gebührenerhebung richtet sich nach den allgemeinen Grundsätzen, welche in der Verordnung über die Kosten in Verwaltungsverfahren (VKV; BR 370.120) geregelt sind. Die betroffene Person ist vor der Gesuchbearbeitung auf die Kostenfolgen hinzuweisen.

Art. 29 Verfahren im Falle der Bekanntgabe von amtlichen Dokumenten, die Personendaten enthalten

Bereits nach geltendem Recht kann die betroffene Person in Verfahren nach dem KGÖ nicht nur verlangen, dass die betreffenden Personendaten nicht bekannt gegeben werden müssen, sondern sie kann auch ihre weiteren Betroffenenrechte geltend machen (vgl. Art. 5 des geltenden KDSG i.V.m. Art. 42 DSG). Diese Möglichkeit dient der Koordination von Verfahren nach dem Datenschutz- und Öffentlichkeitsgesetz und soll daher beibehalten werden.

Art. 30 Aufsichtsstelle

Die behördliche Datenbearbeitung und die Anwendung der Datenschutzvorschriften ist aufgrund des internationalen Rechts durch ein unabhängiges Kontrollorgan zu kontrollieren. Zu diesem Zweck kennt der Kanton Graubünden seit dem Inkrafttreten des KDSG im Jahr 2002 einen Datenschutzbeauftragten als Aufsichtsstelle. Die oder der Datenschutzbeauftragte nimmt gemäss Art. 8 des geltenden KDSG die Aufsicht und Beratung aller dem Gesetz unterstellten öffentlichen Organe wahr. Mit Blick auf den Geltungsbereich sind die Datenbearbeitungen in Gerichtsverfahren und in Verfahren nach bundesrechtlichen Verfahrensordnungen sowie in Verfahren der Verwaltungsrechtspflege von der Aufsicht durch die Aufsichtsstelle auszunehmen (Art. 2). Hinsichtlich anderer Datenbearbeitungen unterstehen die Gerichte jedoch der Aufsichtsstelle (vgl. Art. 15 Ziff. 10 Übereinkommen SEV 108). Im Weiteren wird die Aufsichtsstelle und ihr Tätigkeitsbereich beibehalten. Es wird als nicht zweckmässig angesehen, dass die Gemeinden eigene Datenschutzaufsichtsstellen bezeichnen müssen. Somit bleibt die Aufsichtsstelle wie bisher für die Gemeinden zuständig. Eine wichtige Aufgabe der Aufsichtsstelle wird wie bis anhin die Beratung, Anleitung und Ausbildung der Gemeindebehörden darstellen. Durch den vorgesehenen Ausbau der Aufsichtsstelle (vgl. V.) soll sie künftig in der Lage sein, die Unterstützung gegenüber den Gemeinden besser wahrzunehmen (z.B. durch die Veröffentlichung von Merkblättern).

Art. 31 Zusammensetzung und Stellung

Art. 31 regelt die Zusammensetzung und die Stellung der Aufsichtsstelle. Es wird statuiert, dass diese im Minimum aus der oder dem Datenschutzbeauftragten als Leitung der Aufsichtsstelle sowie einer Stellvertretung besteht. Damit wird die Dotierung im Gegensatz zur bestehenden Aufsichtsstelle erhöht, was zur Umsetzung der künftigen Aufgaben notwendig ist (vgl. unten V.). Um ihre Aufsichtsfunktion wahrnehmen zu können, muss die Aufsichtsstelle fachlich selbstständig und unabhängig sein und darf in der Erfüllung ihrer Aufgaben hinsichtlich des Inhalts und des Umfangs nicht an die Weisungen einer anderen Stelle gebunden sein (wie bereits nach geltendem Recht, vgl. Art. 7 KDSG). Dennoch muss eine gewisse Dienstaufsicht zulässig sein. Diese hat sich gestützt auf das internationale Recht an der Organaufsicht, wie sie etwa gegenüber den Gerichten besteht, auszurichten. Diese Aufsichtsfunktion nimmt die Regierung als Wahlorgan unter Beachtung der Unabhängigkeit der Aufsichtsstelle wahr. Es muss der Regierung insbesondere zustehen, die oder den Datenschutzbeauftragten sowie ihre oder seine Stellvertretung bei schwerer Amtspflichtverletzung oder dauernder Amtsunfähigkeit des Amtes zu entheben (vgl. Art. 32).

Administrativ ist die Aufsichtsstelle wie bisher der Standeskanzlei unterstellt. Die Zuordnung zur Standeskanzlei als Stabs- und Verbindungsstelle von

Parlament, Regierung und Verwaltung wird in verschiedenen anderen Kantonen praktiziert und als vorteilhaft erachtet. Eine fachliche Unterstellung oder eine Weisungsbefugnis seitens der Standeskanzlei besteht nicht. Durch die administrative Unterstellung obliegen der Standeskanzlei nebst der Durchführung von Amtsbesprechungen auch die Vorbereitung der Wahlen (Art. 32) sowie die Instruktion allfälliger Aufsichtsbeschwerden (Art. 31 Abs. 3) oder Amtsenthebungsverfahren zu Handen der Regierung (Art. 32 Abs. 2). Da die Aufsichtsstelle eine Verwaltungseinheit der Kantonalen Verwaltung darstellt (vgl. oben Art. 30), ist grundsätzlich das kantonale Personal- und Pensionskassenrecht auf sie anzuwenden. Aus den völkerrechtlichen Vorgaben an die Unabhängigkeit der Aufsichtsstelle ergeben sich einige Punkte, in denen deren Bestimmungen nicht ohne Weiteres angewendet werden können und daher im vorliegenden Gesetz abweichend geregelt sind. Es geht dabei namentlich um die Weisungsunabhängigkeit, das Wahlverfahren und die Abberufung (vgl. sogleich Art. 32).

Art. 32 Wahl

Das Völkerrecht gibt zur Wahl der oder des Datenschutzbeauftragten vor, dass diese oder dieser in einem transparenten Wahlverfahren durch das Parlament, die Regierung oder eine unabhängige Stelle zu erfolgen hat. Im Kanton Graubünden wird die oder der Datenschutzbeauftragte aktuell auf eine unbeschränkte Zeitdauer durch die Regierung gewählt und in einem jederzeit widerrufbaren Auftragsverhältnis angestellt (vgl. Art. 7 des geltenden KDSG). Die Wahl durch die Regierung hat sich bewährt und soll beibehalten werden. Hingegen wird das jederzeit widerrufbare Auftragsverhältnis unter Unabhängigkeitsaspekten als problematisch angesehen. Daher soll die oder der Datenschutzbeauftragte künftig für eine Amtsdauer von vier Jahren gewählt werden, wie dies für andere öffentliche Ämter im Kanton Graubünden üblich ist und in einer Vielzahl von Kantonen praktiziert wird. Die Wiederwahl ist zulässig. Mit den völkerrechtlichen Vorgaben vereinbar ist die Möglichkeit zur Amtsenthebung bei dauerhafter Amtsunfähigkeit oder wenn sie oder er vorsätzlich oder grobfahrlässig eine schwere Amtspflichtverletzung begangen hat.

Da die oder der Datenschutzbeauftragte die bestehenden und die neu hinzukommenden Aufgaben nicht mit dem bisherigen 50%-Pensum wird bewältigen können, soll die Aufsichtsstelle künftig zumindest eine weitere Person umfassen. Diese kann auch Stellvertretungsaufgaben wahrnehmen. Es gilt zu beachten, dass die Aufgabenerfüllung neben juristischem Fachwissen auch zunehmend Informatikkenntnisse erfordert. Für entsprechendes Fachwissen muss die oder der Datenschutzbeauftragte bisher im Rahmen des zugesprochenen Pauschalbetrags externe Beraterinnen oder Berater mandatieren. Es erscheint sinnvoll, künftig kantonsinternes Fachwissen auf-

zubauen. Bei der Ernennung der Stellvertretung ist darauf zu achten, dass sie die Leitung aufgrund ihrer Expertise ergänzt (z.B. eine IT-Fachperson, wenn die oder der Datenschutzbeauftragte einen juristischen Hintergrund hat). Für die Wahl der Stellvertretung sollen betreffend Wahl und Amtsenthebung dieselben Regelungen gelten wie für die oder den Datenschutzbeauftragten.

Art. 33 Unvereinbarkeiten

Die Unabhängigkeit der Aufsichtsstelle kann durch die Ausübung von Nebentätigkeiten der Leitung oder ihrer Stellvertretung gefährdet sein. Hierzu enthält das KDSG bisher keine Regelung. Um die völkerrechtlichen Vorgaben zu erfüllen wird daher eine Bestimmung eingeführt. Als problematisch wird es einerseits erachtet, wenn die Amtsträgerin oder der Amtsträger ein anderes öffentliches Amt ausübt. Auf diese Weise müsste sie oder er unter Umständen in dieser Funktion ein öffentliches Organ kontrollieren, welchem sie oder er selber angehören. Aufgrund des Wirkungsbereichs der oder des Datenschutzbeauftragten wird anderseits auch die parteipolitische Unbefangenheit als wichtig erachtet. Diese soll insofern eingeschränkt werden, als die oder der Datenschutzbeauftragte nicht eine leitende Funktion innerhalb einer politischen Partei wahrnehmen kann. Sofern die oder der Datenschutzbeauftragte bzw. die Stellvertretung ein Vollpensum bekleidet, wird eine andere Erwerbstätigkeit im Grundsatz ausgeschlossen. Die Regierung kann indes Ausnahmen bewilligen. Dadurch soll ermöglicht werden, dass geeignete Personen, die alle erforderlichen Eigenschaften und Voraussetzungen mitbringen, trotz einer zusätzlichen Tätigkeit, welche die Aufgabenerfüllung nicht beeinträchtigt, das Amt wahrnehmen können. Es kann sich hierbei etwa um die Wahrnehmung von Lehraufträgen oder mit der Aufgabe nicht in Konflikt stehende Nebenerwerbe (z.B. künstlerischer Natur) handeln. Aufgrund der Rückmeldungen in der Vernehmlassung soll bereits im Gesetz festgehalten werden, dass die Regierung als Wahlorgan bei der Erteilung entsprechender Ausnahmegenehmigungen, darauf zu achten hat, dass die Ausübung der Funktion sowie die Unabhängigkeit und das Ansehen nicht beeinträchtigt werden (vgl. oben II.2.1).

Sofern die oder der Datenschutzbeauftragte oder die Stellvertretung nur ein Teilzeitpensum bekleidet, stellt sich die Frage, ob und unter welchen Umständen ihm oder ihr die Ausübung einer Nebentätigkeit gewährt werden soll. Aus dem internationalen Recht lässt sich kein striktes Verbot von Nebentätigkeiten ableiten. Wie in anderen Kantonen soll die Ausübung einer anderen Erwerbstätigkeit daher in diesen Fällen erlaubt sein. Die entsprechende Tätigkeit ist jedoch durch die Regierung als Wahlorgan zu bewilligen. Diese Bewilligung darf in Übereinstimmung mit dem internationalen Recht nur verweigert werden, wenn durch die Erwerbstätigkeit die

Ausübung der Funktion sowie Unabhängigkeit und Ansehen dieser Stelle beeinträchtigt werden (vgl. Art. 42 Abs. 3 RL 2016/680).

Art. 34 Budget

Die Aufsichtsstelle kann ihre von Gesetzes wegen vorgesehenen Aufgaben nur dann vollständig unabhängig erfüllen, wenn sie die erforderlichen Ressourcen erhält und ihr diese zur freien Verfügung stehen. Die Mittel, mit welchen der Datenschutzbeauftragte aktuell finanziert wird, definieren sich nach der Ausgestaltung des privatrechtlichen Auftrags, in dem er angestellt ist. Sie sind dem Budget der Standeskanzlei zugeordnet. Gemäss den in der Jahresrechnung des Kantons ersichtlichen Zahlen handelt es sich dabei um einen gleichbleibenden Fixbeitrag. Aufgrund der mit der Revision hinzukommenden Aufgaben und Verpflichtungen dürfte der damals vereinbarte Betrag kaum mehr zur wirkungsvollen Aufgabenerfüllung ausreichen. Auch wenn die Aufsichtsstelle in der Verwendung der bisher zugesprochenen Mittel grundsätzlich frei ist, soll es ihr aus Gründen der Unabhängigkeit (wie in anderen Kantonen) künftig ermöglicht werden, ein eigenes Budget zu erstellen. Um die Unabhängigkeit von der Regierung als Wahlorgan zu stärken, hat diese den Entwurf grundsätzlich unverändert in ihr Budget zuhanden des Grossen Rats zu übernehmen (ähnlich wird dies bei der Finanzkontrolle gehandhabt, vgl. Art. 6 Gesetz über die Finanzaufsicht [GFA; BR 710.300]). Der Regierung steht es aber frei, dem Grossen Rat eine Änderung zu beantragen. Die Entscheidung über das beantragte Budget verbleibt beim Grossen Rat. Im Rahmen des vom Parlament gesprochenen Budgets ist die oder der Datenschutzbeauftragte in der Verwendung der Mittel (und z.B. auch der Anstellung von weiterem Personal) frei.

Art. 35 Aufgaben

Art. 35 KDSG regelt die Aufgaben der Aufsichtsstelle. Diese sind im geltenden Recht in Art. 8 KDSG vorgesehen und sollen weitgehend übernommen werden. Aufgrund der völkerrechtlichen Vorgaben kommen zusätzliche Aufgaben hinzu. Neu wird im Gesetz festgeschrieben, dass die Aufsichtsstelle einen Sensibilisierungsauftrag gegenüber öffentlichen Organen wahrnehmen sowie die massgeblichen Entwicklungen in der Informations- und Kommunikationstechnologie verfolgen muss. Auch die Zusammenarbeit mit anderen öffentlichen Organen wird explizit betont. Nicht mehr vorgesehen ist, dass die Aufsichtsstelle ein Register über die Datenbearbeitungstätigkeiten führt (vgl. oben Art. 22 KDSG). Die völkerrechtlichen Vorgaben verlangen zudem, dass den Betroffenen ein «Recht auf Beschwerde» bei der Aufsichtsstelle offenstehen muss. Diese Möglichkeit muss ihnen unabhängig von anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfen offenstehen (womit sich das Instrument z.B. von der Aufsichtsbeschwerde

gemäss Art. 68 VRG unterscheidet). Im Kanton Graubünden soll dies so umgesetzt werden, dass die betroffene Person die Missachtung von datenschutzrechtlichen Vorschriften bei der Bearbeitung ihrer Personendaten an die Aufsichtsstelle melden kann. Die Aufsichtsstelle hat sich mit der Meldung zu befassen und kann gestützt darauf weitere Massnahmen ergreifen (vgl. Art. 36 und 37). Die betroffene Person hat in diesem Verfahren keine Parteirechte. Sie ist jedoch innert drei Monaten über das Ergebnis oder den Stand der Abklärungen zu informieren. Diese Regelung kennen auch andere Kantone und sie wird als mit dem Völkerrecht vereinbar erachtet.

Art. 36 Befugnisse 1. Kontrolle und Empfehlung

Zur Erfüllung ihrer Aufgaben benötigt die Aufsichtsstelle gewisse Befugnisse. Nach geltendem Recht ist sie befugt, bei öffentlichen Organen schriftlich und mündlich Auskünfte über das Bearbeiten von Personendaten einzuholen. Zudem kann sie Einsicht in Datensammlungen und ihre Unterlagen nehmen und sich das Bearbeiten von Personendaten vorführen lassen. Die öffentlichen Organe sind verpflichtet, die Aufsichtsstelle bei der Erfüllung ihrer Aufgaben zu unterstützen (vgl. Art. 9 und 10 des bestehenden KDSG). Die bestehenden Befugnisse sollen beibehalten werden. Abs. 1 dient der Koordination mit beim öffentlichen Organ hängigen Verfahren (insbesondere nach Art. 28 KDSG). Er stellt klar, dass die Aufsichtsstelle wie bisher von sich aus oder auf Meldung von Betroffenen (siehe soeben) tätig werden kann. Sofern sie auf Meldung tätig wird, ist das öffentliche Organ über diese Meldung in Kenntnis zu setzen und es ist ihm die Möglichkeit zur Stellungnahme zu geben. Ist bereits ein Verfahren beim öffentlichen Organ hängig, so kann die Aufsichtsstelle beispielsweise bis zu dessen Abschluss ihre eigenen Untersuchungen einstellen oder im Rahmen dieses Verfahrens Empfehlungen an das öffentliche Organ aussprechen (vgl. oben II.2.1).

Art. 37 2. Entscheid

Bisher kann die Aufsichtsstelle ein öffentliches Organ, welches die Datenschutzvorschriften verletzt, lediglich im Sinne einer Empfehlung auffordern, die erforderlichen Massnahmen zu ergreifen. Sofern das öffentliche Organ diese Empfehlung ablehnt oder nicht befolgt, ist die Angelegenheit der Regierung zum Entscheid zu unterbreiten (Art. 9 Abs. 3 und 4 des geltenden KDSG). Um die Stellung der Datenschutzaufsicht zu stärken, muss dieser neu von Völkerrechts wegen die Befugnis zukommen, bei Verstössen gegen das Datenschutzrecht verbindliche Anordnungen (in Form eines Entscheids) zu treffen. Wie weiter oben ausgeführt, reicht das bestehende Antragsrecht an die Regierung nicht aus, um die Vorgaben des Völkerrechts zu erfüllen. Entsprechend verankern praktisch alle Kantone, welche ihre Datenschutzgesetze bereits aufgrund der neuen völkerrechtlichen Vorgaben revidiert ha-

ben, eine Verfügungsbefugnis der Aufsichtsstelle im Gesetz (vgl. auch oben II. 2.1). Diese Möglichkeit wird der Aufsichtsstelle allerdings nur als «ultima ratio» offenstehen, wenn ein Organ einer Empfehlung nicht Folge leistet oder klar zu erkennen gibt, dass es dies nicht tun wird.

Aufgrund des internationalen Rechts muss es der Aufsichtsstelle ermöglicht werden, bei offensichtlichen Gefährdungen oder Verletzungen schutzwürdiger Interessen vorsorgliche Massnahmen zu treffen. Diese Befugnis ergibt sich bereits aus Art. 5 VRG und ist nicht explizit im KDSG zu verankern. Dem von einem Entscheid betroffenen öffentlichen Organ muss es möglich sein, die Entscheide der Aufsichtsstelle bei einem Gericht anzufechten. Aus den weiter oben ausgeführten Überlegungen, sollen entsprechende Entscheide grundsätzlich an das Obergericht weitergezogen werden können. Sofern sie das Obergericht selber betreffen, können sie an das Justizgericht weitergezogen werden (vgl. oben II.2.1).

Art. 38 Berichterstattung

Bereits nach geltendem Recht hat die oder der Datenschutzbeauftragte der Regierung über ihre oder seine Tätigkeit Bericht zu erstatten (Art. 8 Abs. 1 lit. g des geltenden KDSG). Im Rahmen der Revision wird der Gegenstand dieser Berichterstattungspflicht konkretisiert. Zudem soll neu ein öffentliches Organ, das von Empfehlungen oder einem Entscheid der Aufsichtsstelle betroffen ist, vor der Veröffentlichung des Berichts zur Stellungnahme eingeladen werden. Das öffentliche Organ kann in seiner Stellungnahme ausführen, welche Massnahmen geplant, eingeleitet oder bereits getroffen wurden. Diese Stellungnahme des öffentlichen Organs ist dem Bericht anzufügen. Wie bisher ist der Bericht der Aufsichtsstelle zu veröffentlichen.

Art. 39 Verschwiegenheit

Aufgrund ihrer Kontrollbefugnisse (vgl. Art. 36 KDSG) hat die Aufsichtsstelle weitgehende Einsichtsrechte. Es können ihr auch besondere Geheimhaltungsbestimmungen nicht entgegengehalten werden. Um den Geheimnisschutz zu wahren, untersteht die Aufsichtsstelle denselben Verschwiegenheitspflichten wie das datenbearbeitende öffentliche Organ. Diese Verschwiegenheitspflicht ist bereits im geltendem Recht in Art. 10 KDSG verankert. Sie wird weitgehend übernommen. Es wird jedoch klargestellt, dass die Pflicht zur Verschwiegenheit über das Ausscheiden aus dem Amt hinaus bestehen bleibt.

Art. 40 Strafbestimmungen

Bisher ist gemäss Art. 10a Abs. 1 KDSG auf Antrag mit Busse zu bestrafen, «wer als angestellte oder beauftragte Person einer Behörde oder als angestellte Person einer beauftragten Person vorsätzlich gegen die Bestimmungen des kantonalen Datenschutzrechtes verstösst». Diese Bestim-

mung ist aufgrund ihrer Unbestimmtheit zu überarbeiten. Die Mehrheit der Datenschutzverletzungen kann durch personal- und strafrechtliche Konsequenzen wegen der Verletzung des Amts- oder Berufsgeheimnisses bereits nach dem geltenden Recht wirksam anderweitig geahndet werden (vgl. oben II.2.1). Daher sollen nur Handlungen in Bereichen zusätzlich unter Strafe gestellt werden, wo die Sanktionsmöglichkeiten des geltenden Rechts nicht ausreichen. Dies ist dort der Fall, wo die Personendaten den personal- und strafrechtlich relevanten Bereich verlassen. Hierbei geht es insbesondere um die Bekanntgabe von Personendaten im Zusammenhang mit der Auslagerung und im Zusammenhang mit der Bearbeitung zu nicht personenbezogenen Zwecken. In Übereinstimmung mit den Datenschutzgesetzen anderer Kantone werden daher künftig klar umrissene Verhaltensweisen in diesen Bereichen mit Busse bestraft. Das Strafverfahren richtet sich nach den Regeln der StPO.

Art. 41 Übergangsbestimmungen 1. Übergangsbestimmung betreffend laufende Bearbeitungen

Die öffentlichen Organe haben ihre Datenbearbeitungen an das neue Recht anzupassen. Gewisse Personendaten oder Bearbeitungstätigkeiten werden neu als besonders schützenswert oder als Profiling eingeordnet. Diese Kategorisierung führt dazu, dass bestehende Gesetzesgrundlagen hinsichtlich dieser Bearbeitungen unter Umständen hinsichtlich ihrer Bestimmtheit und Normstufe nicht mehr den Anforderungen von Art. 7 KDSG genügen. Es findet im Rahmen der vorliegenden Revision keine systematische Überprüfung hierzu statt. Diese Überprüfung ist bereichsspezifisch vorzunehmen. Daher soll den öffentlichen Organen mit Abs. 1 eine Übergangsfrist eingeräumt werden. Während dieser können Datenbearbeitungen, welche sich nach geltendem Recht auf eine genügende rechtliche Grundlage stützen gestützt auf die bestehenden Rechtsgrundlagen fortdauern, auch wenn sie zukünftig eine höhere Normstufe oder Bestimmtheit erfordern.

Im Weiteren wird die Übergangsbestimmung gegenüber der Vernehmlassungsvorlage konkretisiert. Hier gilt zu beachten, dass die neuen Instrumente und Verpflichtungen aufgrund der dynamischen Verweise bereits seit dem 1. September 2023 gelten und seit diesem Zeitpunkt von den öffentlichen Organen umgesetzt werden müssen. Die bestehende Formulierung hätte dazu geführt, dass ihnen die Umsetzung der neuen Instrumente ab dem Inkrafttreten des Gesetzes für zwei Jahre noch einmal freigestellt gewesen wäre und erst danach wieder verpflichtend gegolten hätte. Dies erscheint weder sinnvoll noch sachlogisch und war daher anzupassen. Eine Übergangsfrist scheint jedoch in einigen ausgewählten Fällen gerechtfertigt. Einerseits ist der Nachweis der Einhaltung der Datenschutzbestimmungen zwar vom Völkerrecht gefordert, ergibt sich aber nicht direkt aus dem DSG. Daher ist

er auch nicht aufgrund des Verweises bereits seit dem 1. September 2023 umzusetzen. Auch wenn dieser Nachweis grundsätzlich auf verschiedene Arten erbracht werden kann (vgl. Art. 4 und IV.1), dürfte die Erarbeitung der Dokumente mit einem gewissen Aufwand verbunden sein. Daher soll der Nachweis auf Verlangen der Aufsichtsstelle erst spätestens nach zwei Jahren erbracht werden müssen. Anderseits ist bei neuen Bearbeitungstätigkeiten künftig eine DSFA und eine Vorabkonsultation durch die Aufsichtsstelle gefordert (vgl. Art. 19 und 20). Dies soll indes nicht dazu führen, dass zu allen bisherigen Bearbeitungstätigkeiten (teilweise erneut) die entsprechenden Dokumente zu erarbeiten sind. Art. 19 und 20 sollen daher nur Anwendung finden, wenn eine Bearbeitungstätigkeit sich wesentlich ändert (z.B. durch einen neuen Bearbeitungszweck oder die Aufnahme neuer Datenkategorien oder eines Profilings).

Zudem kann auf den in der Vernehmlassungsvorlage vorgesehenen Art. 42 verzichtet werden, welcher die erstmalige Wahl der oder des Datenschutzbeauftragten nach den neuen Vorgaben hätte regeln sollen. Diese Bestimmung erweist sich als unnötig, da das Gesetz gestaffelt in Kraft gesetzt werden soll (vgl. unten VII.).

2. Fremdänderungen

2.1 Bürgerrechtsgesetz des Kantons Graubünden (KBüG; BR 130.100)

Art. 24 Bearbeitung von Personendaten

Art. 24 Abs. 1 KBüG spricht von «besonders geschützten Personendaten». Dieser Begriff kommt so im Datenschutzrecht weder nach alter noch nach bestehender Rechtslage vor. Er soll daher an die Terminologie des KDSG angeglichen und durch «besonders schützenswerte Personendaten» ersetzt werden.

