kanton glarus

**Staatskanzlei**
**Fachstelle Datenschutz**
Rathaus
8750 Glarus

Version 1.0 – September 2023

# Erbringen des Datenschutznachweises

Dieses Dokument richtet sich an die öffentlichen Organe des Kantons Glarus. Es dient als Anleitung zum selbständigen Erbringen des Datenschutznachweises gemäss den Artikeln 32 IDAG und 22 VIDAG.[1] Das Erbringen des Datenschutznachweises bezweckt, dass die öffentlichen Organe die datenschutzrechtlichen Mindestanforderungen kennen, praktisch umsetzen, dokumentieren und aktuell halten.

Der Nachweis kann nach den Vorgaben dieses Dokuments oder aber durch Zertifizierung gemäss den Vorschriften des Bundes erbracht werden (Art. 22 Abs. 1 VIDAG). Die öffentlichen Organe erbringen den Nachweis des Datenschutzes regelmässig, spätestens aber alle fünf Jahre (Art. 22 Abs. 3 VIDAG). Er wird selbständig erbracht. Die Umsetzung ist zu dokumentieren.

Ergeben sich Fragen zum Erbringen des Datenschutznachweises, kann die Fachstelle Datenschutz konsultiert werden.

## 1. Ermitteln und bewerten der relevanten Bearbeitungen von Personendaten

Innerhalb des verantwortlichen öffentlichen Organs sind die einzelnen Bearbeitungen von Personendaten zu ermitteln (Datenbestände, Prozesse der Datenbearbeitungen, Informatikmittel mit denen Personendatendaten bearbeitet werden etc.).

Sobald dies geschehen ist, soll einzeln pro Bearbeitungstätigkeit bzw. Datenbestand beurteilt werden, ob eines oder mehrere der nachfolgend genannten hohen Risiken für die Persönlichkeit oder die Grundrechte von Betroffenen vorliegen.

- Datenbearbeitung ermöglicht Profiling.[2]
- Datenbearbeitung von besonders schützenswerte Personendaten.
- Datenbearbeitung in grossem Umfang.[3]
- Datenbearbeitung erfolgt unter Beizug eines Auftragsdatenbearbeiters.
- Datenbearbeitung erfolgt durch zwei oder mehrere öffentliche Organe und/oder kombiniert Personendaten, die durch unterschiedliche Prozesse gewonnen oder zu unterschiedlichen Zwecken erhoben wurden.[4]
- Datenbearbeitung führt im Falle einer Verletzung der Datensicherheit zu einer Gefahr für Leib und Leben.

---

[1] Angelehnt an das Standard-Datenschutzmodell, Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele, Version 3.0 von der 104. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (beschlossen am 24. November 2022, abrufbar unter: Datenschutzkonferenz (datenschutzkonferenz-online.de)). Ebenfalls angelehnt an den Leitfaden «Datenschutz-Managementsystem» der Zürcher Datenschutzbeauftragten, Version 3.3, Mai 2023, abrufbar unter: Datenschutz-Managementsystem.

[2] Automatisierte Auswertung von Personendaten zur Analyse von persönlichen Merkmalen (Profiling) und/oder zur Vorhersage von Entwicklungen (Prognose), hinsichtlich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, Intimsphäre, Mobilität, Integrationsfähigkeit, künftiges Verhalten etc.

[3] Grosse Anzahl von Betroffenen (Kreis der Betroffenen ist nicht von Beginn an auf einzelne wenige, klar bestimmbare Personen einschränkbar ist); grosse Menge von zu bearbeiteten Personendaten; lange Dauer der Bearbeitung bzw. Speicherung von Personendaten; Kreis der Zugriffsberechtigten ist umfangreich etc.

[4] Bspw. Abgleichen oder Zusammenführen von Datensätzen, die aus zwei oder mehreren Datenbearbeitungsvorgängen stammen, die zu unterschiedlichen Zwecken und/oder von verschiedenen für die Datenbearbeitung verantwortlichen öffentlichen Organen durchgeführt wurden, und zwar in einer Weise, die über die vernünftigen Erwartungen der Betroffenen hinausgeht.

- Datenbearbeitung erfolgt unter Einsatz neuer und/oder riskanter Technologien, Mechanismen oder Verfahren oder aber unter Einsatz biometrischer und/oder genetischer Verfahren.
- Datenbearbeitung ermöglicht eine automatisierte Entscheidfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung.[5]
- Datenbearbeitung ermöglicht (systematische) Überwachung.[6]
- Datenbearbeitung mit Personendaten von schutzbedürftigen Personen.[7]
- Datenbearbeitung mit Bekanntgabe von Personendaten in eine Cloud.
- Datenbearbeitung erfolgt zu Testzwecken.
- Datenbearbeitung schafft voraussichtlich weitere hohe Risiken für die Persönlichkeit oder die Grundrechte von Betroffenen.[8]

Wird organisationsintern eines oder mehrere solcher Risiken ermittelt, so ist die Erbringung des Datenschutznachweises geboten. Sofern keines der oben genannten Risiken ermittelt werden konnte, ist das Erbringen des Datenschutznachweises dennoch empfehlenswert, sofern organisationsintern Personendaten bearbeitet werden.

**Beispiel 1**: Das öffentliche Organ speichert und bearbeitet Personendaten von vielen Personen; es führt Personendaten aller Bürgerinnen und Bürger der Gemeinde. Zwar finden sich darunter keine besonders schützenswerten Personendaten. Die Menge an gespeicherten Personendaten führt aber zu einem Risiko, welches das Erbringen des Datenschutznachweises erfordert.
**Beispiel 2**: Das öffentliche Organ nutzt ein Informatikmittel (Software), das Personendaten in einer Cloud speichert. Diese Datenbearbeitung ist mit erhöhten Risiken für all jene verbunden, deren Personendaten in die Cloud bekanntgegeben werden.
**Beispiel 3**: Auch lässt das öffentliche Organ mit einer Videoüberwachungsanlage die Gebäudeeingänge zum Schutz von Personen und Sachen überwachen. Da hiermit Personen, auch Angestellte überwacht werden, ist der Datenschutznachweis, auch mit Fokus auf die Videoüberwachung, zu erbringen.

## 2. Ermitteln des Soll-Zustands anhand der rechtlichen Prüfkriterien

Nachfolgend sind die rechtlichen Prüfkriterien und möglichen risikominierenden Massnahmen (nicht abschliessend) aufgeführt, die bei der Erbringung des Datenschutznachweises im Vordergrund stehen. Das öffentliche Organ arbeitet die Liste unter «**a. Begriffe und Einordnung**» ***bis und mit*** «**2. j. Projektmanagement**» durch. Dabei dokumentiert es, welche Prüfkriterien mittels welchen Massnahmen und Datenschutzinstrumenten pro Datenbearbeitung erfüllt werden sollen (Soll-Zustand).

**Beispiel eines Prüfkriteriums**:
- Gewährleisten, dass Personendaten nur bearbeitet werden, wenn dafür eine gesetzliche Grundlage besteht, die Bearbeitung zur Erfüllung einer öffentlichen Aufgabe erforderlich ist oder in die Bearbeitung eingewilligt wurde.

**Beispiel einer möglichen Massnahme**:
- ✓ Es liegen Muster-Einwilligungsformulare vor, die im Falle einer erforderlichen Einwilligung genutzt werden.

