# Verordnung zum Kantonalen Datenschutzgesetz (Kantonale Datenschutzverordnung, VKDSG)

Vom 16. September 2025 (Stand 1. Januar 2026)

Gestützt auf Art. 45 Abs. 1 der Kantonsverfassung[1)] und Art. 6 Abs. 3 sowie Art. 23 Abs. 1 des Kantonalen Datenschutzgesetzes[2)]

von der Regierung erlassen am 16. September 2025

## 1. Allgemeine Bestimmungen

**Art. 1** Nachweis der Einhaltung der Datenschutzbestimmungen

[1] Das öffentliche Organ erbringt den Nachweis der Einhaltung der Datenschutzbestimmungen, indem mindestens folgende Punkte im Zusammenhang mit den Bearbeitungstätigkeiten dokumentiert werden:

a) die Prozesse der Datenbearbeitung;
b) die verantwortlichen Personen;
c) die rechtlichen Grundlagen für die Datenbearbeitung;
d) die Datenschutzrisiken und die getroffenen Massnahmen.

[2] Das öffentliche Organ kann den Nachweis insbesondere erbringen durch:

a) Geschäftsordnungen und andere allgemeine Festlegungen zu Geschäftsprozessen und zur betrieblichen Organisation;
b) Weisungen zu Datenbearbeitungen und zum Umgang mit Personendaten, einschliesslich der Löschung und der Archivierung;
c) Informationssicherheits- und Datenschutzkonzepte sowie Datenschutz-Folgenabschätzungen;
d) Konzepte für den Zugriff auf Informationen und Informatikmittel;
e) Berichte zum Umgang mit meldepflichtigen Verletzungen der Datensicherheit;
f) sonstige Unterlagen und Hilfsmittel über die sichere Datenbearbeitung.

1) BR 110.100
2) BR 171.100

* Änderungstabellen am Schluss des Erlasses

**Art. 2** Technische und organisatorische Massnahmen
1. Schutzziele

[1] Die öffentlichen Organe stellen mit angemessenen organisatorischen und technischen Massnahmen sicher, dass die Personendaten:

a) nur Berechtigten zugänglich sind (Vertraulichkeit);
b) verfügbar sind, wenn sie benötigt werden (Verfügbarkeit);
c) nicht unberechtigt oder unbeabsichtigt verändert werden (Integrität);
d) nachvollziehbar bearbeitet werden (Nachvollziehbarkeit).

**Art. 3** 2. Angemessenheit

[1] Die Angemessenheit der technischen und organisatorischen Massnahmen richtet sich insbesondere nach folgenden Kriterien:

a) dem Schutzbedarf der bearbeiteten Daten, der sich aus dem Zweck, der Art, dem Umfang und den Umständen der Datenbearbeitung ergibt;
b) der Einschätzung der möglichen Risiken für die betroffenen Personen;
c) dem Stand der Technik.

[2] Die Massnahmen sind periodisch auf ihre Zweck- und Verhältnismässigkeit zu überprüfen und gegebenenfalls anzupassen.

**Art. 4** 3. Massnahmen

[1] Zur Gewährleistung der Datensicherheit können insbesondere die folgenden technischen und organisatorischen Massnahmen ergriffen werden:

a) Zugangsbeschränkungen zu Einrichtungen: unbefugten Personen ist der Zugang zu Einrichtungen, in denen Sach- und Personendaten bearbeitet werden, zu verwehren;
b) Benutzerkontrollen: unbefugten Personen ist die Benutzung von Informatikmitteln, mit denen Sach- und Personendaten bearbeitet werden, zu verwehren;
c) Datenträgerkontrollen: unbefugten Personen ist das Lesen, Kopieren, Verändern oder Entfernen von Datenträgern zu verunmöglichen;
d) Zugriffsbeschränkungen: der Zugriff ist auf diejenigen Sach- und Personendaten zu beschränken, welche die berechtigten Personen für die Erfüllung ihrer Aufgabe benötigen;
e) Bearbeitungsbeschränkungen: das unbefugte Bearbeiten von Sach- und Personendaten wird verhindert;
f) Eingabekontrollen: bei der Verwendung von Informatikmitteln muss nachträglich überprüft werden können, welche Sach- und Personendaten zu welcher Zeit und von welcher Person bearbeitet wurden;
g) Empfängeridentifikation: die Empfängerinnen oder Empfänger, denen Sach- und Personendaten bekannt gegeben werden, müssen identifiziert werden können;
h) Kontinuitätssicherung: Vorkehrungen werden getroffen, damit bei einem Ausfall von Informatikmitteln wichtige Funktionen möglichst rasch weiter erfüllt werden können;

