Kanton Graubünden
Chantun Grischun
Cantone dei Grigioni

Kantonales Datenschutzgesetz (KDSG)

Vom 10. Februar 2025 (Stand 1. Januar 2026)

Der Grosse Rat des Kantons Graubünden[1)],

gestützt auf Art. 31 Abs. 1 der Kantonsverfassung[2)],
nach Einsicht in die Botschaft der Regierung vom 24. Oktober 2024[3)],

beschliesst:

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.

[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[4)] anwendbar. Die Aufsicht richtet sich nach dem vorliegenden Gesetz, ausser bei öffentlichen Organen, die ausschliesslich am wirtschaftlichen Wettbewerb teilnehmen und dabei privatrechtlich handeln.

1) GRP 2024/2025, 542
2) BR 110.100
3) Seite 495
4) SR 235.1

* Änderungstabellen am Schluss des Erlasses

[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.

[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[5)].

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.

[5)] BR 171.000

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[6)] fallen, von der Überwachung ausgenommen sind; und

[6)] SR 312.0

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.

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] Sofern das öffentliche Organ über keine eigene Regelung zur Erhebung einer Gebühr verfügt, gilt die Verordnung über die Kosten in Verwaltungsverfahren sinngemäss.

[5] Im Weiteren richtet sich das Verfahren nach dem Gesetz über die Verwaltungsrechtspflege[7)].

[7)] BR 370.100

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[8)] 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. 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;
c) der Grosse Rat und seine Ratsorgane.

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.

[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.

8) BR 171.000

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[9)].

[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.

9) 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.

Änderungstabelle - Nach Beschluss

Beschluss	Inkrafttreten	Element	Änderung	AGS Fundstelle
10.02.2025	01.01.2026	Erlass	Erstfassung	2025-049

Änderungstabelle - Nach Artikel

Element	Beschluss	Inkrafttreten	Änderung	AGS Fundstelle
Erlass	10.02.2025	01.01.2026	Erstfassung	2025-049