# Verordnung zum Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (VIDAG)

Vom 8. November 2022 (Stand 1. Januar 2023)

*Der Regierungsrat,*

gestützt auf Artikel 99 Absatz 1 Buchstabe b der Kantonsverfassung[1)],

*erlässt:*

## 1. Allgemeine Bestimmungen

### Art. 1 *Gegenstand*

[1] Diese Verordnung regelt in Ergänzung zu den gesetzlichen Bestimmungen:

*a.* den Zugang zu amtlichen Dokumenten;

*b.* die Bearbeitung von Personendaten durch öffentliche Organe;

*c.* die Archivierung amtlicher Dokumente.

### Art. 2 *Geltungsbereich*

[1] Unter Vorbehalt besonderer Bestimmungen findet diese Verordnung auf sämtliche in Artikel 4 Absatz 1 IDAG definierten öffentlichen Organe Anwendung.

## 2. Öffentlichkeitsprinzip

### Art. 3 *Virtuelles Dokument*

[1] Als ein durch einen einfachen elektronischen Vorgang aus aufgezeichneten Informationen erstelltes amtliches Dokument (Art. 3 Abs. 3 IDAG) gilt eine Auswertung, die:

*a.* sich entweder direkt mit Hilfe von oder indirekt durch einen Datenexport aus Informatikmitteln erzeugen lässt; und

*b.* keinen erheblichen Erstellungs- und Nachbearbeitungsaufwand erfordert.

### Art. 4 *Behandlung des Zugangsgesuchs*

[1] Das öffentliche Organ, an welches das Gesuch gerichtet ist, leitet dieses zur Behandlung weiter, wenn es amtliche Dokumente betrifft, die sich im Besitz eines anderen öffentlichen Organs befinden.

---

1) GS I A/1/1

**Art. 5** *Präzisierung des Zugangsgesuchs*

[1] Das öffentliche Organ kann von der gesuchstellenden Person eine Präzisierung verlangen, falls es ihm nicht ohne unverhältnismässigen Aufwand möglich ist, zu bestimmen, auf welche amtlichen Dokumente sich das Gesuch bezieht.
[2] Unterbleibt die Präzisierung innert der angesetzten Frist, wird das Zugangsgesuch gegenstandslos.

## 3. Datenschutz

### *3.1. Begriffe*

**Art. 6** *Besonders schützenswerte Personendaten*

[1] Als besonders schützenswerte Personendaten (Art. 5 Abs. 2 IDAG) gelten 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 und des Kindes- und Erwachsenenschutzes.

**Art. 7** *Stammdaten*

[1] Als Stammdaten (Art. 5 Abs. 3 IDAG) gelten:
*a.* Name;
*b.* Vorname;
*c.* Adresse;
*d.* Geburtstag;
*e.* Heimatort.

### *3.2. Datensicherheit*

**Art. 8** *Verantwortlichkeiten*

[1] Die für die Einhaltung des Datenschutzes verantwortlichen öffentlichen Organe (Art. 32 IDAG) sind auch für die Einhaltung der Datensicherheit verantwortlich.

[2] Ausgehend von den Schutzzielen beurteilen sie:
*a.* den Schutzbedarf;
*b.* die Risiken;
*c.* die zu ergreifenden technischen und organisatorischen Massnahmen und deren Angemessenheit.
[3] Die öffentlichen Organe sorgen dafür, dass die Informatikmittel, welche sie zur Erfüllung ihrer gesetzlichen Aufgaben einsetzen, angemessen vor Missbrauch und Störung geschützt werden.

**Art. 9** *Schutzziele*

[1] Die öffentlichen Organe sorgen dafür, dass Sach- und Personendaten ihrem Schutzbedarf entsprechend:
*a.* nur Berechtigten zugänglich sind (Vertraulichkeit);
*b.* bei Bedarf verfügbar sind (Verfügbarkeit);
*c.* nicht unberechtigt oder unbeabsichtigt verändert, vernichtet oder gelöscht werden (Integrität);
*d.* nachvollziehbar bearbeitet werden (Nachvollziehbarkeit).