2.2 Gesetz über die Einwohnerregister und weitere Personen- und Objektregister (ERG; BR 171.200)

Art. 32 Datenschutz

Art. 32 Abs. 3 sieht in seiner bestehenden Form vor, dass das Sperrecht vorbehalten bleibt. Dabei handelt es sich um das in Art. 20 aDSG verankerte Recht auf Sperrung der Bekanntgabe von Personendaten. Dies bedeutet, dass betroffene Personen bei einem öffentlichen Organ (in diesem Fall der jeweiligen Einwohnerkontrolle) die Bekanntgabe ihrer Personendaten – insbesondere an Private – einschränken können. Diese Möglichkeit soll auch

weiterhin beibehalten werden. Es gilt jedoch zu beachten, dass dieses Instrument im Bundesrecht (Art. 37 DSG) und basierend darauf auch im kantonalen Recht (Art. 26 KDSG) an die völkerrechtliche Terminologie angepasst wurde und neu Widerspruch gegen die Bekanntgabe genannt wird. Diese begriffliche Anpassung wird aus Gründen der Einheitlichkeit auch im ERG nachvollzogen. Eine materielle Änderung ergibt sich daraus nicht.

2.3 Einführungsgesetz zur Schweizerischen Zivilprozessordnung (EGzZPO; BR 320.100)

Art. 14 Aktenaufbewahrung und Akteneinsicht

Das EGzZPO regelt die Einsicht in abgeschlossene Zivilverfahren. Die entsprechende Regelung geht dem KDSG als bereichsspezifisches Datenschutzrecht vor (vgl. Art. 3 Abs. 3). Aktuell sieht die Regelung einen Weiterzug entsprechender Entscheide an die Aufsichtsbehörde der entsprechenden Behörde vor. Nach dieser Regelung müssten Entscheide des Obergerichts über das Akteneinsichtsrecht in abgeschlossene Verfahren an den Grossen Rat weitergezogen werden. Diese Regelung ist im Hinblick auf eine mögliche Anfechtung des entsprechenden Entscheids an das Bundesgericht problematisch. Entscheide über das Akteneinsichtsrecht in abgeschlossene Verfahren sind als Akte der Justizverwaltung mit der Beschwerde in öffentlichrechtlichen Angelegenheiten (BöA) beim Bundesgericht anzufechten. Die BöA ist zulässig gegen Entscheide letzter kantonaler Instanzen, wobei die Kantone als unmittelbare Vorinstanzen des Bundesgerichts obere Gerichte einzusetzen haben (Art. 86 Abs. 2 BGG). Davon kann nur bei Entscheiden mit vorwiegend politischem Charakter abgewichen werden, was vorliegend nicht gegeben ist. Um einen Weiterzug ans Bundesgericht zu ermöglichen, wären solche Fälle allenfalls gestützt auf Art. 49 Abs. 1 lit. g VRG nach der Behandlung durch den Grossen Rat erneut durch das Obergericht zu beurteilen. Sachdienlicher erscheint es, entsprechende Entscheide des Obergerichts als endgültig zu bezeichnen, um einen formalistischen Leerlauf zu vermeiden. Die Überprüfung entsprechender Entscheide ist somit nur, aber immerhin, durch das Bundesgericht möglich. Dieselbe Problematik gilt in abgeschwächter Form für das Justizgericht. Daher sollen auch für dieses die entsprechenden Entscheide als endgültig bezeichnet werden.

2.4 Einführungsgesetz zur Schweizerischen Strafprozessordnung (EGzStPO; BR 350.100)

Art. 36 Aktenaufbewahrung und Akteneinsicht

Art. 36 Abs. 4 EGzStPO sieht wie Art. 14 Abs. 4 EGzZPO eine Bestimmung zum Rechtsweg bei Entscheiden über das Akteneinsichtsrecht bei abgeschlossenen Verfahren vor. Diese Bestimmung muss aus den oben erwähnten Gründen auf dieselbe Weise angepasst werden (vgl. Bemerkungen zu Art. 14 EGzZPO).

2.5 Gesetz über die Finanzaufsicht (GFA; BR 710.300)

Art. 20 Datenzugriff

Der Begriff der Datensammlung kommt im neuen Recht nicht mehr vor. Er soll daher auch in diesem Fachgesetz durch den Begriff der «Datenbestände» ersetzt werden. Eine materielle Änderung ergibt sich daraus nicht.

IV. Ausführungen zu den regierungsrätlichen Ausführungsverordnungen

Die Regierung ist seit dem 1. April 2021 verpflichtet, in Botschaften an den Grossen Rat zu Teil- oder Totalrevisionen von Gesetzen nähere Ausführungen über den Inhalt von Ausführungsverordnungen zu machen, die sie aufgrund einer Gesetzesrevision zu erlassen beabsichtigt (Art. 64a GRG). Im Zusammenhang mit der vorliegenden Totalrevision soll eine Verordnung zum Kantonalen Datenschutzgesetz erlassen werden. Zum geltenden KDSG besteht keine Verordnung. Es wird davon ausgegangen, dass der dynamische Verweis im KDSG auch das Verordnungsrecht und somit namentlich die DSV umfasst. Deren Vorgaben gehen teilweise über das völkerrechtliche Geforderte hinaus (z.B. Bezeichnung einer Datenschutzberaterin oder eines Datenschutzberaters für alle öffentlichen Organe). Sie sind zudem auf Bundesorgane und Private zugeschnitten. Es ist teilweise nicht sinnvoll, dieselben Vorgaben eins zu eins für kantonale und kommunale Organe umzusetzen (z.B. obligatorische Führung eines Bearbeitungsreglements). Wie die Regelungen anderer Kantone zeigen, lassen sich die entsprechenden datenschutzrechtlichen Vorgaben auch auf andere, praxisnähere Weise erfüllen lassen. Es ist daher zielführend eine eigene Verordnung zu schaffen, welche sich insbesondere an entsprechenden Vorgaben in anderen vergleichbaren Kantonen orientiert. Die Bildüberwachungsverordnung konkretisiert die Art. 3a und 3b des geltenden KDSG (neu Art. 14 und 15 KDSG). Da diese

Bestimmungen im Rahmen der Revision geringfügig angepasst wurden (vgl. oben II.2.1 und Art. 14), ist die Verordnung ebenfalls anzupassen. Die vorgesehenen Änderungen ergeben sich aus praktischen Bedürfnissen und der Anpassung von Art. 14 KDSG. Zudem sind die Verweise und Begriffe an das neue KDSG anzupassen.

1. Verordnung zum Kantonalen Datenschutzgesetz (VKDSG; BR 171.110)

Die Verordnung enthält die Ausführungsbestimmungen zum KDSG. In der VKDSG müssen einerseits die Regelungen über den Nachweis der Einhaltung der Datenschutzbestimmungen gegenüber der Aufsichtsstelle konkretisiert werden. Um den Nachweis über die Einhaltung der Datenschutzbestimmungen erbringen zu können, müssen im mindesten die entsprechenden Prozesse, Verantwortlichkeiten und Datenschutzrisiken dokumentiert werden. Es ist davon auszugehen, dass sich ein öffentliches Organ zu diesen Aspekten bereits nach geltendem Recht grundsätzlich bei Datenbearbeitungstätigkeiten Gedanken machen muss und dies entsprechend dokumentiert. Anstelle eines Bearbeitungsreglements (vgl. Art. 6 DSV) kann der Nachweis daher durch verschiedene Dokumente erbracht werden, welche im Rahmen der Verwaltungsorganisation oder von IT-Projekten sowieso erarbeitet werden sollen (z.B. Geschäftsordnungen, Weisungen zu Datenbearbeitungen oder Informationssicherheits- und Datenschutzkonzepte). Der Nachweis kann auch geleistet werden durch Dokumente, welche aufgrund neuer gesetzlicher Vorgaben erarbeitet werden müssen (z.B. DSFA). Gegebenenfalls wird die Aufsichtsstelle weitere Hilfeleistungen darüber bieten, wie entsprechende Dokumente zu gestalten sind, um den Nachweis erbringen zu können. Ein wichtiger Teil der Verordnung befasst sich damit, wie die technischen und organisatorischen Massnahmen zur Wahrung der Datensicherheit ausgestaltet sein sollen (Art. 6 KDSG). Einerseits sollen die Ziele genannt werden, an welchen sich diese Massnahmen zu orientieren haben (Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit). Diese Ziele sind nicht neu, sondern sollten in IT-Projekten z.B. aus Aspekten der Informationssicherheit bereits grundsätzlich beachtet werden. Es müssen lediglich Massnahmen ergriffen werden, welche angemessen sind. Die Angemessenheit der Massnahmen wird dabei insbesondere nach dem Schutzbedarf der Daten, den möglichen Risiken, dem Stand der Technik und den Implementierungskosten zu bewerten sein. Aufgrund der verschiedenen Faktoren und des technologischen Fortschritts ist es kaum möglich und sinnvoll, konkrete Massnahmen auf Verordnungsstufe zu definieren. Daher wird darauf wie in anderen Kantonen grundsätzlich verzichtet. Lediglich in Berei-

chen, wo übergreifende Vorgaben im Sinne eines Mindeststandards gemacht werden müssen, wird dies auf Verordnungsstufe vorgenommen. Die entsprechenden Regelungen besagen, dass Zugriff- und Zugangsberechtigungen nur für diejenigen Personen gelten sollen, welche die entsprechenden Daten benötigen (Umsetzung des Verhältnismässigkeitsgrundsatzes) oder dass die automatisierte Bearbeitung von besonders schützenswerten Personendaten zu protokollieren ist, wenn der Datenschutz nicht durch andere präventive Massnahmen gewährleistet werden kann.

In der Verordnung wird definiert, wann und in welchem Verfahren Pilotversuche zu automatisierten Datenbearbeitungen durchgeführt werden können. Diese Regelungen werden sich am Bundesrecht (Art. 32–35 DSV) orientieren. Betreffend die Auftragsdatenbearbeitung sind gewisse Mindestvorgaben an die entsprechenden Verträge zu statuieren. Die entsprechenden Vorgaben ergeben sich aus der Literatur und Rechtsprechung zu Art. 9a aDSG. Sie werden in anderen Kantonen oft in der Verordnung zur Datenschutzgesetzgebung konkretisiert. Für Organe der Kantonalen Verwaltung werden entsprechende Mindestvorgaben an die Auslagerung von Dienstleistungen bereits in Art. 2 VDVG statuiert. Aufgrund der engen Verzahnung dieser Bestimmung mit dem Datenschutzrecht (vgl. oben Art. 9) wird es als sinnvoll erachtet, die entsprechenden Regeln auch für andere dem KDSG unterstehende Organe zu übernehmen. Es gilt darauf hinzuweisen, dass im Internet eine Vielzahl an Musterverträgen und Wegleitungen existieren, welche sich nach diesen Vorgaben richten. Diese können daher für entsprechende Vertragsdokumente als Vorlage verwendet werden. Bei der Bekanntgabe von Personendaten ins Ausland muss für die Daten auch im Ausland ein angemessener Schutz gewährleistet werden. Die Verordnung soll definieren, wann dies der Fall ist. Es erscheint sinnvoll, dass hier in erster Linie auf die vom Bundesrat als gleichwertig anerkannten Länder verwiesen wird. Diese sind in einer Länderliste als Anhang zur DSV aufgeführt. Zudem sollen auch vom EDÖB anerkannte Standarddatenschutzklauseln und Modellverträge anerkannt werden.

Im Zusammenhang mit den Pflichten der Verantwortlichen soll festgelegt werden, dass die Information über die Beschaffung von Personendaten (Art. 17 KDSG) in präziser, transparenter, verständlicher und leicht zugänglicher Form zu erfolgen hat. In der Verordnung werden zudem die neuen Instrumente und Verpflichtungen aus dem dritten Abschnitt des Gesetzes konkretisiert. Im Hinblick auf die DSFA und die Vorabkonsultation sollen gewisse Mindestvorgaben an die zu erarbeitende Dokumentation und deren Aufbewahrungsdauer gemacht werden. Auch bei diesen Verpflichtungen wird es möglich sein, die Dokumentation durch Dokumente zu erbringen, welche bereits nach geltendem Recht erarbeitet werden (vgl. die Ausführungen zu Art. 19 KDSG). Ebenso werden die Modalitäten hinsichtlich der

Meldepflicht bei Verletzungen der Datensicherheit in der Verordnung konkretisiert. Zudem wird statuiert, dass entsprechende Vorfälle und deren Bewältigung zu dokumentieren und aufzubewahren sind. Die Aufsichtsstelle wird bereits vorab zum Inkrafttreten des KDSG aufgrund der Vorgaben des Bundesrechts gewisse Dokumente im Zusammenhang mit den hier genannten Instrumenten als Hilfestellung veröffentlichen.

Hinsichtlich des Verzeichnisses über die Bearbeitungstätigkeiten und der Ernennung einer Datenschutzberaterin oder eines Datenschutzberaters wird die Verordnung insbesondere die betroffenen öffentlichen Organe konkretisieren. Wie weiter oben ausgeführt, sollen nur die Behörden diese Verpflichtungen erfüllen müssen, welche unter die Vorgaben der RL 2016/680 fallen. Diese sind in Art. 3 Abs. 7 RL 20116/680 umschrieben. Die Verpflichtung umfasst insbesondere die Strafverfolgungs- und die Justizvollzugbehörden; sie gilt für alle Organe, welche Zugriff auf das Schengener Informationssystem haben. Neben der Kantonspolizei und der Staatsanwaltschaft sind somit zurzeit das Amt für Justizvollzug, das Amt für Migration und Zivilrecht sowie die Stadtpolizei Chur betroffen. Diese öffentlichen Organe werden in der Verordnung namentlich aufgeführt. Hinsichtlich der Ausgestaltung dieser Aufgabe soll statuiert werden, dass die Person ein gewisses Fachwissen mitbringen und/oder durch die Aufsichtsstelle zu schulen ist und dass ein öffentliches Organ mehrere Personen als Beraterin oder Berater ernennen kann oder diese mit anderen öffentlichen Organen gemeinsam ernennen kann, sofern dies sinnvoll erscheint.

Ein weiteres Kapitel der Verordnung konkretisiert die Ausgestaltung der Betroffenenrechte. Darin soll statuiert werden, welche Vorgaben entsprechende Gesuche zu erfüllen haben. Die Gesuchstellung darf nicht mit hohen Hürden für die betroffene Person verbunden sein, dennoch muss gerade bei einem Gesuch um Auskunft über die eigenen Personendaten die Identität der betroffenen Person überprüft werden können. Hinsichtlich der Kostentragung wird umschrieben, wann ein unverhältnismässiger Aufwand vorliegt, welcher eine Gebührenerhebung nach Art. 28 KDSG rechtfertigen kann. Dies kann namentlich der Fall sein, wenn komplizierte Verhältnisse vorliegen oder umfangreiche Anonymisierungen vorgenommen werden müssen oder wenn für die gesuchstellende Person Kopien oder sonstige Datenträger angefertigt werden müssen. Auch hinsichtlich des Rechts auf Widerspruch gegen die Bekanntgabe werden die Modalitäten statuiert. In diesem Zusammenhang soll festgeschrieben werden, dass das öffentliche Organ, bei dem der Widerspruch hinterlegt wurde, auch andere öffentliche Organe über diesen Umstand in Kenntnis setzt, denen es die Daten weitergibt. Ansonsten würde der Zweck der Sperrung durch die Weitergabe unterlaufen.

2. Verordnung über die Bildüberwachung des öffentlichen und öffentlich zugänglichen Raums (VBÜ; BR 171.120)

In der VBÜ wird an verschiedenen Stellen explizit auf die Art. 3a und 3b des geltenden KDSG verwiesen. Daher sind diese Verweise anzupassen. Zudem beziehen sich Art. 5 Abs. 2 und Art. 7 explizit auf die oder den Datenschutzbeauftragten. An diesen Stellen wird neu die Aufsichtsstelle genannt werden, welche nicht länger nur aus der oder dem Datenschutzbeauftragten besteht. Zudem ist Art. 9 anzupassen. Diese Bestimmung regelt, wer nachträglich in die Bildaufzeichnung Einsicht nehmen kann. Hier sind bisher in der Allgemeinverfügung zwei Personen zu bezeichnen, welche zur Einsicht berechtigt sind. Diese Regelung hat sich in der Praxis als zu starr erwiesen. Neu wird daher auf eine ausdrückliche Beschränkung der Personenzahl verzichtet. Die Einsichtnahme ist aber auf die Personen zu beschränken, die zur Beurteilung der Aufzeichnung notwendig sind. Zudem wird die Einsichtnahme wie bereits bislang protokolliert (vgl. Art. 10 VBÜ). Bisher wird zudem die Kantonspolizei ermächtigt, Bildaufzeichnungen ohne Hängigkeit eines konkreten Verfahrens einzusehen (Art. 9 Abs. 2 und Art 13. Abs. 2 VBÜ). Zu diesem Zweck ist sie auch über neue Allgemeinverfügungen, in welchen eine Bildüberwachung angeordnet wird, zu informieren (Art. 7 Abs. 1 VBÜ). Zumal aufgrund der Vernehmlassung Einschränkungen zum Schutz der Betroffenen vorgenommen wurden (vgl. Art. 14 VBÜ), sind derart weitreichende Einsichtsrechte der Kantonspolizei ohne das Vorliegen eines entsprechenden Verfahren kaum zu rechtfertigen. Sie sind in den Kantonen, welche die Bildüberwachung geregelt haben, soweit ersichtlich singulär. Die Strafverfolgungs- bzw. Gerichtsbehörden sollen sich erst mit den Daten anderer öffentlicher Organe befassen können, wenn ein Verfahren anhängig gemacht oder sie aufgrund einer anderweitigen Rechtsgrundlage Einsicht in diese Bilder erhalten dürfen. Die entsprechenden Bestimmungen werden daher angepasst.

V. Personelle und finanzielle Auswirkungen

1. Für den Kanton

Die aufgrund der Anpassung an das internationale Recht erforderlichen Neuerungen im Datenschutzrecht führen zu einem gewissen Mehraufwand. Bei der Umsetzung wurde darauf geachtet, dass die vom übergeordneten Recht belassenen Handlungsspielräume wahrgenommen und nur zwingende Vorgaben umgesetzt werden. So müssen z.B. die in der RL 2016/680 vorgesehenen Instrumente (Verzeichnis der Datenbearbeitungstätigkeiten, Datenschutzberatung) nur sektoriell umgesetzt werden. Andere Verpflichtungen, wie die Meldepflicht von Datenschutzverletzungen oder die Datenschutz-Folgenabschätzung, sind jedoch durch alle dem Gesetz unterstellten Organe umzusetzen. Hier ist zu beachten, dass die Aufsichtsstelle mit der vorgeschlagenen höheren Dotierung vermehrt proaktiv tätig sein soll und die Gemeinden, Regionen, Dienststellen und Departemente etwa durch die Publikation von Merkblättern zu den neuen Instrumenten unterstützen kann. Es wird daher davon ausgegangen, dass diese Instrumente und Verpflichtungen in der Kantonalen Verwaltung mit den bestehenden Ressourcen eingeführt werden können. Bei der Datenschutzberaterin oder dem Datenschutzberater, welche für gewisse Behörden zwingend vorgesehen sind, handelt es sich nicht zwingend um neu zu schaffende Stellen. In den bezeichneten Organen muss in einem bestimmten Umfang Fachwissen im Bereich Datenschutz aufgebaut werden, um die Mitarbeitenden zu unterstützen und gegenüber der Aufsichtsstelle als Ansprechpartner auftreten zu können. Dies kann aber auch als Zusatzaufgabe für einen oder mehrere bestehende Mitarbeitende verstanden werden, welche in diesen Bereichen bereits Vorwissen oder Neigungen mitbringen (z.B. IT-Projektleitende). Allfällige zusätzliche Ressourcen sind innerhalb des finanzpolitischen Richtwerts (6) zu schaffen.

Die Aufsichtsstelle wiederum kann ihre Aufgaben nur dann unabhängig erfüllen, wenn sie die für die Aufgabenerfüllung erforderlichen Ressourcen zugesprochen erhält. Der kantonale Datenschutzbeauftragte ist bisher in einem 50%-Pensum tätig und erhält eine fixe Pauschalentschädigung, welche neben einem Honorar auch die weiteren Ausgaben im Zusammenhang mit der Tätigkeit deckt (z.B. Sekretariat, Räumlichkeiten). Mit der Revision werden der Aufsichtsstelle aufgrund des Völkerrechts zwingend umzusetzende, neue Aufgaben und Befugnisse auferlegt. Die bisherige Dotierung dürfte kaum ausreichen, um die bestehenden und insbesondere die neu hinzukommenden Aufgaben wirksam zu erfüllen. Die KdK empfiehlt bereits für kleine Kantone ein Pensum von 50 bis 100 Stellenprozenten (KdK-Leitfaden, S. 27). In Kantonen, welche von ihrer Grösse her mit Graubünden vergleichbar sind, werden die entsprechenden Aufsichtsstellen wesentlich

höher dotiert.[6] Auch wenn diese Behörden teilweise zusätzliche Aufgaben wahrnehmen (z. B. als Öffentlichkeitsbeauftragte) und die Kantone andere Voraussetzungen haben, so zeigt dies dennoch eine Unterdotierung der heutigen Aufsichtsstelle auf. Dies insbesondere zumal die Aufsichtsstelle bereits nach dem geltenden Recht und auch zukünftig die Beratung der und die Aufsicht über die derzeit 101 Gemeinden wahrnimmt. Aus diesem Grund wird im Zusammenhang mit der Revision des Datenschutzgesetzes die Dotierung der oder des Datenschutzbeauftragten anzuheben sein. Die oder der Datenschutzbeauftragte soll aufgrund der neuen Aufgaben als 80 – 100 %-Stelle ausgestaltet werden. Zudem soll eine weitere Mitarbeiterin oder ein weiterer Mitarbeiter als Stellvertretung angestellt werden (50 – 70 %). Überdies scheint es sinnvoll, der Stelle eine oder ein für die Administration verantwortliche Mitarbeiterin oder Mitarbeiter zur Verfügung zu stellen (50 %). Die entsprechenden Aufwände für Sekretariatsarbeiten werden bisher im Pauschalbetrag abgegolten. Zusammengefasst ist mit dem Inkrafttreten des Gesetzes von einem zusätzlichen Stellenbedarf von maximal 170 Stellenprozenten auszugehen, da die Aufsichtsstelle ab diesem Zeitpunkt die neuen Aufgaben wahrnehmen muss.

Bisher wird die oder der Datenschutzbeauftragte in der Jahresrechnung mit einem jährlichen Pauschalbetrag von ca. 160 000 Franken ausgewiesen. Dieser umfasst neben der Entschädigung der Amtsträgerin oder des Amtsträgers auch sämtliche weiteren mit der Tätigkeit verbundenen Kosten (Administration, Beizug externer Sachverständiger, Materialkosten). Die Entlöhnung der oder des Datenschutzbeauftragten und ihrer oder seiner Mitarbeitenden soll sich neu am kantonalen Personalrecht orientieren (vgl. auch Art. 34). Ausgehend von den beantragten Pensen ist dabei mit Lohnkosten in der Höhe von ungefähr maximal 335 000 Franken (inkl. Arbeitgeberbeiträge an die Sozialversicherungen und die Pensionskassen) zu rechnen. Diese setzen sich zusammen aus den Lohnkosten für die oder den Datenschutzbeauftragten als Leiterin oder Leiter der Aufsichtsstelle (bei einem 100 %-Pensum ungefähr 185 000 Franken), der Einstellung einer juristischen oder IT-Fachperson als Stellvertretung (bei einem 70 %-Pensum ungefähr 105 000 Franken) und einer Sekretariatsmitarbeiterin oder eines Sekretariatsmitarbeiters (bei einem 50 %-Pensum ungefähr 45 000 Franken). Hinzu kommen Kosten für Büroräumlichkeiten, welche bisher im Rahmen der Pauschale abgegolten werden. Für die Büroräumlichkeiten wird von zusätzlichen jährlichen Kosten von ca. 20 000 Franken ausgegangen. Auch weiterer Sach- oder Betriebsaufwand (etwa für Büromaterial und Literatur, Mitgliedschaften oder den

[6] Vgl. etwa BL: 530 Stellenprozent; BS: 600 Stellenprozent (ab 2025: 750 Stellenprozent), SO: 360 Stellenprozent, SZ/OW/NW (gemeinsame Aufsichtsstelle): 230 Stellenprozent, ZG: 260 Stellenprozent (die entsprechenden Zahlen ergeben sich aus den jeweiligen Jahresberichten der Behörden für das Jahr 2023).

Beizug externer Experten) wird bisher über den Pauschalbetrag abgegolten. Die entsprechenden Kosten dürften jährlich unterschiedlich ausfallen und sind in anderen Kantonen je nach Grösse der Aufsichtsstelle mit 10 000 bis 200 000 Franken beziffert. Sie dürften im Kanton Graubünden die Grössenordnung von 50 000 Franken nicht übersteigen. Somit ist mit jährlichen Kosten in der Höhe von ca. 405 000 Franken zu rechnen.[7] Die Mehrkosten gegenüber dem bisherigen Pauschalbetrag dürften sich somit auf ca. 245 000 Franken pro Jahr belaufen. Für die Ausstattung der Büroräumlichkeiten ist zudem mit einmaligen Mehrkosten für Mobiliar und IT-Infrastruktur (inkl. Anschliessung an das EDV-Netz des Kantons) zu rechnen. Deren genaue Höhe ist schwer einzuschätzen und beispielsweise abhängig davon, ob bereits im Besitz des Kantons sich befindliche Räumlichkeiten genutzt werden können oder neue hinzugemietet und erschlossen werden müssen. Es wird in diesem Zusammenhang von einem einmaligen Betrag von ca. 130 000 Franken Betrag ausgegangen.

Die erhöhte Dotierung wird im Gegenzug dazu führen, dass die Aufsichtsstelle vermehrt proaktiv tätig werden kann. So kann sie z. B. zuhanden der Gemeinden, Regionen und des Kantons vermehrt Merkblätter oder Hilfestellungen publizieren oder Schulungen durchführen. Dadurch kann wiederum der bei den öffentlichen Organen anfallende Mehraufwand vermindert werden, welchen sie ansonsten weitgehend selbstständig zu tragen hätten.

