CANTON DU VALAIS
KANTON WALLIS

Présidence du Conseil d'Etat
Chancellerie d'Etat
Service administratif et juridique

Präsidium des Staatsrates
Staatskanzlei
Verwaltungs- und Rechtsdienst

Erläuternder Bericht

Zum Vorentwurf über die Revision des Gesetzes über die Information der Öffentlichkeit, den Datenschutz und die Archivierung

Einleitung

Der Abgeordnete Sébastien Nendaz hat am 9. Mai 2019 eine Motion eingereicht, mit der er den Staatsrat aufforderte, die unterschiedlichen Auslegungen des Gesetzes über die Information der Öffentlichkeit, den Datenschutz und die Archivierung vom 9. Oktober 2008 (GIDA / SGS/VS 170.2) zu überprüfen, um die Befugnisse und Organisation der kantonalen Datenschutz- und Öffentlichkeitskommission zu klären und den Anforderungen des Bundesrechts und des Schengen-Datenschutzgesetzes gerecht zu werden. Am 5. Februar 2020 hat der Staatsrat entschieden, die Arbeiten an der Revision des GIDA in Angriff zu nehmen, um es an das Bundesrecht, aber auch an die europäische Gesetzgebung anzupassen.

Das GIDA ist seit seiner Annahme praktisch unverändert geblieben.

Die Gesetze im Bereich des Datenschutzes haben sich jedoch stark weiterentwickelt. Der Bundesrat hat dem eidgenössischen Parlament am 15. September 2017 einen Entwurf zur Totalrevision des Bundesgesetzes über den Datenschutz (DSG) und die Änderung weiterer Erlasse zum Datenschutz unterbreitet. Die Arbeiten im Zusammenhang mit der Revision des DSG (nDSG) sind nun beendet. Auf europäischer Ebene hat die Annahme der Datenschutz-Grundverordnung (DSGVO)[1] am 27. April 2016 am meisten Aufmerksamkeit erhalten. Sie ist seither direkt im ganzen Europäischen Wirtschaftsraum anwendbar und hat in bestimmten Situationen auch Auswirkungen auf die Schweiz[2].

[1] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.
[2] Extraterritoriale Anwendung im Sinne von Artikel 3 Absatz 2 DSGVO.

Das am 10. Oktober 2018 in Strassburg abgeschlossene Protokoll zur Änderung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten[3] wurde vom Bund unterzeichnet. Der Bundesbeschluss über die Genehmigung wurde am 11. März 2020 vom Nationalrat und am 2. Juni 2020 vom Ständerat angenommen. Mit diesem Änderungsprotokoll wird das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981[4] modernisiert, um den Herausforderungen an den Schutz der Privatsphäre zu begegnen, die mit der Nutzung neuer Technologien und immer umfangreicherer Datenströme einhergehen.

Diese Bestimmungen sind jedoch nicht direkt anwendbar und müssen in das nationale und kantonale Recht übertragen werden. Die Anpassung auf Bundesebene erfolgt im Rahmen der Totalrevision des DSG. Die Kantone müssen für ihre jeweiligen Gesetzgebungen dasselbe tun.

Schliesslich wurde die Richtlinie (EU) 2016/680 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 von der Öffentlichkeit weniger beachtet. Sie spielt aber für die Verwaltung dennoch eine wichtige Rolle und hat auf Bundesebene zur Annahme des Schengen-Datenschutzgesetzes (SDSG) am 28. September 2018 geführt. Die Kantone sind ebenfalls daran, ihre diesbezüglichen Gesetze zu aktualisieren.

Die aktuelle Revision bezieht sich nicht auf den Bereich der Information der Öffentlichkeit des GIDA, sondern stellt eine allgemeine Aktualisierung der Bestimmungen zum Datenschutz dar, bei der das Übereinkommen 108, die Totalrevision des DSG, die DSGVO und die Richtlinie (EU) 2016/680 berücksichtigt werden.

Da es sich nicht um eine Totalrevision handelt, wird die Struktur des Gesetzes beibehalten.