i) Generationenfolgesicherung: Vorkehrungen werden getroffen, damit Sach- und Personendaten infolge technologischen Wandels beim Einsatz von Informatikmitteln dauerhaft erhalten werden können.

**Art. 5** 4. Protokollierung

[1] Die öffentlichen Organe protokollieren bei der automatisierten Bearbeitung von Personendaten zumindest das Speichern, Verändern, Lesen, Bekanntgeben, Löschen und Vernichten der Daten, wenn die präventiven Massnahmen den Datenschutz nicht gewährleisten und ein solches System auf dem Markt verfügbar ist.

[2] Die Protokollierung muss Aufschluss geben über die Identität der Person, welche die Bearbeitung vorgenommen hat, die Art, das Datum und die Uhrzeit der Bearbeitung sowie gegebenenfalls die Identität der Empfängerin oder des Empfängers der Daten.

## 2. Bearbeitung von Personendaten

**Art. 6** Pilotversuche
1. Unentbehrlichkeit

[1] Die Durchführung einer Testphase ist für die praktische Umsetzung einer Datenbearbeitung unentbehrlich, wenn eine der folgenden Bedingungen erfüllt ist:

a) Die Erfüllung einer Aufgabe erfordert technische Neuerungen, deren Auswirkungen zunächst evaluiert werden müssen;
b) Die Erfüllung einer Aufgabe erfordert bedeutende organisatorische oder technische Massnahmen, deren Wirksamkeit zunächst geprüft werden muss, insbesondere bei der Zusammenarbeit mit Organen anderer Gemeinwesen und Organisationen, welche von Gemeinwesen geschaffen werden;
c) Die Erfüllung einer Aufgabe erfordert, dass die Personendaten im Abrufverfahren zugänglich sind.

**Art. 7** 2. Verfahren

[1] Das öffentliche Organ, das den Pilotversuch durchführt, holt die Stellungnahme der Aufsichtsstelle ein.

[2] Es stellt der Aufsichtsstelle alle zur Beurteilung der Bewilligungsfähigkeit des Pilotversuchs notwendigen Unterlagen zur Verfügung, insbesondere:

a) eine allgemeine Beschreibung des Pilotversuchs;
b) einen Bericht, der nachweist, dass die Erfüllung der gesetzlich vorgesehenen Aufgaben eine Bearbeitung erfordert und dass eine Testphase vor dem Inkrafttreten des Gesetzes unentbehrlich ist;
c) eine Beschreibung der Sicherheits- und Datenschutzmassnahmen;
d) den Entwurf einer Verordnung, welche die Einzelheiten der Bearbeitung regelt, oder das Konzept einer Verordnung.

[3] Die Stellungnahme ist der Regierung vorzulegen, bevor sie über ein Bewilligungsgesuch entscheidet.

**Art. 8** Auftragsbearbeitung
1. Mindestinhalt von Verträgen

[1] Soweit die Bearbeitung durch eine Auftragsbearbeiterin oder einen Auftragsbearbeiter nicht gesetzlich vorgesehen ist, sind mindestens folgende Punkte vertraglich zu regeln:

a) Gegenstand und Umfang der übertragenen Aufgaben;
b) Wahrung des Amtsgeheimnisses sowie besonderer Geheimhaltungspflichten;
c) Verantwortlichkeiten;
d) technische und organisatorische Massnahmen zur Wahrung des Datenschutzes und der Datensicherheit;
e) Ort der Datenbearbeitung;
f) Kontrolle der Auftragserfüllung;
g) Beizug von Dritten;
h) bei Pflichtverletzung vorgesehene Sanktionen;
i) Vertragsdauer und Voraussetzungen der Vertragsauflösung sowie deren Folgen, insbesondere die Rückführung und Löschung der Daten;
j) anwendbares Recht und Gerichtsstand.