Die neuen Stellen sind mit dem Inkrafttreten des Gesetzes zu schaffen, da die oder der Datenschutzbeauftragte ab diesem Zeitpunkt die neuen Aufgaben wahrnehmen muss. Eine über Jahre anhaltende Stellenschaffung im Rahmen der ordentlichen jährlichen Lohnsummenerhöhung wäre mit der Gefahr verbunden, dass diese Stellen erst nach und nach geschaffen werden können und die Aufsichtsstelle somit ihre Aufgabe nicht gesetzesgetreu wahrnehmen kann. Die Aufsichtsstelle übt bereits heute die Aufsicht über die Gemeinden aus und soll diese aufgrund der besseren Dotierung zukünftig besser unterstützen können. Zudem gilt es der Stellung der Aufsichtsstelle als unabhängiges Aufsichtsorgan, welches nur administrativ an die Verwaltung angegliedert ist, Rechnung zu tragen. Dies verlangt nicht zuletzt die völkerrechtlichen Vorgaben. Um den Vorgaben an die Unabhängigkeit der Stelle gerecht zu werden, wird beantragt, dass die entsprechenden Stellen vom finanzpolitischen Richtwert Nr. 6 betreffend die Lohnsumme für die Stellenbewirtschaftung ausgenommen werden. Dies betrifft einerseits die bestehenden 0.5 Vollzeitstellen des kantonalen Datenschutzbeauftragten, da

[7] Die Aufsichtsstellen in den oben genannten Kantonen (Fussnote 6) operieren gemäss den jeweiligen Jahresberichten bzw. Tätigkeitsberichten 2023 mit einem Budget von ca. 500 000 bis zu 1,3 Mio. Franken.

diese bisher auf privatrechtlicher Basis entstehen und seine Entlohnung somit nicht als Lohnkosten ausgewiesen wird. Zusätzlich sollen aber auch die neu zu schaffenden 1.7 Vollzeitstellen für die Pensenerhöhung sowie die Anstellung einer Stellvertretung und einer administrativen Mitarbeiterin oder eines administrativen Mitarbeiters vom Richtwert ausgenommen werden.

Die Aufsichtsstelle wird administrativ weiterhin der Standeskanzlei unterstellt sein, was insbesondere bedeutet, dass die Standeskanzlei sie bei der Erfüllung der ihr übertragenen Aufgaben unterstützt (vgl. oben Art. 31). Durch die geänderte Ausgestaltung der Aufsichtsstelle (eigene Büroräumlichkeiten, eigenes Budget, Wahl und Wiederwahl durch die Regierung) kommen auch auf die Standeskanzlei neue oder im Vergleich zur heutigen Situation umfangreichere Aufgaben zu. Wie gross der sich daraus ergebende Mehraufwand für die Standeskanzlei sein wird, lässt sich nicht zuverlässig abschätzen. Sollte sich zeigen, dass diese neuen Aufgaben mit den bestehenden Ressourcen nicht bewältigt werden können, wird die Standeskanzlei die erforderlichen personellen Ressourcen im Rahmen des ordentlichen Stellenbeschaffungsprozesses beantragen.

2. Für die Regionen und Gemeinden

Die öffentlichen Organe von Regionen und Gemeinden unterstehen ebenfalls dem KDSG. Aufgrund der völkerrechtlichen Vorgaben haben auch sie gewisse der neu geschaffenen Verpflichtungen umzusetzen, was für sie mit einem Mehraufwand verbunden ist. Im Rahmen der Vernehmlassung wurde insbesondere von Seiten der Gemeinden vorgebracht, dass sich aufgrund der knappen Ausführungen in der Vernehmlassungsvorlage nicht schlüssig beurteilen lasse, welche personellen und finanziellen Auswirkungen auf die Regionen und Gemeinden zukomme. Es wird insbesondere gefordert, dass die neu auf die Gemeinwesen zukommenden Instrumente und Verpflichtungen konkret aufgezeigt werden und der Kanton Hilfestellungen und Vorlagen zu deren Umsetzung bereitstelle.

Der konkrete finanzielle und personelle Mehraufwand, welcher auf die Gemeinwesen zukommt, hängt von einer Vielzahl verschiedener Faktoren ab. Namentlich ist darin etwa die Grösse der Gemeinde oder die Anzahl an Projekten, welche eine DSFA nach sich ziehen, zu berücksichtigen. Dies führt dazu, dass der Aufwand nicht zuverlässig beziffert werden kann. Die neuen Aufgaben ergeben sich grundsätzlich aus den völkerrechtlichen Vorgaben, so dass kaum Handlungsspielraum darüber besteht, ob diese durch die Gemeinden umgesetzt werden müssen und nur in geringem Masse darauf, wie sie umgesetzt werden müssen. Es gilt zu beachten, dass die meisten der neuen Instrumente und Verpflichtungen (namentlich die Anpassung

von Auftragsdatenbearbeitung gemäss Art. 9 KDSG, die Durchführung von DSFA und Vorabkonsultation sowie die Meldepflicht) aufgrund der dynamischen Verweise bereits seit dem Inkrafttreten des DSG am 1. September 2023 gelten. Sie sind daher unabhängig von der vorliegenden Revision umzusetzen. Dies trifft lediglich auf den Nachweis der Einhaltung der Datenschutzbestimmungen nicht zu. Daher soll für dessen Umsetzung auch eine Übergangsfrist gelten (vgl. Art. 41 KDSG). Schlussendlich gilt es erneut darauf hinzuweisen, dass die Aufsichtsstelle durch die beabsichtigte höhere Dotierung in grösserem Masse als bisher proaktiv tätig werden kann. Dies ist mit der Erwartung verbunden, dass sie Gemeinden und Regionen beispielsweise durch die Publikationen von Merkblättern und Leitfäden (wie im Rahmen der Vernehmlassung gefordert) bei der Umsetzung der entsprechenden Neuerungen und Verpflichtung unterstützen kann. Zudem kann die Aufsichtsstelle ihre bereits bisherige Beratungs- und Schulungstätigkeit besser wahrnehmen. Diese Massnahme soll ebenfalls dazu dienen, den für die Gemeinden anfallenden Mehraufwand so gering als möglich zu halten und gleichzeitig die völkerrechtlichen Vorgaben zu erfüllen.

VI. Gute Gesetzgebung

Die Grundsätze der «Guten Gesetzgebung» gemäss den regierungsrätlichen Vorgaben (vgl. RB vom 16.11.2010, Prot. Nr. 1070) werden mit der Revisionsvorlage beachtet.

VII. Inkrafttreten

Zuständig für die Inkraftsetzung ist die Regierung. Für die erstmalige Wahl der oder des neuen Datenschutzbeauftragten wird eine gewisse Zeit benötigt. Daher soll die Inkraftsetzung gestaffelt erfolgen. In einem ersten Schritt sind daher die Bestimmungen zur Wahl der oder des Datenschutzbeauftragten in Kraft zu setzen (Art. 31,32 und 33 KDSG). Dies soll voraussichtlich per 1. Juli 2025 geschehen. Die weiteren Bestimmungen können erst in Kraft treten, wenn die Rekrutierung dieser Person abgeschlossen ist. Es wird davon ausgegangen, dass dies Anfang 2026 der Fall sein wird.

VIII. Anträge

Gestützt auf diese Botschaft beantragen wir Ihnen:

1. auf die Vorlage einzutreten;

2. die 2.2 Vollzeitstellen der Aufsichtsstelle Datenschutz zur Stärkung der Aufsichtsstelle vom finanzpolitischen Richtwert Nr. 6 betreffend die Lohnsumme für die Stellenbewirtschaftung auszunehmen;

3. der Totalrevision des Kantonalen Datenschutzgesetzes zuzustimmen.

Genehmigen Sie, sehr geehrte Frau Standespräsidentin, sehr geehrte Damen und Herren, den Ausdruck unserer vorzüglichen Hochachtung.

Namens der Regierung
Der Präsident: *Parolini*
Der Kanzleidirektor: *Spadin*

Abkürzungsverzeichnis / Abreviaziuns / Elenco delle abbreviazioni

aDSG	Bundesgesetz über den Datenschutz vom 19. Juni 1992 (Datenschutzgesetz; SR 235.1)
vLPD	*Lescha federala dals 19 da zercladur 1992 davart la protecziun da datas (CS 235.1)*
vLPD	*Legge federale del 19 giugno 1992 sulla protezione dei dati (RS 235.1)*
AFI	Amt für Informatik
UI	*Uffizi d'informatica*
UI	*Ufficio d'informatica*
BBl	Bundesblatt
FF	*Fegl uffizial federal*
FF	*Foglio federale*
BGE	Bundesgerichtsentscheid
DTF	*decisiun dal Tribunal federal*
DTF	*Decisione del Tribunale federale*
BGÖ	Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung (SR 152.3)
LTrans	*Lescha federala davart il princip da la transparenza da l'administraziun (CS 152.3)*
LTras	*Legge federale sul principio di trasparenza dell'amministrazione (RS 152.3)*
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft (SR 101)
Cst.	*Constituziun federala da la Confederaziun svizra (CS 101)*
Cost.	*Costituzione federale della Confederazione svizzera (RS 101)*
DSFA	Datenschutz-Folgenabschätzung
VCPD	*valitaziun da las consequenzas per la protecziun da datas*
VIPD	*Valutazione d'impatto sulla protezione dei dati*
DSG	Bundesgesetz über den Datenschutz vom 25. September 2020 (Datenschutzgesetz; SR 235.1)
LPD	*Lescha federala dals 25 da settember 2020 davart la protecziun da datas (CS 235.1)*
LPD	*Legge federale del 25 settembre 2020 sulla protezione dei dati (RS 235.1)*
DSGVO	Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutz-Grundverordnung)
RGPD	*Reglament (UE) 2016/679 davart la protecziun da persunas natiralas concernent l'elavuraziun da datas persunalas (Reglament general davart la protecziun da datas)*
GDPR	*Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (Regolamento generale sulla protezione dei dati)*

DSV	Verordnung über den Datenschutz (SR 235.11)
OPDa	*Ordinaziun davart la protecziun da datas (CS 235.11)*
OPDa	*Ordinanza sulla protezione dei dati (RS 235.11)*
DJSG	Departement für Justiz, Sicherheit und Gesundheit
DGSS	*Departament da giustia, segirezza e sanadad*
DGSS	*Dipartimento di giustizia, sicurezza e sanità*
DVG	Gesetz über die digitale Verwaltung (BR 177.100)
LAD	*Lescha davart l'administraziun digitala (DG 177.100)*
LADig	*Legge sull'amministrazione digitale (CSC 177.100)*
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
IFPDT	*Incumbensà federal per la protecziun da datas e per la transparenza*
IFPDT	*Incaricato federale della protezione dei dati e della trasparenza*
ERG	Gesetz über die Einwohnerregister und weitere Personen- und Objektregister (BR 171.200)
LRAb	*Lescha davart ils registers d'abitantas e d'abitants e davart ulteriurs registers da persunas e d'objects (DG 171.200)*
LRAb	*Legge sui registri degli abitanti e su altri registri delle persone e degli oggetti (CSC 171.200)*
EGzStPO	Einführungsgesetz zur Schweizerischen Strafprozessordnung (BR 350.100)
LItCPP	*Lescha introductiva tar il Cudesch da procedura penala svizzer (DG 350.100)*
LACPP	*Legge d'applicazione del Codice di diritto processuale penale svizzero (CSC 350.100)*
EGzZPO	Einführungsgesetz zur Schweizerischen Zivilprozessordnung (BR 320.100)
LItCPC	*Lescha introductiva tar il Cudesch da procedura civila svizzer (DG 320.100)*
LACPC	*Legge d'applicazione del Codice di diritto processuale civile svizzero (CSC 320.100)*
GAA	Gesetz über die Aktenführung und Archivierung (BR 490.000)
LGDA	*Lescha davart la gestiun da documents e l'archivaziun (DG 490.000)*
LGAA	*Legge sulla gestione degli atti e sull'archiviazione (CSC 490.000)*
GFA	Gesetz über die Finanzaufsicht (BR 710.300)
LSFi	*Lescha davart la surveglianza da las finanzas (DG 710.300)*
LVF	*Legge sulla vigilanza finanziaria (CSC 710.300)*
GKB	Graubündner Kantonalbank
BCG	*Banca Chantunala Grischuna*
BCG	*Banca Cantonale Grigione*
ISDS-Konzept	Informationssicherheits- und Datenschutz-Konzept
concept SIPD	*concept davart la segirezza da las infurmaziuns e la protecziun da datas*
Piano SIPD	*Piano per la sicurezza dell'informazione e la protezione dei dati*

KBüG	Bürgerrechtsgesetz des Kantons Graubünden (BR 130.100)
LDBchant	*Lescha dal dretg da burgais dal chantun Grischun (DG 130.100)*
LCCit	*Legge sulla cittadinanza del Cantone dei Grigioni (CSC 130.100)*
KdK	Konferenz der Kantonsregierungen
CdC	*Conferenza da las regenzas chantunalas*
CdC	*Conferenza dei governi cantonali*
KDSG	Kantonales Datenschutzgesetz (BR 171.100)
LCPD	*Lescha chantunala davart la protecziun da datas (DG 171.100)*
LCPD	*Legge cantonale sulla protezione dei dati (CSC 171.100)*
KGÖ	Gesetz über das Öffentlichkeitsprinzip (BR 171.000)
LCTrans	*Lescha davart il princip da transparenza (DG 171.000)*
LCTras	*Legge sul principio di trasparenza (CSC 171.000)*
PolG	Polizeigesetz des Kantons Graubünden (BR 613.000)
LPol	*Lescha da polizia dal chantun Grischun (DG 613.000)*
LPol	*Legge sulla polizia del Cantone dei Grigioni (CSC 613.000)*
RL 2016/680	Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Bearbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr
Dir 2016/680	*Directiva (UE) 2016/680 per la protecziun da persunas natiralas areguard l'elavuraziun da datas da caracter persunal tras las autoritads cumpetentas per la prevenziun, la retschertga, la scuvrida u la persecuziun da malfatgs u da l'execuziun dal chasti sco er per il traffic liber da datas*
Direttiva 2016/680	*Direttiva (UE) 2016/680 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati*
RVOG	Regierungs- und Verwaltungsorganisationsgesetz (SR 172.010)
LORA	*Lescha davart l'organisaziun da la regenza e da l'administraziun (CS 172.010)*
LOGA	*Legge sull'organizzazione del Governo e dell'Amministrazione (RS 172.010)*
Übereinkommen SEV 108	Europäisches Übereinkommen vom 28. Januar 1981 zum Schutz des Menschen bei der automatisierten Verarbeitung von personenbezogenen Daten (SR 0.235.1) und dessen Zusatzprotokoll (SR 0.235.11)
Convenziun STE 108	*Convenziun europeica dals 28 da schaner 1981 davart la protecziun da persunas tar l'elavuraziun automatisada da datas da caracter persunal (CS 0.235.1) e ses Protocol supplementar (CS 0.235.11)*
Convenzione STE 108	*Convenzione europea del 28 gennaio 1981 per la protezione delle persone in relazione all'elaborazione automatica dei dati a carattere personale (RS 0.235.1) e il suo protocollo aggiuntivo (RS 0.235.11)*
SIS	Schengener Informationssystem
SIS	*sistem d'infurmaziun da Schengen*
SIS	*Sistema d'informazione Schengen*

StG	Steuergesetz für den Kanton Graubünden (BR 720.000)
LT	*Lescha da taglia per il chantun Grischun (DG 720.000)*
LIG	*Legge sulle imposte per il Cantone dei Grigioni (CSC 720.000)*
StPO	Schweizerische Strafprozessordnung (SR 312.0)
CPP	*Cudesch da procedura penala svizzer (CS 312.0)*
CPP	*Codice di diritto processuale penale svizzero (RS 312.0)*
VBÜ	Verordnung über die Bildüberwachung des öffentlichen und öffentlich zugänglichen Raums (BR 171.120)
OSVis	*Ordinaziun davart la surveglianza visuala dal spazi public e dal spazi ch'è accessibel al public (DG 171.120)*
OSImm	*Ordinanza sulla sorveglianza con acquisizione di immagini dello spazio pubblico e pubblicamente accessibile (CSC 171.120)*
VDSG	Verordnung zum Bundesgesetz über den Datenschutz vom 14. Juni 1993 (SR 235.11), ausser Kraft
OLPD	*Ordinaziun dals 14 da zercladur 1993 tar la Lescha federala davart la protecziun da datas (CS 235.11), ord vigur*
OLPD	*Ordinanza del 14 giugno 1993 relativa alla legge federale sulla protezione dei dati (RS 235.11), abrogata*
VDVG	Verordnung zum Gesetz über die digitale Verwaltung (BR 177.110)
OLAD	*Ordinaziun tar la Lescha davart l'administraziun digitala (DG 177.110)*
OLADig	*Ordinanza relativa alla legge sull'amministrazione digitale (CSC 177.110)*
VKDSG	Verordnung zum Kantonalen Datenschutzgesetz (BR 171.110)
OLCPD	*Ordinaziun tar la Lescha chantunala davart la protecziun da datas (DG 171.110)*
OLCPD	*Ordinanza relativa alla legge cantonale sulla protezione dei dati (CSC 171.100)*
VRG	Gesetz über die Verwaltungsrechtspflege (BR 370.100)
LGA	*Lescha davart la giurisdicziun administrativa (DG 370.100)*
LGA	*Legge sulla giustizia amministrativa (CSC 370.100)*

Kantonales Datenschutzgesetz (KDSG)

Vom [Datum]

Von diesem Geschäft tangierte Erlasse (BR Nummern)

Neu:	**171.100**
Geändert:	130.100 | 171.200 | 320.100 | 350.100 | 710.300
Aufgehoben:	171.100

Der Grosse Rat des Kantons Graubünden,

gestützt auf Art. 31 Abs. 1 der Kantonsverfassung[1)],
nach Einsicht in die Botschaft der Regierung vom ...,

beschliesst:

I.

Der Erlass "Kantonales Datenschutzgesetz (KDSG)" BR 171.100 wird als neuer Erlass publiziert.

1. Allgemeine Bestimmungen

Art. 1 Zweck

[1] Dieses Gesetz dient dem Schutz von Personen vor widerrechtlichem Bearbeiten von Personendaten durch öffentliche Organe.

Art. 2 Geltungsbereich

[1] Dieses Gesetz gilt für die Bearbeitung von Personendaten durch öffentliche Organe.

[1)] BR 110.100

[2] Soweit ein öffentliches Organ am wirtschaftlichen Wettbewerb teilnimmt und dabei nicht hoheitlich handelt, sind auf diese Datenbearbeitungen die Regeln des Bundesgesetzes über den Datenschutz[2)] anwendbar. Die Aufsicht richtet sich nach dem vorliegenden Gesetz, ausser bei öffentlichen Organen, die ausschliesslich am wirtschaftlichen Wettbewerb teilnehmen und dabei privatrechtlich handeln.

[3] Das anwendbare Verfahrensrecht regelt die Bearbeitung von Personendaten und die Rechte der betroffenen Personen in Gerichtsverfahren und in Verfahren nach bundesrechtlichen Verfahrensordnungen sowie in Verfahren der Verwaltungsrechtspflege mit Ausnahme der erstinstanzlichen Verfahren vor Verwaltungsbehörden.

[4] Abweichende und ergänzende Bestimmungen in anderen Gesetzen bleiben vorbehalten, sofern sie den Schutz der Grundrechte von Personen, über welche die öffentlichen Organe Personendaten bearbeiten, im Sinne dieses Gesetzes sicherstellen.

Art. 3 Begriffe

[1] Als öffentliche Organe im Sinne dieses Gesetzes gelten:

a) die Behörden, Verwaltungen und Kommissionen des Kantons, der Regionen, Gemeinden und Gemeindeverbindungen;
b) die Behörden, Verwaltungen und Kommissionen der öffentlich-rechtlichen Anstalten, Stiftungen und Körperschaften des Kantons, der Regionen und Gemeinden;
c) natürliche oder juristische Personen oder andere privatrechtliche Organisationen, soweit sie ihnen übertragene öffentliche Aufgaben erfüllen.

[2] Personendaten im Sinne dieses Gesetzes sind alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche oder juristische Person beziehen.

[3] Besonders schützenswerte Personendaten sind Personendaten, bei welchen eine besondere Gefahr für Grundrechtsverletzungen besteht, insbesondere:

a) Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten;
b) Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie;
c) genetische Daten;
d) biometrische Daten, die eine natürliche Person eindeutig identifizieren;
e) Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen;
f) Daten über Massnahmen der sozialen Hilfe.

[4] Persönlichkeitsprofile sind Zusammenstellungen von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlauben.

[5] Profiling ist jede Art der automatisierten Bearbeitung von Personendaten, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser Person zu analysieren oder vorherzusagen.

2) SR 235.1

[6] Bearbeiten ist jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten.

[7] Bekanntgeben ist das Übermitteln oder Zugänglichmachen von Personendaten.

[8] Verletzung der Datensicherheit ist eine Verletzung der Sicherheit, die dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden.

[9] Auftragsbearbeiterin oder Auftragsbearbeiter ist eine Dritte oder ein Dritter, die oder der im Auftrag des verantwortlichen öffentlichen Organs Personendaten bearbeitet.

Art. 4 Verantwortlichkeit

[1] Für den Datenschutz ist dasjenige öffentliche Organ verantwortlich, welches allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung entscheidet.

[2] Bearbeiten mehrere öffentliche Organe Personendaten aus einem Datenbestand, regeln sie die Verantwortung untereinander und legen fest, welches öffentliche Organ die Gesamtverantwortung trägt.

[3] Das verantwortliche öffentliche Organ muss gegenüber der Aufsichtsstelle auf Verlangen nachweisen können, dass es die Datenschutzbestimmungen einhält.

Art. 5 Grundsätze der Datenbearbeitung

[1] Personendaten müssen rechtmässig bearbeitet werden.

[2] Die Bearbeitung muss nach Treu und Glauben erfolgen und verhältnismässig sein.

[3] Personendaten dürfen nur zu einem bestimmten und für die betroffene Person erkennbaren Zweck beschafft werden; sie dürfen nur so bearbeitet werden, dass es mit diesem Zweck vereinbar ist.

[4] Sie werden vernichtet oder anonymisiert, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind.

[5] Wer Personendaten bearbeitet, muss sich über deren Richtigkeit vergewissern. Sie oder er muss alle angemessenen Massnahmen treffen, damit die Daten berichtigt, gelöscht oder vernichtet werden, die im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind. Die Angemessenheit der Massnahmen hängt namentlich von der Art und dem Umfang der Bearbeitung sowie vom Risiko ab, das die Bearbeitung für die Grundrechte der betroffenen Personen mit sich bringt.

[6] Ist die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung nur gültig, wenn sie für eine oder mehrere bestimmte Bearbeitungen nach angemessener Information freiwillig erteilt wird.

[7] Die Einwilligung muss ausdrücklich erfolgen für:

a) die Bearbeitung von besonders schützenswerten Personendaten;
b) ein Profiling oder das Bearbeiten eines Persönlichkeitsprofils.

Art. 6 Datensicherheit

[1] Das verantwortliche öffentliche Organ und die Auftragsbearbeiterin oder der Auftragsbearbeiter gewährleisten durch geeignete technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit.

[2] Die Massnahmen müssen es ermöglichen, Verletzungen der Datensicherheit zu vermeiden.

[3] Die Regierung erlässt Bestimmungen über die Mindestanforderungen an die Datensicherheit.

2. Bearbeiten von Personendaten

Art. 7 Bearbeitung von Personendaten

[1] Öffentliche Organe dürfen Personendaten nur bearbeiten, wenn dafür eine gesetzliche Grundlage besteht oder die Bearbeitung zur Erfüllung einer gesetzlichen Aufgabe unentbehrlich ist.

[2] Eine Grundlage in einem Gesetz ist in folgenden Fällen erforderlich:

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

[3] Für die Bearbeitung von Personendaten nach Absatz 2 Litera a und Litera b ist eine Grundlage in einer Verordnung ausreichend, wenn die folgenden Voraussetzungen erfüllt sind:

a) die Bearbeitung ist für eine in einem Gesetz ausdrücklich umschriebene Aufgabe unentbehrlich;
b) der Bearbeitungszweck birgt für die Grundrechte der betroffenen Person keine besonderen Risiken.

[4] In Abweichung von Absatz 1 bis Absatz 3 dürfen öffentliche Organe Personendaten bearbeiten, wenn eine der folgenden Voraussetzungen erfüllt ist:

a) die betroffene Person hat im Einzelfall in die Bearbeitung eingewilligt oder hat ihre Personendaten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt;
b) die Bearbeitung ist notwendig, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen, und es ist nicht möglich, innerhalb einer angemessenen Frist die Einwilligung der betroffenen Person einzuholen.

Art. 8 Automatisierte Datenbearbeitung im Rahmen von Pilotversuchen

[1] Die Regierung kann vor Inkrafttreten eines Gesetzes die automatisierte Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen oder das Profiling bewilligen, wenn:

a) die Aufgaben, aufgrund deren die Bearbeitung erforderlich ist, in einem bereits in Kraft stehenden Gesetz geregelt sind;
b) ausreichende Massnahmen getroffen werden, um einen Eingriff in die Grundrechte der betroffenen Personen auf das Mindestmass zu begrenzen; und
c) für die praktische Umsetzung der Datenbearbeitung eine Testphase vor dem Inkrafttreten, insbesondere aus technischen Gründen, unentbehrlich ist.

[2] Die Regierung holt vorgängig die Stellungnahme der Aufsichtsstelle ein.

[3] Das verantwortliche öffentliche Organ legt der Regierung spätestens zwei Jahre nach der Aufnahme des Pilotversuchs einen Evaluationsbericht vor. Es schlägt darin die Fortführung oder die Einstellung der Bearbeitung vor.

[4] Die automatisierte Datenbearbeitung muss in jedem Fall abgebrochen werden, wenn innerhalb von fünf Jahren nach Aufnahme des Pilotversuchs kein Gesetz in Kraft getreten ist, das die erforderliche Rechtsgrundlage enthält.

Art. 9 Bearbeitung durch Auftragsbearbeiterin oder Auftragsbearbeiter

[1] Die Bearbeitung von Personendaten kann vertraglich oder durch die Gesetzgebung einer Auftragsbearbeiterin oder einem Auftragsbearbeiter übertragen werden, wenn:

a) die Daten so bearbeitet werden, wie es das verantwortliche öffentliche Organ selbst tun dürfte; und
b) keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet.