Der Abschnitt betreffend den Zugang zu amtlichen Dokumenten wird grundsätzlich nicht geändert, abgesehen von einigen Anpassungen, insbesondere von gemeinsamen Bestimmungen betreffend den Zugang zu Personendaten und amtlichen Dokumenten und das Verfahren.

[3] Übereinkommen 108+ oder modernisiertes Übereinkommen 108.
[4] Übereinkommen 108.

1. Kommentar zu den einzelnen Gesetzesbestimmungen

1.1 Artikel 1

Die Begriffe Organ/e und öffentliche/s Organ/e wurden zwecks Vereinheitlichung der Terminologie im gesamten Gesetz wie auch im Ausführungsreglement durch Behörde/n ersetzt. Der Begriff Behörde/n wird gemäss altem Gesetz beibehalten.

In Bezug auf den Datenschutz bleibt der Zweck des GIDA unverändert. Das GIDA konkretisiert in rechtlicher Hinsicht das Recht auf Selbstbestimmung in Sachen Information, das heisst, das Recht für die betroffene Person, selbst bestimmen zu können, ob und zu welchem Zweck Informationen über sie bearbeitet werden dürfen, ungeachtet ihrer Nationalität oder ihres Wohnortes.

1.2 Artikel 2

Um den Gesetzesänderungen Rechnung zu tragen, wurden die in Artikel 2 Absatz 2 vorgesehenen Verweise geändert. In Artikel 2 Absatz 3 wird neu der Begriff Bearbeitung statt Datensammlung verwendet. Um die Ausnahme in Artikel 2 Absatz 3 nicht nur auf das Gesundheitswesen, die gerichtliche Polizei oder die Gerichte zu beschränken, wurden diese gestrichen. Die Annahme eines Spezialgesetzes über die Bearbeitung von Personendaten in einem spezifischen Bereich bleibt somit möglich, wobei dieses natürlich der Verfassung, den Anforderungen des Übereinkommens 108+ und der EMRK entsprechen muss.

1.3 Artikel 3

Die Definitionen werden an die technologische Entwicklung und die im nDSG und in der DSGVO verwendete Terminologie angepasst.

Absatz 3 Personendaten (Daten)

Im Französischen gibt es keinen Unterschied zwischen dem Begriff *donnée(s) personnelle(s)*, der im DSG verwendet wird, und dem Begriff *donnée(s) à caractère personnel* gemäss GIDA, DSGVO und anderen kantonalen Gesetzen. Der Klarheit halber wurde der gelegentlich benutzte Begriff *donnée(s) personnelle(s)* im ganzen Gesetz wie auch im Ausführungsreglement durch den Begriff d*onnée(s) à caractère personnel* oder einfach nur durch *donnée(s)* ersetzt.

In diesem Absatz ist nicht nur von Daten, sondern auch von der betroffenen Person die Rede. Um die Terminologie zu vereinheitlichen, wird der Begriff «betroffene Person» im gesamten Gesetz wie auch im Ausführungsreglement nur im Singular verwendet.

In Übereinstimmung mit dem nDSG und den Texten zum Datenschutz der EU, des Europarats und den meisten anderen Ländern, wird im Entwurf auf den Datenschutz von juristischen Personen verzichtet. Der Schutz der Persönlichkeit und der Grundrechte juristischer Personen bleibt in anderen Bestimmungen verankert (Persönlichkeitsschutz, unlauterer Wettbewerb, Urheberrecht). Dieser Verzicht wird die Übermittlung von Daten ins Ausland stark vereinfachen und die Pflichten der Behörden für Daten begrenzen, die oft teilweise bereits öffentlich zugänglich sind.

Was den öffentlichen Sektor anbelangt, hat die Aufhebung des Datenschutzes für juristische Personen zur Folge, dass die im kantonalen Recht vorgesehenen gesetzlichen Grundlagen, welche die Behörden dazu ermächtigen, Personendaten zu bearbeiten, künftig nur noch Daten von natürlichen Personen betreffen. Allerdings muss die Tätigkeit des Staates gesetzlich geregelt sein. Die verschiedenen kantonalen Gesetzesbestimmungen, die eine Bearbeitung von Personendaten erlauben, müssen deshalb angepasst werden, um eine Verletzung der Persönlichkeitsrechte und der Grundrechte von juristischen Personen zu begründen. Um Rechtslücken zu vermeiden, wird für eine Dauer von fünf Jahren eine Übergangsbestimmung angenommen (Art. T1-1).