**Art. 9** 2. Beizug von Dritten

[1] Die vorgängige Genehmigung des öffentlichen Organs, die der Auftragsbearbeiterin oder dem Auftragsbearbeiter erlaubt, zur Datenbearbeitung Dritte beizuziehen, kann spezifischer oder allgemeiner Art sein.

[2] Bei einer allgemeinen Genehmigung informiert die Auftragsbearbeiterin oder der Auftragsbearbeiter das verantwortliche öffentliche Organ über jede beabsichtigte Änderung betreffend den Beizug oder die Ersetzung anderer Dritter. Das verantwortliche öffentliche Organ kann diese Änderung ablehnen.

**Art. 10** Grenzüberschreitende Bekanntgabe von Personendaten

[1] Das öffentliche Organ kann für die Beurteilung, ob die Gesetzgebung eines Empfängerstaats einen angemessenen Schutz gewährleistet, auf die vom Bund getroffene Beurteilung der Angemessenheit des Datenschutzes eines Staates, eines Gebiets, eines spezifischen Sektors in einem Staat oder eines internationalen Organs gemäss Artikel 8 der Verordnung über den Datenschutz[3)] abstellen.

[3)] SR 235.11

[2] Wurde die Aufsichtsstelle über die Garantien gemäss Artikel 12 Absatz 3 des Kantonalen Datenschutzgesetzes[4)] informiert, so gilt die Informationspflicht für alle weiteren Bekanntgaben als erfüllt, die unter denselben Garantien erfolgen, soweit die Kategorien der Empfängerinnen und Empfänger, der Zweck der Bearbeitung und die Datenkategorien im Wesentlichen unverändert bleiben.

[3] Die Informationspflicht gilt ebenfalls als erfüllt, wenn Daten gestützt auf Modellverträge oder Standardvertragsklauseln übermittelt werden, die vom eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten erstellt oder anerkannt wurden, und wenn die Aufsichtsstelle vom verantwortlichen öffentlichen Organ in allgemeiner Form über die Verwendung dieser Modellverträge oder Standardvertragsklauseln informiert wurde.

**Art. 11** Veröffentlichung in elektronischer Form im Rahmen der behördlichen Informationstätigkeit

[1] Werden Personendaten mittels automatisierter Informations- und Kommunikationsdienste allgemein zugänglich gemacht, gilt dies nicht als Übermittlung ins Ausland.

**Art. 12** Datenbearbeitung für nicht personenbezogene Zwecke

[1] Sollen Personendaten für einen nicht personenbezogenen Zweck bekannt gegeben werden, so hat die Empfängerin oder der Empfänger mindestens folgende Angaben zu liefern:

a) Bezeichnung der Empfängerin oder des Empfängers;
b) Kurzbeschreibung des Vorhabens;
c) Umschreibung der benötigten Personendaten;
d) Ablauf und Art der Datenbearbeitung;
e) Angaben über die zum Schutz der Personendaten vorzukehrenden Massnahmen.

[2] Das öffentliche Organ holt bei der Empfängerin oder dem Empfänger eine Verpflichtungserklärung ein, dass die Vorgaben von Artikel 13 Absatz 1 Litera a des Kantonalen Datenschutzgesetzes[5)] erfüllt werden. Es kann die Bekanntgabe von Personendaten mit weiteren Auflagen zum Schutz der Personendaten versehen.

4) BR 171.100
5) BR 171.100

## 3. Pflichten des verantwortlichen öffentlichen Organs

### 3.1. ALLGEMEINE VORGABEN

**Art. 13** Durchführung der Vorabkonsultation

[1] Der Aufsichtsstelle sind mindestens die Dokumente vorzulegen, die im Rahmen der Datenschutz-Folgenabschätzung erarbeitet wurden. Die Aufsichtsstelle kann weitere Dokumente anfordern, sofern diese zur Beurteilung des Risikos für die Grundrechte notwendig sind.

