Gesetz über den Datenschutz (DSchG)

vom 12.10.2023 (Fassung in Kraft getreten am 01.01.2024)

Der Grosse Rat des Kantons Freiburg

gestützt auf Artikel 12 Abs. 1 der Verfassung des Kantons Freiburg vom 16. Mai 2004 (KV);

nach Einsicht in die Botschaft 2023-CE-149 des Staatsrats vom 26. Juni 2023;

auf Antrag dieser Behörde,

beschliesst:

1 Allgemeine Bestimmungen

Art. 1 Zweck

[1] Dieses Gesetz bezweckt den Schutz der Grundrechte von Personen, deren Daten bearbeitet werden.

Art. 2 Persönlicher Geltungsbereich

[1] Das Gesetz gilt für folgende öffentliche Organe:

a) die Organe des Staates, der Gemeinden und der übrigen juristischen Personen des öffentlichen Rechts;

b) Privatpersonen und Organe privater Institutionen, soweit sie öffentlich-rechtliche Aufgaben erfüllen.

[2] Es gilt für anerkannte Kirchen, es sei denn, sie haben Datenschutzbestimmungen erlassen, die ein angemessenes Schutzniveau gewährleisten, und eine eigene Aufsichtsbehörde eingesetzt.

Art. 3 Sachlicher Geltungsbereich

[1] Dieses Gesetz gilt für jegliche Bearbeitung von Personendaten, die von einem öffentlichen Organ im Sinne von Artikel 2 ausgeführt wird.

[2] Ausgenommen sind:

a) die Bearbeitungen von Daten, die im Rahmen von laufenden Zivilverfahren, Strafverfahren und Verfahren der Verwaltungsjustizbehörden durchgeführt werden;

b) die Bearbeitungen von Daten, die dem ausschliesslich persönlichen Gebrauch der Person dienen, die sie durchführt;

c) die Bearbeitungen von Daten, die von einem öffentlichen Organ im wirtschaftlichen Wettbewerb mit Personen des Privatrechts durchgeführt werden.

Art. 4 Definitionen

[1] Die folgenden Ausdrücke bedeuten:

a) Personendaten: alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen;

b) betroffene Person: natürliche oder juristische Person, über die Daten bearbeitet werden;

c) besonders schützenswerte Personendaten:

   1. Daten zu den religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten;
   2. Daten zur Gesundheit, zur Intimsphäre oder zur Zugehörigkeit zu einer Rasse oder Ethnie;
   3. genetische Daten;
   4. biometrische Daten, mit denen eine natürliche Person eindeutig identifiziert wird;
   5. Daten zu Massnahmen der Sozialhilfe;
   6. Daten zu Betreibungen oder zu strafrechtlichen und administrativen Sanktionen.

d) Bearbeitung: jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere die Beschaffung, Speicherung, Aufbewahrung, Verwendung, Umarbeitung, Bekanntgabe, Verknüpfung, Auslagerung, Löschung, Archivierung und Vernichtung;

e) Abrufverfahren: ein automatisierter Datenbekanntgabemodus, bei dem die Empfängerin oder der Empfänger der Daten aufgrund einer Bewilligung des Verantwortlichen für die Bearbeitung selber und ohne vorherige Kontrolle über den Zeitpunkt und den Umfang der Bekanntgabe entscheidet;

f) Profiling: jede Art der automatisierten Verarbeitung von Personendaten, die darin besteht, dass diese Personendaten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser Person zu analysieren oder vorherzusagen;

g) Auslagerung: eine qualifizierte Form der Auftragsbearbeitung, welche die Nutzung von Computerressourcen beinhaltet, die über ein Kommunikationsnetz aus der Ferne zugänglich sind, um Daten zu speichern, zu bearbeiten und auszutauschen (Cloud Computing);

h) Verantwortlicher: öffentliches Organ, das allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung von Personendaten entscheidet;

i) Auftragsbearbeiter: private Person oder öffentliches Organ, die oder das im Auftrag des Verantwortlichen Personendaten bearbeitet;

j) Bearbeitungsregister: Onlineverzeichnis, in dem die von den öffentlichen Organen ausgeführten Bearbeitungstätigkeiten verzeichnet sind;

k) Verletzung der Sicherheit von Personendaten: jede Verletzung der Sicherheit, die dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden.

2 Grundsätze für die Bearbeitung von Personendaten

2.1 Allgemeine Bedingungen der Rechtmässigkeit der Bearbeitung

Art. 5 Gesetzliche Grundlage

[1] Das öffentliche Organ darf Personendaten nur dann bearbeiten, wenn es in einer gesetzlichen Bestimmung vorgesehen wird oder wenn die Erfüllung einer gesetzlichen Aufgabe dies erfordert.

[2] Besonders schützenswerte Personendaten dürfen nur bearbeitet werden, wenn:

a) es in einem Gesetz im formellen Sinn ausdrücklich vorgesehen wird oder

b) es für die Erfüllung einer Aufgabe, die in einem Gesetz im formellen Sinne klar definiert wird, unerlässlich ist und der Zweck des Bearbeitens keine besonderen Risiken für die Grundrechte der betroffenen Personen birgt.

[3] Profiling-Aktivitäten und die Bearbeitung von Personendaten, deren Zwecke oder Modalitäten ein hohes Risiko für die Grundrechte der betroffenen Personen bergen, dürfen nur durchgeführt werden, wenn es in einem Gesetz im formellen Sinne ausdrücklich vorgesehen wird.

[4] Ausnahmsweise ist keine gesetzliche Grundlage erforderlich, um Personendaten, einschliesslich besonders schützenswerte, zu bearbeiten, wenn die Bearbeitung nötig ist, um wesentliche Interessen der betroffenen Person oder einer oder eines Dritten zu wahren.

Art. 6 Einwilligung

[1] Ausser in den Fällen nach Artikel 5 kann die betroffene Person im Einzelfall in die Bearbeitung ihrer Personendaten einwilligen.

[2] Die betroffene Person willigt nur gültig ein, wenn sie ihren Willen frei ausdrückt und nachdem sie in angemessener Weise über den Zweck der Bearbeitung aufgeklärt wurde. Die Einwilligung muss ausdrücklich sein, wenn sie sich auf die Bearbeitung besonders schützenswerter Personendaten oder auf Profiling-Aktivitäten bezieht. Die Einwilligung wird jedoch vermutet, wenn die Person ihre Daten selbst frei zugänglich gemacht hat.

[3] Jede Bearbeitung von Daten, die nicht auf den Grundlagen nach Artikel 5 beruht, muss von einem sichtbaren und leicht verständlichen Hinweis auf ihren freiwilligen Charakter begleitet werden.

[4] Wenn sich die Bearbeitung auf die Einwilligung der betroffenen Person stützt, muss der Verantwortliche in der Lage sein, das Vorhandensein einer solchen Einwilligung zu beweisen.

[5] Die Einwilligung kann jederzeit ohne Angabe von Gründen widerrufen werden. Aus technischen Gründen kann aber für die tatsächliche Umsetzung der Widerrufung der Einwilligung eine vernünftige Frist nötig sein.

Art. 7 Zweckbindung

[1] Personendaten dürfen nur für eine bestimmte und erkennbare Verwendung beschafft werden. Sie dürfen später nur zu diesem Zweck oder zu einem Zweck, der mit diesem nach Treu und Glauben vereinbar ist, bearbeitet werden.

[2] Die Fälle, in denen die betroffene Person in eine Änderung der Zweckbestimmung eingewilligt hat, bleiben vorbehalten.

Art. 8 Verhältnismässigkeit

[1] Die Daten und die Art ihrer Bearbeitung müssen für den Zweck der Bearbeitung nötig, geeignet und nicht übertrieben sein.

Art. 9 Richtigkeit

[1] Das öffentliche Organ, das Personendaten bearbeitet, achtet darauf, dass diese richtig sind. Es ergreift alle geeigneten Massnahmen, um falsche oder für den Zweck, für den sie beschafft und bearbeitet werden, unvollständige Daten zu berichtigen, zu ergänzen, zu löschen oder zu vernichten.