Artikel 25 Absatz 8 ARGIDA betreffend die Auskunft über Daten von verstorbenen Personen muss gestrichen werden. Er gründet auf keiner Bestimmung des GIDA. Gemäss Zivilgesetzbuch (ZGB) endet die Persönlichkeit mit dem Tode (Art. 31 Abs. 1 ZGB). Im Rahmen der Revision des DSG lehnte das eidgenössische Parlament die Bestimmungen über die Daten von verstorbenen Personen ab. Eine ähnliche Bestimmung wie jene von Artikel 25 Absatz 8 ARGIDA ist zweifellos nützlich, müsste jedoch im Zivilgesetzbuch oder einem anderen Gesetz verankert sein.

Abs. 4 Bearbeitung

Die Definition von «Bearbeitung» wird nicht geändert, doch die nicht abschliessenden Beispiele von Bearbeitungen werden aktualisiert, damit sie den technischen Gegebenheiten entsprechen und besser mit dem nDSG und den europäischen Texten übereinstimmen. Die Definition der «Bearbeitung» umfasst weiterhin sämtliche Vorgänge im Zusammenhang mit den Daten, ob diese nun vollständig oder nur teilweise automatisiert seien. Da der Begriff der Datensammlung nicht mehr verwendet wird, ist ausdrücklich vorgesehen, dass, sofern keine automatisierten Vorgänge durchgeführt werden, «Datenbearbeitung» einen Vorgang bezeichnet, der im Zusammenhang mit Personendaten innerhalb einer strukturierten Reihe solcher Daten ausgeführt wird, auf die nach spezifischen Kriterien zugegriffen werden kann, und der es dem Verantwortlichen für die Datenbearbeitung oder jeder anderen

Person erlaubt, Personendaten zu suchen, zu kombinieren oder zu korrelieren. Diese Präzisierung ergibt sich aus Artikel 2 Buchstabe c des Übereinkommens 108+.

Abs. 6 Verantwortlicher für die Datenbearbeitung

Der Begriff «Datensammlung» von Absatz 5 wird gestrichen, da er keine grosse Rolle mehr spielt und daher nicht mehr notwendig ist.

Der Begriff «Inhaber der Datensammlung» aus dem alten Absatz 6 wird ersetzt durch den umfassenderen Begriff «Verantwortlicher für die Datenbearbeitung», wie er im nDSG, in der DSGVO und mehreren kantonalen Gesetzen verwendet wird, was jedoch keine materielle Änderung bedeutet. Die Änderungen betreffen das gesamte Gesetz und sein Ausführungsreglement.

Abs. 6bis Auftragsbearbeiter

Da in Artikel 29 die Bearbeitung durch Auftragsbearbeiter behandelt wird, muss die Definition des Begriffs «Auftragsbearbeiter» in Artikel 3 hinzugefügt werden. Der Auftragsbearbeiter ist jene Person, die im Auftrag des Verantwortlichen für die Datenbearbeitung Daten bearbeitet. Der Auftragsbearbeiter kann eine private Person (natürliche oder juristische Person) oder eine Behörde sein.

Absatz 6ter Empfänger

Der Begriff «Empfänger» erscheint in verschiedenen Bestimmungen des Gesetzes. Um eine einheitliche Auslegung dieses Begriffs zu gewährleisten, wird er ebenfalls in Artikel 3 eingeführt. Dem Empfänger werden die Daten bekannt gegeben. Beim Empfänger kann es sich um eine private Person (natürliche oder juristische Person) oder eine Behörde handeln, die als Verantwortlicher für die Datenbearbeitung, Auftragsbearbeiter oder Dritter handelt.