[2] Auf die Vorabkonsultation kann verzichtet werden, soweit die Mitwirkung der Aufsichtsstelle in der Projektorganisation des Vorhabens auf andere Weise sichergestellt wird.

[3] Die Vorabkonsultation ist abgeschlossen, wenn die Aufsichtsstelle die Anwendung für unbedenklich erklärt oder eine Empfehlung gemäss Artikel 36 des Kantonalen Datenschutzgesetzes[6)] abgegeben hat.

**Art. 14** Aufbewahrung der Datenschutz-Folgenabschätzung und der Vorabkonsultation

[1] Das öffentliche Organ hat die Datenschutz-Folgenabschätzung und die Ergebnisse der Vorabkonsultation mindestens zwei Jahre über die Beendigung der Bearbeitungstätigkeit hinaus aufzubewahren.

**Art. 15** Meldung von Verletzungen der Datensicherheit
1. Modalitäten der Meldepflicht und Dokumentation

[1] Die Aufsichtsstelle stellt ein Formular zur Meldung von Verletzungen der Datensicherheit bereit.

[2] Ist es dem öffentlichen Organ nicht möglich, alle Angaben gleichzeitig zu melden, so liefert es die fehlenden Angaben so rasch als möglich nach.

[3] Das öffentliche Organ hat die Verletzung der Datensicherheit zu dokumentieren. Die Dokumentation muss die mit den Vorfällen zusammenhängenden Tatsachen, deren Auswirkungen und die ergriffenen Massnahmen enthalten. Sie ist mindestens zwei Jahre über die Meldung hinaus aufzubewahren.

**Art. 16** 2. Information der betroffenen Person

[1] Ist das öffentliche Organ verpflichtet, die betroffene Person über die Verletzung der Datensicherheit zu informieren, so wird ihr in einfacher und verständlicher Sprache mindestens mitgeteilt:

a) die Art der Verletzung;

[6)] BR 171.100

b) die Folgen, einschliesslich der allfälligen Risiken, für die betroffenen Personen;
c) welche Massnahmen getroffen wurden oder vorgesehen sind, um den Mangel zu beheben und die Folgen, einschliesslich der allfälligen Risiken, zu mindern;
d) den Namen und die Kontaktdaten einer Ansprechperson.

[2] Erscheint eine individuelle Information über die Verletzung der Datensicherheit aufgrund der Vielzahl betroffener Personen als unverhältnismässig, kann die Information in geeigneter Form veröffentlicht werden.

## 3.2. BESONDERE VORGABEN

**Art. 17** Betroffene öffentliche Organe

[1] Die Pflichten dieses Abschnitts gelten für die in Artikel 22 und Artikel 23 des Kantonalen Datenschutzgesetzes[7)] bezeichneten öffentlichen Organe sowie für:

a) das Amt für Justizvollzug;
b) die Kantonspolizei;
c) die Staatsanwaltschaft;
d) die Stadtpolizei Chur.

[2] Andere öffentliche Organe können die besonderen Vorgaben gemäss Artikel 22 und Artikel 23 des Kantonalen Datenschutzgesetzes freiwillig umsetzen. Sofern sie dies tun, haben sie die Bestimmungen dieses Abschnitts zu beachten.

**Art. 18** Verzeichnis der Bearbeitungstätigkeiten

[1] Die betroffenen öffentlichen Organe aktualisieren das Verzeichnis der Bearbeitungstätigkeiten regelmässig.

[2] Änderungen sind der Aufsichtsstelle zu melden.

[3] Von der Meldepflicht ausgenommen sind öffentliche Organe, die das Verzeichnis der Bearbeitungstätigkeiten freiwillig führen.

**Art. 19** Datenschutzberaterin oder Datenschutzberater

[1] Die betroffenen öffentlichen Organe bezeichnen mindestens eine Person als Datenschutzberaterin oder Datenschutzberater, welche über die erforderlichen Fachkenntnisse verfügt.