Art. 10 Aufbewahrungsfrist

[1] Personendaten, die für den Zweck der Bearbeitung nicht mehr nötig sind, werden vernichtet oder anonymisiert. Die Bestimmungen über die Archivierung bleiben vorbehalten.

[2] Mit geeigneten Schutzmassnahmen können sie insofern für längere Zeit aufbewahrt werden, soweit sie gemäss Artikel 26 ausschliesslich zu Zwecken, die sich nicht auf die Person beziehen, dienen.

Art. 11 Besondere Sorgfaltspflicht

[1] Das öffentliche Organ, das besonders schützenswerte Personendaten bearbeitet, Profiling betreibt oder Daten zu Zwecken oder nach Modalitäten, die ein erhöhtes Risiko der Verletzung der Grundrechte mit sich bringt, bearbeitet, muss alle nötigen Massnahmen ergreifen, um dieses Risiko zu verringern.

2.2 Zusätzliche Bedingungen für bestimmte Formen der Bearbeitung

Art. 12 Beschaffen von Daten – Informationspflicht

[1] Der Verantwortliche informiert die betroffene Person angemessen über das Beschaffen von Personendaten.

[2] Wenn die Personendaten direkt bei der betroffenen Person beschafft werden, gibt ihr der Verantwortliche mindestens folgende Informationen:

a) der Verantwortliche und seine Kontaktdaten;

b) der Zweck der Bearbeitung;

c) allenfalls die Empfängerinnen und Empfänger oder die Kategorien von Empfängerinnen und Empfängern, denen die Personendaten bekanntgegeben werden;

d) Informationen dazu, ob das Beschaffen der Daten obligatorisch oder freiwillig ist.

[3] Werden Personendaten bei einem anderen Organ oder bei Dritten beschafft, so teilt der Verantwortliche der betroffenen Person so bald wie möglich, aber spätestens bei ihrer ersten Verwendung die Informationen nach Absatz 1 und die Art der beschafften Daten mit.

Art. 13 Beschaffen von Daten – Ausnahmen von der Informationspflicht

[1] Der Verantwortliche ist von der Informationspflicht entbunden, wenn:

a) die betroffene Person bereits über die entsprechenden Informationen verfügt;

b) es unmöglich ist, die betroffene Person zu informieren, oder die Information nur mit unverhältnismässigem Aufwand möglich ist;

c) die Daten aufgrund einer gesetzlichen Pflicht beschafft werden, ausser sie werden direkt bei der betroffenen Person beschafft.

[2] Ausserdem kann unter denselben Voraussetzungen und aus denselben Gründen wie denjenigen nach Artikel 29 Abs. 1 von der Informationspflicht abgewichen werden.

Art. 14 Bekanntgabe von Daten – Voraussetzung

[1] Personendaten dürfen nur dann systematisch bekanntgegeben, weitergegeben, verbreitet oder zugänglich gemacht werden, wenn es in einer gesetzlichen Bestimmung vorgesehen wird.

[2] Personendaten können im Einzelfall bekanntgegeben werden, wenn:

a) das Bekanntgeben für die Erfüllung der gesetzlichen Aufgaben des Verantwortlichen oder der Datenempfängerin oder des Datenempfängers unerlässlich ist;

b) die betroffene Person in das Bekanntgeben eingewilligt hat;

c) die private Person, welche die Daten anfordert, ein Interesse an der Bekanntgabe nachweisen kann, das dem Interesse der betroffenen Person an der Geheimhaltung der Daten vorgeht.

[3] Im Fall nach Absatz 2 Bst. c wird die betroffene Person vorher aufgefordert, Stellung zu nehmen, es sei denn, dies erweist sich als unmöglich oder ist mit unverhältnismässigem Aufwand verbunden.

[4] Der Zugang zu Personendaten über ein Abrufverfahren, namentlich ein Online-Zugriff, darf nur gewährt werden, wenn es in einer gesetzlichen Bestimmung vorgesehen wird.

Art. 15 Bekanntgabe von Daten – Zusätzliche Bedingungen für die grenzüberschreitende Bekanntgabe

[1] Die Übermittlung von Personendaten einer natürlichen Person an einen ausländischen Staat oder ein internationales Organ ist nur soweit zulässig, als in einem Entscheid des Bundesrats bezeugt wird, dass der Empfängerstaat oder das internationale Organ ein angemessenes Datenschutzniveau gewährleistet.

[2] Fehlt ein solcher Entscheid, so dürfen die Daten nur bekanntgegeben werden, wenn:

a) hinreichende, insbesondere vertragliche, vereinbarte, technische und/ oder organisatorische, Garantien einen angemessenen Schutz im Ausland gewährleisten;

b) die Bekanntgabe im Einzelfall entweder für die Wahrung eines überwiegenden öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich ist;

c) die betroffene Person im Einzelfall der Bekanntgabe ausdrücklich zugestimmt hat;

d) die Bearbeitung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags steht und es sich um Personendaten einer Vertragspartei handelt;

e) die Bekanntgabe im Einzelfall nötig ist, um das Leben oder die körperliche Integrität der betroffenen Person oder einer Drittperson zu schützen.

[3] Die oder der Öffentlichkeits- und Datenschutzbeauftragte (die oder der Beauftragte) wird vor der Bekanntgabe von Personendaten ins Ausland rechtzeitig über die Garantien nach Absatz 2 Bst. a informiert. Auf Anfrage kann sie oder er jederzeit Informationen erhalten, um zu überprüfen, ob eine Bekanntgabe von Daten ins Ausland den Anforderungen nach den Buchstaben b–e entspricht.

[4] Nicht als Bekanntgabe ins Ausland wird die einfache Veröffentlichung von Daten auf einer Website, die der Öffentlichkeit offensteht, betrachtet.

Art. 16 Bekanntgabe von Daten – Einschränkungen

[1] Die Bekanntgabe wird abgelehnt, eingeschränkt oder mit Auflagen verbunden, wenn:

a) ein überwiegendes öffentliches Interesse oder ein schutzwürdiges Interesse der betroffenen Person oder eines Dritten es gebietet, oder

b) eine gesetzliche Geheimhaltungspflicht oder eine besondere Datenschutzbestimmung dies erfordert.

Art. 17 Bekanntgabe von Daten – Vorbehalte

[1] Die Bekanntgabe von Personendaten, die bei der Einwohnerkontrolle oder im Kantonalen Bezugssystem eingetragen sind, wird in den entsprechenden Gesetzen geregelt.

[2] Die öffentliche Bekanntgabe von Personendaten richtet sich ausserdem nach der Gesetzgebung über die Information und den Zugang zu Dokumenten.

Art. 18 Auslagerung – Grundsätze

[1] Die Bearbeitung von Personendaten, einschliesslich besonders schützenswerter Daten, kann unter den in diesem Gesetz festgelegten Bedingungen ausgelagert werden.

[2] Die Daten müssen jederzeit auf dem Gebiet der Schweiz oder auf dem Gebiet eines Staates, der ein angemessenes Schutzniveau gewährleistet, bearbeitet werden.

[3] Wenn die Auslagerung eine Delegation von Aufgaben an Dritte im Sinne von Artikel 54 KV [1)] zur Folge hat, gelten die besonderen Anforderungen gemäss dieser Bestimmung.

[4] Einmal pro Legislaturperiode legt der Staatsrat im Rahmen seines Richtplans der Digitalisierung eine Bestandesaufnahme zur Auslagerung der Datenbearbeitung vor.