[5] Bspw. automatisierte Erstellung von Strafbefehlen, Verfügungen oder Entscheidungen betreffend Zugang zu Dienstleistungen.
[6] Bspw. Bearbeitungsvorgänge, die Beobachtung, Überwachung oder Kontrolle von Betroffenen ermöglichen oder auf eine systematische Überwachung öffentlich zugänglicher Bereiche abzielt.
[7] Als schutzbedürftige Personen gelten bspw. Schulpflichtige, Arbeitnehmer, Personen mit psychischer Beeinträchtigung, Patienten, Personen im Straf- und Massnahmenvollzug etc.
[8] Bspw. Datenbearbeitung, die auch nur mittelbar dazu führen kann, dass Bürgerinnen und Bürger davor zurückschrecken ihre verfassungsmässig garantierten Rechte wahrzunehmen, wie etwa die freie Meinungsäusserung, die Versammlungsfreiheit, die freie Ausübung ihrer Religionszugehörigkeit etc.

**Beispiel 1**: Ist restlos klar, dass keine Personendaten ins Ausland bekanntgegeben werden, können die entsprechende rechtlichen Prüfkriterien und die dazugehörigen Massnahmen bei «2. d. iii. Bekanntgabe ins Ausland» übersprungen werden.
**Beispiel 2**: Setzt das öffentliche Organ keine Videoüberwachung ein und beabsichtigt es in absehbarer Zeit keine solche einzusetzen, dann können die rechtlichen Prüfkriterien und die dazugehörigen Massnahmen in Abschnitt «2. e. iii. Überwachung mit optisch-elektronischen Anlagen» übersprungen werden.
**Beispiel 3**: Werden andere öffentliche Organe oder Private (wiederkehrend) mit der Bearbeitung von Personendaten beauftragt, dann sind die rechtlichen Prüfkriterien und die entsprechenden Massnahmen zu «2. e. ii. Datenbearbeitung im Auftrag» zu beachten.

Zur Dokumentation steht dem öffentlichen Organ die **Vorlage für die Dokumentation des Soll-Zustands** zur Verfügung (Webseite Fachstelle Datenschutz). Es ist dem öffentlichen Organ aber selbst überlassen, ob es den Soll-Zustand anderweitig dokumentieren will. Ein Anwendungsbeispiel ist in diesem Dokument auf den Seiten 13 und 14 zu finden.

---

### a. Begriffe und Einordnung

- Gewährleisten, dass den Mitarbeitenden des öffentlichen Organs bewusst ist, was Personendaten, besonders schützenswerte Personendaten und Stammdaten sind.
- Gewährleisten, dass das Bewusstsein gegeben ist, dass unter Datenbearbeitung jeder Umgang mit Personendaten gemeint ist, also etwa das erheben, speichern, bekanntgegeben an Dritte, abändern, vernichten etc.
- Gewährleisten, dass das Bewusstsein vorliegt, dass Datenschutz ein Grundrecht ist, dessen Einschränkung an verfassungsmässige und datenschutzrechtliche Voraussetzungen geknüpft ist.

### b. Voraussetzungen und Grundsätze für die Bearbeitung von Personendaten

- Gewährleisten, dass das Merkblatt «Voraussetzungen und Grundsätze für die Bearbeitung von Personendaten» zum Erbringen des Datenschutznachweises berücksichtigt wird.

#### i. Rechtmässigkeit

- Gewährleisten, dass Personendaten nur bearbeitet werden, wenn dafür eine gesetzliche Grundlage besteht, die Bearbeitung zur Erfüllung einer öffentlichen Aufgabe erforderlich ist oder in die Bearbeitung eingewilligt wurde.
  - ✓ Pro Organisationseinheit sind die rechtlichen Grundlagen bekannt, die dem öffentlichen Organ seine Aufgaben zuweisen und gemäss denen es Personendaten bearbeiten darf. Fehlt es an den entsprechenden Grundlagen, holt das öffentliche Organ die Einwilligung für die Bearbeitung von Personendaten ein.
  - ✓ Bei seiner Aufgabenerfüllung ist dem öffentlichen Organ bewusst, ob und wenn ja, welche Personendaten und besonders schützenswerten Personendaten es bearbeiten darf.
  - ✓ Personendaten werden nur durch ein Abrufverfahren (bspw. GERES) zugänglich gemacht, wenn dies ausdrücklich in einem Erlass vorgesehen ist.
  - ✓ Gegebenenfalls weitere Massnahmen.
- Gewährleisten, dass besonders schützenswerte Personendaten nur bearbeitet werden, wenn dafür eine Grundlage im Gesetz besteht, dies für die Erfüllung einer im Gesetz klar umschriebenen Aufgabe erforderlich ist oder ausdrücklich in die Bearbeitung eingewilligt wurde.
  - ✓ Werden besonders schützenswerte Personendaten bearbeitet, stützt das öffentliche Organ die Bearbeitung auf eine Grundlage in einem formellen Gesetz oder auf eine im formellen Gesetz klar umschriebene öffentliche Aufgabe, zu deren Erfüllung die Bearbeitung erforderlich ist. Fehlt es an einer solchen Grundlage, holt das öffentliche Organ die ausdrücklich erteilte Einwilligung ein. Ansonsten unterlässt es die Bearbeitung von besonders schützenswerten Personendaten.
  - ✓ Besonders schützenswerte Personendaten werden nur durch ein Abrufverfahren gemacht, wenn dies in einem formellen Gesetz vorgesehen ist.
  - ✓ Gegebenenfalls weitere Massnahmen.

- Gewährleisten, dass wenn die Einwilligung Voraussetzung für das Bearbeiten von Personendaten ist, dass diese bekannt sind. Die Voraussetzungen werden bei Einholen der Einwilligung erfüllt.
  - ✓ Es liegen Muster-Einwilligungsformulare vor, die im Falle einer erforderlichen Einwilligung eingesetzt werden.
  - ✓ Gegebenenfalls weitere Massnahmen.
- Gewährleisten, dass die weiteren Voraussetzungen gemäss Art. 14 Abs. 1 und 2 IDAG bekannt sind, die zur Bearbeitung von Personendaten berechtigen.
  - ✓ Fehlt es an einer gesetzlichen Grundlage, an einer öffentlichen Aufgabe, wie auch an einer rechtsgenüglichen Einwilligung, die zur Bearbeitung ermächtigen würden, sind die weiteren Voraussetzungen aus Art. 14 Abs. 1 und 2 IDAG bekannt, welche allenfalls auch zur Bearbeitung der Personendaten berechtigen.
  - ✓ Gegebenenfalls weitere Massnahmen.

#### ii. Verhältnismässigkeit

- Gewährleisten, dass nur diejenigen Personendaten bearbeitet werden, die für die Erfüllung der öffentlichen Aufgabe geeignet und erforderlich sind.
  - ✓ Sicherstellen, dass die Datenbeschaffung und die weitere Bearbeitung auf die Aufgabenerfüllung und damit auf den eigentlichen Bearbeitungszweck abgestimmt sind. Darüber hinaus sollen keine weiteren Daten beschafft und weiterbearbeitet werden.
  - ✓ Gegebenenfalls weitere Massnahmen.
- Gewährleisten, dass die Prinzipien der Datenvermeidung und Datensparsamkeit umgesetzt werden.
  - ✓ Wenn immer möglich werden keine Personendaten erhoben.
  - ✓ Es werden keine für die Aufgabenerfüllung ungeeigneten Personendaten erhoben.
  - ✓ Gegebenenfalls weitere Massnahmen.

  - ✓ Es werden nicht mehr Personendaten erhoben, als für die Aufgabenerfüllung tatsächlich notwendig sind.
  - ✓ Prozesse, Formulare etc. sind so ausgestaltet, dass nur das Mindestmass an erforderlichen Daten erhoben wird.
  - ✓ Datenbearbeitungssysteme werden auf den Einsatz von Privacy Enhancing Technology (Technologien zum Schutz der Privatsphäre) überprüft. Durch den Einsatz solcher Technologien kann etwa der Umfang der bearbeiteten Daten minimiert werden.
  - ✓ Gegebenenfalls weitere Massnahmen.