[2] Mehrere betroffene öffentliche Organe können gemeinsam eine Datenschutzberaterin oder einen Datenschutzberater ernennen.

[3] Der Name und die Kontaktdaten der Datenschutzberaterin oder des Datenschutzberaters sind der Aufsichtsstelle bekannt zu geben und zu veröffentlichen.

7) BR 171.100

[4] Die Aufsichtsstelle schult die Datenschutzberaterinnen und Datenschutzberater periodisch.

## 4. Rechte der betroffenen Personen

**Art. 20** Gesuchsmodalitäten

[1] Die betroffene Person kann ihre Rechte beim verantwortlichen öffentlichen Organ schriftlich oder mündlich geltend machen.

[2] Das verantwortliche öffentliche Organ muss angemessene Massnahmen treffen, um die betroffene Person zu identifizieren. Diese ist zur Mitwirkung verpflichtet.

**Art. 21** Erteilung des Auskunftsrechts

[1] Das verantwortliche öffentliche Organ macht die Personendaten soweit möglich in der zum amtlichen Gebrauch erstellten Form zugänglich. Die Auskunft kann auf elektronischem Weg erteilt werden, wenn die Übermittlung vor dem Zugriff unberechtigter Dritter ausreichend geschützt ist.

[2] Im Einvernehmen mit dem verantwortlichen öffentlichen Organ kann die betroffene Person ihre Daten an Ort und Stelle einsehen. Die Auskunft kann mündlich erteilt werden, wenn die betroffene Person einverstanden ist.

**Art. 22** Widerspruch

[1] Das verantwortliche öffentliche Organ, welches den Widerspruch erhalten hat, bestätigt die Vornahme des Widerspruchs in geeigneter Form. Es sorgt dafür, dass andere öffentliche Organe, welche von ihm die betroffenen Personendaten erhalten, über den Widerspruch informiert werden.

[2] Verlangt die betroffene Person die Aufhebung des Widerspruchs, teilt sie dies dem verantwortlichen öffentlichen Organ schriftlich mit.

**Art. 23** Ausnahmen von der Kostenlosigkeit

[1] Ein unverhältnismässiger Aufwand liegt insbesondere vor, wenn:

a) die betroffene Person wiederholt in derselben Angelegenheit ein Gesuch stellt;
b) die betroffene Person trotz Aufforderung des verantwortlichen Organs ihrer Mitwirkungspflicht nicht nachkommt; oder
c) mit der Gesuchsbearbeitung ein hoher Sach- oder Zeitaufwand verbunden ist.

[2] Das verantwortliche öffentliche Organ muss der betroffenen Person die Höhe der Kosten vor der Auskunftserteilung mitteilen. Bestätigt die betroffene Person das Gesuch nicht innerhalb von zehn Tagen, so gilt es als zurückgezogen.

## 5. Schlussbestimmungen

**Art. 24** Übergangsbestimmungen

[1] Bestehende Informatiksysteme, die eine Protokollierung gemäss Artikel 5 nicht vorsehen, können bis zum Ende ihres Lebenszyklus weiterbetrieben werden. Artikel 5 ist zu beachten, wenn sie durch ein neues System ersetzt werden.

[2] Bestehende Vereinbarungen über die Auftragsbearbeitung bleiben bis zu ihrem Ablauf gültig. Sie haben Artikel 8 und Artikel 9 zu beachten, wenn sie verlängert oder angepasst werden.

## Änderungstabelle - Nach Beschluss

| Beschluss | Inkrafttreten | Element | Änderung | AGS Fundstelle |
|---|---|---|---|---|
| 16.09.2025 | 01.01.2026 | Erlass | Erstfassung | 2025-050 |

## Änderungstabelle - Nach Artikel

| Element | Beschluss | Inkrafttreten | Änderung | AGS Fundstelle |
|---|---|---|---|---|
| Erlass | 16.09.2025 | 01.01.2026 | Erstfassung | 2025-050 |