Art. 19 Auslagerung – Verantwortung

[1] Das öffentliche Organ, das eine Auslagerung vornimmt, bleibt für den Schutz der Personendaten, insbesondere für die Vertraulichkeit und die Dauerhaftigkeit ihrer Aufbewahrung und Nutzung, verantwortlich. Insbesondere:

a) ergreift es die Vorsichtsmassnahmen, die bei der Wahl des Auftragsbearbeiters, den Weisungen an diesen und der Aufsicht über diesen aufgrund der Umstände geboten sind;

b) gewährleistet es den Schutz und die Sicherheit der Daten und seiner eigenen Informationssysteme, indem es einen Vertrag abschliesst, der mindestens Folgendes beschreibt:

   1. den Gegenstand, die Art, den Zweck und die Dauer der Auslagerung;
   2. die betroffenen Datenkategorien;
   3. die Pflichten und die Rechte jeder Partei;
   4. die Rechte und die Möglichkeiten der Kontrolle über den Auftragsbearbeiter;
   5. das an den Auftragsbearbeiter gerichtete Verbot, ohne vorherige Genehmigung durch den Verantwortlichen seinerseits einen weiteren Auftragsbearbeiter mit der Bearbeitung zu beauftragen;

[1)] SGF 10.1

6. die Pflicht des Auftragsbearbeiters, den Verantwortlichen unverzüglich zu informieren, wenn er aufgrund eines ausländischen Gesetzes oder eines richterlichen Entscheids die Daten einer ausländischen Behörde bekanntgeben muss oder Gefahr läuft, dass er es tun muss.

c) überträgt es dem Auftragsbearbeiter keine Bearbeitung, die es nicht selber ausführen darf;

d) sorgt es dafür, dass es die von einer Auslagerung betroffenen Daten rechtzeitig zurückbekommen kann, namentlich damit es den Auftragsbearbeiter wechseln, die Daten wieder bei sich bearbeiten oder sie dem Historischen Archiv abliefern kann;

e) macht es den Auftragsbearbeiter auf seine Geheimhaltungspflichten aufmerksam, insbesondere auf das Amtsgeheimnis und/oder das Berufsgeheimnis.

[2] Bei der Kantonsverwaltung übernehmen das sachlich zuständige Organ und das Amt, das für die Informatik zuständig ist [2)], gemeinsam die Verantwortung für die Umsetzung und die Kontrolle der Vorschriften über die Auslagerung. Fälle, in denen das sachlich zuständige Organ seine Informatiksysteme ganz oder teilweise autonom verwaltet, bleiben vorbehalten.

[3] Wenn die Auslagerung mehrere verschiedene Organe desselben Gemeinwesens betrifft, wird ein hauptverantwortliches Organ bezeichnet. Im Übrigen gilt Absatz 2.

Art. 20 Auslagerung – Sicherheitsmassnahmen

[1] Die Integrität, die Authentizität, die Verfügbarkeit und die Vertraulichkeit der ausgelagerten Personendaten sowie die Dauerhaftigkeit ihrer Aufbewahrung und Nutzung müssen durch geeignete organisatorische und technische Massnahmen, die der Entwicklung der verfügbaren Technologien angepasst sind, sichergestellt werden.

[2] Die Definition der Sicherheitsmassnahmen berücksichtigt das Risiko, welches das Bearbeiten der fraglichen Daten für die Grundrechte der betroffenen Personen mit sich bringt.

[3] Wenn die Auslagerung Daten betrifft, die für den Betrieb der Verwaltung unentbehrlich sind, muss die Fortführung der ausgelagerten Tätigkeiten bei einem Zwischenfall mit einem angemessenen Dispositiv sichergestellt werden.

[2)] Heute: Amt für Informatik und Telekommunikation.

Art. 21 Auslagerung – Massnahmen für besonders schützenswerte Personendaten

[1] Die Bearbeitung von besonders schützenswerten Personendaten und die Bearbeitung von Daten, die einer gesetzlichen oder vertraglichen Geheimhaltungspflicht unterliegen, darf dann ausgelagert werden, wenn die Vertraulichkeit gegenüber dem Auftragsbearbeiter sichergestellt ist, so dass dieser auf deren Inhalt keinen Zugriff hat.

[2] Wenn der Auftragsbearbeiter aus technischen Gründen unbedingt Zugriff auf die Daten haben muss, werden im Auslagerungsvertrag die nötigen besonderen Anforderungen festgelegt, insbesondere die Verpflichtung des Auftragsbearbeiters, nur mit ausdrücklicher Zustimmung des öffentlichen Organs, das die Daten auslagert, auf den Inhalt der Daten zuzugreifen, und die Pflicht, ein Zugriffsjournal zu führen.

[3] Bei der Auslagerung von Daten, die einer gesetzlichen Geheimhaltungspflicht unterliegen, stellt der Verantwortliche sicher, dass der Auftragsbearbeiter den Status einer Hilfsperson des Geheimnisträgers hat.

Art. 22 Pilotprojekte, welche die Bearbeitung bestimmter Datenkategorien beinhalten

[1] Wenn ein Pilotprojekt im Sinne von Artikel 35 des E-Government-Gesetzes vom 18. Dezember 2020 (E-GovG) [3)] die Bearbeitung besonders schützenswerter Personendaten oder andere Arten der Bearbeitung im Sinn von Artikel 5 Abs. 3 beinhaltet, so unternimmt das für das Pilotprojekt verantwortliche Organ Folgendes:

a) es übermittelt der Kantonalen Behörde für Öffentlichkeit, Datenschutz und Mediation (Aufsichtsbehörde) spätestens einen Monat vor seiner Übermittlung an den Staatsrat das Dossier nach Artikel 35 Abs. 2 Bst. d E-GovG [4)];

b) es übermittelt der Aufsichtsbehörde spätestens einen Monat vor seiner Übermittlung an den Staatsrat den Evaluierungsbericht nach Artikel 35a Abs. 2 E-GovG [5)];

c) es ergreift die erforderlichen Massnahmen, um den Schutz der Grundrechte und der Personendaten der betroffenen Personen während der gesamten Dauer des Pilotprojekts zu gewährleisten.

[2] Die Unterlagen des Pilotprojekts und der Evaluierungsbericht müssen jeweils mindestens einen Teil enthalten, der sich mit der Bearbeitung von Personendaten und deren Schutz befasst.

---

3) SGF 184.1
4) SGF 184.1
5) SGF 184.1

[3] Die Aufsichtsbehörde kann zum Inhalt der Unterlagen des Pilotprojekts und des Evaluierungsberichts Stellung nehmen. Ihre Stellungnahme wird dem Staatsrat mitgeteilt.

Art. 23 Archivierung

[1] Personendaten unterliegen der Gesetzgebung über die Archivierung; ihre Archivwürdigkeit wird in Zusammenarbeit mit den für das historische Archiv zuständigen Organen bestimmt.

Art. 24 Löschen und Vernichten

[1] Personendaten, deren Aufbewahrung keinem Zweck mehr dient und die nicht archivwürdig sind, werden so bald wie möglich mit geeigneten Mitteln, welche die gesicherte Beseitigung gewährleisten, gelöscht oder vernichtet.

[2] Die Datenträger werden beim Recycling oder beim Ersetzen zerstört, wenn das Risiko besteht, dass unbefugte Personen besonders schützenswerte Personendaten, die gelöscht wurden, einsehen könnten.

Art. 25 Videoüberwachung

[1] Die Vorschriften über die Videoüberwachung befinden sich in der einschlägigen Gesetzgebung.

2.3 Bearbeitung von Daten für nicht personenbezogene Zwecke

Art. 26 Vorschriften

[1] Die öffentlichen Organe dürfen Personendaten bearbeiten und für nicht personenbezogene Zwecke, namentlich für die Forschung, die Planung und die Statistik, unter folgenden Voraussetzungen bekanntgeben:

a) die Daten werden vernichtet oder anonymisiert, sobald der Bearbeitungszweck dies erlaubt;

b) die Empfängerin oder der Empfänger gibt die Daten nur mit dem Einverständnis der Person oder des Organs, die oder das sie ihm weitergegeben hat, Dritten bekannt;

c) besonders schützenswerte Personendaten werden Privatpersonen nur in einer Form, in der es nicht möglich ist, die betroffenen Personen zu identifizieren, weitergegeben;

d) die Ergebnisse müssen so veröffentlicht werden, dass die betroffenen Personen nicht bestimmbar sind.

[2] Die Artikel 5 Abs. 2 und 3, 7 und 14 Abs. 1 gelten nicht.

[3] Privatpersonen, die von einem öffentlichen Organ Personendaten für die Bearbeitung zu nicht personenbezogenen Zwecken erhalten, verpflichten sich schriftlich, die nötigen Vorsichtsmassnahmen zu ergreifen, um die Persönlichkeit der betroffenen Personen zu schützen.

3 Rechte der betroffenen Personen

Art. 27 Auskunftsrecht – Grundsätze

[1] Jede Person kann vom Verantwortlichen Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden.