[2] Das verantwortliche öffentliche Organ muss sich insbesondere vergewissern, dass die Auftragsbearbeiterin oder der Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten.

[3] Die Auftragsbearbeiterin oder der Auftragsbearbeiter darf die Bearbeitung nur mit vorgängiger Genehmigung des verantwortlichen öffentlichen Organs einem Dritten übertragen.

Art. 10 Bekanntgabe von Personendaten
1. Allgemeine Vorgaben

[1] Öffentliche Organe dürfen Personendaten nur bekanntgeben, wenn eine gesetzliche Grundlage nach Artikel 7 Absatz 1 bis Absatz 3 besteht.

[2] Sie dürfen Personendaten in Abweichung von Absatz 1 im Einzelfall bekanntgeben, wenn eine der folgenden Voraussetzungen erfüllt ist:

a) die Bekanntgabe der Daten ist für das verantwortliche öffentliche Organ oder für die Empfängerin oder den Empfänger zur Erfüllung einer gesetzlichen Aufgabe unentbehrlich;

b) die betroffene Person hat in die Bekanntgabe eingewilligt oder ihre Daten allgemein zugänglich gemacht und eine Bekanntgabe nicht ausdrücklich untersagt;
c) die Bekanntgabe der Daten ist notwendig, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen, und es ist nicht möglich, innerhalb einer angemessenen Frist die Einwilligung der betroffenen Person einzuholen;
d) die Empfängerin oder der Empfänger macht glaubhaft, dass die betroffene Person die Einwilligung verweigert oder Widerspruch gegen die Bekanntgabe einlegt, um ihr oder ihm die Durchsetzung von Rechtsansprüchen oder die Wahrnehmung anderer schutzwürdiger Interessen zu verwehren; der betroffenen Person ist vorgängig Gelegenheit zur Stellungnahme zu geben, es sei denn, dies ist unmöglich oder mit unverhältnismässigem Aufwand verbunden.

[3] Sie dürfen Name, Vorname, Adresse und Geburtsdatum einer Person auf Anfrage auch bekanntgeben, wenn die Voraussetzungen nach Absatz 1 oder Absatz 2 nicht erfüllt sind.

[4] Die öffentlichen Organe lehnen die Bekanntgabe ab, schränken sie ein oder verbinden sie mit Auflagen, wenn:

a) wesentliche öffentliche Interessen oder offensichtlich schutzwürdige Interessen der betroffenen Person es verlangen; oder
b) gesetzliche Geheimhaltungspflichten oder besondere Datenschutzvorschriften es verlangen.

Art. 11 2. Bekanntgabe von Personendaten im Rahmen der behördlichen Informationstätigkeit

[1] Die öffentlichen Organe dürfen Personendaten darüber hinaus im Rahmen der behördlichen Information der Öffentlichkeit von Amtes wegen bekanntgeben, wenn:

a) die Daten im Zusammenhang mit der Erfüllung öffentlicher Aufgaben stehen; und
b) an der Bekanntgabe ein überwiegendes öffentliches Interesse besteht.

[2] Sie dürfen Personendaten mittels automatisierter Informations- und Kommunikationsdienste allgemein zugänglich machen, wenn eine Rechtsgrundlage die Veröffentlichung dieser Daten vorsieht oder wenn sie Daten gestützt auf Absatz 1 bekanntgeben. Besteht kein öffentliches Interesse mehr daran, die Daten allgemein zugänglich zu machen, so werden die betreffenden Daten aus dem automatisierten Informations- und Kommunikationsdienst gelöscht.

[3] Das Verfahren für den Zugang zu amtlichen Dokumenten richtet sich nach dem Gesetz über das Öffentlichkeitsprinzip[3)].

[3)] BR 171.000

Art. 12 3. Grenzüberschreitende Bekanntgabe von Personendaten

[1] Personendaten dürfen ins Ausland bekanntgegeben werden, wenn die Gesetzgebung des betreffenden Staates oder das internationale Organ einen angemessenen Schutz gewährleistet.

[2] In Staaten, deren Gesetzgebung keinen angemessenen Schutz gewährleistet, können Personendaten nur bekanntgegeben werden, wenn:

a) hinreichende Garantien, insbesondere durch Vertrag, einen angemessenen Schutz im Ausland gewährleisten;
b) die betroffene Person ausdrücklich in die Bekanntgabe eingewilligt hat;
c) die Bekanntgabe in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags zwischen dem verantwortlichen öffentlichen Organ und der betroffenen Person oder zwischen dem verantwortlichen öffentlichen Organ und seiner Vertragspartnerin oder seinem Vertragspartner im Interesse der betroffenen Person steht;
d) die Bekanntgabe notwendig ist für die Wahrung eines überwiegenden öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor einem Gericht oder einer anderen zuständigen ausländischen Behörde;
e) die Bekanntgabe notwendig ist, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen, und es nicht möglich ist, innerhalb einer angemessenen Frist die Einwilligung der betroffenen Person einzuholen;
f) die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat; oder
g) die Daten aus einem gesetzlich vorgesehenen Register stammen, das öffentlich oder Personen mit einem schutzwürdigen Interesse zugänglich ist, soweit im Einzelfall die gesetzlichen Voraussetzungen der Einsichtnahme erfüllt sind.

[3] Vor der Bekanntgabe der Personendaten ins Ausland informiert das öffentliche Organ die Aufsichtsstelle über die Garantien nach Absatz 2 Litera a.

Art. 13 Datenbearbeitung für nicht personenbezogene Zwecke

[1] Öffentliche Organe dürfen Personendaten für nicht personenbezogene Zwecke, insbesondere für Forschung, Planung oder Statistik, bearbeiten, wenn:

a) die Daten anonymisiert werden, sobald der Bearbeitungszweck dies erlaubt;
b) das öffentliche Organ privaten Personen besonders schützenswerte Personendaten nur so bekanntgibt, dass die betroffenen Personen nicht bestimmbar sind;
c) die Empfängerin oder der Empfänger Dritten die Daten nur mit der Zustimmung des öffentlichen Organs weitergibt, das die Daten bekanntgegeben hat; und
d) die Ergebnisse nur so veröffentlicht werden, dass die betroffenen Personen nicht bestimmbar sind.

[2] Artikel 5 Absatz 3, Artikel 7 Absatz 2 sowie Artikel 10 Absatz 1 sind nicht anwendbar.

Art. 14 Bildüberwachung des öffentlichen und öffentlich zugänglichen Raums
1. Allgemeine Vorgaben

[1] Der öffentliche und öffentlich zugängliche Raum kann mit Bildübermittlungs- und Bildaufzeichnungsgeräten zur Personenidentifikation überwacht werden, sofern:

a) die öffentliche Sicherheit und Ordnung konkret gefährdet ist; oder
b) dies zum Schutz von öffentlichen Zwecken dienenden Gebäuden oder deren Benutzerinnen und Benutzern erforderlich ist.

[2] Bei der Bearbeitung von Personendaten sind die allgemeinen Grundsätze zu respektieren. Zusätzlich ist sicherzustellen, dass:

a) auf die Überwachungsgeräte in geeigneter und erkennbarer Weise hingewiesen wird;
b) Bereiche, die der Ausübung von Tätigkeiten dienen, die unter das Berufsgeheimnis im Sinne von Artikel 171 der Schweizerischen Strafprozessordnung[4)] fallen, von der Überwachung ausgenommen sind; und
c) aufgezeichnete Personendaten innert maximal 90 Tagen gelöscht werden oder der zuständigen Behörde zur Nutzung in einem Strafverfahren oder zur Durchsetzung zivilrechtlicher Ansprüche aufgrund einer Straftat übergeben werden.

Art. 15 2. Anordnung der Bildüberwachung des öffentlichen und öffentlich zugänglichen Raums

[1] Die Bildüberwachung des öffentlichen und öffentlich zugänglichen Raums kann von einem öffentlichen Organ angeordnet werden, dem das Gebrauchsrecht oder die Hoheit über den zu überwachenden Raum zusteht.

[2] Das öffentliche Organ erlässt eine Allgemeinverfügung, in welcher der Zweck, die Art und die Dauer der Überwachung, die zu überwachenden Örtlichkeiten, die Standorte der Überwachungsgeräte, die Massnahmen zum Hinweis auf die Überwachung, die Zugriffsrechte sowie die zur Datensicherheit getroffenen Massnahmen bestimmt werden. Die Allgemeinverfügung gilt für maximal fünf Jahre.

[3] Das öffentliche Organ hat die zu erlassende Allgemeinverfügung vorgängig zu veröffentlichen. Es hört Personen an, indem es ihnen eine angemessene Frist zur Stellungnahme einräumt.

[4] Vorgängiger Rechtsschutz ist nicht zu gewähren für anlassbezogene Bildüberwachungen mit einer Dauer von höchstens drei Monaten und für Bildüberwachungen zum Schutz öffentlichen Zwecken dienenden Gebäuden, die ereignisbezogen in Betrieb genommen werden und keine Personendaten aufzeichnen.

4) SR 312.0

Art. 16 Archivierung und Vernichtung

[1] Das öffentliche Organ bietet Personendaten, die es nicht mehr benötigt, nach den dafür geltenden Vorschriften dem zuständigen Archiv an.

[2] Es vernichtet die vom zuständigen Archiv als nicht archivwürdig bezeichneten Personendaten, es sei denn:

a) diese werden anonymisiert;
b) diese müssen zu Beweis- oder Sicherheitszwecken oder zur Wahrung der schutzwürdigen Interessen der betroffenen Person aufbewahrt werden.

3. Pflichten des verantwortlichen öffentlichen Organs

Art. 17 Informationspflicht bei der Beschaffung von Personendaten

[1] Das verantwortliche öffentliche Organ informiert die betroffene Person angemessen über die Beschaffung von Personendaten; diese Informationspflicht gilt auch, wenn die Daten nicht bei der betroffenen Person beschafft werden.

[2] Es teilt der betroffenen Person bei der Beschaffung diejenigen Informationen mit, die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist; es teilt ihr mindestens mit:

a) die Identität und die Kontaktdaten des verantwortlichen öffentlichen Organs;
b) die Rechtsgrundlage und den Bearbeitungszweck;
c) die Rechte der betroffenen Person;
d) gegebenenfalls die Empfängerinnen und Empfänger oder die Kategorien von Empfängerinnen und Empfängern, denen Personendaten bekanntgegeben werden;
e) die Kategorien der bearbeiteten Personendaten, sofern die Daten nicht bei der betroffenen Person beschafft werden;
f) falls die Daten ins Ausland bekanntgegeben werden, auch den Staat oder das internationale Organ und gegebenenfalls die Garantien oder die Anwendung einer Ausnahme nach Artikel 12 Absatz 2.

[3] Werden die Daten nicht bei der betroffenen Person beschafft, so teilt das verantwortliche öffentliche Organ der betroffenen Person die Informationen nach Absatz 2 spätestens einen Monat, nachdem es die Daten erhalten hat, mit. Gibt es die Personendaten vor Ablauf dieser Frist bekannt, so informiert es die betroffene Person spätestens im Zeitpunkt der Bekanntgabe.

Art. 18 Ausnahmen von der Informationspflicht und Einschränkungen

[1] Die Informationspflicht bei der Beschaffung von Personendaten entfällt, wenn eine der folgenden Voraussetzungen erfüllt ist:

a) die betroffene Person verfügt bereits über die entsprechenden Informationen;
b) die Bearbeitung ist gesetzlich vorgesehen;

c) die Personendaten werden nicht bei der betroffenen Person beschafft und die Information ist nicht möglich oder erfordert einen unverhältnismässigen Aufwand.

[2] Das verantwortliche öffentliche Organ kann die Mitteilung der Informationen unter denselben Voraussetzungen einschränken, aufschieben oder darauf verzichten wie beim Auskunftsrecht nach Artikel 25.

Art. 19 Datenschutz-Folgenabschätzung

[1] Das verantwortliche öffentliche Organ erstellt vorgängig eine Datenschutz-Folgenabschätzung, wenn eine Bearbeitung ein hohes Risiko für die Grundrechte der betroffenen Person mit sich bringen kann. Sind mehrere ähnliche Bearbeitungsvorgänge geplant, so kann eine gemeinsame Abschätzung erstellt werden.

[2] Das hohe Risiko ergibt sich, insbesondere bei Verwendung neuer Technologien, aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung. Es liegt namentlich vor:

a) bei der umfangreichen Bearbeitung besonders schützenswerter Personendaten;
b) wenn systematisch umfangreiche öffentliche Bereiche überwacht werden.

[3] Die Datenschutz-Folgenabschätzung enthält eine Beschreibung der geplanten Bearbeitung, eine Bewertung der Risiken für die Grundrechte der betroffenen Person sowie die Massnahmen zum Schutz der Grundrechte.

Art. 20 Vorabkonsultation

[1] Ergibt sich aus der Datenschutz-Folgenabschätzung, dass die geplante Bearbeitung trotz der vom verantwortlichen öffentlichen Organ vorgesehenen Massnahmen noch ein hohes Risiko für die Grundrechte der betroffenen Person zur Folge hat, so holt es vorgängig die Stellungnahme der Aufsichtsstelle ein.

[2] Die Aufsichtsstelle teilt dem verantwortlichen öffentlichen Organ innert angemessener Frist seine Einwände gegen die geplante Bearbeitung mit und schlägt geeignete Massnahmen vor.

Art. 21 Meldung von Verletzungen der Datensicherheit

[1] Das verantwortliche öffentliche Organ meldet der Aufsichtsstelle so rasch als möglich eine Verletzung der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Grundrechte der betroffenen Person führt.

[2] In der Meldung nennt es mindestens die Art der Verletzung der Datensicherheit, deren Folgen und die ergriffenen oder vorgesehenen Massnahmen.

[3] Die Auftragsbearbeiterin oder der Auftragsbearbeiter meldet dem verantwortlichen öffentlichen Organ so rasch als möglich eine Verletzung der Datensicherheit.

[4] Das verantwortliche öffentliche Organ informiert die betroffene Person, wenn es zu ihrem Schutz erforderlich ist oder die Aufsichtsstelle es verlangt.

[5] Es kann die Information an die betroffene Person einschränken, aufschieben oder darauf verzichten, wenn:

a) dies aufgrund überwiegender Interessen Dritter erforderlich ist;
b) dies aufgrund überwiegender öffentlicher Interessen, insbesondere zur Wahrung der inneren oder äusseren Sicherheit, erforderlich ist;
c) die Mitteilung der Information eine Ermittlung, eine Untersuchung oder ein behördliches oder gerichtliches Verfahren gefährden kann;
d) eine gesetzliche Geheimhaltungspflicht dies verbietet;
e) die Information unmöglich ist oder einen unverhältnismässigen Aufwand erfordert;
f) die Information der betroffenen Person durch eine öffentliche Bekanntmachung in vergleichbarer Weise sichergestellt ist.

Art. 22 Verzeichnis der Bearbeitungstätigkeiten

[1] Die von der Regierung bezeichneten öffentlichen Organe und die Strafgerichte führen zum Nachweis der Einhaltung der Datenschutzvorschriften ein Verzeichnis ihrer Bearbeitungstätigkeiten.

[2] Das Verzeichnis enthält mindestens:

a) die Identität und die Kontaktdaten des verantwortlichen öffentlichen Organs;
b) die Rechtsgrundlage und den Bearbeitungszweck;
c) eine Beschreibung der Kategorien betroffener Personen und der Kategorien bearbeiteter Personendaten;
d) gegebenenfalls die Empfängerinnen und Empfänger oder die Kategorien von Empfängerinnen und Empfängern, denen Personendaten bekanntgegeben werden;
e) die Aufbewahrungsdauer der Personendaten oder die Kriterien zur Festlegung dieser Dauer;
f) eine allgemeine Beschreibung der Massnahmen zur Gewährleistung der Datensicherheit;
g) die Angabe, ob die Daten ins Ausland bekanntgegeben werden und gegebenenfalls die Garantien oder die Anwendung einer Ausnahme nach Artikel 12 Absatz 2.

[3] Das verantwortliche öffentliche Organ meldet seine Verzeichnisse der Aufsichtsstelle und kann sie veröffentlichen.

Art. 23 Datenschutzberaterin oder -berater

[1] Die von der Regierung bezeichneten öffentlichen Organe und die Strafgerichte bezeichnen eine für die Datenschutzberatung zuständige Person. Diese hat namentlich folgende Aufgaben:

a) sie berät und unterstützt die Mitarbeitenden bei der Bearbeitung von Personendaten hinsichtlich der Einhaltung der Datenschutzvorschriften;
b) sie sorgt für die Vornahme der Datenschutz-Folgenabschätzungen;
c) sie ist Ansprechperson der Aufsichtsstelle und arbeitet mit dieser zusammen.

4. Rechte der betroffenen Person

Art. 24 Auskunftsrecht

[1] Jede betroffene Person kann vom verantwortlichen öffentlichen Organ Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden.

[2] Die betroffene Person erhält diejenigen Informationen, die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist. In jedem Fall werden ihr folgende Informationen mitgeteilt:

a) die Angaben nach Artikel 17 Absatz 2;
b) die Aufbewahrungsdauer der Personendaten oder die Kriterien zur Festlegung dieser Dauer;
c) die verfügbaren Angaben über die Herkunft der Personendaten, soweit sie nicht bei der betroffenen Person beschafft wurden.

[3] Personendaten über die Gesundheit können der betroffenen Person mit ihrer Einwilligung durch eine von ihr bezeichnete Gesundheitsfachperson mitgeteilt werden.

[4] Lässt das verantwortliche öffentliche Organ Personendaten von einer Auftragsbearbeiterin oder einem Auftragsbearbeiter bearbeiten, so bleibt es auskunftspflichtig.

[5] Niemand kann im Voraus auf das Auskunftsrecht verzichten.

[6] Die Auskunft wird in der Regel innerhalb von 30 Tagen erteilt.

Art. 25 Einschränkungen des Auskunftsrechts

[1] Das verantwortliche öffentliche Organ kann die Auskunft verweigern, einschränken oder aufschieben, wenn:

a) eine besondere, gesetzliche Geheimhaltungspflicht dies vorsieht;
b) dies aufgrund überwiegender Interessen Dritter erforderlich ist;
c) die Massnahme wegen überwiegender öffentlicher Interessen, insbesondere der inneren oder der äusseren Sicherheit, erforderlich ist; oder
d) die Mitteilung der Information eine Ermittlung, eine Untersuchung oder ein behördliches oder gerichtliches Verfahren gefährden kann.

Art. 26 Widerspruch gegen die Bekanntgabe von Personendaten

[1] Die betroffene Person, die ein schutzwürdiges Interesse glaubhaft macht, kann gegen die Bekanntgabe bestimmter Personendaten durch das verantwortliche öffentliche Organ Widerspruch einlegen.

[2] Das öffentliche Organ weist das Begehren ab, wenn eine der folgenden Voraussetzungen erfüllt ist:

a) es besteht eine Rechtspflicht zur Bekanntgabe;
b) die Erfüllung seiner Aufgaben wäre sonst gefährdet.

[3] Artikel 11 Absatz 1 bleibt vorbehalten.

Art. 27 Weitere Ansprüche

[1] Wer ein schutzwürdiges Interesse hat, kann vom verantwortlichen öffentlichen Organ verlangen, dass es:

a) die widerrechtliche Bearbeitung der betreffenden Personendaten unterlässt;
b) die Folgen einer widerrechtlichen Bearbeitung beseitigt;
c) die Widerrechtlichkeit der Bearbeitung feststellt.

[2] Die Gesuchstellerin oder der Gesuchsteller kann insbesondere verlangen, dass das verantwortliche öffentliche Organ:

a) die betreffenden Personendaten berichtigt, löscht oder vernichtet;
b) seinen Entscheid, namentlich über die Berichtigung, Löschung oder Vernichtung, den Widerspruch gegen die Bekanntgabe oder den Bestreitungsvermerk Dritten mitteilt oder veröffentlicht.

[3] Kann weder die Richtigkeit noch die Unrichtigkeit der betreffenden Personendaten festgestellt werden, so bringt das verantwortliche öffentliche Organ bei den Daten einen Bestreitungsvermerk an.

Art. 28 Verfahren

[1] Entspricht ein öffentliches Organ einem Begehren aufgrund dieses Gesetzes nicht, erlässt es einen begründeten Entscheid.

[2] Die Ausübung des Auskunftsrechts und des Anspruchs auf Berichtigung von Personendaten sowie das Gesuch um Widerspruch gegen die Bekanntgabe von Personendaten sind in der Regel kostenlos.

[3] Eine angemessene Gebühr kann verlangt werden, wenn:

a) die Ausübung der Rechte mit einem unverhältnismässigen Aufwand verbunden ist; oder
b) das Gesuch offensichtlich unbegründet, namentlich wenn es einen datenschutzwidrigen Zweck verfolgt, oder offensichtlich querulatorisch ist.

[4] Im Weiteren richtet sich das Verfahren nach dem Gesetz über die Verwaltungsrechtspflege[5)].

Art. 29 Verfahren im Falle der Bekanntgabe von amtlichen Dokumenten, die Personendaten enthalten

[1] Ist ein Verfahren betreffend den Zugang zu amtlichen Dokumenten, die Personendaten enthalten, im Sinne des Gesetzes über das Öffentlichkeitsprinzip[6)] hängig, so kann die betroffene Person in diesem Verfahren diejenigen Rechte geltend machen, die ihr nach Artikel 27 bezogen auf diejenigen Dokumente zustehen, die Gegenstand des Zugangsverfahrens sind.

[5)] BR 370.100
[6)] BR 171.000

5. Aufsicht

Art. 30 Aufsichtsstelle

[1] Die Aufsichtsstelle Datenschutz beaufsichtigt die Anwendung der Datenschutzvorschriften.

[2] Der Aufsicht der Aufsichtsstelle unterstehen nicht:

a) Datenbearbeitungen in hängigen Verfahren der Zivil- und Strafrechtspflege;
b) Datenbearbeitungen in hängigen Verfahren der Verfassungs- und Verwaltungsgerichtsbarkeit.

Art. 31 Zusammensetzung und Stellung

[1] Die Aufsichtsstelle besteht im Minimum aus der oder dem Datenschutzbeauftragten und einer Stellvertretung.

[2] Die Aufsichtsstelle erfüllt ihre Aufgaben fachlich selbständig und unabhängig. Sie ist in der Erfüllung ihrer Aufgaben weisungsungebunden.

[3] Administrativ ist sie der Standeskanzlei unterstellt.

[4] Die Regierung übt die Aufsicht über die Aufsichtsstelle aus. Sie kann ihr im Rahmen der aufsichtsrechtlichen Befugnisse Weisungen erteilen.

[5] Die Arbeitsverhältnisse und die berufliche Vorsorge aller Mitarbeitenden der Aufsichtsstelle richten sich nach dem kantonalen Personal- beziehungsweise Pensionskassenrecht, soweit dieses Gesetz nichts anderes vorsieht.

[6] Die Regierung reiht die Stellen der oder des Datenschutzbeauftragten sowie der Stellvertretung in die Funktionsklassen nach kantonalem Personalrecht ein.

Art. 32 Wahl

[1] Die Regierung wählt eine in Datenschutzfragen ausgewiesene Fachperson als Datenschutzbeauftragte oder Datenschutzbeauftragter sowie eine Stellvertretung für eine Amtszeit von vier Jahren. Die Wiederwahl ist zulässig.

[2] Die Regierung kann die oder den Datenschutzbeauftragten und die Stellvertretung vor Ablauf der Amtsdauer des Amtes entheben, wenn sie oder er:

a) vorsätzlich oder grobfahrlässig Amtspflichten schwer verletzt hat; oder
b) die Fähigkeit, das Amt auszuüben, auf Dauer verloren hat.

Art. 33 Unvereinbarkeiten

[1] Die oder der Datenschutzbeauftragte und die Stellvertretung darf kein anderes öffentliches Amt, keine leitende Funktion in einer politischen Partei und keine andere Erwerbstätigkeit ausüben. Die Regierung kann Ausnahmen bewilligen, wenn die Ausübung der Funktion sowie die Unabhängigkeit und das Ansehen nicht beeinträchtigt werden.

[2] Versieht die oder der Datenschutzbeauftragte und die Stellvertretung ihre Tätigkeit in einem Teilpensum, so ist eine andere Erwerbstätigkeit durch die Regierung zu bewilligen. Die Bewilligung darf nur verweigert werden, wenn durch diese Erwerbstätigkeit die Ausübung der Funktion sowie die Unabhängigkeit und das Ansehen beeinträchtigt werden.

Art. 34 Budget

[1] Die oder der Datenschutzbeauftragte erstellt ein eigenes Budget.

[2] Die Regierung gibt in der Budgetbotschaft bekannt, ob der Vorschlag unverändert übernommen wurde. Abweichungen sind zu begründen.

[3] Im Rahmen des Budgets ist die oder der Datenschutzbeauftragte zuständig für die Anstellung, die Beendigung und die Umgestaltung des Arbeitsverhältnisses der Mitarbeitenden.

Art. 35 Aufgaben

[1] Die Aufsichtsstelle:

a) überwacht die Anwendung der Vorschriften über den Datenschutz;
b) berät die betroffenen Personen über ihre Rechte;
c) vermittelt zwischen den betroffenen Personen und den öffentlichen Organen;
d) berät die öffentlichen Organe in Fragen des Datenschutzes und überwacht die Datensicherung;
e) nimmt Stellung zu Erlassen und Informatikprojekten, soweit sie für den Datenschutz erheblich sind;
f) behandelt Meldungen von Betroffenen betreffend die Missachtung von Vorschriften dieses Gesetzes und informiert sie innerhalb von höchstens drei Monaten über das Ergebnis oder den Stand der Abklärungen;
g) sensibilisiert die öffentlichen Organe für ihre datenschutzrechtlichen Pflichten und die Öffentlichkeit für die Anliegen des Datenschutzes;
h) verfolgt die für den Schutz von Personendaten massgeblichen Entwicklungen;
i) arbeitet zur Erfüllung ihrer Aufgaben mit den Organen der anderen Kantone, des Bundes und des Auslandes, welche die gleichen Aufgaben erfüllen, zusammen.