**Art. 10** *Schutzbedarf*

[1] Der Schutzbedarf orientiert sich insbesondere an:
*a.* der Art der bearbeiteten Sach- und Personendaten;
*b.* dem Risiko einer Persönlichkeits- oder Grundrechtsverletzung für die betroffenen Personen;
*c.* der Art der Datenbearbeitung, insbesondere bei Verwendung riskanter oder neuer Technologien, Mechanismen oder Verfahren;
*d.* der Anzahl von der Datenbearbeitung betroffener Personen;
*e.* dem Umfang der bearbeiteten Sach- und Personendaten.
[2] Für den Einsatz von Informatikmitteln kann der zuständige Informatikdienst abhängig vom Schutzbedarf Sicherheitsstufen und Mindestanforderungen für die Datensicherheit festlegen.

**Art. 11** *Risikobeurteilung*

[1] Die öffentlichen Organe prüfen zusammen mit dem für sie zuständigen Informatikdienst ihre Informatikmittel und sonstigen Sammlungen von Sach- und Personendaten mit Blick auf die Eintretenswahrscheinlichkeit und die möglichen Folgen einer Verletzung der Datensicherheit.
[2] Sie ergreifen auf der Grundlage der Ergebnisse der Risikobeurteilung angemessene technische und organisatorische Massnahmen.

**Art. 12** *Technische und organisatorische Massnahmen*

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

*a.* Zugangsbeschränkungen: 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 eingegeben wurden;

*g.* Transportsicherung: bei der Bekanntgabe von Sach- und Personendaten sowie beim Transport von Datenträgern ist zu verhindern, dass die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können;

*h.* Empfängeridentifikation: Datenempfänger, denen Sach- und Personendaten bekannt gegeben werden, müssen identifiziert werden können;

*i.* Kontinuitätssicherung: Vorkehrungen werden getroffen, damit bei einem Ausfall von Informatikmitteln wichtige Funktionen möglichst rasch weiter erfüllt werden können;

*j.* Generationenfolgesicherung: Vorkehrungen werden getroffen, dass Sach- und Personendaten infolge technologischen Wandels beim Einsatz von Informatikmitteln dauerhaft erhalten werden können.

[2] Die zu ergreifenden Massnahmen sind angemessen, wenn sie sich eignen, dem Risiko einer Verletzung der Datensicherheit und des Datenschutzes effektiv zu begegnen.

[3] Die öffentlichen Organe prüfen periodisch die Angemessenheit der in ihrer Organisation ergriffenen Sicherheitsmassnahmen und passen diese bei Bedarf an.

[4] Dabei tragen die öffentlichen Organe den Grundsätzen der Zweckmässigkeit, der Wirtschaftlichkeit, dem Stand der jeweiligen Technik und der Benutzerfreundlichkeit Rechnung.

**Art. 13** *Protokollierung*

[1] Öffentliche Organe protokollieren die Bearbeitung von Sach- und Personendaten mit Informatikmitteln, wenn technische und organisatorische Massnahmen (Art. 12) zur Gewährleistung der Datensicherheit und zur Wahrung des Datenschutzes nicht genügen.
[2] Eine Protokollierung hat insbesondere dann zu erfolgen, wenn sonst nachträglich nicht festgestellt werden kann, ob die Sach- und Personendaten für diejenigen Zwecke bearbeitet wurden, für die sie erhoben oder bekannt gegeben worden sind.

### *3.3. Informationspflicht*

**Art. 14** *Modalitäten der Informationspflicht*

[1] Das öffentliche Organ teilt der betroffenen Person die Information über die Beschaffung von Personendaten (Art. 21 Abs. 1 IDAG) in präziser, verständlicher und leicht zugänglicher Form mit.
[2] Ist die betroffene Person nicht zur Auskunft verpflichtet, weist das öffentliche Organ sie bei der Beschaffung von Personendaten auf die Freiwilligkeit hin.

**Art. 15** *Ausnahmen von der Informationspflicht*

[1] In Ergänzung zu Artikel 21 Absatz 3 IDAG entfällt die Informationspflicht auch, wenn:

*a.* Personendaten zum Zweck der Einhaltung der Datensicherheit bearbeitet werden;
*b.* Personendaten für archivische Zwecke bearbeitet werden.

### *3.4. Datenbekanntgabe*

**Art. 16** *Schutzwürdige Interessen*

[1] Verlangt die gesuchstellende Person eine Bekanntgabe von Personendaten gestützt auf Artikel 23 Absatz 1 Buchstabe d IDAG oder die Aufhebung einer Datensperre gestützt auf Artikel 40 Absatz 2 Buchstabe c IDAG, so hat sie konkret aufzuzeigen, wozu ihr die nachgefragten Informationen dienen sollen.
[2] Ein allgemeines Interesse, das sich aus dem Umstand ergibt, dass zwischen den Personen eine rechtliche, wirtschaftliche oder persönliche Beziehung besteht, genügt für den Nachweis nicht.