Abs. 7 Besonders schützenswerte Daten

Gemäss nDSG und europäischem Recht wird der Begriff «besonders schützenswerte Daten» auf «Daten über philosophische Ansichten oder Tätigkeiten», «Daten über das Sexualleben», «Daten über die ethnische Zugehörigkeit», «genetische Daten» und «biometrische Daten, welche die eindeutige Identifizierung einer Person ermöglichen» ausgedehnt. Der Schweizer Begriff der besonders schützenswerten Daten wurde den besonderen Kategorien personenbezogener Daten aus der DSGVO vorgezogen.

Genetische Daten sind Informationen über das Erbgut einer Person, die durch eine genetische Untersuchung gewonnen werden, einschliesslich des DNA-Profils[5].

[5] Artikel 3 Buchstabe l des Bundesgesetzes über genetische Untersuchungen beim Menschen (GUMG) vom 8. Oktober 2014.

Unter biometrischen Daten versteht man mit speziellen technischen Verfahren gewonnene Personendaten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, welche die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Fingerabdrücke, Gesichtsbilder, die Iris oder die Stimme. Diese Daten müssen zwingendermassen mit speziellen technischen Verfahren gewonnen werden, welche die Identifizierung oder eindeutige Authentifizierung einer Person ermöglichen. Mit einem einfachen Foto ist dies zum Beispiel nicht möglich.

Absatz 8 Profiling

Der statische und veraltete Begriff «Persönlichkeitsprofil», der eine schweizerische Besonderheit darstellt, verschwindet ebenfalls zugunsten des dynamischeren Begriffs «Profiling» wie im nDSG.

Profiling umschreibt eine bestimmte Form der Datenbearbeitung, die auf einen bestimmten Zweck ausgerichtet ist. Es kann definiert werden als die Bewertung bestimmter Merkmale einer Person auf der Grundlage von automatisiert bearbeiteten Personendaten, insbesondere um bestimmte persönliche Aspekte, die sich auf eine Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser Person zu analysieren oder vorherzusagen. Ein Profiling ist mit anderen Worten dadurch gekennzeichnet, dass Personendaten automatisiert ausgewertet werden, um auf der Grundlage dieser Auswertung, ebenfalls in automatisierter Weise, die Merkmale einer Person zu bewerten. Ein Profiling liegt somit nur vor, wenn der Bewertungsprozess vollständig automatisiert ist.

Absatz 8bis Verletzung der Datensicherheit

Die Einführung von Artikel 30a, der eine Meldung von Verletzungen der Datensicherheit vorsieht, bedingt eine vorgängige Definition derselben. Eine Verletzung der Datensicherheit ist somit eine Verletzung der Sicherheit, die ungeachtet der Absicht oder der Widerrechtlichkeit dazu führt, dass Personendaten verloren gehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden.

Dieser Begriff steht natürlich in Zusammenhang mit Artikel 21, der vorsieht, dass der Verantwortliche für die Datenbearbeitung und gegebenenfalls der Auftragsbearbeiter zu jedem Zeitpunkt der Bearbeitung und unter Einhaltung der

Datenschutzbestimmungen geeignete organisatorische und technische Massnahmen ergreifen müssen.

Massgebend ist alleine, ob die fraglichen Vorgänge geschehen. Irrelevant für das Vorliegen einer Verletzung der Datensicherheit ist ebenfalls, ob lediglich die Möglichkeit besteht, dass die Personendaten Unbefugten offengelegt oder zugänglich gemacht worden sind, oder ob ein solcher Zugang tatsächlich stattgefunden hat. Geht beispielsweise ein Datenträger verloren, lässt sich oft kaum nachweisen, ob die darauf gespeicherten Daten tatsächlich durch Unbefugte eingesehen oder verwendet worden sind. Daher stellt bereits der Verlust als solcher eine Verletzung der Datensicherheit dar. Für die nach einem solchen Vorfall zu treffenden Massnahmen, insbesondere für die Einschätzung des Risikos nach Artikel 30a, sind der Umfang und die Bedeutung einer Verletzung der Datensicherheit relevant.

1.4 Artikel 12 Absatz 2

Artikel 12 Absatz 2 wird geändert, um einen Fehler zu korrigieren, der nur die französische Version betrifft.