Art. 36 Befugnisse
1. Kontrolle und Empfehlung

[1] Die Aufsichtsstelle wird von Amtes wegen oder auf Meldung der Betroffenen hin tätig. Das verantwortliche öffentliche Organ ist von einer Meldung in Kenntnis zu setzen und es ist ihm Gelegenheit zur Stellungnahme zu geben.

[2] Die Aufsichtsstelle kann ungeachtet allfälliger Geheimhaltungsvorschriften alle für die Erfüllung des Kontrollauftrages erforderlichen Informationen über Datenbearbeitungen einholen, Einsicht in alle Unterlagen nehmen, Besichtigungen durchführen und sich Bearbeitungen vorführen lassen.

[3] Die Aufsichtsstelle kann zum Bearbeiten von Personendaten Empfehlungen abgeben. Das öffentliche Organ, an welches sich die Empfehlung richtet, hat gegenüber der Aufsichtsstelle zu erklären, ob es der Empfehlung folgen will.

[4] Die öffentlichen Organe und die Auftragsbearbeiterin oder der Auftragsbearbeiter sind verpflichtet, die Aufsichtsstelle bei der Erfüllung ihrer Aufgaben zu unterstützen. Sie wirken insbesondere bei der Feststellung des Sachverhalts mit.

Art. 37 2. Entscheid

[1] Wenn ein öffentliches Organ erklärt, der Empfehlung der Aufsichtsstelle nicht folgen zu wollen, oder tatsächlich der Empfehlung nicht folgt, kann die Aufsichtsstelle die Empfehlung oder Teile davon als Entscheid erlassen.

[2] Die Aufsichtsstelle kann direkt einen Entscheid erlassen, wenn absehbar ist, dass das öffentliche Organ eine Empfehlung ablehnen oder ihr keine Folge leisten wird.

[3] Gegen Entscheide gemäss Artikel 37 Absatz 1 und Absatz 2 kann das betroffene öffentliche Organ Beschwerde beim Obergericht erheben. Es gilt das Gesetz über die Verwaltungsrechtspflege[7)].

[4] Gegen Entscheide, welche das Obergericht betreffen, kann das Obergericht Beschwerde an das Justizgericht erheben.

Art. 38 Berichterstattung

[1] Die Aufsichtsstelle erstattet der Regierung jährlich Bericht über Umfang und Schwerpunkte ihrer Tätigkeit sowie über wichtige Feststellungen und Beurteilungen.

[2] Die Aufsichtsstelle gibt dem öffentlichen Organ, das von Empfehlungen und Entscheiden betroffen ist, Gelegenheit, schriftlich Stellung nehmen. Die Stellungnahmen werden dem Bericht angefügt.

[3] Der Bericht wird veröffentlicht.

Art. 39 Verschwiegenheit

[1] Die Aufsichtsstelle ist hinsichtlich der Personendaten zur gleichen Verschwiegenheit verpflichtet wie das öffentliche Organ, welches die Daten bearbeitet. Die Pflicht zur Verschwiegenheit gilt über die Beendigung der Funktion hinaus.

[2] Die Aufsichtsstelle darf unter Vorbehalt besonderer Geheimhaltungsvorschriften Kenntnisse, die sie bei ihrer Tätigkeit erlangt, nur soweit bekannt geben, als es zur Erfüllung ihrer Aufgaben notwendig ist.

7) BR 370.100

6. Straf- und Übergangsbestimmungen

Art. 40 Strafbestimmungen

[1] Wer als Auftragsbearbeiterin oder Auftragsbearbeiter ohne ausdrückliche Ermächtigung des auftraggebenden öffentlichen Organs vorsätzlich oder fahrlässig Personendaten für sich oder andere verwendet oder anderen bekannt gibt, wird mit Busse bestraft.

[2] Wer Personendaten, die sie oder er von einem öffentlichen Organ zum Bearbeiten zu nicht personenbezogenen Zwecken erhalten hat, vorsätzlich oder fahrlässig entgegen der Verpflichtung gemäss Artikel 13 für andere Zwecke bearbeitet oder an Dritte weitergibt, wird mit Busse bestraft.

Art. 41 Übergangsbestimmungen

[1] Datenbearbeitungen, welche sich nach bisherigem Recht auf eine genügende rechtliche Grundlage stützen, können während zwei Jahren gestützt auf die bestehenden Rechtsgrundlagen weiterbetrieben werden.

[2] Der Nachweis über die Einhaltung der Datenschutzbestimmungen muss spätestens zwei Jahre nach dem Inkrafttreten dieses Gesetzes erbracht werden können.

[3] Artikel 19 und Artikel 20 sind auf Datenbearbeitungen nicht anwendbar, die vor Inkrafttreten dieses Gesetzes begonnen wurden, sofern keine wesentlichen Änderungen am Bearbeitungszweck oder an der Bearbeitungstätigkeit vorgenommen werden.

II.

1.
Der Erlass "Bürgerrechtsgesetz des Kantons Graubünden (KBüG)" BR 130.100 (Stand 1. Januar 2025) wird wie folgt geändert:

Art. 24 Abs. 1 (geändert)

[1] Die zuständigen kantonalen und kommunalen Behörden sowie die von ihnen beauftragten Stellen können für die Erfüllung ihrer Aufgaben nach diesem Gesetz Daten bearbeiten, einschliesslich der Persönlichkeitsprofile und der besonders ~~geschützten~~**schützenswerten** Personendaten über:

Aufzählung unverändert.

2.
Der Erlass "Gesetz über die Einwohnerregister und weitere Personen- und Objektregister (Einwohnerregistergesetz, ERG)" BR 171.200 (Stand 1. Januar 2018) wird wie folgt geändert:

Art. 32 Abs. 3 (geändert)

[3] Das ~~Sperrrecht~~**Recht auf Widerspruch gegen die Bekanntgabe von Personendaten gemäss dem Kantonalen Datenschutzgesetz**[8)] bleibt vorbehalten.

3.

Der Erlass "Einführungsgesetz zur Schweizerischen Zivilprozessordnung (EGzZPO)" BR 320.100 (Stand 1. Januar 2025) wird wie folgt geändert:

Art. 14 Abs. 5 (neu)

[5] Entscheide über die Akteneinsicht in Verfahren vor dem Obergericht und dem Justizgericht sind nach dem kantonalen Recht endgültig.

4.

Der Erlass "Einführungsgesetz zur Schweizerischen Strafprozessordnung (EGzStPO)" BR 350.100 (Stand 1. Januar 2025) wird wie folgt geändert:

Art. 36 Abs. 5 (neu)

[5] Entscheide über die Akteneinsicht in Verfahren vor dem Obergericht und dem Justizgericht sind nach dem kantonalen Recht endgültig.

5.

Der Erlass "Gesetz über die Finanzaufsicht (GFA)" BR 710.300 (Stand 1. Januar 2025) wird wie folgt geändert:

Art. 20 Abs. 1 (geändert), **Abs. 2 (geändert)**

[1] Die Finanzkontrolle hat das Recht, die für die Wahrnehmung der Finanzaufsicht erforderlichen Daten einschliesslich Personendaten aus den ~~Datensammlungen~~**Datenbeständen** der Departemente und der Dienststellen sowie der Gerichte und der Schlichtungsbehörden abzurufen. Soweit die Daten für die Aufgabenerfüllung geeignet und erforderlich sind, erstreckt sich das Zugriffsrecht auch auf besonders schützenswerte Personendaten.

[2] Die Finanzkontrolle darf die ihr derart zur Kenntnis gebrachten Personendaten nur bis zum Abschluss des Revisionsverfahrens aufbewahren oder speichern. Die Zugriffe auf die verschiedenen ~~Datensammlungen~~**Datenbestände** und die damit verfolgten Zwecke müssen dokumentiert werden.

[8)] BR 171.100

III.

Der Erlass "Kantonales Datenschutzgesetz (KDSG)" BR 171.100 (Stand 1. Januar 2025) wird aufgehoben.

IV.

Dieses Gesetz untersteht dem fakultativen Referendum.
Die Regierung bestimmt den Zeitpunkt des Inkrafttretens dieses Gesetzes.

Lescha chantunala davart la protecziun da datas (LCPD)

Dals [Data]

Relaschs tangads da questa fatschenta (numers dal DG)

Nov:	**171.100**
Midà:	130.100 | 171.200 | 320.100 | 350.100 | 710.300
Abolì:	171.100

Il Cussegl grond dal chantun Grischun,

sa basond sin l'art. 31 al. 1 da la Constituziun chantunala[1)],
suenter avair gì invista da la missiva da la Regenza dals …,

concluda:

I.

Il relasch "Lescha chantunala davart la protecziun da datas (LCPD)" DG 171.100 vegn publitgà sco nov relasch.

1. Disposiziuns generalas

Art. 1 Intent

[1] Questa lescha serva a proteger persunas cunter l'elavurazion illegala da datas persunalas tras organs publics.

Art. 2 Champ da validitad

[1] Questa lescha vala per l'elavurazion da datas persunalas tras organs publics.

1) DG 110.100

[2] Sch'in organ public sa participescha a la concurrenza economica senza agir da maniera suverana, èn applitgablas las reglas da la Lescha federala davart la protecziun da datas[2)] per questas elavuraziuns da datas. La surveglianza sa drizza tenor la lescha qua avant maun, quai cun excepziun d'organs publics che participeschan unicamain a la concurrenza economica e che fan quai tenor il dretg privat.

[3] Il dretg processual applitgabel regla l'elavuraziun da datas persunalas ed ils dretgs da las persunas pertutgadas en proceduras giudizialas ed en proceduras tenor urdens da procedura dal dretg federal sco er en proceduras da la giurisdicziun administrativa, cun excepziun da las proceduras d'emprima instanza davant autoritads administrativas.

[4] Disposiziuns divergentas e cumplementaras en autras leschas restan resalvadas, premess ch'ellas garanteschan la protecziun dals dretgs fundamentals da persunas en il senn da questa lescha, en cas ch'ils organs publics elavuran datas persunalas davart questas persunas.

Art. 3 Noziuns

[1] Organs publics en il senn da questa lescha èn:

a) las autoritads, las administraziuns e las cumissiuns dal chantun, da las regiuns, da las vischnancas e da las colliaziuns da vischnancas;
b) las autoritads, las administraziuns e las cumissiuns dals instituts da dretg public, da las fundaziuns e da las corporaziuns dal chantun, da las regiuns e da las vischnancas;
c) persunas natiralas u giuridicas ubain autras organisaziuns da dretg privat, uschenavant ch'ellas adempleschan incumbensas publicas ch'èn vegnidas surdadas ad ellas.

[2] Datas persunalas en il senn da questa lescha èn tut las indicaziuns che sa refereschan ad ina persuna natirala u giuridica identifitgada u identifitgabla.

[3] Datas persunalas spezialmain sensiblas èn datas persunalas ch'èn expostas ad in privel spezial, ch'ils dretgs fundamentals vegnian violads, particularmain:

a) datas davart ideas u activitads religiusas, ideologicas, politicas u sindicalas;
b) datas davart la sanadad, davart la sfera intima u davart l'appartegnientscha ad ina razza u ad in'etnia;
c) datas geneticas;
d) datas biometricas che permettan d'identifitgar cleramain ina persuna natirala;
e) datas davart persecuziuns u sancziuns administrativas e penalas;
f) datas davart mesiras da l'agid social.

[4] Profils da la persunalitad èn cumpilaziuns da datas che permettan da giuditgar aspects essenzials da la persunalitad d'ina persuna natirala.

2) CS 235.1

[5] Profiling è mintga gener da l'elavuraziun automatisada da datas persunalas, che consista en l'utilisaziun da questas datas per valitar tscherts aspects persunals che sa refereschan ad ina persuna natirala, en spezial per analisar u predir aspects areguard la prestaziun da lavur, la situaziun economica, la sanadad, las preferenzas persunalas, ils interess, la fidadadad, il cumportament, il lieu da dimora u la midada da lieu da questa persuna.

[6] Elavuraziun è mintga tractament da datas persunalas, independentamain da las proceduras e dals meds applitgads, en spezial la procuraziun, l'arcunaziun, la conservaziun, l'utilisaziun, la midada, la communicaziun, l'archivaziun, la stizzada u la destrucziun da datas.

[7] Communicaziun è la transmissiun u il render accessibel datas persunalas.

[8] Violaziun da la segirezza da las datas è ina violaziun da la segirezza, cun la consequenza che datas persunalas van a perder, vegnan stizzadas, destruidas u midadas nunintenziunadamain u illegalmain ubain vegnan mussadas u rendidas accessiblas a persunas nunautorisadas.

[9] Elavuratura incumbensada u elavuratur incumbensà è ina terza persuna ch'elavura datas persunalas per incumbensa da l'organ public responsabel.

Art. 4 Responsabladad

[1] Per la protecziun da datas è responsabel quel organ public, che decida sulet u ensemen cun auters davart l'intent e davart ils meds da l'elavuraziun.

[2] Sche plirs organs publics elavuran datas persunalas d'in effectiv da datas, reglan els tranter sai la responsabladad e fixeschan, tge organ public che surpiglia la responsabladad generala.

[3] Envers il post da surveglianza sto l'organ public responsabel pudair cumprovar sin dumonda, ch'el observia las disposiziuns davart la protecziun da datas.

Art. 5 Princips da l'elavuraziun da datas

[1] Datas persunalas ston vegnir elavuradas en moda legala.

[2] L'elavuraziun sto succeder en buna fai ed esser commensurada.

[3] Datas persunalas dastgan vegnir procuradas mo per in intent definì ch'è visibel per la persuna pertutgada; las datas dastgan vegnir elavuradas mo en ina moda e maniera ch'è cumpatibla cun quest intent.

[4] Ellas vegnan destruidas u anonimisadas, uschespert ch'ellas n'èn betg pli necessarias per l'intent da l'elavuraziun.

[5] Tgi ch'elavura datas persunalas, sto controllar che las datas sajan correctas. Ella u el sto prender tut las mesiras commensuradas, per che las datas ch'èn incorrectas u incumplettas en vista a l'intent da lur procuraziun u elavuraziun, vegnian rectifitgadas, stizzadas u destruidas. La commensurabladad da las mesiras dependa en spezial dal gener e da la dimensiun da l'elavuraziun sco er da la ristga che l'elavuraziun represchenta per ils dretgs fundamentals da las persunas pertutgadas.

[6] Sch'i dovra il consentiment da la persuna pertutgada, è quest consentiment mo valaivel, sch'el vegn concedì voluntarmain per ina u pliras elavuraziuns definidas suenter ina infurmaziun commensurada.

[7] Il consentiment è explicitamain necessari per:

a) l'elavuraziun da datas persunalas spezialmain sensiblas;
b) in profiling u l'elavuraziun d'in profil da la persunalitad.

Art. 6 Segirezza da las datas

[1] Tras mesiras tecnicas ed organisatoricas adattadas garanteschan l'organ public responsabel e l'elavuratura incumbensada u l'elavuratur incumbensà, che la segirezza da las datas tegnia quint da la ristga.

[2] Las mesiras ston permetter d'evitar violaziuns da la segirezza da las datas.

[3] La Regenza decretescha disposiziuns davart las pretensiuns minimalas a la segirezza da las datas.

2. Elavurar datas persunalas

Art. 7 Elavuraziun da datas persunalas

[1] Organs publics dastgan elavurar datas persunalas mo, sch'igl exista ina basa legala correspundenta u sche l'elavuraziun è indispensabla per ademplir ina incumbensa legala.

[2] Ina basa en ina lescha è necessaria en ils suandants cas:

a) sch'i sa tracta d'elavurar datas persunalas spezialmain sensiblas;
b) sch'i sa tracta d'in profil da la persunalitad u d'in profiling;
c) sche l'intent u la moda e maniera da l'elavuraziun da datas po chaschunar ina intervenziun gravanta en ils dretgs fundamentals da la persuna pertutgada.

[3] Per elavurar datas persunalas tenor l'alinea 2 litera a e litera b basta ina basa en in'ordinaziun, sche las suandantas premissas èn ademplidas:

a) l'elavuraziun è indispensabla per ina incumbensa ch'è descritta explicitamain en ina lescha;
b) l'intent da l'elavuraziun na cuntegna naginas ristgas particularas per ils dretgs fundamentals da la persuna pertutgada.

[4] En divergenza da l'alinea 1 fin l'alinea 3 dastgan ils organs publics elavurar datas persunalas, sch'ina da las suandantas premissas è ademplida:

a) la persuna pertutgada ha dà ses consentiment a l'elavuraziun en il cas singul u ha rendì accessibel sias datas persunalas al public e n'ha betg scumandà explicitamain l'elavuraziun;
b) l'elavuraziun è necessaria per proteger la vita u l'integritad corporala da la persuna pertutgada u d'ina terza persuna, ed i n'è betg pussaivel da survegnir il consentiment da la persuna pertutgada entaifer in termin adequat.

Art. 8 Elavuraziun da datas automatisada en il rom d'emprovas da pilot

[1] Avant l'entrada en vigur d'ina lescha po la Regenza permetter l'elavuraziun automatisada da datas persunalas spezialmain sensiblas u da profils da la persunalitad ubain il profiling, sche:

a) las incumbensas ch'èn il motiv per l'elavuraziun necessaria, èn regladas en ina lescha ch'è gia en vigur;
b) i vegnan prendidas mesiras suffizientas, per ch'ina intervenziun en ils dretgs fundamentals da la persuna pertutgada vegnia limitada al minimum; e
c) ina fasa da test è, cunzunt per motivs tecnics, indispensabla per realisar l'elavuraziun da datas en la pratica avant l'entrada en vigur.

[2] La Regenza sa procura ordavant la posiziun dal post da surveglianza.

[3] Il pli tard 2 onns suenter il cumenzament da l'emprova da pilot suttametta l'organ public responsabel in rapport d'evaluaziun a la Regenza. En quest rapport propona el da cuntinuar cun l'elavuraziun u da terminar tala.

[4] L'elavuraziun da datas automatisada sto vegnir terminada en mintga cas, sch'ina lescha che cuntegna la basa giuridica necessaria, n'è betg entrada en vigur entaifer 5 onns suenter il cumenzament da l'emprova da pilot.

Art. 9 Elavuraziun tras in'elavuratura incumbensada u in elavuratur incumbensà

[1] L'elavuraziun da datas persunalas po vegnir surdada ad in'elavuratura incumbensada u ad in elavuratur incumbensà sin basa d'in contract u tras la legislaziun, sche:

a) las datas vegnan elavuradas uschia, sco quai che l'organ public responsabel las dastgass sez elavurar; e
b) naginas obligaziuns legalas u contractualas da mantegnair il secret na scumondan la surdada.

[2] L'organ public responsabel sto controllar en spezial, che l'elavuratura incumbensada u l'elavuratur incumbensà saja bun da garantir la segirezza da las datas.

[3] L'elavuratura incumbensada u l'elavuratur incumbensà dastga surdar l'elavuraziun ad ina terza persuna mo, suenter che l'organ public responsabel ha approvà la surdada.

Art. 10 Communicaziun da datas persunalas
1. prescripziuns generalas

[1] Ils organs publics dastgan mo communitgar datas persunalas, sch'igl exista ina basa legala tenor l'artitgel 7 alinea 1 fin alinea 3.

[2] En divergenza da l'alinea 1 dastgan els communitgar datas persunalas en il cas singul, sch'ina da las suandantas premissas è ademplida:

a) la communicaziun da las datas è indispensabla, per che l'organ public responsabel ubain la retschavidra u il retschavider possia ademplir ina incumbensa legala;
b) la persuna pertutgada ha dà ses consentiment a la communicaziun u ha rendì accessibel sias datas al public e n'ha betg scumandà explicitamain la communicaziun;
c) la communicaziun da las datas è necessaria per proteger la vita u l'integritad corporala da la persuna pertutgada u d'ina terza persuna, ed i n'è betg pussaivel da survegnir il consentiment da la persuna pertutgada entaifer in termin adequat;
d) la retschavidra u il retschavider fa valair vardaivlamain, che la persuna pertutgada refusia il consentiment u s'opponia a la communicaziun, per impedir ch'ella u el possia cuntanscher pretensiuns giuridicas u defender auters interess degns da protecziun; la persuna pertutgada sto survegnir ordavant la pussaivladad da prender posiziun, nun che quai saja nunpussaivel u pretendia sforzs sproporziunads.

[3] Sin dumonda dastgan ils organs publics er communitgar il num, il prenum, l'adressa e la data da naschientscha d'ina persuna, sche las premissas tenor l'alinea 1 u l'alinea 2 n'èn betg ademplidas.

[4] Ils organs publics refusan la communicaziun, restrenschan ella u permettan ella sut cundiziuns, sche:

a) interess publics impurtants u interess evidentamain degns da protecziun da vart da la persuna pertutgada pretendan quai; u
b) obligaziuns legalas da mantegnair il secret u prescripziuns spezialas davart la protecziun da datas pretendan quai.

Art. 11 2. communicaziun da datas persunalas en il rom da l'activitad d'infurmaziun uffiziala

[1] D'uffizi dastgan ils organs publics ultra da quai communitgar datas persunalas en il rom da l'infurmaziun uffiziala da la publicitad, sche:

a) las datas stattan en connex cun l'adempliment d'incumbensas publicas; e
b) igl exista in interess public predominant da communitgar las datas.

[2] Ils organs publics dastgan render accessiblas datas persunalas al public cun agid da servetschs d'infurmaziun e da communicaziun automatisads, sch'ina basa giuridica prevesa la publicaziun da questas datas u sche las datas vegnan communitgadas sin fundament da l'alinea 1. Sche l'interess public da render accessiblas las datas al public n'exista betg pli, vegnan las datas respectivas stizzadas or dal servetsch d'infurmaziun e da communicaziun automatisà.

[3] La procedura per l'access a documents uffizials sa drizza tenor la Lescha davart il princip da transparenza[3)].

[3)] DG 171.000

Art. 12 3. communicaziun transcunfinala da datas persunalas

[1] Datas persunalas dastgan vegnir communitgadas a l'exteriur, sche la legislaziun dal stadi respectiv u l'organ internaziunal garantescha ina protecziun commensurada.

[2] En stadis, nua che la legislaziun na garantescha nagina protecziun commensurada, dastgan datas persunalas vegnir communitgadas mo, sche:

a) garanzias suffizientas, en spezial contractualas, garanteschan ina protecziun commensurada a l'exteriur;
b) la persuna pertutgada ha dà ses consentiment explicit a la communicaziun;
c) la communicaziun stat en in connex direct cun la conclusiun u cun la liquidaziun d'in contract tranter l'organ public responsabel e la persuna pertutgada ubain tranter l'organ public responsabel e sia partenaria u ses partenari da contract, en l'interess da la persuna pertutgada;
d) la communicaziun è necessaria per proteger in interess public predominant u per constatar, exequir u far valair dretgs davant dretgira u davant in'autra autoritad estra cumpetenta;
e) la communicaziun è necessaria per proteger la vita u l'integritad corporala da la persuna pertutgada u d'ina terza persuna, ed i n'è betg pussaivel da survegnir il consentiment da la persuna pertutgada entaifer in termin adequat;
f) la persuna pertutgada ha rendì accessibel sias datas al public e n'ha betg scumandà explicitamain l'elavuraziun; u
g) las datas derivan d'in register ch'è previs tras lescha e ch'è accessibel al public u a persunas cun in interess degn da protecziun, sche las premissas legalas per prender invista da las datas èn ademplidas en il cas singul.

[3] Avant che communitgar las datas persunalas a l'exteriur, infurmescha l'organ public il post da surveglianza davart las garanzias tenor l'alinea 2 litera a.

Art. 13 Elavuraziun da datas per intents che na sa refereschan betg a persunas

[1] Ils organs publics dastgan elavurar datas persunalas per intents che na sa refereschan betg a persunas, en spezial per la perscrutaziun, la planisaziun u la statistica, sche:

a) las datas vegnan anonimisadas, uschespert che l'intent da l'elavuraziun permetta quai;
b) l'organ public communitgescha datas persunalas spezialmain sensiblas a persunas privatas mo uschia, che las persunas pertutgadas n'èn betg identifitgablas;
c) la retschavidra u il retschavider dat vinavant las datas a terzas persunas mo cun il consentiment da l'organ public che ha communitgà las datas; e
d) ils resultats vegnan publitgads mo uschia, che las persunas pertutgadas n'èn betg identifitgablas.

[2] L'artitgel 5 alinea 3, l'artitgel 7 alinea 2 e l'artitgel 10 alinea 1 n'èn betg applitgabels.

Art. 14 Surveglianza visuala dal spazi public e dal spazi ch'è accessibel al public
1. prescripziuns generalas

[1] Il spazi public ed il spazi ch'è accessibel al public pon vegnir surveglіads cun apparats per transmetter e registrar maletgs cun l'intent d'identifitgar persunas, sche:

a) la segirezza publica e l'urden public èn periclitads concretamain; u
b) quai è necessari per proteger edifizis che servan ad intents publics u lur utilisadras ed utilisaders.

[2] En connex cun l'elavuraziun da datas persunalas ston vegnir respectads ils princips generals. Ultra da quai stoi vegnir garantì:

a) ch'i vegnia rendì attent en moda adequata e visibla als apparats da surveglianza;
b) che secturs, che servan a pratitgar activitads suttamessas al secret professiunal en il senn da l'artitgel 171 dal Cudesch da procedura penala svizzer[4)], sajan exceptads da la surveglianza; e
c) che datas persunalas registradas vegnian stizzadas entaifer maximalmain 90 dis u vegnian surdadas a l'autoritad cumpetenta per las utilisar en ina procedura penala u per far valair pretensiuns civilas pervia d'in malfatg.

Art. 15 2. ordinaziun da la surveglianza visuala dal spazi public e dal spazi ch'è accessibel al public

[1] La surveglianza visuala dal spazi public e dal spazi ch'è accessibel al public po vegnir ordinada d'in organ public che ha il dretg da diever u la suveranitad dal spazi che duai vegnir surveglià.