[2] Das Auskunftsrecht gilt namentlich für folgende Informationen:

a) der Verantwortliche und seine Kontaktdaten;

b) bearbeitete Personendaten;

c) Zweck und allenfalls rechtliche Grundlagen der Bearbeitung;

d) Aufbewahrungsfrist der Personendaten oder, wenn das nicht möglich ist, die Kriterien, um diese zu bestimmen;

e) die verfügbaren Informationen über die Herkunft der Personendaten;

f) allenfalls Logik und Kriterien einer Massnahme oder eines Entscheids, die oder der aufgrund einer automatisierten Bearbeitung von Daten ergriffen oder gefällt wurde;

g) allenfalls Empfängerinnen und Empfänger oder die Empfängerkategorien, denen diese Daten bekanntgegeben werden, und die Informationen nach Artikel 15 Abs. 3.

[3] Lässt ein öffentliches Organ Daten durch einen Auftragsbearbeiter bearbeiten, so bleibt es verpflichtet, die Daten bekanntzugeben und die verlangten Auskünfte zu erteilen.

[4] Niemand darf im Voraus auf das Auskunftsrecht verzichten.

Art. 28 Auskunftsrecht – Modalitäten

[1] Wer das Auskunftsrecht geltend macht, muss seine Identität nachweisen.

[2] Die Auskünfte werden in der Regel schriftlich auf einem physischen Träger oder elektronisch erteilt. Im Einvernehmen mit dem Verantwortlichen kann die betroffene Person ihre Daten auch vor Ort einsehen.

[3] Das Verfahren ist kostenlos. Der Staatsrat kann Ausnahmen vorsehen.

Art. 29 Auskunftsrecht – Einschränkungen

[1] Der Verantwortliche kann die Auskunft verweigern, einschränken oder aufschieben, wenn und soweit:

a) es in einem Gesetz im formellen Sinn vorgesehen wird;

b) ein überwiegendes öffentliches Interesse es gebietet, namentlich wenn die Auskunft ein laufendes Verfahren oder eine laufende Untersuchung beeinträchtigen könnte;

c) das überwiegende Interesse eines Dritten es gebietet;

d) das Auskunftsgesuch offensichtlich missbräuchlich ist, namentlich aufgrund der Wiederholung.

[2] Die Bekanntgabe von Daten, die im historischen Archiv abgelegt sind, kann ebenfalls verweigert, eingeschränkt oder aufgeschoben werden, wenn die Behandlung des Gesuchs nicht mit einer rationellen Verwaltungsführung vereinbar ist und die betroffene Person kein schutzwürdiges Interesse geltend macht.

[3] Der Verantwortliche muss angeben, aus welchem Grund er die Auskunft verweigert, einschränkt oder aufschiebt.

Art. 30 Daten verstorbener Personen

[1] Auf Verlangen gewährt der Verantwortliche kostenlos Einsicht in die Personendaten einer verstorbenen Person, wenn:

a) die ersuchende Person ein Interesse daran hat, diese Auskünfte zu erhalten, und

b) kein überwiegendes öffentliches oder privates Interesse, insbesondere der verstorbenen Person oder ihrer Angehörigen, entgegensteht.

[2] Ein Interesse an der Einsichtnahme besteht, wenn ein nahes Verwandtschaftsverhältnis, eine Ehe oder eine eheähnliche Gemeinschaft mit der verstorbenen Person vorliegt.

[3] Für den Zugang zu Daten, die dem Berufsgeheimnis unterliegen, bleibt Artikel 321 StGB [6)] vorbehalten.

Art. 31 Einsprache gegen die Bekanntgabe von Personendaten

[1] Die betroffene Person kann gegen das Bekanntgeben bestimmter Personendaten durch den Verantwortlichen Einsprache einlegen.

[2] Personendaten dürfen trotz Einsprache von Seiten der betroffenen Person bekanntgegeben werden, wenn:

a) es gesetzlich vorgesehen ist;

[6)] SR 311.0

b) die Unterlassung der Mitteilung die Erfüllung der Aufgaben des öffentlichen Organs gefährden könnte;

c) die Person, welche die Daten anfordert, eine Privatperson ist und die beiden folgenden Bedingungen erfüllt sind:

1. es existieren keine rechtlichen Hindernisse für die Bekanntgabe;

2. die Gesuchstellerin oder der Gesuchsteller beweist, dass die betroffene Person sich wahrscheinlich der Bekanntgabe nur widersetzt, um sie oder ihn daran zu hindern, rechtliche Forderungen oder andere rechtmässige Interessen geltend zu machen.

[3] In den Situationen nach Absatz 2 Bst. c wird die betroffene Person soweit möglich vorgängig angehört. Der Verantwortliche entscheidet über die Bekanntgabe mit einem Entscheid.

[4] Die Artikel 11 und 27 Abs. 1 Bst. c und Abs. 2 des Gesetzes vom 9. September 2009 über die Information und den Zugang zu Dokumenten (InfoG) [7)] bleiben vorbehalten.

Art. 32 Datenübertragbarkeit

[1] Die betroffene Person kann vom Verantwortlichen verlangen, dass er ihr die sie betreffenden Personendaten in einem häufig verwendeten elektronischen Format zur Verfügung stellt, wenn die folgenden Bedingungen erfüllt sind:

a) der Verantwortliche bearbeitet Personendaten automatisiert; und

b) in der Sondergesetzgebung ist ausdrücklich das Bestehen eines Rechts auf Übertragbarkeit vorgesehen, oder der Verantwortliche hat von sich aus beschlossen, eine solche Möglichkeit einzuführen.

[2] Sofern die Voraussetzungen nach Absatz 1 erfüllt sind und kein unverhältnismässiger Aufwand nötig ist, kann die betroffene Person ausserdem vom Verantwortlichen verlangen, dass er die sie betreffenden Personendaten einem anderen Verantwortlichen übermittelt.

[3] Der Verantwortliche händigt die Personendaten kostenlos aus oder übermittelt sie. Die Spezialgesetzgebung bleibt vorbehalten.

Art. 33 Abwehrklagen

[1] Wer ein schutzwürdiges Interesse hat, kann vom Verantwortlichen verlangen, dass er:

a) die widerrechtliche Bearbeitung von Personendaten unterlässt;

b) die widerrechtliche Bearbeitung beendet;

c) die Widerrechtlichkeit einer Bearbeitung feststellt.

---

7) SGF 17.5

[2] Sie oder er kann insbesondere verlangen, dass der Verantwortliche:

a) falsche Daten über sie oder ihn berichtigt oder Daten löscht, deren Aufbewahrung keinem Zweck mehr dient;

b) die Bearbeitung von bestimmten Daten über sie oder ihn, namentlich die Änderung und die Bekanntgabe an Dritte, vorübergehend einschränkt;

c) bei Daten, die sie oder ihn betreffen und bei denen weder die Richtigkeit noch die Unrichtigkeit bewiesen werden kann, einen entsprechenden Vermerk anbringt;

d) einen Entscheid über sie oder ihn veröffentlicht oder Dritten mitteilt.

[3] Personendaten in Archivbeständen oder in öffentlich zugänglichen Beständen dürfen weder berichtigt noch vernichtet werden. Die betroffene Person oder jede Person, die ein schutzwürdiges Interesse hat, kann jedoch verlangen, dass die Einrichtung den Zugang zu den umstrittenen Daten einschränkt und/oder einen entsprechenden Vermerk anbringt.

Art. 34 Verfahren und Rechtsmittel

[1] Für Entscheide, die nach diesem Abschnitt getroffen werden, gilt das Gesetz über die Verwaltungsrechtspflege [8)]. Gegen diese Entscheide kann Beschwerde eingereicht werden.

[2] Ausser wenn sich die betroffene Person dagegen wehrt, teilt das Organ, das den Entscheid gemäss Absatz 1 gefällt hat, ihn der Aufsichtsbehörde mit.

[3] Die Aufsichtsbehörde kann gegen den Entscheid Beschwerde erheben.

Art. 35 Schadenersatz und Genugtuung

[1] Die Person, die einen Schaden erleidet, weil die Bestimmungen dieses Gesetzes verletzt wurden, kann Schadenersatz- und Genugtuungsansprüche gemäss dem Gesetz über die Haftung der Gemeinwesen und ihrer Amtsträger [9)] geltend machen.