  - ✓ Das öffentliche Organ hat die Aufbewahrungsfristen der Personendaten bestimmt, auch für allfällige Beweis- und Sicherungszwecke.
  - ✓ Das öffentliche Organ vernichtet oder löscht jene Personendaten unwiderruflich, die nicht mehr zur Aufgabenerfüllung oder zu Sicherungs- und Beweiszwecken benötigt werden – dies unter Wahrung der archivrechtlichen Vorschriften (dazu auch Art 21 VIDAG).
  - ✓ Hierzu werden Prozesse definiert, die bestimmen, welche Datenbestände nach welchem zeitlichen Intervall auf die zulässige Aufbewahrungsdauer und Vernichtung überprüft werden müssen.
  - ✓ Durch den Einsatz von Privacy Enhancing Technology (Technologien zum Schutz der Privatsphäre) werden Personendaten nach vordefiniertem Zeitpunkt automatisiert vernichtet bzw. gelöscht (Achtung: spezialgesetzliche Bestimmungen hinsichtlich Beweis- und Sicherungszwecke und Archivierung).
  - ✓ Gegebenenfalls weitere Massnahmen.

  - ✓ Dem öffentlichen Organ sind wirkungsvolle Mittel zur Anonymisierung und Pseudonymisierung bekannt und es nutzt diese.
  - ✓ Personendaten, die nicht zu vernichten sind, werden anonymisiert.
  - ✓ Personendaten, die nicht anonymisiert werden können, werden teilanonymisiert.
  - ✓ Personendaten, die nicht teilanonymisiert werden können, werden pseudonymisiert.
  - ✓ Gegebenenfalls weitere Massnahmen.

#### iii. Zweckbindung

- Gewährleisten, dass Personendaten nur für Zwecke bearbeitet werden, die bei der Beschaffung angegeben wurden.

- Gewährleisten, dass Personendaten nur für Zwecke bearbeitet werden, die aus den Umständen ersichtlich sind.
- Gewährleisten, dass Personendaten nur für Zwecke bearbeitet werden, die gesetzlich vorgesehen sind.

✓ Die Personen, über die Daten bearbeitet werden, wissen von Beginn an, wofür ihre Daten bearbeitet und verwendet werden (dazu auch Informationspflicht gem. Art. 21 IDAG).
✓ Periodische stichprobeweise Überprüfung, ob die Personendaten zum zulässigen Zweck bearbeitet werden.
✓ Überprüfen, ob sich eine Änderung des ursprünglichen Bearbeitungszwecks auf eine rechtliche Grundlage oder eine Einwilligung der Betroffenen stützt. Sicherstellen, dass jede nachträgliche Zweckänderung nachvollziehbar ist.
✓ Sobald der Verwendungszweck erfüllt ist, dürfen die Daten nicht weiter aufbewahrt werden und sie sind unter Vorbehalt von Beweis- und Sicherungszwecken sowie archivrechtlichen Vorgaben zu vernichten.
✓ Daten dürfen ohne Zweckbestimmung nicht erhoben werden. Massnahmen gegen die Vorratsdatenspeicherung sind zwingend umzusetzen.
✓ Gegebenenfalls weitere Massnahmen.

#### iv. Datensicherheit

- Gewährleisten der Datensicherheit von Informatikmittel durch das verantwortliche öffentliche Organ zusammen mit der Hautabteilung Informatik (Art. 17 IDAG, Art. 8 – 13 VIDAG).
- Gewährleisten, dass die Informatikmittel, welche die verantwortlichen öffentlichen Organe zur Erfüllung ihrer gesetzlichen Aufgaben einsetzen, angemessen vor Missbrauch und Störung geschützt werden. Namentlich soll ausgehend von den Schutzzielen (Richtigkeit / Integrität, Vertraulichkeit, Verfügbarkeit, Nachvollziehbarkeit) folgendes beurteilt werden:
  - der Schutzbedarf (Art. 10 VIDAG);
  - die Risiken für die Datensicherheit (und damit den Datenschutz) (Art. 11 VIDAG);
  - die zur Risikoreduktion erforderlichen technischen und organisatorischen Massnahmen (Art. 12 und 13 VIDAG).
- Gewährleisten, dass die Schutzziele (Richtigkeit / Integrität, Vertraulichkeit, Verfügbarkeit, Nachvollziehbarkeit) bekannt sind und mittels den ergriffenen technischen und organisatorischen Massnahmen effektiv gewahrt werden:

✓ Richtigkeit / Integrität
  - Gewährleisten, dass Personendaten so bearbeitet werden, dass diese und das Erzeugnis der Bearbeitung richtig sind.
  - Gewährleisten, dass Personendaten so bearbeitet werden, dass diese und das Erzeugnis daraus aktuell geführt sind.
  - Gewährleisten, dass Personendaten so bearbeitet werden, dass diese und das Erzeugnis daraus vollständig sind.
  - Gewährleisten, dass das Berichtigungsrecht und die Rechte bei widerrechtlicher Datenbearbeitung bekannt sind und Betroffene gemäss den gesetzlichen Voraussetzungen ungehindert ihre Rechte wahrnehmen können.

✓ Vertraulichkeit
  - Gewährleisten, dass Personendaten nur so bearbeitet werden, dass diese ausschliesslich Berechtigten zugänglich gemacht werden.
  - Es liegen Zugriffs- bzw. Berechtigungskonzepte vor, die regeln, welche Personen auf welche Datensammlung zugreifen dürfen.
  - Es werden nur Zugriffe gewährt für Personen, die den Zugriff zur Aufgabenerfüllung benötigen.
  - Werden die Zugriffe nicht benötigt, werden sie entzogen.
  - Es werden zeitliche Intervalle definiert, in denen die Informatikmittel durch den zuständigen Informationssicherheitsbeauftragten auf ihre Vertraulichkeit überprüft werden.

✓ Verfügbarkeit
  - Gewährleisten, dass die notwendigen Personendaten und weitere systemrelevante Informationen rechtzeitig, in gewünschter Form und an gewünschter Stelle bezogen werden können.
  - Es wurden Massnahmen umgesetzt, die die Verfügbarkeit von systemrelevanten Informationen gewährleisten.

- Es werden zeitliche Intervalle definiert, während denen die Informatikmittel durch den zuständigen Informationssicherheitsbeauftragten auf ihre Verfügbarkeit überprüft werden.

✓ Nachvollziehbarkeit
- Gewährleisten, dass nachvollzogen werden kann, welche Personendaten von wem, zu welchem Zeitpunkt, inwiefern, zu welchem Zweck bearbeitet wurden.
  - Bei der Nutzung von Informatikmittel erfolgt wann immer möglich eine automatisierte Protokollierung der Bearbeitungen.

✓ Gegebenenfalls weitere Massnahmen.

- Gewährleisten, dass die zu ergreifenden technischen und organisatorischen Massnahmen zur Erreichung der Schutzziele geeignet und effektiv sind.
- Gewährleisten, dass ein Prozess besteht, der sicherstellt, dass das öffentliche Organ periodisch überprüft, ob die ergriffenen Sicherheitsmassnahmen pro Datenbearbeitung weiterhin geeignet und effektiv sind.
- Gewährleisten, dass innerhalb des öffentlichen Organs bekannt ist, dass die Hauptabteilung Informatik und die Fachstelle Datenschutz bei Unterstützungsbedarf beigezogen werden sollen.

✓ Die Datensicherheit von Informatikmitteln, insbesondere die zu ergreifenden technischen und organisatorischen Massnahmen zur Reduktion der ermittelten Risiken, werden zusammen mit dem Chief Information Security Officer (CISO) der Hauptabteilung Informatik geprüft. Die angemessenen technischen und organisatorischen Massnahmen werden umgesetzt.