Der Begriff *juridictionnelles* wird gestrichen, da die französische Version nicht mit der deutschen übereinstimmt, in der auf sämtliche hängigen Verwaltungsverfahren Bezug genommen wird. Ein Verwaltungsstreitverfahren ist ein Streitverfahren infolge der Anfechtung einer erstinstanzlichen administrativen Verfügung[6]. In der französischen Version der ursprünglichen Botschaft wurde bereits auf hängige Verfahren Bezug genommen, ohne zu unterscheiden, ob es Streitverfahren sind oder nicht, was der deutschen Version entspricht, in der diese Unterscheidung auch nicht gemacht wird[7].

Um die Sprachversionen des Gesetzestextes zu vereinheitlichen, wird die Präzisierung *juridictionnelles* aus der französischen Bestimmung gestrichen.

1.5 Artikel 12a

Bisher war der Zugang zu Personendaten und amtlichen Dokumenten in den Artikeln 48 ff. geregelt, obwohl die Ziele und Modalitäten unterschiedlich waren. Das Verfahren wird künftig in separaten Bestimmungen geregelt.

Ein neuer Artikel 12a wird eingefügt, um den Ablauf von Gesuchen um Zugang zu amtlichen Dokumenten klarzustellen. Er nimmt bezüglich den Zugang zu amtlichen Dokumenten den Inhalt der Artikel 48 und 49 auf. Der Zugang zu Personendaten wird im entsprechenden Kapitel behandelt.

---

[6] Sébastien Fanti, *La notion de document officiel en droit fédéral, ainsi qu'en droit valaisan*, ZWR 2016 S. 410; Basler Kommentar zum Öffentlichkeitsgesetz, STAMM-PFISTER, 3. Ausgabe, Basel 2014, Bemerkung 21 zu Artikel 3.
[7] Erwägung 3.2.1 des oben genannten Entscheids.

Die Absätze 1 bis 3 entsprechen im Wesentlichen dem bisherigen Artikel 48 Absätze 1 bis 3. Die Absätze 4 bis 6 entsprechen im Wesentlichen dem bisherigen Artikel 49 Absätze 1 bis 3.

1.6 Artikel 12b

Artikel 12b entspricht im Wesentlichen dem bisherigen Artikel 50. Im Gegensatz zur im geltenden Gesetz vorgesehenen Frist von 10 Tagen, sieht der Vorentwurf eine Verlängerung auf 20 Tage vor, wie dies auch im Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung (BGÖ) vorgesehen ist.

Ausnahmsweise kann die Frist von 20 Tagen verlängert werden, wenn sich das Gesuch auf eine grosse Anzahl von Dokumenten, auf komplexe oder schwer beschaffbare Dokumente bezieht oder zur Abwägung der vorhandenen Interessen einer eingehenden Prüfung bedarf. Sobald die Behörde erkennt, dass eine Fristverlängerung erforderlich ist, informiert sie die gesuchstellende Person rasch über diese Verlängerung, deren Dauer und die Gründe dafür. Die Behörde ist verpflichtet, das Gesuch gemäss dem Beschleunigungsgebot zu bearbeiten.

1.7 Artikel 13

Zwecks Präzision wurde der Verweis auf andere Gesetzesbestimmungen in Absatz 2 geändert und enthält nur noch Artikel 22. Das Vorprojekt sieht auch die Möglichkeit vor, der Zustimmung der betroffenen Person Rechnung zu tragen. Die Zustimmung ist keiner Formvorschrift unterworfen, muss jedoch die in Artikel 18 Absatz 4 festgehaltenen Kriterien erfüllen, um gültig zu sein. Es ist in jedem Fall Aufgabe der Behörde, das Vorhandensein der Zustimmung zu beweisen, weshalb sie ein Interesse daran hat, diese zu dokumentieren.

1.8 Artikel 15 Absatz 7

Artikel 15 wird um einen Absatz 7 ergänzt. Der Wortlaut dieses Absatzes stammt im Wesentlichen aus dem bisherigen Artikel 15. Obwohl in Absatz 4 nur die Verweigerung erwähnt ist, kann die Behörde gemäss dem Grundsatz «wer mehr kannn, kann auch weniger» den Zugang beschränken oder aufschieben.