[2] L'organ public decretescha ina disposiziun generala che fixescha l'intent, il gener e la durada da la surveglianza, las localitads che duain vegnir surveglіadas, las posiziuns dals apparats da surveglianza, las mesiras per render attent a la surveglianza, ils dretgs d'access sco er las mesiras prendidas per la segirezza da las datas. La disposiziun generala vala maximalmain 5 onns.

[3] L'organ public sto publitgar la disposiziun generala, avant ch'el decretescha quella. El fa in'audiziun, cun fixar per las persunas tadladas in termin adequat per prender posiziun.

[4] La protecziun giuridica precedenta n'è betg da conceder per surveglianzas visualas che sa refereschan ad occurrenzas d'ina durada da maximalmain 3 mais e per surveglianzas visualas ch'èn destinadas a proteger edifizis che servan ad intents publics, che vegnan messas en funcziun per in eveniment specific e che na registreschan naginas datas persunalas.

Art. 16 Archivaziun e destrucziun

[1] Las datas persunalas che l'organ public na dovra betg pli, offrescha el a l'archiv cumpetent tenor las prescripziuns che valan en chaussa.

4) CS 312.0

[2] El destruescha las datas persunalas che vegnan designadas da l'archiv cumpetent sco betg degnas da vegnir archivadas, nun che questas datas:

a) vegnian anonimisadas;
b) stoppian vegnir conservadas per intents da cumprova u da segirezza ubain per defender ils interess degns da protecziun da la persuna pertutgada.

3. Obligaziuns da l'organ public responsabel

Art. 17 Obligaziun d'infurmaziun en connex cun la procuraziun da datas persunalas

[1] L'organ public responsabel infurmescha commensuradamain la persuna pertutgada davart la procuraziun da datas persunalas; questa obligaziun d'infurmaziun vala er, sche las datas na vegnan betg procuradas tar la persuna pertutgada.

[2] A chaschun da la procuraziun da las datas communitgescha el a la persuna pertutgada las infurmaziuns ch'èn necessarias, per ch'ella possia far valair ses dretgs tenor questa lescha e per ch'ina elavuraziun da datas transparenta saja garantida; el communitgescha almain:

a) l'identitad e las datas da contact da l'organ public responsabel;
b) la basa giuridica e l'intent da l'elavuraziun;
c) ils dretgs da la persuna pertutgada;
d) eventualmain las retschavidras ed ils retschaviders u las categorias da retschavidras e retschaviders, als quals las datas persunalas vegnan communitgadas;
e) las categorias da las datas persunalas elavuradas, sche las datas na vegnan betg procuradas tar la persuna pertutgada;
f) en cas che las datas vegnan communitgadas a l'exteriur: er il stadi u l'organ internaziunal ed eventualmain las garanzias u l'applicaziun d'ina excepziun tenor l'artitgel 12 alinea 2.

[3] Sche las datas na vegnan betg procuradas tar la persuna pertutgada, communitgescha l'organ public responsabel a la persuna pertutgada las infurmaziuns tenor l'alinea 2 entaifer maximalmain 1 mais, dapi ch'el ha survegnì las datas. Sch'el communitgescha las datas persunalas avant la scadenza da quest termin, infurmescha el la persuna pertutgada il pli tard il mument da la communicaziun.

Art. 18 Excepziuns da l'obligaziun d'infurmaziun e restricziuns

[1] L'obligaziun d'infurmaziun en connex cun la procuraziun da datas persunalas scroda, sch'ina da las suandantas premissas è ademplida:

a) la persuna pertutgada ha gia las infurmaziuns correspundentas;
b) l'elavuraziun è previsa tras lescha;
c) las datas persunalas na vegnan betg procuradas tar la persuna pertutgada e l'infurmaziun n'è betg pussaivla u pretenda sforzs sproporziunads.

[2] L'organ public responsabel po restrenscher u suspender la communicaziun da las infurmaziuns ubain renunziar a tala sut las medemas premissas sco tar il dretg d'infurmaziun tenor l'artitgel 25.

Art. 19 Valitaziun da las consequenzas per la protecziun da datas

[1] Sch'ina elavuraziun da datas pudess cuntegnair ina gronda ristga per ils dretgs fundamentals da la persuna pertutgada, fa l'organ public responsabel l'emprim ina valitaziun da las consequenzas per la protecziun da datas. Sch'i èn planisadas pliras proceduras d'elavuraziun sumegliantas, po vegnir fatga ina valitaziun cuminaivla.

[2] Ina gronda ristga resulta tras il gener, la dimensiun, las circumstanzas e l'intent da l'elavuraziun, quai en spezial en connex cun l'utilisaziun da novas tecnologias. Ina gronda ristga è avant maun en spezial:

a) en cas d'ina elavuraziun voluminusa da datas persunalas spezialmain sensiblas;
b) sche vasts secturs publics vegnan survegliads sistematicamain.

[3] La valitaziun da las consequenzas per la protecziun da datas cuntegna ina descripziun da l'elavuraziun planisada, ina valitaziun da las ristgas per ils dretgs fundamentals da la persuna pertutgada sco er las mesiras per proteger ils dretgs fundamentals.

Art. 20 Consultaziun preliminara

[1] Sche la valitaziun da las consequenzas per la protecziun da datas mussa, che l'elavuraziun planisada chaschuna anc ina gronda ristga per ils dretgs fundamentals da la persuna pertutgada, malgrà las mesiras che l'organ public responsabel ha previs, procura quel ordavant per la posiziun dal post da surveglianza.

[2] Il post da surveglianza communitgescha a l'organ public responsabel entaifer in termin adequat sias objecziuns cunter l'elavuraziun planisada e propona mesiras adattadas.

Art. 21 Annunzia da violaziuns da la segirezza da las datas

[1] L'organ public responsabel annunzia uschè svelt sco pussaivel al post da surveglianza ina violaziun da la segirezza da las datas, che chaschuna previsiblamain ina gronda ristga per ils dretgs fundamentals da la persuna pertutgada.

[2] En l'annunzia numna el almain il gener da la violaziun da la segirezza da las datas, sias consequenzas sco er las mesiras prendidas u previsas.

[3] L'elavuratura incumbensada u l'elavuratur incumbensà annunzia uschè svelt sco pussaivel a l'organ public responsabel ina violaziun da la segirezza da las datas.

[4] L'organ public responsabel infurmescha la persuna pertutgada, sche quai è necessari per proteger la persuna pertutgada u sch'il post da surveglianza pretenda quai.

[5] El po restrenscher u suspender l'infurmaziun a la persuna pertutgada ubain renunziar a tala, sche:

a) quai è necessari pervia d'interess predominants da terzas persunas;
b) quai è necessari pervia d'interess publics predominants, en spezial per proteger la segirezza interna u externa;
c) la communicaziun da l'infurmaziun po periclitar ina retschertga, ina investigaziun u ina procedura uffiziala u giudiziala;
d) in'obligaziun legala da mantegnair il secret scumonda quai;
e) l'infurmaziun n'è betg pussaivla u pretenda sforzs sproporziunads;
f) l'infurmaziun da la persuna pertutgada è garantida en moda cumparegliabla tras ina publicaziun uffiziala.

Art. 22 Glista da las activitads d'elavuraziun

[1] Per cumprovar che las prescripziuns davart la protecziun da datas vegnian observadas, mainan ils organs publics nominads da la Regenza e las dretgiras penalas ina glista da lur activitads d'elavuraziun.

[2] La glista cuntegna almain:

a) l'identitad e las datas da contact da l'organ public responsabel;
b) la basa giuridica e l'intent da l'elavuraziun;
c) ina descripziun da las categorias da persunas pertutgadas e da las categorias da datas persunalas elavuradas;
d) eventualmain las retschavidras ed ils retschaviders u las categorias da retschavidras e retschaviders, als quals las datas persunalas vegnan communitgadas;
e) la durada da conservaziun da las datas persunalas u ils criteris per fixar questa durada;
f) ina descripziun generala da las mesiras che duain garantir la segirezza da las datas;
g) l'indicaziun, sche las datas vegnan communitgadas a l'exteriur, ed eventualmain las garanzias u l'applicaziun d'ina excepziun tenor l'artitgel 12 alinea 2.

[3] L'organ public responsabel annunzia sias glistas al post da surveglianza e po publitgar las glistas.

Art. 23 Consulenta u consulenta per la protecziun da datas

[1] Ils organs publics designads da la Regenza e las dretgiras nomineschan ina persuna ch'è responsabla per la cussegliaziun en dumondas da la protecziun da datas. Questa persuna ha en spezial las suandantas incumbensas:

a) cussegliar e sustegnair las collavuraturas ed ils collavuraturs ch'elavuran datas persunalas, areguard l'observaziun da las prescripziuns davart la protecziun da datas;
b) procurar ch'i vegnian fatgas valitaziuns da las consequenzas per la protecziun da datas;
c) fungar sco persuna da contact dal post da surveglianza e collavurar cun tal.

4. Dretgs da la persuna pertutgada

Art. 24 Dretg d'infurmaziun

[1] Mintga persuna pertutgada po dumandar l'organ public responsabel, sch'i vegnan elavuradas datas persunalas davart sia persuna.

[2] La persuna pertutgada survegn quellas infurmaziuns ch'èn necessarias, per ch'ella possia far valair ses dretgs tenor questa lescha e per ch'ina elavuraziun da datas transparenta saja garantida. A la persuna pertutgada vegnan en mintga cas communitgadas las suandantas infurmaziuns:

a) las indicaziuns tenor l'artitgel 17 alinea 2;
b) la durada da conservaziun da las datas persunalas u ils criteris per fixar questa durada;
c) las indicaziuns disponiblas davart la derivanza da las datas persunalas, nun ch'ellas sajan vegnidas procuradas tar la persuna pertutgada.

[3] Datas persunalas davart la sanadad pon vegnir communitgadas a la persuna pertutgada, cun ses consentiment, tras ina persuna spezialisada dal sectur da sanadad ch'ella ha nominà.

[4] L'organ public responsabel è obligà da dar las infurmaziuns dumandadas er, sch'el lascha elavurar las datas persunalas tras in'elavuratura incumbensada u in elavuratur incumbensà.

[5] Nagin na po renunziar ordavant al dretg d'infurmaziun.

[6] Las infurmaziuns vegnan per regla dadas entaifer 30 dis.

Art. 25 Restricziuns dal dretg d'infurmaziun

[1] L'organ public responsabel po refusar, restrenscher u suspender l'infurmaziun, sche:

a) in'obligaziun legala speziala da mantegnair il secret prevesa quai;
b) quai è necessari pervia d'interess predominants da terzas persunas;
c) la mesira è necessaria pervia d'interess publics predominants, en spezial pervia da la segirezza interna u externa; u
d) la communicaziun da l'infurmaziun po periclitar ina retschertga, ina investigaziun u ina procedura uffiziala u giudiziala.

Art. 26 Opposiziun cunter la communicaziun da datas persunalas

[1] La persuna pertutgada che fa valair vardaivlamain in interess degn da protecziun, po far opposiziun cunter la communicaziun da tschertas datas persunalas tras l'organ public responsabel.

[2] L'organ public refusa la dumonda, sch'ina da las suandantas premissas è ademplida:

a) igl exista in'obligaziun giuridica da communitgar las datas;
b) l'adempliment da sias incumbensas fiss periclità senza la communicaziun.

[3] L'artitgel 11 alinea 1 resta resalvà.

Art. 27 Ulteriuras pretensiuns

[1] Tgi che ha in interess degn da protecziun, po pretender da l'organ public responsabel, ch'el:

a) desistia da l'elavuraziun illegala da las datas persunalas respectivas;
b) elimineschia las consequenzas d'ina elavuraziun illegala;
c) constateschia l'illegalitad da l'elavuraziun.

[2] La petenta u il petent po pretender en spezial, che l'organ public responsabel:

a) rectifitgeschia, stizzia u destrueschia las datas persunalas respectivas;
b) communitgeschia a terzas persunas u publitgeschia sia decisiun, en spezial davart la rectificaziun, la stizzada u la destrucziun da las datas, l'opposiziun cunter la communicaziun u la menziun da contestaziun.

[3] Sche ni la correctadad ni l'incorrectadad da las datas persunalas pertutgadas na po vegnir constatada, agiunta l'organ public responsabel ina menziun da contestaziun a las datas.

Art. 28 Proceduras

[1] Sch'in organ public refusa ina dumonda sin basa da questa lescha, pronunzia el ina decisiun motivada.

[2] L'execuziun dal dretg d'infurmaziun e dal dretg da rectifitgar datas persunalas sco er la dumonda d'opposiziun cunter la communicaziun da datas persunalas èn per regla gratuitas.

[3] Ina taxa commensurada po vegnir pretendida, sche:

a) l'execuziun dals dretgs pretenda sforzs sproporziunads; u
b) la dumonda è evidentamain nunmotivada, en spezial sch'ella persequitescha in intent che cuntrafa a la protecziun da datas, u sch'ella è evidentamain querulatorica.

[4] Dal rest sa drizza la procedura tenor la Lescha davart la giurisdicziun administrativa[5)].

Art. 29 Procedura en cas d'ina communicaziun da documents uffizials che cuntegnan datas persunalas

[1] Sch'ina procedura concernent l'access a documents uffizials che cuntegnan datas persunalas en il senn da la Lescha davart il princip da transparenza[6)] è pendenta, po la persuna pertutgada far valair en questa procedura quels dretgs, che cumpetan ad ella tenor l'artitgel 27 areguard quels documents, ch'èn l'object da la procedura d'access.

5) DG 370.100
6) DG 171.000

5. Surveglianza

Art. 30 Post da surveglianza

[1] Il post da surveglianza per la protecziun da datas surveglia l'applicaziun da las prescripziuns davart la protecziun da datas.

[2] Betg suttamessas a la surveglianza dal post da surveglianza n'èn:

a) elavuraziuns da datas en proceduras pendentas da la giurisdicziun civila e penala;
b) elavuraziuns da datas en proceduras pendentas da la giurisdicziun constituziunala ed administrativa.

Art. 31 Cumposiziun e posiziun

[1] Il post da surveglianza sa cumpona almain da l'incumbensada u da l'incumbensà per la protecziun da datas e d'ina substituziun.

[2] Il post da surveglianza ademplescha sias incumbensas specificas en moda autonoma ed independenta. En l'adempliment da sias incumbensas na sto el observar naginas instrucziuns.

[3] En reguard administrativ è il post da surveglianza suttamess a la Chanzlia chantunala.

[4] La Regenza surveglia il post da surveglianza. En il rom da las cumpetenzas da surveglianza po la Regenza dar directivas al post da surveglianza.

[5] Las relaziuns da lavur ed il provediment professiunal da tut las collavuraturas e da tut ils collavuraturs dal post da surveglianza sa drizzan tenor il dretg chantunal da persunal respectivamain tenor il dretg chantunal davart la cassa da pensiun, uschenavant che questa lescha na prevesa betg insatge auter.

[6] La Regenza attribuescha las plazzas da l'incumbensada u da l'incumbensà per la protecziun da datas e da la substituziun a las classas da funcziun tenor il dretg chantunal da persunal.

Art. 32 Elecziun

[1] La Regenza elegia ina persuna spezialisada qualifitgada en dumondas da la protecziun da datas sco incumbensada u incumbensà per la protecziun da datas ed ina substituziun per in temp d'uffizi da 4 onns. La reelecziun è pussaivla.

[2] La Regenza po destituir l'incumbensada u l'incumbensà per la protecziun da datas e la substituziun da ses uffizi avant la scadenza da la durada d'uffizi, sch'ella u el:

a) ha violà sapientivamain u per greva negligientscha en moda gravanta las obligaziuns d'uffizi; u
b) ha pers per adina l'abilitad d'ademplir ses uffizi.

Art. 33 Incumpatibilitads

[1] L'incumbensada u l'incumbensà per la protecziun da datas e la substituziun na dastgan exequir nagins auters uffizis publics, naginas funcziuns directivas d'ina partida politica e naginas autras activitads da gudogn. La Regenza po permetter excepziuns, sche l'execuziun da la funcziun sco er l'independenza e la reputaziun na vegnan betg influenzadas en moda negativa.

[2] Sche l'incumbensada u l'incumbensà per la protecziun da datas u la substituziun exequescha sia activitad en in pensum parzial, sto la Regenza approvar in'ulteriura activitad da gudogn. La permissiun dastga vegnir refusada mo, sche questa activitad da gudogn influenzescha en moda negativa l'execuziun da la funcziun sco er l'independenza e la reputaziun.

Art. 34 Preventiv

[1] L'incumbensada u l'incumbensà per la protecziun da datas fa in agen preventiv.

[2] En la missiva dal preventiv communitgescha la Regenza, sche la proposta è vegnida surpigliada senza midadas. Divergenzas ston vegnir motivadas.

[3] En il rom dal preventiv è l'incumbensada u l'incumbensà per la protecziun da datas cumpetent per engaschar las collavuraturas ed ils collavuraturs sco er per terminar e per midar lur relaziun da lavur.

Art. 35 Incumbensas

[1] Il post da surveglianza:

a) surveglia l'applicaziun da las prescripziuns davart la protecziun da datas;
b) cusseglia las persunas pertutgadas davart lur dretgs;
c) intermediescha tranter las persunas pertutgadas ed ils organs publics;
d) cusseglia ils organs publics en dumondas da la protecziun da datas e surveglia la segirada da datas;
e) prenda posiziun davart decrets e davart projects d'informatica, sche quels èn relevants per la protecziun da datas;
f) tracta las annunzias da persunas pertutgadas concernent l'inobservanza da prescripziuns da questa lescha ed infurmescha ellas entaifer maximalmain 3 mais davart il resultat u davart il stadi dals scleriments;
g) sensibilisescha ils organs publics per lur obligaziuns en la protecziun da datas e la publicitad per las finamiras da la protecziun da datas;
h) persequitescha ils svilups ch'èn decisivs per la protecziun da datas persunalas;
i) collavura – en vista a l'adempliment da sias incumbensas – cun ils organs dals auters chantuns, da la Confederaziun e da l'exteriur che adempleschan las medemas incumbensas.

Art. 36 Cumpetenzas
1. controlla e recumandaziun

[1] Il post da surveglianza daventa activ d'uffizi u sin basa d'ina annunzia da las persunas pertutgadas. L'organ public responsabel sto vegnir infurmà davart in'annunzia e sto survegnir la pussaivladad da prender posiziun.

[2] Independentamain d'eventualas prescripziuns da mantegnair il secret po il post da surveglianza sa procurar tut las infurmaziuns davart elavuraziuns da datas ch'èn necessarias per ademplir l'incumbensa da controlla, prender invista da tut ils documents, far inspecziuns e sa laschar preschentar elavuraziuns.

[3] Il post da surveglianza po far recumandaziuns per l'elavuraziun da datas persunalas. L'organ public, al qual la recumandaziun sa drizza, sto declerar al post da surveglianza, sch'el vul suandar la recumandaziun.

[4] Ils organs publics sco er las elavuraturas incumbensadas ed ils elavuraturs incumbensads èn obligads da sustegnair il post da surveglianza tar l'adempliment da sias incumbensas. Ellas ed els coopereschan en spezial a la constataziun dals fatgs.

Art. 37 2. decisiun

[1] Sch'in organ public declera, ch'el na veglia betg suandar la recumandaziun dal post da surveglianza, u sch'el na suonda effectivamain betg la recumandaziun, po il post da surveglianza decretar la recumandaziun u parts da tala en furma d'ina decisiun.

[2] Il post da surveglianza po decretar directamain ina decisiun, sch'igl è previsibel che l'organ public vegn a refusar ina recumandaziun u na vegn betg a suandar tala.

[3] Cunter decisiuns tenor l'artitgel 37 alinea 1 ed alinea 2 po l'organ public pertutgà far recurs tar la Dretgira superiura. Valair vala la Lescha davart la giurisdicziun administrativa[7)].

[4] Cunter decisiuns che concernan la Dretgira superiura, po la Dretgira superiura far recurs tar la Dretgira da giustia.

Art. 38 Rapportaziun

[1] Il post da surveglianza suttametta mintga onn a la Regenza in rapport davart la dimensiun e davart ils puncts centrals da sia activitad sco er davart constataziuns relevantas e davart giudicaments impurtants.

[2] A l'organ public ch'è pertutgà da recumandaziuns e da decisiuns dat il post da surveglianza l'occasiun da prender posiziun en scrit. Las posiziuns vegnan agiuntadas al rapport.

[3] Il rapport vegn publitgà.

7) DG 370.100

Art. 39 Discreziun

[1] Il post da surveglianza è obligà da mantegnair la medema discreziun areguard las datas persunalas sco l'organ public ch'elavura las datas. L'obligaziun da discreziun vala er suenter la terminaziun da la funcziun.

[2] Cun resalva da prescripziuns spezialas da mantegnair il secret dastga il post da surveglianza mo communitgar enconuschientschas fatgas durant sia activitad, sche quai è necessari per ademplir sias incumbensas.

6. Disposiziuns penalas e transitoricas

Art. 40 Disposiziuns penalas

[1] In'elavuratura incumbensada u in elavuratur incumbensà che utilisescha, senza autorisaziun explicita da l'organ public incaricant, datas persunalas per sasez u per autras persunas u communitgescha datas persunalas ad autras persunas, e quai intenziunadamain u per negligientscha, vegn chastià cun ina multa.

[2] Tgi che ha survegnì datas persunalas d'in organ public en vista ad in'elavuraziun per intents che na sa refereschan betg a persunas, ed elavura questas datas – cuntrari a l'obligaziun tenor l'artitgel 13 – per auters intents u dat vinavant las datas a terzas persunas, e quai intenziunadamain u per negligientscha, vegn chastià cun ina multa.

Art. 41 Disposiziuns transitoricas

[1] Elavuraziuns da datas che han ina basa giuridica suffizienta tenor il dretg vertent, pon vegnir cuntinuadas durant 2 onns tenor las basas giuridicas vertentas.

[2] La cumprova che las disposiziuns davart la protecziun da datas vegnian observadas, sto pudair vegnir furnida il pli tard 2 onns suenter che questa lescha è entrada en vigur.

[3] L'artitgel 19 e l'artitgel 20 n'èn betg applitgabels per elavuraziuns da datas ch'èn vegnidas cumenzadas avant che questa lescha è entrada en vigur, uschenavant che l'intent da l'elavuraziun u l'activitad d'elavuraziun na vegn betg midada essenzialmain.

II.

1.
Il relasch "Lescha dal dretg da burgais dal chantun Grischun (LDBchant)" DG 130.100 (versiun dals 01-01-2025) vegn midà sco suonda:

Art. 24 al. 1 (midà)

[1] Per ademplir lur incumbensas tenor questa lescha pon las autoritads chantunalas e communalas cumpetentas sco er ils posts ch'ellas han incumbensà elavurar datas, inclusiv ~~ils~~ profils da **la** persunalitad e ~~las~~ datas persunalas spezialmain ~~protegidas~~ **sensiblas,** davart:

Enumeraziun senza midadas.

2.

Il relasch "Lescha davart ils registers d'abitantas e d'abitants e davart ulteriurs registers da persunas e d'objects (lescha da registers, LRAb)" DG 171.200 (versiun dals 01-01-2018) vegn midà sco suonda:

Art. 32 al. 3 (midà)

[3] Il dretg **d'opposiziun cunter la communicaziun** da ~~bloccada~~**datas persunalas tenor la Lescha chantunala davart la protecziun da datas**[8)] resta resalvà.

3.

Il relasch "Lescha introductiva tar il cudesch da procedura civila svizzer (LItCPC)" DG 320.100 (versiun dals 01-01-2025) vegn midà sco suonda:

Art. 14 al. 5 (nov)

[5] Las decisiuns davart l'invista da las actas en proceduras davant la Dretgira superiura e davant la Dretgira da giustia èn definitivas tenor il dretg chantunal.

4.

Il relasch "Lescha introductiva tar il cudesch da procedura penala svizzer (LItCPP)" DG 350.100 (versiun dals 01-01-2025) vegn midà sco suonda:

Art. 36 al. 5 (nov)

[5] Las decisiuns davart l'invista da las actas en proceduras davant la Dretgira superiura e davant la Dretgira da giustia èn definitivas tenor il dretg chantunal.

5.

Il relasch "Lescha davart la surveglianza da las finanzas (LSFi)" DG 710.300 (versiun dals 01-01-2025) vegn midà sco suonda:

8) DG 171.100

Art. 20 al. 1 (midà), **al. 2 (midà)**

[1] La ~~controlla~~**Controlla** da finanzas ha il dretg da consultar las datas ch'èn necessarias per ademplir la surveglianza da las finanzas**,** inclusiv las datas ~~da persunas~~ **persunalas** or da collecziuns da datas dals departaments e dals posts da servetsch sco er da las dretgiras e da las autoritads da mediaziun. Sche las datas èn adattadas e necessarias per ademplir las incumbensas, vala il dretg d'access er per las datas ~~da persunas ch'èn~~ **persunalas** spezialmain ~~degnas da vegnir protegidas~~ **sensiblas**.

[2] La ~~controlla~~**Controlla** da finanzas dastga tegnair en salv u arcunar las datas ~~da persunas~~**persunalas**, da las qualas ella ha prendì enconuschientscha en ~~tala moda~~ **questa maniera**, mo fin che la procedura da revisiun è terminada. Ils access a las differentas collecziuns da datas ed ils intents che duain vegnir cuntanschids cun quai**,** ston vegnir documentads.

III.

Il relasch "Lescha chantunala davart la protecziun da datas (LCPD)" DG 171.100 (versiun dals 01-01-2025) vegn abolì.

IV.

Questa lescha è suttamessa al referendum facultativ.

La Regenza fixescha il termin da l'entrada en vigur da questa lescha.

Legge cantonale sulla protezione dei dati (LCPD)

Del [Data]

Atti normativi interessati (numeri CSC)

Nuovo:	**171.100**
Modificato:	130.100 | 171.200 | 320.100 | 350.100 | 710.300
Abrogato:	171.100

Il Gran Consiglio del Cantone dei Grigioni,

visto l'art. 31 cpv. 1 della Costituzione cantonale[1)],
visto il messaggio del Governo del ...,

decide:

I.

L'atto normativo "Legge cantonale sulla protezione dei dati (LCPD)" CSC 171.100 viene pubblicato quale nuovo atto normativo.