✓ Die Datensicherheit der Datenbearbeitungen, welche sich ausserhalb eines Informatikmittels abspielen (Datensicherheit der Gesamtorganisation, der internen Prozesse etc.), insbesondere die zu ergreifenden organisatorischen Massnahmen, werden mit der Fachstelle Datenschutz geprüft. Die ermittelten Massnahmen werden umgesetzt.

### c. Beschaffung von Personendaten

#### i. Quellen

- Gewährleisten, dass Personendaten bei den betroffenen Personen selbst beschafft werden.
- Gewährleisten, dass Personendaten nur ausnahmsweise / im Einzelfall gemäss den gesetzlichen Voraussetzungen bei anderen öffentlichen Organen oder Dritten beschafft werden. Die gesetzlichen Voraussetzungen sind:
  - eine spezialgesetzliche Bestimmung erlaubt es oder
  - eine direkte Erhebung bei der betroffenen Person ist nicht möglich oder unverhältnismässig oder
  - die Natur der öffentlichen Aufgabe erfordert es, sprich wenn die Datenerhebung bei der betroffenen Person selbst die Erfüllung einer öffentlichen Aufgabe verunmöglichen würde.
- Gewährleisten, dass bei der Beschaffung von Personendaten bei anderen öffentlichen Organen das Amtsgeheimnis gewahrt wird bzw. die Voraussetzungen der zulässigen Amtshilfe erfüllt werden.

✓ Es sind interne Weisungen und/oder Merkblätter zu erstellen, worin die Prozesse der Datenbeschaffung gemäss den rechtlichen Vorschriften (Art. 20 IDAG) definiert sind. Es wird sichergestellt, dass die Datenbeschaffung gemäss den rechtlichen Vorschriften erfolgt.

✓ Gegebenenfalls weitere Massnahmen.

#### ii. Informationspflichten

- Gewährleisten, dass bei der Beschaffung von Personendaten die Betroffenen vom öffentlichen Organ angemessen darüber informiert werden, auch wenn die Personendaten bei einem anderen öffentlichen Organ oder Dritten erhoben werden.
- Gewährleisten, dass bekannt ist, wann die Informationspflicht entfällt oder eingeschränkt, aufgeschoben oder unterlassen werden kann.
- Gewährleisten, dass zur Ausgestaltung der Informationspflichten das entsprechende Merkblatt konsultiert wird.

- ✓ Informationen werden in präziser, verständlicher und leicht zugänglicher Form mitgeteilt. Bei der Wahl der Form ist sicherzustellen, dass die betroffene Person die wichtigsten Informationen stets auf der ersten Kommunikationsstufe erhält (bspw. Einsatz von Cookie-Bannern sofern über eine Webseite Personendaten erhoben werden).
- ✓ Das öffentliche Organ stützt seine Datenbeschaffungen auf eine hinreichende Rechtsgrundlage oder auf eine rechtsgenügliche Einwilligung ab (siehe oben «Rechtmässigkeit»).
- ✓ Das öffentliche Organ erstellt ein Verzeichnis der einzelnen Datenbearbeitungen, worin die bearbeiteten Personendaten und deren Kategorie, die Rechtsgrundlage und der Zweck der Bearbeitung, die Empfängerinnen und Empfänger oder die Kategorie der Empfängerinnen und Empfänger aufgeführt sind. Das Verzeichnis dient als Grundlage für die Information gem. Art. 21 IDAG. Zusätzlich dient es dem öffentlichen Organ als Information gegen innen, um den Umfang der zulässigen Bearbeitung kommunizieren zu können (Weisungen an Mitarbeitende).
- ✓ Werden besonders schützenswerte Personendaten beschafft, muss der Zweck der einzelnen Bearbeitungen aus der Rechtsgrundlage ersichtlich sein.
- ✓ Gegebenenfalls weitere Massnahmen.

### d. Bekanntgabe von Personendaten

#### i. Bekanntgabe an öffentliche Organe

- Gewährleisten, dass Personendaten an andere inner- oder ausserkantonale öffentliche Organe nur bekanntgegeben werden, wenn die Bekanntgabe rechtmässig und verhältnismässig erfolgt, oder aber die Bekanntgabe zwecks Erfüllung einer Aufsichtstätigkeit erforderlich ist.
  - ✓ Zudem ist sicherzustellen, dass keine überwiegenden öffentlichen oder privaten Interessen der Bekanntgabe entgegenstehen und dass spezialgesetzliche Geheimhaltungsvorschriften, insbesondere das Amtsgeheimnis, und besondere Datenschutzvorschriften gewahrt werden (dazu auch nachfolgend «2. d. v. Einschränkung der Bekanntgabe»).
  - ✓ Gegebenenfalls weitere Massnahmen.

#### ii. Bekanntgabe an Private

- Gewährleisten, dass Personendaten an Dritte nur bekannt gegeben werden, wenn eine Voraussetzung gemäss Art. 23 Abs. 1 Bst. a. – f. IDAG erfüllt ist (und gegebenenfalls die Voraussetzungen gemäss Art. 16 Abs. 1 – 3 VIDAG erfüllt sind).
- Gewährleisten, dass auch Stammdaten zur Erfüllung eines wirtschaftlichen Zwecks nur bekannt gegeben werden dürfen, sofern dies in einer Grundlage im Gesetz vorgesehen ist.
  - ✓ Zudem ist sicherzustellen, dass keine überwiegenden öffentlichen oder privaten Interessen der Bekanntgabe entgegenstehen und dass spezialgesetzliche Geheimhaltungsvorschriften, insbesondere das Amtsgeheimnis, und besondere Datenschutzvorschriften gewahrt werden (dazu auch nachfolgend «2. d. v. Einschränkung der Bekanntgabe»).
  - ✓ Gegebenenfalls weitere Massnahmen.

#### iii. Bekanntgabe ins Ausland

- Gewährleisten, dass Personendaten grundsätzlich nur in ein Empfängerland mit angemessenem Datenschutz bekanntgegeben werden, sprich sofern der Bund festgestellt hat, dass die Gesetzgebung des Empfängerlandes oder das internationale Organ einen angemessenen Schutz gewährleistet (Länderliste).
  - ✓ Die Länderliste wurde konsultiert. Befindet sich der Empfängerstaat nicht auf der Liste (fehlender Angemessenheitsbeschluss), ist zu prüfen, ob eine Voraussetzung für die einzelfallweise Bekanntgabe gemäss Art. 24 Abs. 2 Bst. a. – e. IDAG vorliegt.
  - ✓ Befindet sich der Empfängerstaat der Personendaten nicht auf der Länderliste des Bundes und handelt es sich nicht ausschliesslich um eine einzelfallweise Bekanntgabe von Personendaten – sprich soll eine grössere Anzahl bzw. Menge an Personendaten, u.U. auch wiederkehrende in einen entsprechenden Staat bekanntgegeben werden – so sind die vom Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) bestimmten Voraussetzungen zu erfüllen (Art. 17 Abs. 1 Bst. b. i.V.m. Abs. 2 VIDAG). Bei diesen Voraussetzungen handelt es sich insbesondere um geeignete Garantien zum Erreichen eines angemessenen Schutzniveaus (dazu siehe insbesondere auch die vom EDÖB anerkannten Standardvertragsklauseln und Musterverträge: Die Übermittlung von

Personendaten in ein Land ohne angemessenes Datenschutzniveau gestützt auf anerkannte Standardvertragsklauseln und Musterverträge (PDF, 279 kB, 10.05.2023).
- ✓ Immer ist sicherzustellen, dass keine überwiegenden öffentlichen oder privaten Interessen der Bekanntgabe entgegenstehen und dass spezialgesetzliche Geheimhaltungsvorschriften, insbesondere das Amtsgeheimnis, und besondere Datenschutzvorschriften gewahrt werden (dazu auch nachfolgend «2. d. v. Einschränkung der Bekanntgabe»).
- ✓ Gegebenenfalls weitere Massnahmen.