1.9 Artikel 17

Die Absätze 1 und 3 betrafen bisher das Erfordernis der gesetzlichen Grundlage, während es in Absatz 2 um die Grundsätze ging. Zur Verbesserung der Lesbarkeit wird Artikel 17 fortan einzig der Frage der gesetzlichen Grundlage gewidmet sein.

Absatz 1 sieht vor, dass eine Datenbearbeitung nur zulässig ist, wenn sie auf einer gesetzlichen Grundlage beruht. Um dem nDSG zu entsprechen, wurde die Erfüllung einer gesetzlichen Aufgabe gestrichen.

Artikel 17 wird durch die neuen Absätze 2 und 3 ergänzt, in denen präzisiert wird, wann eine formelle gesetzliche Grundlage erforderlich ist. In Artikel 18 werden die Grundsätze behandelt; teilweise wird der bisherige Artikel 17 Absatz 2 übernommen.

Wie bisher ist ein Gesetz im formellen Sinn erforderlich, wenn es sich um die Bearbeitung besonders schützenswerter Daten handelt (Abs. 2 Bst. a). Diese Hypothese wird auch durch den Fall eines Profilings (der Begriff «Persönlichkeitsprofil», der mit schützenswerten Daten gleichgesetzt wurde, entfällt) vervollständigt. Es wird ergänzt (Abs. 2 Bst. b), dass eine Bearbeitung einer gesetzlichen Grundlage im formellen Sinn bedarf, wenn der Bearbeitungszweck oder die Art und Weise der Datenbearbeitung zu einem schwerwiegenden Eingriff in die Grundrechte der betroffenen Person führen kann.

In Absatz 3 ist vorgesehen, dass Daten nur auf der Grundlage eines Gesetzes im materiellen Sinn bearbeitet werden können, wenn die Bearbeitung für die Grundrechte der betroffenen Person keine besonderen Risiken birgt und eine der Bedingungen unter Buchstaben a bis c erfüllt ist. Nicht nur die Bearbeitung an sich, sondern auch ihr Ergebnis darf keine besonderen Risiken bergen. Ausnahmen dürfen nur beschränkt zugelassen werden. Sie müssen insbesondere vermeiden, dass die Behörde nur deshalb an der Bearbeitung von Daten gehindert wird, weil das Gesetz eine solche nicht ausdrücklich vorsieht, obwohl sie der Erfüllung einer behördlichen Aufgabe entspricht. Der Schutz lebenswichtiger Interessen bezieht sich auf Fälle, in denen der Gesetzgeber offensichtlich nicht über die Zeit verfügt, um gesetzliche Grundlagen zu verabschieden, und die durch die Bedeutung des zu verteidigenden Rechtsguts begründet werden. Was die Bearbeitung von Daten anbelangt, die von der betroffenen Person öffentlich gemacht wurden, wäre es störend, diese zu stark einzuschränken, obwohl die Person ihr nicht widersprochen hat.

1.10 Artikel 18

Der bisherige Artikel 18 zur Datenerhebung wird aufgehoben, da die Verstärkung der Informationspflicht in Artikel 19 ausreichend ist.

Die allgemeinen Grundsätze im Bereich des Datenschutzes, die zum Teil in Absatz 2 des bisherigen Artikels 17 zu finden waren, werden fortan in Artikel 18 Absatz 1 aufgeführt, der auch vervollständigt wurde. Diese Grundsätze müssen bei jeder Datenbearbeitung befolgt werden. Es geht dabei um die klassischen Grundsätze von Loyalität (Treu und Glauben), Transparenz, Zweck, Verhältnismässigkeit und Genauigkeit. Die Terminologie ist aus Artikel 5 des Übereinkommens 108+ übernommen.