1. Disposizioni generali

Art. 1 Scopo

[1] La presente legge serve a proteggere le persone dal trattamento illecito di dati personali da parte di organi pubblici.

Art. 2 Campo d'applicazione

[1] La presente legge si applica al trattamento di dati personali da parte di organi pubblici.

1) CSC 110.100

[2] Se un organo pubblico prende parte alla concorrenza economica e in questo ambito non agisce in veste decisionale, per il trattamento di tali dati sono applicabili le normative della legge federale sulla protezione dei dati[2)]. La vigilanza si conforma alla presente legge, tranne nel caso di organi pubblici che prendono parte esclusivamente alla concorrenza economica e in questo ambito agiscono in base al diritto privato.

[3] Il trattamento di dati personali e i diritti delle persone interessate nei procedimenti giudiziari e nei procedimenti secondo gli ordinamenti procedurali federali nonché nelle procedure della giurisdizione amministrativa, ad eccezione delle procedure di prima istanza dinanzi ad autorità amministrative, sono retti dal diritto processuale applicabile.

[4] Le disposizioni divergenti e complementari in altre leggi sono fatte salve a condizione che garantiscano la protezione dei diritti fondamentali di persone i cui dati personali sono oggetto di trattamento da parte di organi pubblici ai sensi della presente legge.

Art. 3 Definizioni

[1] Sono considerati organi pubblici ai sensi della presente legge:

a) le autorità, le amministrazioni e le commissioni del Cantone, delle regioni, dei comuni e delle unioni di comuni;
b) le autorità, le amministrazioni e le commissioni di istituti, fondazioni ed enti di diritto pubblico del Cantone, delle regioni e dei comuni;
c) le persone fisiche o giuridiche o altre organizzazioni di diritto privato per quanto adempiano compiti pubblici loro delegati.

[2] Per dati personali ai sensi della presente legge si intendono tutte le informazioni concernenti una persona fisica identificata o identificabile.

[3] Per dati personali degni di particolare protezione si intendono dati personali associati a un pericolo particolare che vengano violati diritti fondamentali, segnatamente:

a) i dati concernenti le opinioni o attività religiose, filosofiche, politiche o sindacali;
b) i dati concernenti la salute, la sfera intima o l'appartenenza a una razza o a un'etnia;
c) i dati genetici;
d) i dati biometrici che identificano in modo univoco una persona fisica;
e) i dati concernenti perseguimenti e sanzioni amministrativi e penali;
f) i dati concernenti le misure d'assistenza sociale.

[4] Per profili della personalità si intendono raccolte di dati che permettono di valutare aspetti essenziali della personalità di una persona fisica.

2) RS 235.1

[5] Per profilazione si intende qualsiasi tipo di trattamento automatizzato di dati personali consistente nell'utilizzazione degli stessi per valutare determinati aspetti personali di una persona fisica, in particolare per analizzare o prevedere aspetti concernenti il rendimento professionale, la situazione economica, la salute, le preferenze, gli interessi, l'affidabilità, il comportamento, i luoghi di permanenza e gli spostamenti di tale persona.

[6] Per trattamento si intende qualsiasi operazione relativa a dati personali, indipendentemente dai mezzi e dalle procedure impiegati, segnatamente la raccolta, la registrazione, la conservazione, l'utilizzazione, la modificazione, la comunicazione, l'archiviazione, la cancellazione o la distruzione di dati.

[7] Per comunicazione si intende la trasmissione di dati personali o il fatto di renderli accessibili.

[8] Per violazione della sicurezza dei dati si intende la violazione della sicurezza in seguito alla quale, in modo accidentale o illecito, dati personali vengono persi, cancellati, distrutti, modificati oppure divulgati o resi accessibili a persone non autorizzate.

[9] Per responsabile del trattamento si intende una terza persona che tratta dati personali per conto dell'organo pubblico titolare del trattamento.

Art. 4 Responsabilità

[1] Per la protezione dei dati è responsabile l'organo pubblico che, singolarmente o insieme ad altri, determina lo scopo e i mezzi del trattamento.

[2] Se più organi pubblici trattano dati personali di un insieme di dati, disciplinano tra loro le responsabilità e designano l'organo che detiene la responsabilità globale.

[3] Su richiesta, l'organo pubblico titolare del trattamento deve essere in grado di dimostrare nei confronti dell'organo di vigilanza il rispetto delle disposizioni in materia di protezione dei dati.

Art. 5 Principi del trattamento di dati

[1] I dati personali devono essere trattati in modo lecito.

[2] Il trattamento deve essere conforme ai principi della buona fede e della proporzionalità.

[3] I dati personali possono essere raccolti soltanto per uno scopo determinato e riconoscibile per la persona interessata; possono essere trattati ulteriormente soltanto in modo compatibile con tale scopo.

[4] I dati personali sono distrutti o resi anonimi appena non sono più necessari per lo scopo del trattamento.

[5] Chi tratta dati personali deve accertarsi della loro esattezza. Deve prendere tutte le misure adeguate per rettificare, cancellare o distruggere i dati inesatti o incompleti rispetto allo scopo per il quale sono stati raccolti o trattati. L'adeguatezza delle misure dipende segnatamente dal tipo e dall'entità del trattamento come pure dai rischi derivanti dal trattamento per i diritti fondamentali delle persone interessate.

[6] Laddove una condizione sia necessaria per il trattamento, il consenso della persona interessata è valido soltanto se, dopo debita informazione, è dato in modo libero in riferimento a uno o più trattamenti specifici.

[7] È necessario l'espresso consenso per:

a) il trattamento di dati personali degni di particolare protezione;
b) la profilazione o il trattamento di un profilo della personalità.

Art. 6 Sicurezza dei dati

[1] L'organo pubblico titolare del trattamento e il responsabile del trattamento garantiscono, mediante appropriati provvedimenti tecnici e organizzativi, che la sicurezza dei dati personali sia adeguata al rischio.

[2] I provvedimenti devono permettere di evitare violazioni della sicurezza dei dati.

[3] Il Governo emana disposizioni sui requisiti minimi in materia di sicurezza dei dati.

2. Trattamento di dati personali

Art. 7 Trattamento di dati personali

[1] Gli organi pubblici hanno il diritto di trattare dati personali soltanto se lo prevede una base legale o se il trattamento è indispensabile all'adempimento di un compito legale.

[2] La base legale deve figurare in una legge nei casi seguenti:

a) sono trattati dati personali degni di particolare protezione;
b) è allestito un profilo della personalità o è effettuata una profilazione;
c) lo scopo del trattamento o il tipo di trattamento può comportare una grave ingerenza nei diritti fondamentali della persona interessata.

[3] Per il trattamento di dati personali secondo il capoverso 2 lettera a e lettera b è sufficiente una base legale figurante in un'ordinanza se:

a) il trattamento è indispensabile per l'adempimento di un compito esplicitamente descritto in una legge;
b) lo scopo del trattamento non comporta rischi particolari per i diritti fondamentali della persona interessata.

[4] In deroga al capoverso 1 fino al capoverso 3, gli organi pubblici possono trattare dati personali se una delle seguenti condizioni è soddisfatta:

a) la persona interessata ha dato, nel caso specifico, il suo consenso al trattamento oppure ha reso i suoi dati personali accessibili a chiunque e non si è opposta espressamente al trattamento;
b) il trattamento è necessario per proteggere la vita o l'integrità fisica della persona interessata o di un terzo e non è possibile ottenere il consenso della persona interessata entro un termine ragionevole.

Art. 8 Trattamento automatizzato di dati personali nell'ambito di sistemi pilota

[1] Il Governo può autorizzare il trattamento automatizzato di dati personali degni di particolare protezione o di profili della personalità o la profilazione prima dell'entrata in vigore di una legge se:

a) i compiti che richiedono tale trattamento sono disciplinati in una legge già in vigore;
b) sono prese misure sufficienti per ridurre al minimo l'ingerenza nei diritti fondamentali delle persone interessate; e
c) per l'attuazione pratica del trattamento è imprescindibile una fase sperimentale prima dell'entrata in vigore, in particolare per ragioni tecniche.

[2] Il Governo chiede previamente il parere dell'organo di vigilanza.

[3] L'organo pubblico titolare del trattamento presenta un rapporto di valutazione al Governo al più tardi due anni dopo la messa in opera del sistema pilota. Nel rapporto propone la continuazione o l'interruzione del trattamento.

[4] Il trattamento automatizzato di dati personali deve in ogni caso essere interrotto se entro cinque anni dalla messa in opera del sistema pilota non è entrata in vigore una legge che prevede la pertinente base legale.

Art. 9 Trattamento da parte di un responsabile del trattamento

[1] Il trattamento di dati personali può essere affidato a un responsabile del trattamento per contratto o per legge se:

a) questi effettua soltanto i trattamenti di dati che l'organo pubblico titolare del trattamento avrebbe il diritto di effettuare; e
b) nessun obbligo legale o contrattuale di serbare il segreto lo vieta.

[2] L'organo pubblico titolare del trattamento deve in particolare accertarsi che il responsabile del trattamento sia in grado di garantire la sicurezza dei dati.

[3] Il responsabile del trattamento può affidare il trattamento a un terzo soltanto previa autorizzazione dell'organo pubblico titolare del trattamento.

Art. 10 Comunicazione di dati personali
1. Direttive generali

[1] Gli organi pubblici hanno il diritto di comunicare dati personali soltanto se lo prevede una base legale ai sensi dell'articolo 7 capoverso 1 fino al capoverso 3.

[2] In deroga al capoverso 1, gli organi pubblici possono, nel caso specifico, comunicare dati personali se una delle seguenti condizioni è soddisfatta:

a) la comunicazione dei dati è indispensabile all'adempimento dei compiti legali dell'organo pubblico titolare del trattamento o del destinatario;
b) la persona interessata ha dato il suo consenso alla comunicazione o ha reso i suoi dati personali accessibili a chiunque e non si è opposta espressamente alla comunicazione;

c) la comunicazione è necessaria per proteggere la vita o l'integrità fisica della persona interessata o di un terzo e non è possibile ottenere il consenso della persona interessata entro un termine ragionevole;
d) il destinatario rende verosimile che la persona interessata rifiuta di dare il proprio consenso, oppure si oppone alla comunicazione, al solo scopo di impedirgli l'attuazione di pretese giuridiche o la difesa di altri interessi degni di protezione; la persona interessata deve previamente essere invitata a pronunciarsi, salvo che ciò sia impossibile o richieda un onere sproporzionato.

[3] Gli organi pubblici possono comunicare, su richiesta, cognome, nome, indirizzo e data di nascita di una persona anche se le condizioni del capoverso 1 o del capoverso 2 non sono soddisfatte.

[4] Gli organi pubblici rifiutano o limitano la comunicazione, oppure la vincolano a oneri, se lo esige:

a) un importante interesse pubblico o un interesse manifestamente degno di protezione della persona interessata; o
b) un obbligo legale di serbare il segreto o una disposizione speciale concernente la protezione dei dati.

Art. 11 2. Comunicazione di dati personali nell'ambito dell'attività di informazione ufficiale

[1] Nell'ambito dell'informazione ufficiale del pubblico, gli organi pubblici possono inoltre comunicare dati personali d'ufficio se:

a) i dati sono in rapporto con l'adempimento di compiti pubblici; e
b) sussiste un interesse pubblico preponderante alla comunicazione.

[2] Gli organi pubblici possono rendere accessibili a chiunque dati personali mediante servizi di informazione e comunicazione automatizzati se una base legale prevede la pubblicazione di questi dati oppure se comunicano dati in virtù del capoverso 1. Se cessa l'interesse pubblico a renderli accessibili a chiunque, i dati contenuti nel servizio di informazione e comunicazione automatizzato sono cancellati.

[3] La procedura di accesso a documenti ufficiali si conforma alla legge sul principio di trasparenza[3)].

Art. 12 3. Comunicazione di dati personali all'estero

[1] Dati personali possono essere comunicati all'estero soltanto se la legislazione dello Stato destinatario o l'organismo internazionale garantisce una protezione adeguata.

[2] Negli Stati la cui legislazione non garantisce una protezione adeguata i dati personali possono essere comunicati soltanto se:

a) garanzie sufficienti, in particolare mediante contratto, garantiscono una protezione adeguata all'estero;
b) la persona interessata ha dato il suo espresso consenso alla comunicazione;

[3)] CSC 171.000

c) la comunicazione è in relazione diretta con la conclusione o l'esecuzione di un contratto tra l'organo pubblico titolare del trattamento e la persona interessata o tra l'organo pubblico titolare del trattamento e un altro contraente, nell'interesse della persona interessata;
d) la comunicazione è necessaria per tutelare un interesse pubblico preponderante o per accertare, esercitare o far valere un diritto dinanzi a un giudice o a un'altra autorità estera competente;
e) la comunicazione è necessaria per proteggere la vita o l'integrità fisica della persona interessata o di un terzo e non è possibile ottenere il consenso della persona interessata entro un termine ragionevole;
f) la persona interessata ha reso i dati personali accessibili a chiunque e non si è opposta espressamente al loro trattamento; o
g) i dati provengono da un registro previsto dalla legge accessibile al pubblico o alle persone con un interesse degno di protezione, sempreché nel caso specifico siano adempiute le condizioni legali per la consultazione.

[3] Prima della comunicazione dei dati personali all'estero l'organo pubblico informa l'organo di vigilanza in merito alle garanzie di cui al capoverso 2 lettera a.

Art. 13 Trattamento di dati personali per scopi impersonali

[1] Gli organi pubblici hanno il diritto di trattare dati personali per scopi impersonali, in particolare nei settori della ricerca, della pianificazione o della statistica, se:

a) rendono anonimi i dati non appena lo scopo del trattamento lo permette;
b) comunicano a privati i dati personali degni di particolare protezione soltanto in una forma che non permetta d'identificare le persone interessate;
c) il destinatario trasmette a terzi i dati soltanto con l'autorizzazione dell'organo pubblico che glieli ha comunicati; e
d) i risultati sono pubblicati soltanto in una forma che non permetta d'identificare le persone interessate.

[2] L'articolo 5 capoverso 3, l'articolo7 capoverso 2 nonché l'articolo 10 capoverso 1 non sono applicabili.

Art. 14 Sorveglianza con acquisizione di immagini dello spazio pubblico e pubblicamente accessibile
1. Direttive generali

[1] Lo spazio pubblico e pubblicamente accessibile può essere sorvegliato con apparecchi di trasmissione e di registrazione di immagini allo scopo di identificare persone se:

a) la sicurezza e l'ordine pubblici sono esposti a una minaccia concreta; oppure
b) ciò è necessario a protezione di edifici destinati a usi pubblici o dei loro utenti.

[2] In sede di trattamento dei dati personali devono essere rispettati i principi generali. In aggiunta occorre garantire che:

a) gli impianti di sorveglianza siano segnalati in maniera adeguata e riconoscibile;

b) settori funzionali allo svolgimento di attività coperte dal segreto professionale ai sensi dell'articolo 171 del Codice di diritto processuale penale svizzero[4] siano esclusi dalla sorveglianza; e

c) dati personali registrati vengano cancellati entro 90 giorni o vengano trasmessi all'autorità competente ai fini dell'utilizzo in un procedimento penale o dell'attuazione di pretese di diritto civile a seguito di un reato.

Art. 15 2. Disposizione della sorveglianza con acquisizione di immagini dello spazio pubblico e pubblicamente accessibile

[1] La sorveglianza con acquisizione di immagini dello spazio pubblico e pubblicamente accessibile può essere disposta da un organo pubblico titolare del diritto d'uso o della sovranità sullo spazio oggetto di sorveglianza.

[2] L'organo pubblico emana una decisione generale in cui vengono definiti lo scopo, la tipologia e la durata della sorveglianza, i luoghi oggetto di sorveglianza, le ubicazioni degli apparecchi di sorveglianza, le misure con le quali viene segnalata la sorveglianza, i diritti d'accesso nonché le misure adottate per garantire la sicurezza dei dati. La decisione generale è valida per al massimo cinque anni.

[3] L'organo pubblico è tenuto a pubblicare in precedenza la decisione generale da emanare. Concede il diritto di essere sentiti prevedendo un termine adeguato per prendere posizione.

[4] Non va concessa una previa protezione giuridica per sorveglianze con acquisizione di immagini riferite a un evento con una durata di al massimo tre mesi e per sorveglianze con acquisizione di immagini a protezione di edifici destinati a usi pubblici che vengono impiegate in relazione a un evento e non registrano dati personali.

Art. 16 Archiviazione e distruzione

[1] L'organo pubblico offre all'archivio competente i dati personali di cui non necessita più secondo le prescrizioni vigenti in materia.

[2] Esso distrugge i dati personali che l'archivio competente ha designato come non aventi valore archivistico, salvo che tali dati:

a) siano resi anonimi;

b) debbano essere conservati a titolo di prova, per misura di sicurezza o per salvaguardare un interesse degno di protezione della persona interessata.

3. Obblighi dell'organo pubblico titolare del trattamento

Art. 17 Obbligo di informare sulla raccolta di dati personali

[1] L'organo pubblico titolare del trattamento informa in modo adeguato la persona interessata sulla raccolta di dati personali; tale obbligo sussiste anche se i dati non sono raccolti presso la persona interessata.

[4] RS 312.0

[2] Al momento della raccolta, l'organo pubblico titolare del trattamento fornisce alla persona interessata le informazioni necessarie affinché questa possa far valere i propri diritti secondo la presente legge e sia garantito un trattamento trasparente dei dati; fornisce almeno le informazioni seguenti:

a) l'identità e i dati di contatto dell'organo pubblico titolare del trattamento;
b) la base legale e lo scopo del trattamento;
c) i diritti della persona interessata;
d) se del caso, i destinatari o le categorie di destinatari cui sono comunicati dati personali;
e) le categorie di dati personali trattati se i dati non sono raccolti presso la persona interessata;
f) se i dati sono comunicati all'estero, anche lo Stato o l'organismo internazionale destinatario e, se del caso, le garanzie o l'applicazione di un'eccezione secondo l'articolo 12 capoverso 2.

[3] Se i dati personali non sono raccolti presso la persona interessata, l'organo pubblico titolare del trattamento fornisce alla persona interessata le informazioni di cui al capoverso 2 entro un mese dalla ricezione dei dati. Se comunica questi dati personali prima della scadenza di detto termine, l'organo pubblico titolare del trattamento fornisce alla persona interessata tali informazioni al più tardi al momento della comunicazione.

Art. 18 Eccezioni all'obbligo di informare e limitazioni

[1] L'obbligo di informare sulla raccolta di dati personali non sussiste se una delle seguenti condizioni è soddisfatta:

a) la persona interessata dispone già delle pertinenti informazioni;
b) il trattamento è previsto dalla legge;
c) i dati personali non sono raccolti presso la persona interessata e l'informazione non è possibile o richiede un onere sproporzionato.

[2] L'organo pubblico titolare del trattamento può limitare o differire l'informazione oppure rinunciarvi alle stesse condizioni valide per il diritto d'accesso secondo l'articolo 25.

Art. 19 Valutazione d'impatto sulla protezione dei dati

[1] L'organo pubblico titolare del trattamento effettua previamente una valutazione d'impatto sulla protezione dei dati quando il trattamento può comportare un rischio elevato per i diritti fondamentali della persona interessata. Se prevede più operazioni di trattamento simili può procedere a una valutazione d'impatto comune.

[2] Il rischio elevato, in particolare in caso di utilizzazione di nuove tecnologie, risulta dal tipo, dall'entità, dalle circostanze e dallo scopo del trattamento. Sussiste segnatamente nel caso di:

a) trattamento su grande scala di dati personali degni di particolare protezione;
b) sorveglianza sistematica di ampi spazi pubblici.

[3] La valutazione d'impatto sulla protezione dei dati contiene una descrizione del trattamento previsto, una valutazione dei rischi per i diritti fondamentali della persona interessata nonché i provvedimenti a loro tutela.

Art. 20 Consultazione preliminare

[1] L'organo pubblico titolare del trattamento chiede previamente il parere dell'organo di vigilanza se dalla valutazione d'impatto sulla protezione dei dati emerge che, nonostante i provvedimenti previsti dall'organo pubblico titolare, il trattamento previsto comporta un rischio elevato per i diritti fondamentali della persona interessata.

[2] L'organo di vigilanza comunica entro un termine adeguato all'organo pubblico titolare del trattamento le sue obiezioni contro il trattamento previsto e propone provvedimenti idonei.

Art. 21 Notifica di violazioni della sicurezza dei dati

[1] L'organo pubblico titolare del trattamento notifica quanto prima all'organo di vigilanza ogni violazione della sicurezza dei dati che comporta verosimilmente un rischio elevato per i diritti fondamentali della persona interessata.

[2] Nella notifica l'organo pubblico titolare del trattamento menziona almeno il tipo di violazione della sicurezza dei dati, le sue conseguenze e le misure disposte o previste.

[3] Il responsabile del trattamento informa quanto prima l'organo pubblico titolare del trattamento su ogni violazione della sicurezza dei dati.

[4] L'organo pubblico titolare del trattamento informa la persona interessata sulla violazione della sicurezza dei dati, se ciò è necessario per proteggere la persona interessata o se lo esige l'organo di vigilanza.

[5] L'organo pubblico titolare del trattamento può limitare o differire l'informazione della persona interessata o rinunciarvi se:

a) lo esigono interessi preponderanti di terzi;
b) lo esigono interessi pubblici preponderanti, in particolare a tutela della sicurezza interna o esterna;
c) la fornitura delle informazioni rischia di compromettere un'indagine, un'istruzione o un procedimento giudiziario o amministrativo;
d) sussiste un obbligo legale di serbare il segreto;
e) l'informazione è impossibile o richiede un onere sproporzionato;
f) l'informazione è garantita in modo equivalente con una comunicazione pubblica.

Art. 22 Registro delle attività di trattamento

[1] Quale comprova del rispetto delle disposizioni sulla protezione dei dati, gli organi pubblici designati dal Governo e i tribunali penali tengono un registro delle rispettive attività di trattamento.

[2] Il registro contiene almeno:

a) l'identità e i dati di contatto dell'organo pubblico titolare del trattamento;
b) la base legale e lo scopo del trattamento;
c) una descrizione delle categorie di persone interessate e delle categorie di dati personali trattati;
d) se del caso, i destinatari o le categorie di destinatari cui sono comunicati dati personali;
e) la durata di conservazione dei dati personali o i criteri per stabilire tale durata;
f) una descrizione generale dei provvedimenti tesi a garantire la sicurezza dei dati personali;
g) l'indicazione se i dati personali sono comunicati all'estero e, se del caso, le garanzie o l'applicazione di un'eccezione secondo l'articolo 12 capoverso 2.

[3] L'organo pubblico notifica i suoi registri all'organo di vigilanza e può pubblicarli.

Art. 23 Consulente per la protezione dei dati

[1] Gli organi pubblici designati dal Governo e i tribunali penali designano una persona competente per la consulenza in materia di protezione dei dati. Questa ha segnatamente i compiti seguenti:

a) fornire consulenza e sostegno ai collaboratori in sede di trattamento di dati personali per quanto riguarda il rispetto delle disposizioni sulla protezione dei dati;
b) provvedere allo svolgimento delle valutazioni d'impatto sulla protezione dei dati;
c) essere la persona di riferimento dell'organo di vigilanza e collaborare con quest'ultimo.

4. Diritti della persona interessata

Art. 24 Diritto d'accesso

[1] Ogni persona interessata può domandare all'organo pubblico titolare del trattamento se dati personali che lo concernono sono oggetto di trattamento.

[2] Alla persona interessata sono fornite le informazioni necessarie affinché possa far valere i suoi diritti secondo la presente legge e sia garantito un trattamento trasparente dei dati. In ogni caso le sono fornite le informazioni seguenti:

a) le indicazioni di cui all'articolo 17 capoverso 2;
b) la durata di conservazione dei dati personali o i criteri per stabilire tale durata;
c) le informazioni disponibili sulla provenienza dei dati personali che non sono stati raccolti presso la persona interessata.

[3] I dati personali concernenti la salute possono essere comunicati alla persona interessata per il tramite di un professionista della salute da lei designato; a tale scopo è necessario il consenso della persona interessata.

[4] L'organo pubblico titolare del trattamento è tenuto a fornire le informazioni richieste anche se ha affidato il trattamento dei dati personali a un responsabile del trattamento.

[5] Nessuno può rinunciare preventivamente al diritto d'accesso.

[6] Di norma l'informazione è fornita entro 30 giorni.

Art. 25 Restrizione del diritto d'accesso

[1] L'organo pubblico titolare del trattamento può rifiutare, limitare o differire l'informazione se:

a) lo prevede un obbligo legale particolare di serbare il segreto;
b) lo esigono interessi preponderanti di terzi;
c) lo esige un interesse pubblico preponderante, in particolare la sicurezza interna o esterna della Svizzera; oppure
d) la fornitura delle informazioni rischia di compromettere un'indagine, un'istruzione o un procedimento giudiziario o amministrativo.

Art. 26 Opposizione alla comunicazione di dati personali

[1] La persona interessata che rende verosimile un interesse degno di protezione può opporsi alla comunicazione di determinati dati personali da parte dell'organo pubblico titolare del trattamento.

[2] L'organo pubblico respinge l'opposizione se una delle seguenti condizioni è soddisfatta:

a) sussiste un obbligo legale alla comunicazione;
b) l'adempimento del suo compito ne risulterebbe altrimenti pregiudicato.

[3] È fatto salvo l'articolo 11 capoverso 1.

Art. 27 Altre pretese

[1] Chi ha un interesse degno di protezione può esigere che l'organo pubblico titolare del trattamento:

a) si astenga dal trattamento illecito dei pertinenti dati personali;
b) elimini le conseguenze di un trattamento illecito;
c) accerti il carattere illecito del trattamento.

[2] Il richiedente può in particolare esigere che l'organo pubblico titolare del trattamento:

a) rettifichi, cancelli o distrugga i pertinenti dati personali;
b) comunichi a terzi o pubblichi la sua decisione, in particolare la rettifica, la cancellazione o la distruzione dei dati, l'opposizione alla comunicazione o la menzione del carattere contestato dei dati.