[3] Gesuchstellende Personen, welche die Bekanntgabe von Personendaten gestützt auf Artikel 23 Absatz 1 Buchstabe f IDAG verlangen, können den Nachweis der Gemeinnützigkeit anhand des Gütesiegels der Zertifizierungsstelle für gemeinnützige nicht gewinnorientierte Organisationen (Zewo-Gütesiegel) oder der entsprechenden Anerkennung durch die zuständigen Steuerbehörden erbringen.

**Art. 17** *Angemessener Datenschutz*

[1] Ein angemessener Datenschutz für die Bekanntgabe von Personendaten ins Ausland (Art. 24 Abs. 1 IDAG) liegt vor, wenn:

*a.* der Bund festgestellt hat, dass die Gesetzgebung des Empfängerlandes oder das internationale Organ einen angemessenen Schutz gewährleistet (Länderliste);

*b.* bei einem Nichteintrag auf der Länderliste des Bundes ein angemessener Datenschutz durch andere Mittel gewährleistet ist.

[2] Die Fachstelle Datenschutz legt fest, welche anderen Mittel geeignet sind, einen angemessenen Datenschutz zu gewährleisten.

[3] Die Bekanntgabe von Personendaten in ein Empfängerland oder an ein internationales Organ ohne angemessenen Datenschutz im Einzelfall (Art. 24 Abs. 2 IDAG) bleibt vorbehalten.

### *3.5. Bearbeitung von Personendaten zu besonderen Zwecken*

**Art. 18** *Datenbearbeitung im Auftrag*

[1] Das auftraggebende öffentliche Organ wählt seinen Auftragsdatenbearbeiter unter besonderer Berücksichtigung der Einhaltung der Datensicherheit und des Datenschutzes sorgfältig aus.

[2] Vertraglich festzulegen sind insbesondere:

*a.* Gegenstand und Dauer des Auftrags;

*b.* Umfang, Art und Zweck der vorgesehenen Datenbearbeitung, die Art der Daten und der Kreis der betroffenen Personen;

*c.* die zur Einhaltung der Datensicherheit zu treffenden technischen und organisatorischen Massnahmen, deren Kontrolle und Dokumentation;

*d.* Durchsetzung von Ansprüchen betroffener Personen;

*e.* Verpflichtung zur Verschwiegenheit und Überbindung dieser Pflicht auf alle Datenbearbeitenden;

*f.* allfällige Berechtigung zur Vergabe von Unteraufträgen und damit einhergehende Verpflichtungen;

*g.* Kontrollrechte des auftraggebenden öffentlichen Organs und seiner Aufsichtsbehörden sowie entsprechende Duldungs- und Mitwirkungspflichten des Auftragsdatenbearbeiters;

*h.* Mitteilungspflicht des Auftragsdatenbearbeiters bei Verletzungen der Datensicherheit;
*i.* Weisungsbefugnisse des auftraggebenden öffentlichen Organs;
*j.* die Rückgabe überlassener Daten und Datenträger sowie die Vernichtung oder Löschung von beim Auftragsdatenbearbeiter gespeicherter Daten;
*k.* anwendbares Recht und Gerichtsstand.

[3] Die Verpflichtung zur Einhaltung der Datensicherheit und des Datenschutzes kann mit der Vereinbarung einer Konventionalstrafe gesichert werden.

**Art. 19** *Überwachung mit optisch-elektronischen Anlagen*

[1] Die Überwachung mit optisch-elektronischen Anlagen ist sachlich, räumlich und zeitlich auf das zum Erreichen des konkreten Zwecks Erforderliche zu beschränken.
[2] Die Fachstelle Datenschutz führt ein öffentlich zugängliches Verzeichnis von Videoüberwachungen.
[3] Das Verzeichnis gibt insbesondere Auskunft über:
*a.* den überwachten Ort;
*b.* den Überwachungszweck;
*c.* die Art der Überwachung;
*d.* den Überwachungsperimeter;
*e.* die Anzahl eingesetzter Kameras;
*f.* das für die Überwachung verantwortliche öffentliche Organ.