[2] Sie kann von der Richterin oder vom Richter verlangen, dass sie oder er das Urteil vollständig oder teilweise veröffentlicht oder Dritten mitteilen lässt.

4 Durchführung des Datenschutzes

Art. 36 Verantwortung – Im Allgemeinen

[1] Jedes öffentliche Organ, das Personendaten bearbeitet, ist für den Datenschutz verantwortlich.

8) SGF 150.1
9) SGF 16.1

[2] Bearbeiten mehrere öffentliche Organe zusammen Daten, so ist die Verteilung ihrer Pflichten beim Datenschutz in der Meldung nach Artikel 38 zu regeln, es sei denn, dass sie ausdrücklich aus einer gesetzlichen Bestimmung hervorgeht.

[3] Die Aufteilung der Verantwortung nach Absatz 2 kann der betroffenen Person nicht entgegengehalten werden.

Art. 37 Verantwortung – Auftragsbearbeitung

[1] Das öffentliche Organ, das Personendaten von einem Auftragsbearbeiter bearbeiten lässt, bleibt für die Verpflichtungen nach der Gesetzgebung über den Datenschutz verantwortlich.

[2] Die Bearbeitung von Personendaten kann einem Auftragsbearbeiter übertragen werden, sofern es in einem Vertrag oder einer Vereinbarung vorgesehen wird und die folgenden Bedingungen erfüllt sind:

a) ausgeführt werden nur Bearbeitungen, welche der Verantwortliche selber durchführen dürfte;

b) keine gesetzliche oder vertragliche Geheimhaltungspflicht verbietet es;

c) der Auftragsbearbeiter darf nicht ohne vorherige Bewilligung des Verantwortlichen seinerseits einen Dritten mit dem Bearbeiten beauftragen.

[3] Der Verantwortliche muss insbesondere sicherstellen, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten.

[4] Der Auftragsbearbeiter kann die gleichen Rechtfertigungsgründe geltend machen wie der Verantwortliche.

[5] Sofern das Gesetz oder eine Vereinbarung zwischen Organen nichts anderes vorsieht, gelten die Vorschriften über die Auftragsbearbeitung nicht zwischen Organen, die derselben Körperschaft angehören. Artikel 36 Abs. 2 ist anwendbar.

Art. 38 Bearbeitungsregister – Grundsätze

[1] Die Aufsichtsbehörde führt ein öffentliches Register der Bearbeitungstätigkeiten, die von den diesem Gesetz unterstellten Organen ausgeführt werden.

[2] Für jede Bearbeitungstätigkeit enthält dieses Register die folgenden Informationen:

a) der Verantwortliche, bei dem die betroffenen Personen ihre Rechte hauptsächlich geltend machen können;

b) allenfalls die übrigen Verantwortlichen und die Aufteilung der Verantwortung;

c) allenfalls Auftragsbearbeiter und ihre Kontaktdaten;

d) die Bezeichnung, die gesetzliche Grundlage und die Zweckbindung der Bearbeitung;

e) Beschreibung der Kategorien der betroffenen Personen und der Kategorien der bearbeiteten Personendaten;

f) die regelmässigen Datenempfängerinnen und Datenempfänger.

[3] Alle Verantwortlichen melden der Aufsichtsbehörde die von ihnen durchgeführten Bearbeitungstätigkeiten und ihre jeweiligen Änderungen.

[4] Bei der gemeinsamen Bearbeitung von Daten richtet der Verantwortliche, der die Erklärung für die Bearbeitung ausfüllt, eine Kopie an die übrigen Verantwortlichen.

Art. 39 Bearbeitungsregister – Ausnahmen

[1] Soweit sie ausschliesslich zu internen Verwaltungszwecken, die für ein öffentliches Organ typisch sind, durchgeführt werden, unterliegen die folgenden Bearbeitungen nicht der Meldepflicht:

a) Datensammlungen, die nur öffentlich zugängliche Informationen enthalten;

b) Korrespondenzablagen;

c) Adressensammlungen;

d) Lieferanten- und Kundendateien;

e) Führen und Verwalten von Buchhaltungsbelegen, wenn sie Personendaten enthalten;

f) Verwalten und Führen der Dokumente, die im Historischen Archiv abgelegt wurden;

g) Bearbeitungstätigkeiten, die nicht personenbezogene Zwecke betreffen, insbesondere im Rahmen von Forschung, Planung und Statistik.

[2] Auf Stellungnahme der Aufsichtsbehörde kann der Staatsrat für andere Kategorien der Bearbeitung, die offensichtlich kein Risiko für die Rechte der betroffenen Personen darstellen, Ausnahmen von der Meldepflicht vorsehen.

Art. 40 Organisatorische und technische Massnahmen

[1] Der Verantwortliche ist verpflichtet, geeignete technische und organisatorische Massnahmen zu treffen, damit bei der Bearbeitung dieses Gesetz und insbesondere die Grundsätze nach Abschnitt 2.1 beachtet werden. Er tut dies bereits bei der Konzeption der Bearbeitung.

[2] Die getroffenen Massnahmen werden mit denjenigen, mit denen die Informationssicherheit der Verwaltung im Allgemeinen sichergestellt werden soll, und mit den Massnahmen zur Informatiksicherheit harmonisiert.

[3] Der Verantwortliche muss durch geeignete Voreinstellungen sicherstellen, dass die Bearbeitung auf das für den verfolgten Zweck erforderliche Mindestmass beschränkt wird.

[4] Die ergriffenen Massnahmen und die Wahl der Einstellungen werden dokumentiert.

Art. 41 Folgenabschätzung – Grundsätze

[1] Führt eine neue Bearbeitung von Daten voraussichtlich zu einem erhöhten Risiko für die Grundrechte der betroffenen Person, so muss der Verantwortliche vorgängig eine Datenschutz-Folgenabschätzung durchführen.

[2] Ob das Risiko erhöht ist, hängt von der Art, vom Umfang, von den Umständen und von der Zweckbindung der Bearbeitung ab. Es ist namentlich in folgenden Fällen gegeben:

a) grossflächige Bearbeitung von besonders schützenswerten Personendaten;

b) Profiling-Tätigkeiten;

c) systematische Überwachung von grossen Teilen des öffentlichen Raums;

d) Bearbeitungen in einem Umfang oder in einer Intensität mit Technologien, Mechanismen und Verfahren, bei denen das Risiko, dass die Grundrechte der betroffenen Personen beeinträchtigt werden, besonders ausgeprägt ist.

[3] Die Folgenabschätzung enthält eine Beschreibung der geplanten Bearbeitung, eine Bewertung der Risiken aus technischer und rechtlicher Sicht sowie eine Beschreibung der Massnahmen, die zum Schutz der Grundrechte der betroffenen Personen vorgesehen sind.

Art. 42 Folgenabschätzung – Anhörung der Aufsichtsbehörde

[1] Der Verantwortliche hört die Aufsichtsbehörde an, wenn das Ergebnis der Folgenabschätzung bestätigt, dass ein erhöhtes Risiko für die Grundrechte der betroffenen Personen besteht, bei denen besondere Vorsichtsmassnahmen getroffen werden müssen.

[2] Die Aufsichtsbehörde teilt innerhalb von zwei Monaten Einwände und Empfehlungen zur geplanten Bearbeitung mit. Ausnahmsweise kann diese Frist um einen Monat verlängert werden, wenn es sich um eine komplexe Bearbeitung von Daten handelt.

[3] Der Verantwortliche informiert die Aufsichtsbehörde spätestens darüber, welche Folge seinen Empfehlungen gegeben wird, wenn die Bearbeitung, für welche die Folgenabschätzung gemacht wurde, beginnt.

Art. 43 Verletzungen der Datensicherheit – Zu ergreifende Massnahmen

[1] Wenn der Verantwortliche eine Verletzung der Sicherheit der Personendaten feststellt, ergreift er unverzüglich geeignete Massnahmen, um die Verletzung zu beenden und ihre Auswirkungen zu minimieren.