#### iv. Bekanntgabe in eine Cloud

- Gewährleisten, dass vor Bekanntgabe von Personendaten in eine Cloud das Merkblatt Cloud-spezifische Risiken und Massnahmen der Konferenz der schweizerischen Datenschutzbeauftragten konsultiert wird und die darin enthaltenen risikominierenden Massnahmen noch vor der Bekanntgabe umgesetzt werden.
- Gewährleisten, dass die Vorgaben aus dem Merkblatt für jegliche Cloud-Services gelten, unabhängig davon, ob Personendaten an einen Privaten oder ins Ausland bekanntgegeben werden sollen.
- Gewährleisten, dass die fünf Risikobereiche aus dem Merkblatt berücksichtigt und hierzu wirksame Massnahmen zur Risikoreduktion ergriffen wurden. Können die Risiken nicht hinreichend wirksam reduziert werden, ist auf die Bekanntgabe in die Cloud zu verzichten.
  - ✓ Risikobereich 1: Wirksame und rechtsgenügliche Vertragsgestaltung (Merkblatt Ziffer 2.1; dazu auch nachfolgend «2. e. ii. Datenbearbeitung im Auftrag»;
  - ✓ Risikobereich 2: Ermittlung der Orte der Datenbearbeitungen einschliesslich Ermittlung potentieller ausländische Behördenzugriffe (Merkblatt Ziffer 2.2; dazu auch oben «2. d. iii. Bekanntgabe ins Ausland»);
  - ✓ Risikobereich 3: Es ist sicherzustellen, dass keine überwiegenden öffentlichen oder privaten Interessen der Bekanntgabe entgegenstehen und dass spezialgesetzliche Geheimhaltungsvorschriften, insbesondere das Amtsgeheimnis, und besondere Datenschutzvorschriften gewahrt werden. Zudem ist darauf zu achten, dass es zu einer wirksamen Verschlüsselung kommt (Merkblatt Ziffer 2.3; dazu auch nachfolgend «2. d. v. Einschränkung der Bekanntgabe»);
  - ✓ Risikobereich 4: Umgang mit Daten über die Nutzerinnen und Nutzer der Cloud-Dienste: generierte Rand-, Telemetrie- oder Protokollierungsdaten (Merkblatt Ziffer 2.4);
  - ✓ Risikobereich 5: Übersicht der Unterauftragsverhältnisse (Merkblatt Ziffer 2.5).
  - ✓ Gegebenenfalls weitere Massnahmen.

#### v. Einschränkung der Bekanntgabe

- Gewährleisten, dass vor jeder Datenbekanntgabe geprüft wird, ob überwiegende öffentliche oder private Interesse dazu führen, dass die Bekanntgabe eingeschränkt, zeitlich aufgeschoben oder gar verweigert werden muss.
- Gewährleisten, dass spezialgesetzliche Geheimhaltungsvorschriften, insbesondere das Amtsgeheimnis und besondere Datenschutzvorschriften bekannt sind und dass bei Vorliegen dieser Vorschriften die Anforderungen an den Geheimnisschutz gewahrt werden.
- Gewährleisten, dass den Mitarbeitenden des öffentlichen Organs der Umgang mit Geheimhaltungs- und Datenschutzvorschriften einerseits, und der Umgang mit der einzelfallweisen zulässigen Amtshilfe andererseits bekannt sind.
  - ✓ Es sind interne Weisungen und/oder Merkblätter zu erstellen, die die Mitarbeitenden befähigen, die Einschränkungen zur Datenbekanntgabe nachzuvollziehen und die rechtlichen Vorgaben umzusetzen.
  - ✓ Gegebenenfalls weitere Massnahmen.

### e. Bearbeitung von Personendaten zu besonderen Zwecken

#### i. Datenbearbeitung für nicht personenbezogene Zwecke

- Gewährleisten, dass die Voraussetzungen für die Bearbeitung von Personendaten zu nicht personenbezogene Zwecke, wie insbesondere für die Wissenschaft, Forschung, Planung und Statistik, bekannt sind (Art. 26 Abs. 1 Bst. a. – e. IDAG).
- Gewährleisten, dass solche Daten nicht für andere Zwecke bearbeitet werden und insbesondere die Daten vernichtet, anonymisiert oder pseudonymisiert werden, sobald es der Zweck des Bearbeitens erlaubt.

- ✓ Es sind interne Weisungen und/oder Merkblätter zu erstellen, die die Mitarbeitenden befähigen, die rechtlichen Vorgaben zu Datenbearbeitungen für nicht personenbezogene Zwecke umzusetzen.
- ✓ Mögliche Massnahmen zur Anonymisierung und Pseudonymisierung werden berücksichtigt (dazu auch vorne «2. b. ii. Verhältnismässigkeit»).
- ✓ Gegebenenfalls weitere Massnahmen.

#### ii. Datenbearbeitung im Auftrag

- Gewährleisten, dass die Voraussetzungen umgesetzt werden, nach welchen andere öffentliche Organe oder Private Personendaten des verantwortlichen öffentlichen Organs bearbeiten dürfen (Art. 27 Abs. 1 Bst. a. – d., Abs. 2 und Abs. 3 IDAG).
- Gewährleisten, dass der Auftragnehmer unter besonderer Berücksichtigung der Einhaltung der Datensicherheit und des Datenschutzes sorgfältig ausgewählt wird.

- ✓ Dem Auftrag stehen keine gesetzlichen oder vertraglichen Regelungen (Geheimhaltungspflichten) entgegen.
- ✓ Für den Auftrag besteht eine schriftliche Regelung: Sicherstellen, dass noch vor Bekanntgabe der Personendaten ein Auftragsdatenbearbeitungsvertrag nach den Mindestvorgaben gemäss Art. 18 Abs. 2 Bst. a. – k. VIDAG unterzeichnet wurde und die Verpflichtungen nach Möglichkeiten mit einer Konventionalstrafe gesichert werden:
  - Gegenstand und Dauer des Auftrags;
  - Umfang, Art und Zweck der vorgesehenen Datenbearbeitung, die Art der Daten und der Kreis der betroffenen Personen;
  - die zur Einhaltung der Datensicherheit zu treffenden technischen und organisatorischen Massnahmen, deren Kontrolle und Dokumentation (oben «2. b. iv. Datensicherheit»);
  - Durchsetzung von Rechten und Ansprüche betroffener Personen (nachfolgend «2. g. Rechte der Betroffenen»);
  - Verpflichtung zur Verschwiegenheit und Überbindung dieser Pflicht auf alle Datenbearbeitenden;
  - allfällige Berechtigung zur Vergabe von Unteraufträgen und damit einhergehende Verpflichtungen;
  - Kontrollrechte des auftraggebenden öffentlichen Organs und seiner Aufsichtsbehörden sowie entsprechende Duldungs- und Mitwirkungspflichten des Auftragsdatenbearbeiters;
  - Mitteilungspflicht des Auftragsdatenbearbeiters bei Verletzungen der Datensicherheit (nachfolgend «2. f. iii. Meldung von Verletzungen der Datensicherheit»);
  - Weisungsbefugnisse des auftraggebenden öffentlichen Organs;
  - die Rückgabe überlassener Daten und Datenträger sowie die Vernichtung oder Löschung von beim Auftragsdatenbearbeiter gespeicherter Daten (oben «2. b. ii. Verhältnismässigkeit»);
  - anwendbares Recht und Gerichtsstand.
- ✓ Der Auftrag ist klar umschrieben. Die Verantwortlichkeiten sind klar definiert.
- ✓ Durch geeignete technischen, organisatorischen und rechtliche Massnahmen ist sichergestellt, dass die Personendaten durch den Auftragnehmer nur so bearbeitet werden, wie es ihm selbst erlaubt ist.
- ✓ Die Weiterübertragung durch den Auftragnehmer an Unterauftragnehmer bedarf der schriftlichen Zustimmung des auftraggebenden öffentlichen Organs.
- ✓ Ist eine Datenbekanntgabe ins Ausland beabsichtigt, so sind die zusätzlichen Massnahmen analog zu «2. d. iii. Bekanntgabe ins Ausland» umzusetzen.
- ✓ Periodische Kontrollen, um zu gewährleisten, dass die vertraglichen Vorgaben durch den Auftragnehmer erfüllt werden. Falls nötig sind Korrekturen einzuleiten und (angepasste) Weisungen zu erteilen. Werden (erhebliche) Verstösse gegen datenschutzrechtliche Vorschriften festgestellt, soll die Kündigung des Vertragsverhältnisses geprüft werden.
- ✓ Nebst dem Auftragsdatenbearbeitungsvertrag sind die AGB SIK und weitere erforderliche Verträge (bspw. Dienstleistungs- und Softwarevertrag) zu prüfen und zu unterzeichnen.
- ✓ Gegebenenfalls weitere Massnahmen.