**Art. 20** *Datenbearbeitung zu Testzwecken*

[1] Das öffentliche Organ legt der Fachstelle Datenschutz spätestens zwei Jahre nach der Aufnahme der Testphase einen Evaluationsbericht vor.
[2] Es schlägt darin die Fortführung, Einstellung oder Überführung des Pilotbetriebs in den ordentlichen Betrieb vor.

### *3.6. Aufbewahrung und Vernichtung*

**Art. 21** *Aufbewahrungsfristen*

[1] Die Aufbewahrungsfristen bestimmen, für welche Dauer den öffentlichen Organen Sach- und Personendaten zur Erfüllung ihrer Aufgaben sowie zu Beweis- und Sicherungszwecken zur Verfügung stehen müssen, bevor sie dem zuständigen Archiv für archivische Zwecke angeboten werden müssen.
[2] Die öffentlichen Organe legen in Absprache mit dem zuständigen Archiv die minimalen Aufbewahrungsfristen für ihre Sach- und Personendaten fest.
[3] Nach Ablauf der minimalen Aufbewahrungsfrist dürfen Sach- und Personendaten nur mit Zustimmung des zuständigen Archivs vernichtet oder gelöscht werden.

[4] Vom zuständigen Archiv nicht übernommene Sach- und Personendaten, die nicht weiterhin zur Aufgabenerfüllung des öffentlichen Organs oder zu Beweis- und Sicherungszwecken benötigt werden, müssen spätestens 30 Jahre nach Ablauf der minimalen Aufbewahrungsfrist vernichtet oder gelöscht werden.
[5] Spezialgesetzliche Bestimmungen bleiben vorbehalten.

### *3.7. Durchsetzung des Datenschutzes*

**Art. 22** *Datenschutznachweis*

[1] Die Anforderungen an den Nachweis zur Einhaltung des Datenschutzes (Art. 32 Abs. 3 IDAG) richten sich nach den Vorgaben der Fachstelle Datenschutz. Er kann auch durch Zertifizierung erbracht werden. Diese richtet sich nach den Vorschriften des Bundes.
[2] Die öffentlichen Organe erbringen den Nachweis bis spätestens fünf Jahre nach Inkrafttreten dieser Verordnung. Sie können ihn einzeln oder zusammen mit anderen öffentlichen Organen erbringen.
[3] Die öffentlichen Organe haben den Nachweis des Datenschutzes regelmässig, spätestens aber alle fünf Jahre neu zu erbringen.

**Art. 23** *Pflicht zur Datenschutz-Folgenabschätzung*

[1] Die Pflicht der öffentlichen Organe zur Durchführung einer Datenschutz-Folgenabschätzung (Art. 33 IDAG) ist auf die Einführung und Erweiterung von Informatikmitteln, mit denen Personendaten bearbeitet werden, beschränkt.
[2] Ein hohes Risiko für die Persönlichkeit und die Grundrechte der betroffenen Personen nach Artikel 33 Absatz 1 IDAG ist voraussichtlich gegeben, wenn:

*a.* die eingesetzten Informatikmittel Profiling ermöglichen;
*b.* besonders schützenswerte Personendaten bearbeitet werden;
*c.* Personendaten von einer Vielzahl betroffener Personen bearbeitet werden;
*d.* Bearbeitungen von Personendaten durch Auftragsdatenbearbeiter durchgeführt werden;
*e.* zwei oder mehrere öffentliche Organe Personendaten gemeinsam bearbeiten.

[3] Ergänzend zu Artikel 33 Absatz 3 IDAG können die öffentlichen Organe auf die Datenschutz-Folgenabschätzung verzichten, sofern und soweit die Datenbearbeitungen bereits in den gesetzlichen Grundlagen ausdrücklich geregelt werden.

[4] Die öffentlichen Organe teilen der Fachstelle Datenschutz das dokumentierte Ergebnis der Datenschutz-Folgenabschätzung unabhängig davon mit, ob die Einführung oder Erweiterung von Informatikmitteln eine Vorab-Konsultation bedingt oder nicht.