Der Grundsatz der Verhältnismässigkeit, der in der Praxis am ehesten verletzt wird, erfordert besondere Aufmerksamkeit. Dabei ist zu betonen, dass jede Datenbearbeitung in einem angemessenen Verhältnis zum verfolgten rechtmässigen Zweck stehen muss und in jeder Phase der Bearbeitung ein gesundes Gleichgewicht zwischen allen öffentlichen oder privaten Interessen sowie zwischen den auf dem Spiel stehenden Rechten und Freiheiten gefunden werden muss. Somit müssen sowohl die Wahl der Mittel als auch die Modalitäten der Bearbeitung und deren Umfang dem Grundsatz der Verhältnismässigkeit entsprechen.

Artikel 18 wird gemäss den im nDSG und im europäischen Recht enthaltenen Verpflichtungen zum Datenschutz durch Technik (*privacy by design*, Abs. 2) und durch datenschutzfreundliche Voreinstellungen (*privacy by default*, Abs. 3) zusätzlich ergänzt. Es handelt sich dabei nicht um Grundsätze im eigentlichen Sinn, sondern um Pflichten, die eng mit ihnen verbunden sind, weshalb es gerechtfertigt ist, sie hier anzufügen. Der Verantwortliche für die Datenbearbeitung muss die Datenbearbeitung von Anfang an so ausgestalten, dass die Datenschutzvorschriften eingehalten werden. Der Verantwortliche für die Datenbearbeitung trifft ab der Planung sowohl zum Zeitpunkt der Festlegung der Mittel für die Bearbeitung als auch zum Zeitpunkt der eigentlichen Bearbeitung geeignete technische und organisatorische Massnahmen, um die Datenschutzgrundsätze wie die Pseudonymisierung oder die Datenminimierung umzusetzen und die notwendigen Garantien in die Bearbeitung aufzunehmen. Bei diesen Massnahmen sind der Kenntnisstand, die Implementierungskosten und die Art, der Umfang, die Umstände und der Zweck der Bearbeitung zu berücksichtigen. Sie müssen an die Risiken angepasst sein, welche die Bearbeitung für die Rechte und Freiheiten der Personen birgt.

Diese Pflicht beruht auf dem Grundsatz des «Datenschutzes durch Technik». Die gesetzlichen Anforderungen für eine datenschutzkonforme Bearbeitung werden bereits so im System verwirklicht, dass dieses die Gefahr von Verstössen gegen Datenschutzvorschriften reduziert oder ausschliesst. Bereits vor dem Beginn muss eine Datenbearbeitung so angelegt werden, dass möglichst wenige Daten bearbeitet werden und dass die Daten nur für möglichst kurze Zeit aufbewahrt werden (Konzept der Datenminimierung).

Zudem ist der Verantwortliche verpflichtet, mittels geeigneter Voreinstellungen sicherzustellen, dass die Bearbeitung der Personendaten auf das für den Verwendungszweck nötige Mindestmass beschränkt ist, soweit die betroffene Person nicht etwas anderes bestimmt.

Der Verantwortliche trifft geeignete technische und organisatorische Massnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur Personendaten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen Personendaten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Bei Voreinstellungen handelt es sich um jene Einstellungen, die standardmässig zur Anwendung kommen, das heisst, falls keine abweichende Eingabe durch den Nutzer erfolgt. Im Zusammenhang mit dem Datenschutz bedeutet dies, dass der fragliche Bearbeitungsvorgang standardmässig möglichst datenschutzfreundlich eingerichtet ist, ausser, die betroffene Person würde diese vorgegebenen Einstellungen verändern. Die Verbindung zwischen dem Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen ist also eng und fügt sich in ein datenschutzfreundliches Gesamtsystem ein.

Der Begriff der Zustimmung wird in Absatz 4 mit Blick auf die Übereinstimmung mit den Anforderungen des Übereinkommens 108+ genauer umschrieben. Die Zustimmung der betroffenen Person muss freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich erfolgen. Die Zustimmung muss den freien Ausdruck einer bewussten Entscheidung darstellen. Dies kann durch eine schriftliche oder mündliche Erklärung oder eine affirmative Handlung geschehen, welche die Zustimmung zur Bearbeitung von Personendaten zum Ausdruck bringt. Die Zustimmung muss sämtliche Bearbeitungstätigkeiten umfassen, die den- oder dieselben Zwecke verfolgen. Liegen mehrere Bearbeitungszwecke vor, muss jedem Einzelnen von ihnen zugestimmt werden. Die betroffene Person muss über die Auswirkungen ihrer Entscheidung informiert werden. Auf die betroffene Person darf kein unzulässiger direkter oder indirekter Druck ausgeübt werden.