#### iii. Überwachung mit optisch-elektronischen Anlagen

- Gewährleisten, dass sofern der Einsatz von Bildaufzeichnungs- und Bildübermittlungsgeräten (Videoüberwachung) beabsichtigt wird, die Voraussetzungen zur Überwachung vor deren Einsatz erfüllt sind (Art. 28 Abs. 1 – 4 IDAG und Art. 19 Abs. 1 IDAG).

- ✓ Es ist mindestens sicherzustellen, dass:

- die Überwachung ausschliesslich zur Wahrung des Hausrechts von öffentlich (zugänglichen) Gebäuden und den entsprechenden Gebäudearealen, insbesondere zum Schutz von Personen und Sachen vor Übergriffen sowie zur Verfolgung und Ahndung von solchen, eingesetzt wird;
- die Fachstelle Datenschutz vorgängig über die beabsichtigte Überwachung informiert ist;
- am überwachten Ort in geeigneter Weise auf die Überwachung und das verantwortliche öffentliche Organ hingewiesen wird;
- die unwiderrufliche Vernichtung der Bilddateien nach einer Woche sichergestellt ist, sofern sie nicht zu Beweis- und Sicherungszwecken benötigt werden;
- die Überwachung sachlich, räumlich und zeitlich auf das mögliche Mindestmass beschränkt wird (Verhältnismässigkeit);
- die Datensicherheit der Bilddateien sichergestellt ist (dazu auch vorne «2. b. iv. Datensicherheit»).

✓ Gegebenenfalls weitere Massnahmen.

#### iv. Datenbearbeitung zu Testzwecken

- Gewährleisten, dass bekannt ist, unter welchen Voraussetzungen Personendaten zu Testzwecken bearbeitet werden dürfen (Art. 29 IDAG und Art. 20 VIDAG).

✓ Soll eine Datenbearbeitung zu Testzwecken erfolgen, so sind die rechtlichen Vorschriften hierzu bekannt und sie werden umgesetzt.
✓ Gegebenenfalls weitere Massnahmen.

### f. Verantwortlichkeiten für die Durchsetzung des Datenschutzes

#### i. Verantwortliches öffentliches Organ

- Gewährleisten, dass das öffentliche Organ, welches Personendaten erhebt, speichert oder sonst wie bearbeitet, sich bewusst ist, dass es verantwortliches öffentliches Organ ist.
- Gewährleisten, dass das verantwortliche öffentliche Organ sich bewusst ist, dass es die Verantwortung für den Datenschutz und die Datensicherheit trägt und diese Verantwortung nicht übertragen kann.
- Gewährleisten, dass das verantwortliche öffentliche Organ seine Pflicht wahrnimmt, den Nachweis zu erbringen, dass der Datenschutz eingehalten wird.

✓ Der Datenschutznachweis wird mindestens alle fünf Jahre wie folgt erbracht:

1. Der Datenschutznachweis über Informatikmittel, die eingeführt oder erweitert werden erfolgt anhand der Datenschutz-Folgenabschätzung und gegebenenfalls der Vorab-Konsultation (direkt nachfolgend «2. f. ii. Datenschutz-Folgenabschätzung und Vorab-Konsultation»). Für alle Informatikmittel sollen die Vorgaben nach «2. b. iv. Datensicherheit» erfüllt werden.
2. Der Datenschutznachweis über die Datenbearbeitung ausserhalb eingesetzter Informatikmittel erfolgt gemäss den in diesem Merkblatt enthaltenen datenschutzrechtlichen Vorgaben. Ausgenommen davon sind die Vorgaben «2. b. iv. Datensicherheit», welche sich auf die Datenbearbeitung mittels Informatikmittel beziehen.

Alternativ kann der Datenschutznachweis auch durch Zertifizierung erfolgen. Hierzu sind die Vorgaben des Bundes zu konsultieren.

✓ Gegebenenfalls weitere Massnahmen.

#### ii. Datenschutz-Folgenabschätzung und Vorab-Konsultation

- Gewährleisten, dass bei Einführung oder Erweiterung eines Informatikmittels durch das verantwortliche öffentliche Organ die erforderliche Datenschutz-Folgenabschätzung durchgeführt wird (Art. 33 IDAG, Art. 23 und 24 VIDAG).
- Gewährleisten, dass bekannt ist, wann eine beabsichtigte Datenbearbeitung zur Vorab-Konsultation der Fachstelle Datenschutz vorgelegt werden muss.

✓ Das verantwortliche öffentliche Organ berücksichtigt bei Einführung oder Erweiterung eines Informatikmittels das Merkblatt und Formular zur Datenschutz-Folgenabschätzung, um überprüfen zu können, ob eine Datenschutz-Folgenabschätzung und eine Vorab-Konsultation erforderlich sind. Das Merkblatt wird sodann konsultiert, um die Datenschutz-Folgenabschätzung möglichst selbständig durchführen zu können.
✓ Gegebenenfalls weitere Massnahmen.

#### iii. Meldung von Verletzungen der Datensicherheit

- ✓ Gewährleisten, dass bei einer Verletzung der Datensicherheit das Merkblatt und Formular zur Meldung von Verletzungen der Datensicherheit beigezogen und die darin vorgegebenen Prozesse eingehalten werden.
- ✓ Gegebenenfalls weitere Massnahmen.

### g. Rechte der Betroffenen

#### i. Recht auf Zugang zu eigenen Personendaten

- Gewährleisten, dass den Mitarbeitenden des öffentlichen Organs bewusst ist, dass jede Person das Recht hat vom verantwortlichen öffentlichen Organ Informationen darüber zu verlangen, ob und wenn ja, welche Personendaten über sie bearbeitet werden (Art. 21 IDAG).
- Gewährleisten, dass der gesuchstellenden Person die gesetzlich vorgeschriebenen Angaben mitgeteilt werden, nämlich mindestens:
  - die Identität und die Kontaktdaten des verantwortlichen öffentlichen Organs;
  - die bearbeiteten Personendaten und deren Kategorie;
  - die Rechtsgrundlage und den Zweck der Bearbeitung;
  - die Empfängerinnen und Empfänger oder die Kategorie der Empfängerinnen und Empfänger, falls die Daten weitergegeben werden;
  - Herkunft der Personendaten;
  - Aufbewahrungsdauer der Personendaten.
- Gewährleisten, dass bekannt ist, wann das Zugangsrecht ausgeschlossen ist, eingeschränkt, aufgeschoben oder verweigert werden kann (insbesondere Art. 36 Abs. 4 und Art. 37 IDAG).