**Art. 24** *Anforderungen an die Datenschutz-Folgenabschätzung*

[1] Die Datenschutz-Folgenabschätzung benennt mindestens:

*a.* das verantwortliche öffentliche Organ, die rechtliche Grundlage, den Zweck und eine systematische Beschreibung der geplanten Datenbearbeitungen, insbesondere in Bezug auf die zu bearbeitenden Personendaten;

*b.* eine Bewertung der Notwendigkeit und Verhältnismässigkeit der Datenbearbeitungen in Bezug auf den Zweck, wobei potenziell mildere Mittel zu erörtern sind;

*c.* eine Bewertung der Risiken für die Persönlichkeit und die Grundrechte der betroffenen Personen;

*d.* die technischen und organisatorischen Massnahmen, die zur Bewältigung der Risiken geplant sind, insbesondere in Bezug auf Datenbearbeitungen im Auftrag.

**Art. 25** *Vorab-Konsultation*

[1] Zusammen mit dem Gesuch um Vorab-Konsultation reicht das öffentliche Organ das dokumentierte Ergebnis der Datenschutz-Folgenabschätzung ein.

[2] Die Konsultation ist abgeschlossen, wenn die Fachstelle Datenschutz die Anwendung für unbedenklich erklärt oder eine Empfehlung (Art. 58 Abs. 3 IDAG) abgegeben hat.

[3] Das öffentliche Organ führt die geplanten Datenbearbeitungen erst nach Abschluss der Konsultation durch.

**Art. 26** *Öffentliche Bekanntmachung von Datensicherheitsverletzungen*

[1] Erscheint eine individuelle Information über Verletzungen der Datensicherheit aufgrund der Vielzahl betroffener Personen als unverhältnismässig (Art. 35 Abs. 5 Bst. b IDAG), kann die Information durch öffentliche Bekanntmachung in geeigneter Form erfolgen.

### *3.8. Rechte der Betroffenen*

**Art. 27** *Bestätigung und Aufhebung der Datensperre*

[1] Die Datensperre ist der betroffenen Person in geeigneter Form zu bestätigen.

[2] Das Gesuch um Aufhebung der Datensperre ist schriftlich oder elektronisch zu stellen.

### *3.9. Aufsichts- und Kontrollorgan*

**Art. 28** *Stellvertretung*

[1] Der Regierungsrat bezeichnet nach Rücksprache mit der Leitung der Fachstelle Datenschutz deren Stellvertretung für Ausstandsfälle und längere Abwesenheiten.
[2] Vorbehalten bleibt eine anderweitige Stellvertretungsregelung für eine kantonsübergreifende Aufsichtsstelle (Art. 59 IDAG).

**Art. 29** *Stellungnahmerecht*

[1] Die öffentlichen Organe unterbreiten der Fachstelle Datenschutz Rechtsetzungsprojekte und beabsichtigte Massnahmen, welche für den Datenschutz erheblich sind (Art. 57 Abs. 1 Bst. c IDAG), unaufgefordert zur Stellungnahme.

**Art. 30** *Anzeige*

[1] Die Fachstelle Datenschutz wird auf eine Anzeige hin aufsichtsrechtlich tätig, wenn sich daraus Tatsachen ergeben, die ein Einschreiten im öffentlichen Interesse erfordern.
[2] Liegen hingegen Tatsachen vor, deren Behandlung nicht im öffentlichen Interesse liegt, so verweist die Fachstelle Datenschutz die anzeigende Person auf den Weg des Individualrechtsschutzes.
[3] Die Möglichkeit einer Vermittlung (Art. 57 Abs. 1 Bst. e IDAG) bleibt vorbehalten.

**Art. 31** *Fristansetzung*

[1] Stellt die Fachstelle Datenschutz fest, dass Vorschriften über den Datenschutz verletzt werden und gibt sie eine Empfehlung ab, so setzt sie dem öffentlichen Organ eine angemessene Frist, um zu erklären, ob es der Empfehlung folgt oder nicht.

## 4. Archivwesen

### *4.1. Aktenführung und Aktenaufbewahrung*

**Art. 32** *Aktenführung*

[1] Die öffentlichen Organe führen die amtlichen Dokumente vollständig, systematisch und nachvollziehbar.

[2] Die Aktenführung erfolgt nach einem Ordnungssystem und in der Regel in digitaler Form.
[3] Das Ordnungssystem bildet Grundlage für die spätere Archivierung. Änderungen des Ordnungssystems dürfen nur in Zusammenarbeit mit dem zuständigen Archiv erfolgen. Es ist bei der Planung des Einsatzes neuer Informatikmittel, in welchen amtliche Dokumente abgelegt werden, frühzeitig mit einzubeziehen und kann eine Überarbeitung des Ordnungssystems verlangen.
[4] Jedes öffentliche Organ bezeichnet eine für das Ordnungssystem und die weitere Organisation der Ablage verantwortliche Person.
[5] Die Digitalisierung physischer amtlicher Dokumente richtet sich nach den Vorgaben des zuständigen Archivs.