[3] Se non possono essere accertate né l'esattezza né l'inesattezza dei dati personali, l'organo pubblico titolare del trattamento aggiunge agli stessi una menzione che ne indica il carattere contestato.

Art. 28 Procedura

[1] Se un organo pubblico non accoglie una richiesta in virtù della presente legge, emana una decisione motivata.

[2] Di norma, l'esercizio del diritto d'accesso e del diritto di rettifica di dati personali nonché la domanda di opposizione alla comunicazione di dati personali sono gratuiti.

[3] È possibile riscuotere una tassa adeguata se:

a) l'esercizio dei diritti è associato a spese sproporzionate; oppure
b) la domanda è manifestamente infondata, segnatamente se persegue uno scopo contrario alla protezione dei dati, o se è querulosa.

[4] Per il resto la procedura si conforma alla legge sulla giustizia amministrativa[5)].

Art. 29 Procedura in caso di comunicazione di documenti ufficiali che contengono dati personali

[1] Se è in corso una procedura ai sensi della legge sul principio di trasparenza[6)] concernente l'accesso a documenti ufficiali che contengono dati personali, la persona interessata può, in tale procedura, far valere i diritti che le spettano in virtù dell'articolo 27 in riferimento ai documenti oggetto della procedura di accesso.

5. Vigilanza

Art. 30 Organo di vigilanza

[1] L'organo di vigilanza per la protezione dei dati vigila sull'applicazione delle disposizioni sulla protezione dei dati.

[2] Non sono soggetti alla vigilanza dell'organo di vigilanza:

a) i trattamenti di dati in procedimenti in corso dell'amministrazione della giustizia civile e penale;
b) i trattamenti di dati in procedimenti in corso della giurisdizione costituzionale e amministrativa.

Art. 31 Composizione e posizione

[1] L'organo di vigilanza è composto almeno dall'incaricato della protezione dei dati e da un supplente.

[2] Dal profilo professionale l'organo di vigilanza adempie i suoi compiti in maniera autonoma ed indipendente. Nell'adempimento dei suoi compiti l'organo di vigilanza non è vincolato a direttive.

[3] Dal profilo amministrativo l'organo di vigilanza è subordinato alla Cancelleria dello Stato.

---

5) CSC 370.100
6) CSC 171.000

[4] Il Governo esercita la vigilanza sull'organo di vigilanza. Nei limiti delle facoltà di vigilanza, può impartirgli istruzioni.

[5] I rapporti di lavoro e la previdenza professionale di tutti i collaboratori dell'organo di vigilanza si conformano al diritto cantonale sul personale rispettivamente al diritto cantonale sulla Cassa pensioni, per quanto la presente legge non preveda nulla di diverso.

[6] Il Governo classifica gli impieghi dell'incaricato della protezione dei dati e del suo supplente in classi di funzione secondo il diritto cantonale sul personale.

Art. 32 Nomina

[1] Il Governo nomina uno specialista in questioni concernenti la protezione dei dati quale incaricato della protezione dei dati nonché un supplente per un mandato di quattro anni. La riconferma è ammessa.

[2] Il Governo può destituire l'incaricato della protezione dei dati e il suo supplente prima della scadenza del mandato se questi:

a) intenzionalmente o per negligenza grave, ha violato gravemente i suoi doveri d'ufficio; o
b) ha durevolmente perso la capacità di esercitare il suo ufficio.

Art. 33 Incompatibilità

[1] L'incaricato della protezione dei dati e il supplente non possono ricoprire un'altra carica pubblica, esercitare una funzione direttiva in seno a un partito politico o svolgere un'altra attività lavorativa. Il Governo può autorizzare eccezioni sempreché non siano pregiudicati l'adempimento della funzione nonché l'indipendenza e la reputazione.

[2] Se l'incaricato della protezione dei dati e il supplente svolgono la loro attività a tempo parziale, un'altra attività lucrativa deve essere autorizzata dal Governo. L'autorizzazione può essere negata se tale attività lucrativa pregiudica l'adempimento della funzione nonché l'indipendenza e la reputazione.

Art. 34 Preventivo

[1] L'incaricato della protezione dei dati allestisce un proprio preventivo.

[2] Nel messaggio sul preventivo il Governo comunica se la proposta è stata ripresa senza modifiche. Le divergenze devono essere motivate.

[3] Nel quadro del preventivo l'incaricato della protezione dei dati è competente per l'assunzione di impiegati nonché per la disdetta e la riconfigurazione dei rispettivi rapporti di lavoro.

Art. 35 Compiti

[1] L'organo di vigilanza:

a) vigila sull'applicazione delle disposizioni sulla protezione dei dati;

b) fornisce consulenza alle persone interessate in merito ai loro diritti;
c) funge da mediatore tra le persone interessate e gli organi pubblici;
d) fornisce consulenza alle autorità in questioni concernenti la protezione dei dati e vigila sulla sicurezza dei dati;
e) si pronuncia in merito ad atti legislativi e a progetti d'informatica, per quanto essi siano rilevanti per la protezione dei dati;
f) si occupa di notifiche inoltrate da persone interessate concernenti la violazione di disposizioni della presente legge e informa queste persone entro al massimo tre mesi in merito al risultato o allo stato degli accertamenti;
g) sensibilizza gli organi pubblici in merito ai loro obblighi previsti dal diritto in materia di protezione dei dati e il pubblico in merito alle esigenze della protezione dei dati;
h) segue gli sviluppi determinanti per la protezione di dati personali;
i) ai fini dell'adempimento dei suoi compiti, collabora con organi degli altri Cantoni, della Confederazione e dell'estero che adempiono gli stessi compiti.

Art. 36 Competenze
1. Controllo e raccomandazione

[1] L'organo di vigilanza si attiva d'ufficio o a seguito di notifiche da parte delle persone interessate. L'organo pubblico competente deve essere messo a conoscenza della notifica e deve essere invitato a esprimere un parere.

[2] Indipendentemente da eventuali disposizioni relative all'obbligo di serbare il segreto, l'organo di vigilanza può raccogliere tutte le informazioni relative al trattamento di dati necessarie per l'adempimento del mandato di controllo, prendere visione di tutta la documentazione, svolgere sopralluoghi e farsi spiegare lo svolgimento di trattamenti di dati.

[3] L'organo di vigilanza può formulare raccomandazioni per il trattamento di dati personali. L'organo pubblico al quale è destinata la raccomandazione deve dichiarare all'organo di vigilanza se intende dare seguito alla raccomandazione.

[4] Gli organi pubblici e il responsabile del trattamento sono tenuti a sostenere l'organo di vigilanza nell'adempimento dei suoi compiti. Essi partecipano in particolare all'accertamento della fattispecie.

Art. 37 2. Decisione

[1] Se un organo pubblico dichiara di non dare seguito alla raccomandazione dell'organo di vigilanza o non vi dà effettivamente seguito, l'organo di vigilanza può emanare la raccomandazione o parti di essa sotto forma di decisione.

[2] L'organo di vigilanza può emanare una decisione direttamente quando è prevedibile che l'organo pubblico rifiuterà una raccomandazione o non vi darà seguito.

[3] Contro decisioni ai sensi dell'articolo 37 capoverso 1 e capoverso 2 l'organo pubblico può interporre ricorso al Tribunale d'appello. Fa stato la legge sulla giustizia amministrativa[7)].

[4] Contro decisioni concernenti il Tribunale d'appello quest'ultimo può interporre ricorso al Tribunale della magistratura.

Art. 38 Rapporto

[1] L'organo di vigilanza riferisce ogni anno al Governo in merito all'entità e ai punti centrali della propria attività nonché a importanti constatazioni e valutazioni.

[2] L'organo di vigilanza consente all'organo pubblico interessato da raccomandazioni e decisioni di prendere posizione per iscritto. Le prese di posizione vengono allegate al rapporto.

[3] Il rapporto viene pubblicato.

Art. 39 Discrezione

[1] Per quanto attiene ai dati personali, l'organo di vigilanza è tenuto al medesimo obbligo di discrezione cui soggiace l'organo pubblico che tratta i dati. L'obbligo di discrezione si protrae oltre la cessazione della funzione.

[2] Fatte salve particolari disposizioni relative all'obbligo di serbare il segreto, l'organo di vigilanza può trasmettere informazioni delle quali è venuto a conoscenza durante l'esercizio della propria funzione soltanto nella misura in cui ciò sia necessario per l'adempimento dei suoi compiti.

6. Disposizioni penali e transitorie

Art. 40 Disposizioni penali

[1] Chi in veste di responsabile del trattamento senza autorizzazione esplicita da parte dell'organo pubblico intenzionalmente o per negligenza utilizza per sé stesso o per terzi oppure comunica a terzi dati personali è punito con la multa.

[2] Chi, contrariamente all'obbligo di cui all'articolo 13, intenzionalmente o per negligenza tratta per scopi diversi o trasmette a terzi dati personali che ha ricevuto da un organo pubblico per il trattamento per scopi impersonali è punito con la multa.

Art. 41 Disposizioni transitorie

[1] I trattamenti di dati che secondo il diritto anteriore si fondano su una base legale sufficiente possono essere proseguiti per due anni in virtù delle basi legali esistenti.

[2] La comprova del rispetto delle disposizioni in materia di protezione dei dati deve essere fornita entro due anni dall'entrata in vigore della presente legge.

7) CSC 370.100

[3] L'articolo 19 e l'articolo 20 non sono applicabili ai trattamenti di dati avviati prima dell'entrata in vigore della presente legge, se lo scopo del trattamento o l'attività di trattamento non ha subito cambiamenti sostanziali.

II.

1.
L'atto normativo "Legge sulla cittadinanza del Cantone dei Grigioni (LCCit)" CSC 130.100 (stato 1 gennaio 2025) è modificato come segue:

Art. 24 cpv. 1 (modificato)

[1] Per adempiere i compiti conformemente alla presente legge, le competenti autorità cantonali e comunali~~,~~ nonché gli uffici da ~~essi~~**esse** incaricati~~,~~ possono trattare dati, compresi profili ~~di~~**della** personalità e dati personali degni di particolare protezione, concernenti:

Elenco invariato.

2.
L'atto normativo "Legge sui registri degli abitanti e su altri registri delle persone e degli oggetti (legge sui registri degli abitanti, LRAb)" CSC 171.200 (stato 1 gennaio 2018) è modificato come segue:

Art. 32 cpv. 3 (modificato)

[3] È fatto salvo il diritto **all'opposizione alla comunicazione** di ~~bloccare la trasmissione di~~ **dati personali conformemente alla legge cantonale sulla protezione dei** dati[8)].

3.
L'atto normativo "Legge d'applicazione del Codice di diritto processuale civile svizzero (LACPC)" CSC 320.100 (stato 1 gennaio 2025) è modificato come segue:

Art. 14 cpv. 5 (nuovo)

[5] Secondo il diritto cantonale, le decisioni relative alla presa in visione degli atti in procedimenti dinanzi al Tribunale d'appello e al Tribunale della magistratura sono definitive.

4.
L'atto normativo "Legge d'applicazione del Codice di diritto processuale penale svizzero (LACPP)" CSC 350.100 (stato 1 gennaio 2025) è modificato come segue:

8) CSC 171.100

Art. 36 cpv. 5 (nuovo)

[5] Secondo il diritto cantonale, le decisioni relative alla presa in visione degli atti in procedimenti dinanzi al Tribunale d'appello e al Tribunale della magistratura sono definitive.

5.

L'atto normativo "Legge sulla vigilanza finanziaria (LVF)" CSC 710.300 (stato 1 gennaio 2025) è modificato come segue:

Art. 20 cpv. 1 (modificato), **cpv. 2 (modificato)**

[1] Il Controllo delle finanze ha il diritto di consultare i dati necessari all'adempimento della vigilanza finanziaria, inclusi i dati di persone delle ~~collezioni~~**raccolte** di dati dei Dipartimenti e dei servizi, nonché dei tribunali e delle autorità di conciliazione. Per quanto i dati siano adatti e necessari all'adempimento del compito, il diritto d'accesso si estende anche ai dati di persone degni di particolare protezione.

[2] Il Controllo delle finanze è autorizzato a conservare o salvare i dati di persone di cui è venuto a conoscenza in questo modo soltanto fino alla conclusione della procedura di revisione. Gli accessi alle diverse ~~collezioni~~**raccolte** di dati e gli scopi così perseguiti devono essere documentati.

III.

L'atto normativo "Legge cantonale sulla protezione dei dati (LCPD)" CSC 171.100 (stato 1 gennaio 2025) è abrogato.

IV.

La presente legge è soggetta a referendum facoltativo.

Il Governo stabilisce la data dell'entrata in vigore della presente legge.

Geltendes Recht

Kantonales Datenschutzgesetz (KDSG)

Vom 10. Juni 2001 (Stand 1. Januar 2025)

Vom Volke angenommen am 10. Juni 2001[1)]

Art. 1 Geltungsbereich

[1] Dieses Gesetz dient dem Schutz von Personen vor widerrechtlichem Bearbeiten von Personendaten durch Behörden.

[2] Als Behörden im Sinne dieses Gesetzes gelten:

a) * Behörden und Amtsstellen des Kantons, der Regionen, Gemeinden und Gemeindeverbindungen;

b) * öffentlich-rechtliche Anstalten, Stiftungen und Körperschaften des Kantons, der Regionen und Gemeinden;

c) Private, soweit ihnen öffentliche Aufgaben übertragen sind.

[3] … *

[4] Die Ausschlussgründe des Bundesgesetzes über den Datenschutz[2)] gelten sinngemäss.

[5] Zudem ist das Gesetz nicht anwendbar für:

a) Behörden, die am wirtschaftlichen Wettbewerb teilnehmen und dabei nicht hoheitlich handeln;

b) Personendaten, die in einem öffentlichen Archiv archiviert sind.

Art. 2 Bearbeiten von Personendaten
1. Grundsätze

[1] Das Bearbeiten von Personendaten hat die Grundsätze der Rechtmässigkeit, der Verhältnismässigkeit, der Zweckmässigkeit, der Zweckgebundenheit, der Richtigkeit und der Datensicherheit zu beachten.

[2] Die Vorschriften des Bundesgesetzes[3)] für das Bearbeiten von Personendaten durch Bundesorgane finden sinngemäss Anwendung.

[3] Soweit das kantonale Datenschutzgesetz und die Ausführungsbestimmungen keine abweichenden oder ergänzenden Bestimmungen enthalten, gelten die Definitionen des Bundesgesetzes sinngemäss.

---

1) B vom 5. September 2000, 493; GRP 2000/2001, 530
2) SR 235.1
3) SR 235.1

* Änderungstabellen am Schluss des Erlasses

Art. 3 2. Bekanntgabe in besonderen Fällen

[1] Entstehen Anstände zwischen zwei Behörden über die Bekanntgabe von Personendaten, so entscheidet die gemeinsame übergeordnete Instanz.

[2] Wer Personendaten im Auftrag einer Behörde bearbeitet, bedarf zur Bekanntgabe von Personendaten an Dritte der ausdrücklichen Zustimmung des Auftraggebers.

Art. 3a * Besondere Form der Bearbeitung von Personendaten
1. Bildüberwachung des öffentlichen und öffentlich zugänglichen Raums

[1] Der öffentliche und öffentlich zugängliche Raum kann mit Bildübermittlungs- und Bildaufzeichnungsgeräten zur Personenidentifikation überwacht werden, sofern:

a) die öffentliche Sicherheit und Ordnung konkret gefährdet ist;
b) dies zum Schutz von öffentlichen Zwecken dienenden Gebäuden oder deren Benutzerinnen und Benutzern erforderlich ist.

[2] Bei der Bearbeitung von Personendaten sind die allgemeinen Grundsätze zu respektieren. Zusätzlich ist sicherzustellen, dass:

a) auf die Überwachungsgeräte in geeigneter Weise hingewiesen wird;
b) Bereiche, die der Ausübung von Tätigkeiten dienen, die unter das Berufsgeheimnis im Sinne von Artikel 171 der Strafprozessordnung[4)] fallen, von der Überwachung ausgenommen sind;
c) aufgezeichnete Personendaten innert 90 Tagen gelöscht werden, soweit sie nicht in einem Strafverfahren oder zur Gefahrenabwehr benötigt werden.

Art. 3b * 2. Anordnung der Bildüberwachung des öffentlichen und öffentlich zugänglichen Raums

[1] Die Bildüberwachung des öffentlichen und öffentlich zugänglichen Raums kann von einer Behörde angeordnet werden, der das Gebrauchsrecht oder die Hoheit über den zu überwachenden Raum zusteht.

[2] Die Behörde erlässt eine Allgemeinverfügung, in welcher der Zweck, die Art und die Dauer der Überwachung, die zu überwachenden Örtlichkeiten, die Standorte der Überwachungsgeräte, die Massnahmen zum Hinweis auf die Überwachung, die Zugriffsrechte sowie die zur Datensicherheit getroffenen Massnahmen bestimmt werden. Die Allgemeinverfügung gilt für maximal fünf Jahre.

[3] Die Behörde hat die zu erlassende Allgemeinverfügung vorgängig zu veröffentlichen. Sie hört Personen an, indem sie ihnen eine angemessene Frist zur Stellungnahme einräumt.

[4] Vorgängiger Rechtsschutz ist nicht zu gewähren für anlassbezogene Bildüberwachungen mit einer Dauer von höchstens drei Monaten und Bildüberwachungen zum Schutz öffentlichen Zwecken dienenden Gebäuden, die ereignisbezogen in Betrieb genommen werden und keine Personendaten aufzeichnen.

---

4) SR 312.0

Art. 4 Register

[1] Die Behörden melden der Aufsichtsstelle ihre Datensammlungen.

[2] Soweit das kantonale Datenschutzgesetz und die Ausführungsbestimmungen keine abweichenden oder ergänzenden Bestimmungen enthalten, finden die Bestimmungen über die Registrierung von Datensammlungen des Bundesgesetzes[5)] sinngemäss Anwendung.

Art. 5 Rechte der betroffenen Personen

[1] Jede betroffene Person hat das Recht auf:

a) Auskunft der über sie in einer Datensammlung bearbeiteten Daten;
b) Einsicht in das Register der Datensammlungen;
c) Berichtigung unrichtiger Personendaten;
d) Vernichtung nicht notwendiger oder widerrechtlich bearbeiteter Personendaten;
e) Sperrung schutzwürdiger Personendaten.

[2] Bestreitet die Behörde die Unrichtigkeit der Personendaten, so hat sie deren Richtigkeit zu beweisen. *

[3] Die durch das Bundesgesetz[6)] den betroffenen Personen eingeräumten Rechte gelten sinngemäss. *

Art. 6 Rechtsschutz

[1] Entscheide von Behörden und Amtsstellen der Verwaltung und von un-selbständigen Anstalten des kantonalen öffentlichen Rechts können beim vorgesetzten Departement angefochten werden.

[2] Gegen Entscheide Privater, die öffentliche Aufgaben erfüllen, steht die Beschwerde an die auftraggebende Instanz offen.

[3] Entscheide der Departemente, der Gemeinde- und Regionalbehörden, der Gemeindeverbindungen sowie der selbständigen öffentlich-rechtlichen Anstalten und Körperschaften können beim Obergericht mit Beschwerde angefochten werden. *

[4] Das Beschwerderecht steht auch der Aufsichtsstelle zu. *

Art. 7 Aufsichtsstelle
1. Wahl

[1] Die Regierung wählt als Aufsichtsstelle einen Beauftragten oder eine Beauftragte für den Datenschutz.

[2] Die Aufsichtsstelle erfüllt ihre Aufgaben fachlich selbständig und unabhängig. Sie ist weisungsungebunden.

---

5) SR 235.1
6) SR 235.1

Art. 8 2. Aufgaben

[1] Die Aufsichtsstelle:

a) überwacht die Anwendung der Vorschriften über den Datenschutz;
b) führt ein Register der Datensammlungen und der allfälligen Verknüpfungen;
c) berät die betroffenen Personen über ihre Rechte;
d) vermittelt zwischen den betroffenen Personen und den Behörden;
e) berät die Behörden in Fragen des Datenschutzes und überwacht die Datensicherung;
f) nimmt Stellung zu Erlassen und Informatikprojekten, soweit sie für den Datenschutz erheblich sind;
g) erstattet jährlich Bericht über ihre Tätigkeit. Der Bericht wird veröffentlicht.

Art. 9 3. Arbeitsweise

[1] Die Behörden sind verpflichtet, die Aufsichtsstelle bei der Erfüllung ihrer Aufgaben zu unterstützen.

[2] Die Aufsichtsstelle kann ungeachtet allfälliger Geheimhaltungsvorschriften bei Behörden schriftlich und mündlich Auskünfte über das Bearbeiten von Personendaten einholen, Einsicht in Datensammlungen und ihre Unterlagen nehmen und sich das Bearbeiten von Personendaten vorführen lassen.

[3] Ergibt die Abklärung, dass Datenschutzvorschriften verletzt werden, fordert die Aufsichtsstelle die verantwortliche oder deren vorgesetzte Behörde auf, die erforderlichen Massnahmen zu ergreifen.

[4] Wird die Aufforderung nicht befolgt oder abgelehnt, unterbreitet sie die Angelegenheit der Regierung zum Entscheid.

Art. 10 4. Verschwiegenheitspflicht

[1] Die Aufsichtsstelle ist hinsichtlich der Personendaten zur gleichen Verschwiegenheit verpflichtet wie die Behörde, welche die Daten bearbeitet.

[2] Die Aufsichtsstelle darf unter Vorbehalt besonderer Geheimhaltungsvorschriften Kenntnisse, die sie bei ihrer Tätigkeit erlangt, nur soweit bekannt geben, als es zur Erfüllung ihrer Aufgaben notwendig ist.

Art. 10a * Strafbestimmungen

[1] Wer als angestellte oder beauftragte Person einer Behörde oder als angestellte Person einer beauftragten Person vorsätzlich gegen die Bestimmungen des kantonalen Datenschutzrechtes verstösst, wird auf Antrag mit Busse bestraft.

[2] Die Verletzung der datenschutzrechtlichen Vorschriften ist auch nach Beendigung des Vertragsverhältnisses strafbar.

Art. 11 Ausführungsbestimmungen

[1] Die Regierung erlässt die erforderlichen Ausführungsbestimmungen.

Art. 12 Übergangsbestimmungen

[1] Inhaber von Datensammlungen überprüfen und passen diese innerhalb von drei Jahren seit In-Kraft-Treten des Datenschutzgesetzes an.

[2] Die Regierung kann die Frist aus wichtigen Gründen erstrecken.

[3] Der Betrieb von Überwachungsgeräten, die unter Artikel 3a fallen und zum Zeitpunkt des Inkrafttretens dieses Gesetzes im Einsatz sind, darf fortgesetzt werden, sofern innert zwölf Monaten die für die Bildüberwachung vorgesehenen Voraussetzungen erfüllt werden. *****

Art. 13 In-Kraft-Treten

[1] Die Regierung bestimmt den Zeitpunkt des In-Kraft-Tretens[7)] dieses Gesetzes.

[7)] Mit RB vom 19. Februar 2002 auf den 1. Mai 2002 in Kraft gesetzt.

Änderungstabelle - Nach Beschluss

Beschluss	Inkrafttreten	Element	Änderung	AGS Fundstelle
10.06.2001	01.05.2002	Erlass	Erstfassung	-
31.08.2006	01.10.2008	Art. 5 Abs. 2	geändert	-
31.08.2006	01.10.2008	Art. 5 Abs. 3	eingefügt	-
31.08.2006	01.10.2008	Art. 6 Abs. 3	geändert	-
31.08.2006	01.10.2008	Art. 6 Abs. 4	eingefügt	-
31.08.2006	01.10.2008	Art. 10a	eingefügt	-
13.01.2015	01.01.2016	Art. 1 Abs. 2, a)	geändert	2015-005
13.01.2015	01.01.2016	Art. 1 Abs. 2, b)	geändert	2015-005
13.01.2015	01.01.2016	Art. 1 Abs. 3	aufgehoben	2015-005
13.01.2015	01.01.2016	Art. 6 Abs. 3	geändert	2015-005
02.02.2016	01.01.2017	Art. 1 Abs. 2, a)	geändert	2016-001
02.02.2016	01.01.2017	Art. 1 Abs. 2, b)	geändert	2016-001
02.02.2016	01.01.2017	Art. 6 Abs. 3	geändert	2016-001
31.08.2018	01.01.2019	Art. 3a	eingefügt	2018-023
31.08.2018	01.01.2019	Art. 3b	eingefügt	2018-023
31.08.2018	01.01.2019	Art. 12 Abs. 3	eingefügt	2018-023
14.06.2022	01.01.2025	Art. 6 Abs. 3	geändert	2023-008

Änderungstabelle - Nach Artikel

Element	Beschluss	Inkrafttreten	Änderung	AGS Fundstelle
Erlass	10.06.2001	01.05.2002	Erstfassung	-
Art. 1 Abs. 2, a)	13.01.2015	01.01.2016	geändert	2015-005
Art. 1 Abs. 2, a)	02.02.2016	01.01.2017	geändert	2016-001
Art. 1 Abs. 2, b)	13.01.2015	01.01.2016	geändert	2015-005
Art. 1 Abs. 2, b)	02.02.2016	01.01.2017	geändert	2016-001
Art. 1 Abs. 3	13.01.2015	01.01.2016	aufgehoben	2015-005
Art. 3a	31.08.2018	01.01.2019	eingefügt	2018-023
Art. 3b	31.08.2018	01.01.2019	eingefügt	2018-023
Art. 5 Abs. 2	31.08.2006	01.10.2008	geändert	-
Art. 5 Abs. 3	31.08.2006	01.10.2008	eingefügt	-
Art. 6 Abs. 3	31.08.2006	01.10.2008	geändert	-
Art. 6 Abs. 3	13.01.2015	01.01.2016	geändert	2015-005
Art. 6 Abs. 3	02.02.2016	01.01.2017	geändert	2016-001
Art. 6 Abs. 3	14.06.2022	01.01.2025	geändert	2023-008
Art. 6 Abs. 4	31.08.2006	01.10.2008	eingefügt	-
Art. 10a	31.08.2006	01.10.2008	eingefügt	-
Art. 12 Abs. 3	31.08.2018	01.01.2019	eingefügt	2018-023