#### ii. Recht bei widerrechtlicher Datenbearbeitung

- Gewährleisten, dass sofern eine widerrechtliche Datenbearbeitung festgestellt wurde, den Mitarbeitenden des öffentlichen Organs die Rechte der betroffenen Personen bekannt sind und dass es:
  - widerrechtliches Bearbeiten von Personendaten unterlässt;
  - Personendaten, die widerrechtlich bearbeitet worden sind, vernichtet oder löscht;
  - die Folgen eines widerrechtlichen Bearbeitens beseitigt;
  - die Widerrechtlichkeit des Bearbeitens feststellt und/oder
  - den Entscheid Dritten mitteilt oder veröffentlicht, wenn sie ein schutzwürdiges Interesse hat.

#### iii. Berichtigungsrecht

Gewährleisten, dass insbesondere auch das Berichtigungsrecht bei unrichtig geführten Personendaten wirksam und gemäss den datenschutzrechtlichen Vorgaben (Art. 39 IDAG) umgesetzt wird.

#### iv. Recht auf Datensperrung

Gewährleisten, dass das Recht auf Datensperrung wirksam und gemäss den datenschutzrechtlichen Vorgaben (Art. 40 IDAG) umgesetzt wird.

#### v. Zugang zu Daten verstorbener Personen

Gewährleisten, dass das Recht auf Zugang zu Daten verstorbener Personen wirksam und gemäss den datenschutzrechtlichen Vorgaben (Art. 41 IDAG) umgesetzt wird.

#### vi. Formelle Anforderungen im Rahmen der Gesuchstellung

- Gewährleisten, dass die Ansprüche mündlich oder schriftlich geltend gemacht werden können.
- Gewährleisten, dass die Rechte auf Mitteilung und Anhörung gewährleistet werden (Art. 50 IDAG).
- Gewährleisten, dass auf Verlangen innert 30 Tagen nach Mitteilung gemäss Art. 50 Abs. 1 und 3 IDAG ein anfechtbarer Entscheid erlassen wird.
- Gewährleisten, dass die Formen der Zugangsgewährung eingehalten werden (Art. 52 IDAG).

#### vii. Kosten und Gebühren

- Gewährleisten, dass für die Geltendmachung der Rechte keine Kosten erhoben werden.
- Gewährleisten, dass sofern eine Gebühr erhoben wird, diese angemessen und gemäss den rechtlichen Vorgaben erhoben wird (Art. 54 Abs. 2 und 3 IDAG, Art. 46 – 48 VIDAG).

- ✓ Das für den Informationsbestand verantwortliche öffentliche Organ hat die Instrumente (Gesuchformulare) und Prozesse zur Behandlung der Gesuche definiert.
- ✓ Dabei wird sichergestellt, dass die gesetzlich vorgeschriebenen Angaben erteilt werden. Hierzu erstellt das öffentliche Organ ein Verzeichnis der einzelnen Datenbearbeitungen, worin die bearbeiteten Personendaten und deren Kategorie, die Rechtsgrundlage und der Zweck der Bearbeitung, die Empfängerinnen und Empfänger oder die Kategorie der Empfängerinnen und Empfänger sowie die Herkunft und die Aufbewahrungsdauer der Personendaten aufgeführt sind. Das Verzeichnis dient als Grundlage für einen schnellen Zugang zu den eigenen Personendaten gem. Art. 36 IDAG.
- ✓ Darüber hinaus ist sichergestellt, dass das öffentliche Organ den gesetzlichen Ansprüchen bei widerrechtlicher Datenbearbeitung, im Rahmen der Berichtigung und der Datensperre nachkommt. Unrichtige Personendaten werden durch das öffentliche Organ berichtigt oder vernichtet. Widerrechtliche Datenbearbeitungen werden festgestellt, unterlassen und die Folgen beseitigt.
- ✓ Die formellen Anforderungen sind in den Prozessen ebenfalls beschrieben, so dass die Form der Eingaben (mündlich und schriftlich) und das Recht auf Gehör und Mitteilung eingehalten werden. Zudem wird sichergestellt, dass innert angemessener Frist über das Gesuch befunden und ggf. auf Verlangen innert 30 Tagen ein anfechtbarer Entscheid erlassen wird.
- ✓ Kosten und Gebühren werden im Rahmen des Rechts erhoben; in den Prozessen ist der Umgang mit Kosten und Gebühren definiert.
- ✓ Gegebenenfalls weitere Massnahmen.

### h. Aufsichts- und Kontrollorgan

- Gewährleisten, dass das Bewusstsein vorhanden ist, dass die Fachstelle Datenschutz die Anwendung der Vorschriften über den Datenschutz beaufsichtigt und dabei fachlich selbstständig, unabhängig und bei der Erfüllung ihrer Aufgaben an keine Weisungen gebunden ist.
- Gewährleisten, dass die rechtlichen Aufgaben der Fachstelle Datenschutz und ihre rechtlichen Befugnisse bekannt sind (Art. 57 und 58 IDAG, Art. 29 – 31 VIDAG).

### i. Straf- und vermögensrechtliche Verantwortlichkeit

- Bewusstsein darüber, dass Verstösse gegen Datenschutzvorschriften strafrechtliche Konsequenzen nach sich ziehen können.
- Bewusstsein darüber, dass Verstösse gegen Datenschutzvorschriften Schadenersatz- und Genugtuungsansprüche gemäss dem Staatshaftungsgesetz zur Folge haben können.

### j. Projektmanagement

- Die HERMES-Projektmanagementmethode ist bekannt. Das öffentliche Organ weiss, welche Informationen der Methode für eigene Projekte von Relevanz sind. Insbesondere orientiert es sich aber an den einzelnen Phasen und Rollen (Verantwortlichkeiten), soweit diese für ein konkretes Projekt geeignet sind.

---

## 3. Umsetzung der erforderlichen Massnahmen und Datenschutzinstrumente (Umsetzung des dokumentierten Soll-Zustands)

Nachdem die Liste (oben «**a. Begriffe und Einordnung**» ***bis und mit*** «**2. j. Projektmanagement**») durchgearbeitet und die Dokumentation erfolgt ist, werden in dieser Phase die erforderlichen Massnahmen bzw. die erforderlichen Datenschutzinstrumente durch das verantwortliche öffentliche Organ umgesetzt bzw. produziert. Der dokumentierte Soll-Zustand wird in dieser Phase also implementiert.

**Beispiel 1**: Es fehlt an der rechtlichen Grundlage zur Bearbeitung der in Frage stehenden Personendaten. Das Formular zur rechtsgenüglichen Einwilligung in die Bearbeitung von Personendaten wird erstellt, so dass es einzelfallweise eingesetzt werden kann.
**Beispiel 2**: Das öffentliche Organ muss regelmässig Informatikmittel neu beschaffen oder erweitern. Hierbei werden des Öfteren auch Personendaten durch Dritte bearbeitet. Es betraut deshalb eine Person, die bei den Beschaffungen projektverantwortlich ist und die Datenschutz-Folgenabschätzungen durchführt. Zudem lässt es einen Entwurf des Auftragsdatenbearbeitungsvertrags gemäss den Mindestvoraussetzungen von Art. 18 Abs. 2 Bst. a. – k. VIDAG erstellen, den es jeweils an die konkreten Begebenheiten anpassen kann.
**Beispiel 3**: Das öffentliche Organ hält einen Teil der Personendaten, für die es verantwortlich ist, in einer Cloud. Da ihm nach Bekanntgabe der Daten in die Cloud bewusst wird, dass das Vorgehen Datenschutz- und weitere Rechtsrisiken mit sich bringen könnte und die Cloud-Nutzung darüber hinaus nicht notwendig ist, weil es gleichgeeignete und datensicherere Alternative gibt, entscheidet es sich, die Daten binnen zweier Monate aus der Cloud auszuführen und auf einem internen Server zu halten.