**Art. 33** *Aktenaufbewahrung*

[1] Die öffentlichen Organe bewahren ihre amtlichen Dokumente sachgerecht und sicher auf.
[2] Sie schützen sie vor Missbrauch, Beschädigung und Verlust. Dabei achten sie auf die Verwendung alterungsbeständiger Informationsträger und von Hilfsmitteln, die Gewähr für eine ausreichende Lebensdauer bieten.
[3] Sie sind für ihre amtlichen Dokumente bis zum Ablauf der Aufbewahrungsfristen gemäss Artikel 21 Absatz 2 bzw. bis zu ihrer Vernichtung oder Löschung verantwortlich.

**Art. 34** *Gemeinsamer Datenbestand*

[1] Bearbeiten mehrere öffentliche Organe amtliche Dokumente gemeinsam, so regeln sie die Verantwortlichkeit zur Aktenführung und Aktenaufbewahrung.

### *4.2. Archivierung*

**Art. 35** *Anbietepflicht*

[1] Die öffentlichen Organe bieten ihre amtlichen Dokumente dem zuständigen Archiv regelmässig zur Übernahme an, spätestens aber nach Ablauf der Aufbewahrungsfristen gemäss Artikel 21 Absatz 2.
[2] Bei Auflösung eines öffentlichen Organs oder bei dessen Überführung ins Zivilrecht sind seine amtlichen Dokumente in Absprache mit dem Rechtsnachfolger dem zuständigen Archiv anzubieten.

**Art. 36** *Bewertung und Übernahme*

[1] Das zuständige Archiv bewertet die ihm angebotenen amtlichen Dokumente hinsichtlich ihrer Archivwürdigkeit. Dabei hört es das anbietende öffentliche Organ an.

[2] Archivwürdig sind amtliche Dokumente insbesondere dann, wenn sie von dauerndem Wert sind für:

*a.* die Dokumentierung der Organisation und der Tätigkeit des öffentlichen Organs;
*b.* die Sicherung berechtigter Interessen betroffener Personen oder Dritter;
*c.* das Verständnis der Gegenwart und der Geschichte;
*d.* die Gesetzgebung;
*e.* die Verwaltungstätigkeit oder die Rechtsprechung;
*f.* die Wissenschaft und die Forschung.

[3] Das zuständige Archiv entscheidet aufgrund seiner Bewertung abschliessend über die Übernahme von amtlichen Dokumenten ins Archivgut.
[4] Mit der Übernahme der amtlichen Dokumente ins Archivgut geht die Verantwortlichkeit an das zuständige Archiv über.

**Art. 37** *Ablieferung*

[1] Die öffentlichen Organe liefern die zur Übernahme bestimmten amtlichen Dokumente dem zuständigen Archiv in auf- und vorbereitetem Zustand und mit einem Ablieferungsverzeichnis versehen ab.
[2] Das zuständige Archiv legt die Anforderungen an das Ablieferungsverzeichnis sowie an die Auf- und Vorbereitung fest, insbesondere hinsichtlich:

*a.* Verpackung, Beschriftung und Transport;
*b.* Standards für Ablieferungspakete und Datentransfer.

[3] Es kann hierfür mit den abliefernden öffentlichen Organen Ablieferungsvereinbarungen abschliessen.

**Art. 38** *Sicherung des Archivguts*

[1] Die von den zuständigen Archiven übernommenen und als archivwürdig bewerteten amtlichen Dokumente bilden das Archivgut.
[2] Das zuständige Archiv sorgt für die dauerhafte Erhaltung sowie Nutzbarkeit des Archivguts und schützt es vor unbefugter Kenntnisnahme, Vernichtung oder Löschung.

### *4.3. Zugang zum Archivgut*

**Art. 39** *Ausleihe*

[1] Das zuständige Archiv kann Archivgut an das abliefernde öffentliche Organ oder zu Ausstellungszwecken ausleihen.
[2] Sofern der Schutz des Archivguts es erfordert, kann das zuständige Archiv anstelle von Originalen Kopien der amtlichen Dokumente zur Verfügung stellen.