[2] Er hält in einem internen Dokument die Art der Verletzung, die Art der betroffenen Daten und die betroffenen Personenkategorien, die wahrscheinlichen Folgen für letztere und die Massnahmen fest, die ergriffen wurden, um die Situation zu verbessern.

[3] Der Verantwortliche meldet der oder dem Beauftragten so schnell wie möglich Fälle von Verletzungen der Sicherheit von Personendaten, die voraussichtlich ein hohes Risiko für die Grundrechte der betroffenen Person mit sich bringen.

[4] Der Verantwortliche sorgt dafür, dass der Auftragsbearbeiter ihm unverzüglich jede Verletzung der Sicherheit der Personendaten meldet, die bei ihm aufgetreten ist.

Art. 44 Verletzungen der Datensicherheit – Meldung an die betroffene Person

[1] Wenn dies aus Gründen der Transparenz erforderlich ist und/oder um der betroffenen Person die Möglichkeit zu geben, geeignete Massnahmen zur Wahrung ihrer Interessen zu ergreifen, informiert der Verantwortliche die betroffene Person über das Auftreten einer Verletzung der Datensicherheit.

[2] In den folgenden Fällen kann er ausnahmsweise die Information der betroffenen Person einschränken, aufschieben oder darauf verzichten:

a) überwiegende Interessen eines Dritten gebieten es;

b) ein überwiegendes öffentliches Interesse, namentlich die innere Sicherheit und die öffentliche Ordnung, gebietet es;

c) mit der Information kann eine laufende Untersuchung, Instruktion oder ein laufendes Justiz- oder Verwaltungsverfahren gefährdet werden;

d) die Informationspflicht kann unmöglich erfüllt werden oder es braucht dazu einen unverhältnismässigen Aufwand.

[3] Wenn eine grosse Anzahl Personen von einer Verletzung der Datensicherheit betroffen ist, kann die Information in Form einer öffentlichen Mitteilung erfolgen. Der Verantwortliche sorgt in diesem Fall dafür, dass die Informationen so umfassend wie möglich sind.

[4] Eine Verletzung der Datensicherheit kann auch auf Ersuchen der oder des Beauftragten gemeldet werden, wenn sie oder er der Meinung ist, dass die Voraussetzungen für eine solche Meldung erfüllt sind.

Art. 45 Ansprechperson für den Datenschutz

[1] Jede Direktion bezeichnet mindestens eine Ansprechperson für den Datenschutz. Diese Funktion kann mit anderen Funktionen, insbesondere im Bereich der Informationssicherheit, kombiniert werden.

[2] Die Ansprechperson für den Datenschutz erfüllt insbesondere folgende Aufgaben:

a) sie sensibilisiert die Verantwortlichen für den Bereich des Datenschutzes;

b) sie berät und unterstützt die Verantwortlichen auf deren Verlangen oder wenn ein Fall dies erfordert;

c) sie wirkt zusammen mit dem Verantwortlichen an der Durchführung der Datenschutz-Folgenabschätzungen nach Artikel 41 mit;

d) sie ist die Hauptansprechpartnerin der Aufsichtsbehörde in allen Fragen des Datenschutzes;

e) sie erfüllt alle anderen Aufgaben, die das Gesetz ihr überträgt.

[3] Die Ansprechperson für Datenschutz übt ihre Aufgaben selbstständig aus. Die Verantwortlichen geben ihr von Amtes wegen oder auf Verlangen alle Informationen, die sie für die Erfüllung ihrer Aufgaben braucht.

[4] Die Ansprechpersonen für den Datenschutz bilden untereinander ein Kompetenznetzwerk. Der Staatsrat regelt die Organisation und die Arbeitsweise des Netzwerks.

[5] Der Staatsrat kann die Pflicht zur Bezeichnung einer Ansprechperson für den Datenschutz über die Direktionen hinaus auch auf andere Einheiten der Kantonsverwaltung ausdehnen.

5 Aufsicht

Art. 46 Im Allgemeinen

[1] Die Aufsicht über den Datenschutz wird auf Kantonsebene und auf Gemeindeebene von der Kantonalen Behörde für Öffentlichkeit, Datenschutz und Mediation (Aufsichtsbehörde) ausgeübt.

5.1 Aufsichtsbehörde

Art. 47 Organisation

[1] Die Aufsichtsbehörde setzt sich aus der Kantonalen Öffentlichkeits-, Datenschutz- und Mediationskommission (der Kommission), der oder dem Öffentlichkeits- und Datenschutzbeauftragten (der oder dem Beauftragten) und der kantonalen Mediatorin oder dem kantonalen Mediator zusammen.

[2] Sie erfüllt die Aufgaben, die ihr aufgrund dieses Gesetzes übertragen werden, durch die Kommission und die Beauftragte oder den Beauftragten.

[3] Die Aufgaben, die sie in den Bereichen des Rechts auf Zugang zu amtlichen Dokumenten und der Mediation für Verwaltungsangelegenheiten wahrnimmt, werden in den einschlägigen Gesetzgebungen geregelt.

Art. 48 Stellung

[1] Die kantonale Aufsichtsbehörde erfüllt ihre Aufgaben unabhängig.

[2] Sie ist der Direktion, der sie angehört, administrativ zugewiesen. Sie verfügt über ein eigenes Sekretariat und die notwendigen Ressourcen, um ihre Aufgaben und die Ausübung ihrer Befugnisse effektiv wahrzunehmen.

[3] Die Behörde verfügt über ein Globalbudget, dessen Betrag alljährlich bei der Verabschiedung des Staatsvoranschlags festgelegt wird. Zuvor richtet sie ihren eigenen Voranschlagsantrag an den Staatsrat. Dieser Antrag wird gemäss Artikel 61 Abs. 1 Bst. a des Gesetzes vom 16. Oktober 2001 über die Organisation des Staatsrates und der Verwaltung [10)] behandelt.

[4] Die Mitglieder der Behörde unterstehen ebenso wie deren Mitarbeiterinnen und Mitarbeiter dem Amtsgeheimnis und der Schweigepflicht.

[5] Bei ihrem Amtsantritt und bei jeder späteren Änderung der Situation teilen die Mitglieder der Behörde ihre besonderen privaten und öffentlichen Interessenbindungen mit. Artikel 14 Abs. 1 Bst. b und 2 und 3 InfoG [11)] gelten sinngemäss.

[6] Für den Ausstand von Mitgliedern der Behörde gelten die Artikel 21–25 des Gesetzes über die Verwaltungsrechtspflege [12)].

Art. 49 Kommission – Zusammensetzung und Organisation

[1] Die kantonale Öffentlichkeits-, Datenschutz- und Mediationskommission setzt sich aus der Präsidentin oder dem Präsidenten und sechs Mitgliedern zusammen, die vom Grossen Rat auf Vorschlag des Staatsrats gewählt werden.

[10)] SGF 122.0.1
[11)] SGF 17.5
[12)] SGF 150.1

[2] Die Präsidentin oder der Präsident und die Mitglieder müssen in ihrer Gesamtheit über die Kenntnisse verfügen, die zur Erfüllung der Aufgaben der Kommission erforderlich sind; dieser gehören insbesondere eine Juristin oder ein Jurist, eine Fachperson aus dem Gesundheitswesen, eine Informatik- und Datensicherheitsspezialistin oder ein Informatik- und Datensicherheitsspezialist und eine Fachperson aus dem Medienbereich an.

[3] Das Sekretariat der Kommission wird von der oder dem Beauftragten geführt; für die Dossiers in Zusammenhang mit den Mediationstätigkeiten kann das Sekretariat von der kantonalen Mediatorin oder dem kantonalen Mediator geführt werden.

[4] Wenn nötig kann die Kommission Sachverständige beiziehen oder Drittpersonen zu einer Sitzung oder einem Teil einer Sitzung einladen und ihnen gegebenenfalls beratende Stimme geben.

[5] Im Übrigen regelt die Kommission ihre Organisation und ihre Arbeitsweise.