## 4. Dokumentation des Ist-Zustands

Nachdem das verantwortliche öffentliche Organ die Massnahmen umgesetzt und die Datenschutzinstrumente hergestellt hat und diese zum Einsatz kommen, ist der Ist-Zustand prüffähig zu dokumentieren. Hierbei ist darauf zu achten, dass prüfrelevante Unterlagen, wie Verträge, Protokolle etc. über einen angemessenen Zeitraum ebenfalls mitdokumentiert werden.

Zur Dokumentation steht dem öffentlichen Organ eine **Vorlage für die Dokumentation des Ist-Zustands** zur Verfügung (Webseite Fachstelle Datenschutz). Es ist dem öffentlichen Organ aber selbst überlassen, ob es den Soll-Zustand anderweitig dokumentieren will.

**Anwendungsbeispiel Dokumentation Ist-Zustand:**

| DATENBEARBEITUNG | RECHTLICHES KRITERIUM | UMGESETZTE MASSNAHMEN UND INSTRUMENTE |
|---|---|---|
| Erheben und kontrollieren von Gesundheitsdaten zwecks schulmedizinischen Untersuchungen | b. i. Rechtmässigkeit (notwendige Einwilligung, da es sowohl an einer Grundlage im Gesetz, wie auch einer im Gesetz klar umschriebenen Aufgabe fehlt) | b. i.: Die notwendige Information zur rechtsgenüglichen Einwilligung wurde erstellt und in Briefform an die Erziehungsberechtigten übergeben. Gestützt auf diese Information entscheiden die Erziehungsberechtigten frei, ob sie die Gesundheitsdaten an den schulmedizinischen Dienst bekanntgeben wollen oder die Untersuchung durch den Hausarzt vornehmen lassen wollen. |
| Beschaffung einer Vielzahl von Informatikmitteln, darunter eines, welches das Schwimmbad der Gemeinde Glarus mit künstlicher «Intelligenz» ausstatten soll, um Ertrinkende ermitteln zu können | j. Projektmanagement: Organisation einer projektverantwortlichen Person;<br>f. ii. Datenschutz-Folgenabschätzung: Spezialisierte Durchführung;<br>e. ii. Datenbearbeitung im Auftrag: Vertragsmanagement. | j.: Die Gemeinde hat sich entschieden, aufgrund einer Vielzahl von Beschaffungen eine Projektleiterin ICT einzustellen;<br>f. ii.: binnen sieben Monaten hat die Projektverantwortliche bereits drei Datenschutz-Folgenabschätzungen durchgeführt. Die Gemeinde ist im Umgang mit diesem Datenschutzinstrument inzwischen vertraut, weshalb die Beschaffung effizienter abläuft. Die Beschaffung der künstlichen «Intelligenz» zwecks Rettung von Ertrinkenden wurde jedoch eingestellt, da potentiell die Persönlichkeitsrechte einer Vielzahl von Badegästen verletzt worden wären; es wurde bekannt, dass die Bilddateien der Badegäste in eine Cloud bekanntgegeben und zu Trainigszwecken in nicht anonymisierter Form weiterbearbeitet worden wären.<br>e. ii.: der Entwurf des Auftragsdatenbearbeitungsvertrags wurde durch die Projektverantwortliche in Zusammenarbeit mit dem Gemeindejuristen erstellt und vom kantonalen Datenschutzbeauftragten abgenommen. Für die zwei erfolgreich durchgeführten Beschaffungen wurde der Auftragsdatenbearbeitungsvertrag, zusammen mit den AGB SIK, und allenfalls weiteren erforderlichen Verträgen |

| | | |
|---|---|---|
| | | (bspw. Dienstleistungs- und Softwarevertrag), unterzeichnet. |
| Personaldienst hält Personendaten der Mitarbeitenden in einer Cloud | d. iv. Bekanntgabe in eine Cloud;<br>b. ii. Verhältnismässigkeit;<br>b. i. Rechtmässigkeit (fehlende Einwilligung);<br>d. v.: Einschränkung der Bekanntgabe | Nachdem in Erfahrung gebracht wurde, dass das Bekanntgeben von Mitarbeiterdaten in eine Cloud mit Datensicherheits- und weiteren Rechtsrisiken verbunden sein kann (allfällige Informationen, die der Geheimhaltung unterstehen; fehlende Einwilligung der Mitarbeitenden in Bekanntgabe in die Cloud; Cloud wurde von chinesischen Hackern unterwandert) wurde entschieden, die Personendaten aus der Cloud auszuführen und die Software OnPremise zu beziehen, so dass die Daten auf den behördlichen Servern gespeichert werden (fehlende zwingende Erforderlichkeit der Cloud-Nutzung und somit unverhältnismässige Datenbekanntgabe). |

## 5. Abgleich des Ist-Zustands mit dem Soll-Zustand – Beurteilungsergebnisse erstellen

Der ermittelte Soll-Zustand ist mit dem Ist-Zustand – also den tatsächlich umgesetzten Massnahmen und den zum Einsatz kommenden Instrumenten – abzugleichen. Hierzu können die dokumentierten Soll-Werte mit den tatsächlich umgesetzten Massnahmen abgeglichen werden. So kann festgestellt werden, welche Massnahmen und Instrumente erfolgreich umgesetzt worden sind und wo noch Handlungsbedarf bzw. Mängel bestehen; werden nicht alle ermittelten Massnahmen und Instrumente (Soll-Zustand) in hinreichender Form implementiert (Ist-Zustand), so bedeutet dies zugleich, dass das zugrundeliegende rechtliche Prüfkriterium nicht hinreichend erfüllt ist und datenschutzrechtliche Vorschriften ganz oder teilweise verletzt sind oder sein könnten.

Die Ergebnisse des Abgleichs sind sinnvollerweise in einem möglichst kurzen Bericht festzuhalten; die festgestellten Mängel, die der Abgleich ergeben hat, sind im Bericht möglichst so festzuhalten, dass daraus konkrete Verbesserungsvorschläge bzw. Handlungsanweisungen im Sinne von Ergänzungsmassnahmen, Anpassungen der Datenschutzinstrumente, Anpassungen der Prüfzyklen, etc. hergeleitet werden können.

## 6. Finalisieren des Datenschutznachweises gestützt auf den Beurteilungsergebnissen

Der Datenschutznachweis ist erbracht, wenn die Verbesserungsvorschläge bzw. Handlungsanweisungen innerhalb des öffentlichen Organs diskutiert und die tatsächlich geeigneten, erforderlichen und angemessenen Massnahmen implementiert und umgesetzt sind; der vormals ermittelte Ist-Zustand hat sich also in den wesentlichen Grundzügen dem Soll-Zustand angeglichen. Bestenfalls ermöglicht der Abgleich sogar eine Optimierung des ursprünglich ermittelten Soll-Zustands.

Zum erbringen des Datenschutznachweises gehört auch die nachvollziehbare Dokumentation der umgesetzten Handlungsanweisungen (Ergänzungsmassnahmen), bspw. durch ergänzen des Berichts (Ziffer 5.). Die Dokumentation soll so erfolgen, dass sie im Rahmen einer Datenschutzkontrolle gut nachvollziehbar ist.

## 7. Neuermitteln und –beurteilen – neuer Prüfzyklus

Wird der Datenschutznachweis durch das öffentliche Organ erneut erbracht, spätestens aber nach der Frist von fünf Jahren (Art. 22 Abs. 3 IDAG), ist in einem neuen Prüfzyklus das hier beschriebene Vorgehen (vorangehende Ziffern 1. – 6.) zu wiederholen. Die Wiederholung ist deshalb wichtig, da im Laufe der Zeit Datenbestände veralten, so dass Personendaten vernichtet oder aktualisiert werden müssen etc. Es ist deshalb notwendig, die eigenen Bearbeitungen von Personendaten wiederholden darauf zu überprüfen, ob die datenschutzrechtlichen Mindestanforderungen erfüllt werden.