**Art. 40** *Überwiegendes privates Interesse*

[1] Ein überwiegendes privates Interesse nach Artikel 46 Absatz 2 Buchstabe c IDAG liegt in der Regel dann vor, wenn eine Person:

*a.* Zugang zu Informationen über sich selbst verlangt;

*b.* Zugang zu Informationen über eine Person des öffentlichen Lebens verlangt, sofern diese Informationen mit dem Wirken dieser Person in der Öffentlichkeit zu tun haben.

**Art. 41** *Zugang über das Internet*

[1] Das zuständige Archiv kann Verzeichnisdaten schon während der Schutzfrist über das Internet zugänglich machen, sofern sie keine schützenswerten Sach- und Personendaten enthalten.

[2] Nach Ablauf der Schutzfrist kann es elektronische Fassungen von amtlichen Dokumenten über das Internet zugänglich machen.

### *4.4. Bestand und Nutzung des Landesarchivs*

**Art. 42** *Archivgut*

[1] Das Landesarchiv ist das zentrale Archiv des Kantons und seiner Rechtsvorgänger.

[2] Es bewahrt die archivwürdigen amtlichen Dokumente folgender öffentlicher Organe sicher und dauerhaft auf:

*a.* der Landsgemeinde;

*b.* des Landrates;

*c.* des Regierungsrates;

*d.* der gerichtlichen Behörden;

*e.* der kantonalen Kommissionen;

*f.* der kantonalen Verwaltung;

*g.* der kantonalen öffentlich-rechtlichen Anstalten und Stiftungen;

*h.* der interkantonalen Organisationen, Einrichtungen und Institutionen, an denen der Kanton beteiligt ist, soweit für diese glarnerisches Recht anwendbar ist;

*i.* weiterer Personen, Organisationen und Institutionen des öffentlichen und privaten Rechts, die öffentliche Aufgaben des Kantons erfüllen, mit Ausnahme der Glarner Kantonalbank.

[3] Es kann Archivgut Dritter übernehmen, die keine öffentlichen Aufgaben des Kantons erfüllen.

**Art. 43** *Erschliessung und Nutzung*

[1] Das Landesarchiv sorgt für eine angemessene Erschliessung des Archivgutes.

[2] Es erlässt eine Ordnung über die Nutzung seiner Archivalien, Räume und Einrichtungen.
[3] Es kann Personen, die in schwerwiegender Weise gegen die Nutzungsordnung verstossen, wegweisen und ihnen den Zugang zum Landesarchiv verweigern.

### *4.5. Weitere Aufgaben und Befugnisse des Landesarchivs*

**Art. 44** *Aufgaben*

[1] Das Landesarchiv:
*a.* berät die kantonalen öffentlichen Organe bei der Organisation ihrer Aktenführung und Aktenaufbewahrung sowie in Bezug auf die Aufbereitung und Ablieferung von amtlichen Dokumenten;
*b.* begleitet Projekte der elektronischen Aktenführung und Aktenaufbewahrung der kantonalen öffentlichen Organe;
*c.* berät die Gemeinden in Archivfragen.

**Art. 45** *Befugnisse*

[1] Das Landesarchiv kann sich an der Erforschung und Veröffentlichung seines Archivgutes beteiligen.
[2] Wer ein Werk veröffentlicht, das in wesentlichen Teilen auf der Nutzung von Archivgut des Landesarchivs beruht, hat diesem ein unentgeltliches Belegexemplar abzuliefern.

## 5. Ausnahmen von der Kostenlosigkeit

**Art. 46** *Information über Kosten*

[1] Das öffentliche Organ informiert die gesuchstellende Person unverzüglich über eine mögliche Gebührenpflicht, wenn Kopien angefertigt werden oder die Behandlung von aus dem IDAG geltend gemachten Rechten und Ansprüchen ein aufwendiges Verfahren verursacht.

**Art. 47** *Aufwendiges Verfahren*

[1] Ein aufwendiges Verfahren (Art. 54 Abs. 2 Bst. a IDAG) liegt vor, wenn die Behandlung der aus dem IDAG geltend gemachten Rechte und Ansprüche mehr als drei Stunden in Anspruch nimmt.

**Art. 48** *Missbräuchliche Erneuerung eines Gesuchs*

[1] Eine angemessene Gebühr kann ebenfalls erhoben werden, wenn die gesuchstellende Person wiederholt ohne schutzwürdiges Interesse oder in rechtsmissbräuchlicher Art und Weise die gleichen Begehren bei öffentlichen Organen stellt.