Art. 50 Kommission – Befugnisse

[1] Die Kommission übt die allgemeine Aufsicht auf dem Gebiet des Datenschutzes aus. Sie hat namentlich folgende Befugnisse:

a) sie führt in Zusammenarbeit mit der Direktion, der sie zugewiesen ist, für den Staatsrat das Verfahren zur Ernennung der oder des Beauftragten durch und nimmt zuhanden des Staatsrats Stellung zu den von ihr bevorzugten Kandidatinnen und Kandidaten;

b) sie leitet die Tätigkeit der oder des Beauftragten;

c) sie nimmt Stellung zu Entwürfen von Erlassen, die den Datenschutz berühren, und in den vom Gesetz vorgesehenen Fällen;

d) sie nimmt Stellung zu Pilotprojekten, die gemäss Artikel 22 durchgeführt werden;

e) sie legt Beschwerde gemäss Artikel 34 Abs. 3 ein;

f) sie fällt Entscheide über den Datenschutz gemäss Artikel 58;

g) sie sorgt für die Koordination zwischen den Anforderungen des Datenschutzes und der Ausübung des Rechts auf Zugang zu amtlichen Dokumenten.

[2] Die Kommission erstattet dem Staatsrat zuhanden des Grossen Rates alljährlich einen Bericht über ihre Tätigkeit und über die Tätigkeit der oder des Beauftragten und der kantonalen Mediatorin oder des kantonalen Mediators. Sie kann, sofern dies durch das öffentliche Interesse gerechtfertigt ist, die Öffentlichkeit über ihre Feststellungen informieren.

Art. 51 Beauftragte/r – Ernennung und Stellung

[1] Die oder der Öffentlichkeits- und Datenschutzbeauftragte wird vom Staatsrat für eine individuelle Amtszeit von fünf Jahren ernannt. Diese Anstellung kann erneuert werden.

[2] Während der gesamten Dauer ihrer oder seiner Anstellung darf die oder der Beauftragte keine Tätigkeit ausüben, welche die Unabhängigkeit des Amtes beeinträchtigen könnte oder die auf andere Weise mit den Aufgaben der Aufsichtsbehörde unvereinbar wäre. Die Ausübung eines öffentlichen Nebenamtes oder einer nebenberuflichen Erwerbstätigkeit bedarf der Genehmigung durch die Kommission.

[3] Zum Zeitpunkt der Anstellung und während der gesamten Dauer des Dienstverhältnisses muss die oder der Beauftragte über die für die Ausübung ihrer oder seiner Aufgaben erforderlichen Qualifikationen und/oder Erfahrungen verfügen.

[4] Soweit in diesem Gesetz oder in der dazugehörigen Ausführungsverordnung nichts anderes bestimmt wird, wird das Dienstverhältnis der oder des Beauftragten in der Gesetzgebung über das Staatspersonal geregelt. Die jährliche Beurteilung im Sinne dieser Gesetzgebung wird von der Kommission durchgeführt.

Art. 52 Beauftragte/r – Eneuerung und Beendigung des Dienstverhältnisses

[1] Die Amtszeit der oder des Beauftragten wird stillschweigend verlängert. Der Staatsrat kann jedoch spätestens sechs Monate vor Ablauf der Amtszeit einen Entscheid über die Nichterneuerung treffen. Er bittet zu diesem Zweck um die Stellungnahme der Kommission. Diesem Entscheid müssen triftige Gründe zugrunde liegen.

[2] Die oder der Beauftragte kann den Staatsrat unter Einhaltung einer dreimonatigen Kündigungsfrist ersuchen, die Amtszeit auf das Ende eines Monats zu beenden.

[3] Die oder der Beauftragte wird in folgenden Fällen des Amtes enthoben:

a) sie oder er ist dauerhaft nicht in der Lage ihre oder seine Aufgaben im Sinn der Personalgesetzgebung zu erfüllen;

b) sie oder er hat die Amtspflichten vorsätzlich oder grob fahrlässig in schwerwiegender Weise verletzt.

[4] Der Entscheid, die Beauftragte oder den Beauftragten gemäss Absatz 3 Bst. b des Amtes zu entheben, liegt in der Kompetenz des Staatsrats. Dieser Entscheid kann auf Veranlassung des Staatsrats oder der Kommission getroffen werden. In jedem Fall holt der Staatsrat die Stellungnahme der Kommission ein.

Art. 53 Beauftragte/r – Verhinderung

[1] Ist die oder der Beauftragte dauerhaft verhindert, so ernennt der Staatsrat eine Person ad interim. Das Bezeichnungsverfahren wird gemeinsam von der Kommission und der Direktion, der die Behörde zugewiesen ist, durchgeführt.

[2] Bei punktueller Verhinderung wird er oder sie von einer Person, die von der Kommission dazu bestimmt wird, vertreten.

Art. 54 Beauftragte/r – Aufgaben

[1] Die oder der Beauftragte hat namentlich folgende Aufgaben:

a) sie oder er überwacht die Anwendung der Gesetzgebung über den Datenschutz, namentlich durch systematische Überprüfungen bei den betreffenden Organen;

b) sie oder er gibt Stellungnahmen und Ratschläge zu den ihr vorgelegten Datenbearbeitungen aus rechtlicher und/oder technischer Sicht ab;

c) sie oder er nimmt Stellung und schlägt allenfalls geeignete Massnahmen vor, wenn die Aufsichtsbehörde nach der Durchführung einer Datenschutz-Folgenabschätzung angehört wird;

d) sie oder er informiert und berät die öffentlichen Organe im Bereich des Datenschutzes und unterstützt sie, namentlich bei der Prüfung von Bearbeitungsprojekten;

e) sie oder er wirkt an der Schulung öffentlicher Organe in Datenschutzfragen mit;

f) sie oder er sensibilisiert die Öffentlichkeit für die Fragen des Datenschutzes und erteilt den betroffenen Personen Auskünfte über ihre Rechte;

g) sie oder er behandelt Ersuchen und Anzeigen, die betroffene Personen an die Aufsichtsbehörde richten, wenn sie Datenschutzfragen betreffen;

h) sie oder er führt das Bearbeitungsregister nach Artikel 38;

i) sie oder er leistet ihren Beitrag bei Verletzungen der Sicherheit von Personendaten, die Gegenstand einer Meldung nach Artikel 43 Abs. 3 sind;

j) sie oder er sorgt dafür, dass beim Datenaustausch über die Landesgrenzen hinweg die Rechte der betroffenen Personen beachtet werden;

k) sie oder er gibt Empfehlungen zuhanden öffentlicher Organe ab, die Personendaten bearbeiten, wenn sich zeigt, dass eine oder mehrere Datenschutzbestimmungen nicht eingehalten werden;

l) sie oder er arbeitet mit der oder dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten sowie mit den Aufsichtsbehörden über den Datenschutz der anderen Kantone und des Auslandes zusammen;

m) sie oder er führt die Arbeiten aus, die ihr oder ihm von der Kommission übertragen werden;

n) sie oder er erstattet der Kommission Bericht über ihre oder seine Tätigkeit und Feststellungen.

Art. 55 Selbstkontrolle der Aufsichtsbehörde

[1] Die Aufsichtsbehörde stellt durch geeignete Kontrollmassnahmen, insbesondere in Bezug auf die Datensicherheit, sicher, dass die Beachtung und die richtige Anwendung der kantonalen Datenschutzbestimmungen innerhalb ihrer Behörde gewährleistet ist.

5.2 Kontroll- und Eingriffsbefugnis

Art. 56 Kontrolle durch die Beauftragte oder den Beauftragten

[1] Die oder der Beauftragte ist befugt, von Amtes wegen oder auf Klage hin eine Kontrolle bei einem Verantwortlichen oder einem Auftragsbearbeiter durchzuführen, um zu prüfen, ob er die Datenschutzbestimmungen einhält.

[2] Sie oder er kann namentlich Auskünfte einholen, die Herausgabe von Akten verlangen, Inspektionen durchführen und sich Datenbearbeitungen vorführen lassen.

[3] Gegenüber der kantonalen Aufsichtsbehörde können weder das Amtsgeheimnis noch weitere Geheimhaltungspflichten geltend gemacht werden. Das Berufsgeheimnis bleibt vorbehalten.

[4] Wenn die oder der Beauftragte aufgrund einer Klage der betroffenen Person eine Kontrolle durchführt, informiert sie oder er diese Person über die Folge, die ihrer Klage gegeben wurde, und das Ergebnis einer allfälligen Untersuchung. Die betroffene Person hat keine Parteistellung im Verfahren.

Art. 57 Empfehlungen der oder des Beauftragten

[1] Bei einer Verletzung oder einer möglichen Verletzung der Datenschutzvorschriften kann die oder der Beauftragte eine Empfehlung an das betroffene öffentliche Organ richten und es auffordern, innert einer bestimmten Frist die nötigen Abhilfemassnahmen zu treffen.

[2] Handelt es sich um eine unterstellte Verwaltungseinheit, so ergeht die Empfehlung direkt an das hierarchisch übergeordnete Organ.

[3] Das Organ, an das die Empfehlung gerichtet wird, gibt innert der von der oder dem Beauftragen gesetzten Frist eine Stellungnahme zur Folge ab, die es der Empfehlung leisten will, und teilt die Stellungnahme der oder dem Beauftragten mit. Eine fehlende Stellungnahme wird als Ablehnung der Empfehlung betrachtet.

[4] Wird die Empfehlung ganz oder teilweise abgelehnt, so kann die oder der Beauftragte den Fall zum Entscheid an die Kommission weiterleiten.

[5] Wenn das öffentliche Organ im Laufe des Verfahrens die notwendigen Massnahmen zur Wiederherstellung eines datenschutzkonformen Zustandes getroffen hat, stellt die oder der Beauftragte das Verfahren ein und verzichtet auf eine Empfehlung.

Art. 58 Entscheid der Kommission

[1] Die Kommission fällt in den Angelegenheiten, welche die oder der Beauftragte ihr gemäss Artikel 57 Abs. 4 übermittelt, einen Entscheid.

[2] Wenn ein Organ, das diesem Gesetz unterstellt ist, die Bestimmungen über den Datenschutz nicht beachtet, kann die Kommission verfügen, dass die ganze Bearbeitung oder ein Teil davon ausgesetzt, geändert oder eingestellt wird und dass alle Personendaten oder ein Teil davon gelöscht oder vernichtet werden.

[3] Im Falle einer unmittelbar drohenden ernsthaften Bedrohung oder einer Datenschutzverletzung, welche die Rechte einer oder mehrerer betroffener Personen ernsthaft beeinträchtigen könnte, kann die Kommission von Amtes wegen oder auf Verlangen der oder des Beauftragten dringende vorsorgliche Massnahmen verfügen, um die strittige Datenbearbeitung einzuschränken oder auszusetzen, bis sie in der Sache entschieden hat.

[4] Die oder der Beauftragte wirkt mit beratender Stimme am Verfahren vor der Kommission mit. Sie oder er kann mit der Instruktion der Angelegenheit beauftragt werden.

[5] Wenn das betroffene öffentliche Organ im Laufe des Verfahrens die nötigen Massnahmen zur Wiederherstellung eines datenschutzkonformen Zustands ergriffen hat, kann die Kommission das Verfahren einstellen oder lediglich eine Verwarnung aussprechen

Art. 59 Verfahren

[1] Das Verfahren wird im Gesetz über die Verwaltungsrechtspflege [13)] geregelt. Das betroffene Organ hat insbesondere das Recht, angehört zu werden; Artikel 58 Abs. 3 bleibt vorbehalten.

[13)] SGF 150.1

[2] Das öffentliche Organ, gegen das sich ein Entscheid der Kommission richtet, kann gegen diesen Entscheid Beschwerde einlegen.

Art. 60 Zusammenarbeit mit anderen Datenschutzbehörden in der Schweiz und im Ausland

[1] Bei der Ausübung ihrer Funktionen kann die Aufsichtsbehörde mit den kantonalen, eidgenössischen und ausländischen Behörden, die mit dem Datenschutz beauftragt sind, zusammenarbeiten.

[2] Sie kann zur Erfüllung ihrer jeweiligen gesetzlichen Aufgaben mit anderen Behörden, die mit dem Datenschutz beauftragt sind, Informationen oder Personendaten austauschen, sofern die folgenden Bedingungen erfüllt sind:

a) die Gegenseitigkeit der Amtshilfe ist sichergestellt;

b) die ausgetauschten Informationen und Personendaten werden nur für das den Personendatenschutz betreffende Verfahren verwendet, das dem Amtshilfeersuchen zugrunde liegt;

c) die Informationen und Personendaten werden Dritten nur bekanntgegeben, wenn die Behörde, die sie übermittelt hat, dies vorgängig genehmigt;

d) die empfangende Behörde verpflichtet sich, das Berufsgeheimnis sowie Geschäfts- und Fabrikationsgeheimnisse zu wahren;

e) die empfangende Behörde verpflichtet sich, die Auflagen und Einschränkungen der Behörde einzuhalten, die ihr die Informationen und Personendaten übermittelt hat.

[3] Bevor die Behörde Informationen, die Berufs-, Fabrikations- oder Geschäftsgeheimnisse enthalten können, an eine andere Behörde, die mit dem Datenschutz beauftragt ist, weiterleitet, informiert sie die Inhaberinnen und Inhaber dieser Geheimnisse und fordert sie auf, Stellung zu nehmen, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismässigen Aufwand verbunden.

6 Schluss- und Übergangsbestimmungen

Art. 61 Ausführungsreglement

[1] Der Staatsrat erlässt die nötigen Bestimmungen zur Umsetzung dieses Gesetzes. Diese betreffen namentlich:

a) die Sicherheitsmassnahmen;

b) die Ausübung der Rechte der betroffenen Personen;

c) die Durchführung von Pilotprojekten;

d) die Stellung und die Aufgaben der Ansprechpersonen für den Datenschutz;

e) das Arbeitsverhältnis der Mitglieder der Aufsichtsbehörde.

Art. 62 Übergangsrecht

[1] Für die Bearbeitungen, die bereits am Laufen sind, wenn dieses Gesetz in Kraft tritt, verfügen die Verantwortlichen über eine Frist von zwei Jahren, um die neu vorgeschriebenen Anforderungen zu erfüllen. Die Artikel 43 und 44 sind direkt anwendbar.

[2] Sofern die Zweckbindung des Bearbeitens unverändert bleibt und keine neuen Daten beschafft werden, welche die Durchführung einer Folgenabschätzung rechtfertigen, gelten die Artikel 41 und 42 nicht für Bearbeitungen, die vor dem Inkrafttreten dieses Gesetzes begonnen wurden.

[3] Die Bearbeitungen, die abgeschlossen sind, wenn dieses Gesetz in Kraft tritt, werden im alten Recht geregelt, ausser was die Rechte der betroffenen Person angeht (3. Abschnitt).

[4] Die Artikel 12, 13, 40, 41 und 42 gelten für Bearbeitungstätigkeiten, die durch die Richtlinie (EU) 2016/680 [14)] ab dem Inkrafttreten dieses Gesetzes geregelt sind.

Art. 63 Anpassung der Gesetzgebung

[1] Die Direktionen verfügen über eine Frist von zwei Jahren ab Inkrafttreten dieses Gesetzes, um die Gesetzgebung, für die sie zuständig sind, an die Anforderungen von Artikel 5 anzupassen.

Art. 64 Dienstverhältnis der oder des Beauftragten

[1] Bei Inkrafttreten des Gesetzes passt die Anstellungsbehörde den Arbeitsvertrag der Stelleninhaberin oder des Stelleninhabers im Einklang mit der Personalgesetzgebung an die Anforderungen des neuen Gesetzes an.

[2] Wird der Vorschlag zur Umwandlung des Arbeitsvertrags abgelehnt, so wird die Situation gemäss den Bestimmungen über die Abschaffung von Stellen im Sinne der Personalgesetzgebung geregelt.

[14)] Autorenhinweis: Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, JO L 119 vom 4.5.2016, S. 89.

Änderungstabelle – Nach Beschlussdatum

Beschluss	Berührtes Element	Änderungstyp	Inkrafttreten	Quelle (ASF seit 2002)
12.10.2023	Erlass	Grunderlass	01.01.2024	2023_087

Änderungstabelle – Nach Artikel

Berührtes Element	Änderungstyp	Beschluss	Inkrafttreten	Quelle (ASF seit 2002)
Erlass	Grunderlass	12.10.2023	01.01.2024	2023_087