1.11 Artikel 19

Absatz 2 wird insbesondere gemäss Artikel 8 des Übereinkommens 108+ ergänzt. Die neuen Informationen, die der betroffenen Person gegeben werden müssen, sind die Angaben zur gesetzlichen Grundlage (Bst. b), die bearbeiteten Daten oder Datenkategorien (Bst. d) und sämtliche Rechte der betroffenen Person (Bst. f). Die Informationspflicht betreffend die Zugangsberechtigung ist nicht mehr erforderlich, da sie fortan durch die Rechte der betroffenen Person abgedeckt ist (Zugangsberechtigung, Recht auf Berichtigung oder Vernichtung usw.). Um dem Mindestkatalog an Informationen Rechnung zu tragen, die zur Gewährleistung einer ausreichenden Transparenz im Sinne des Übereinkommens 108+ erforderlich sind, muss der Verantwortliche für die Datenbearbeitung auch jede für die Gewährleistung

einer fairen und transparenten Datenbearbeitung (Bst. h) nötige zusätzliche Information übermitteln, beispielsweise die Aufbewahrungsdauer.

Zudem wurden die Absätze 2bis und 3 zwecks Klarheit und Vereinfachung umgestellt.

1.12 Artikel 19a

Die französische Überschrift der Bestimmung wird nur geändert, um die Terminologie betreffend die Informationspflicht zu vereinheitlichen.

In Artikel 19a werden verschiedene Situationen definiert, in denen der Verantwortliche für die Datenbearbeitung vollständig von seiner Pflicht, die betroffene Person zu informieren, entbunden ist. Die Einschränkungen von Artikel 19a entsprechen dem, was im nDSG vorgesehen ist. Da es sich beim Öffentlichkeitsprinzip im Zusammenhang mit der Datenbearbeitung um einen wesentlichen Grundsatz des Datenschutzrechts handelt, müssen die Einschränkungen der Informationspflicht strikt ausgelegt werden.

1.13 Artikel 20

Artikel 20 wird angepasst, um den Anforderungen des Übereinkommens 108+ und der Artikel 19 nDSG und 22 DSGVO zu entsprechen.

Eine automatisierte Entscheidung bedeutet, dass diese nicht von einer natürlichen Person auf der Grundlage ihrer eigenen Beurteilung der Situation getroffen wird. Eine automatisierte Einzelentscheidung besteht, wenn eine Verarbeitung von Daten erfolgt und eine Entscheidung oder Bewertung darauf gestützt wird, die nicht durch eine natürliche Person vorgenommen wird. Eine automatisierte Einzelentscheidung kann selbst dann vorliegen, wenn sie anschliessend durch eine natürliche Person mitgeteilt wird, da diese die automatisch gefällte Entscheidung nicht mehr beeinflussen kann. Massgebend ist somit, inwieweit eine natürliche Person eine inhaltliche Prüfung vornehmen und darauf aufbauend die endgültige Entscheidung fällen kann.

Gemäss Absatz 1 muss die betroffene Person ausdrücklich informiert werden, wenn eine Entscheidung auf der ausschliesslichen Basis einer automatisierten Datenbearbeitung Rechtswirkungen für die betroffene Person nach sich zieht oder sie erheblich beeinträchtigt. Es ist deshalb nicht nötig, dass die betroffene Person über jede automatisierte Einzelentscheidung informiert wird, sondern lediglich, wenn die Entscheidung für sie Rechtswirkungen nach sich zieht oder sie erheblich beeinträchtigt. Zum Beispiel entstehen Rechtswirkungen, wenn sich eine Entscheidung aus einer automatischen Steuerveranlagung ergibt. Man kann davon ausgehen, dass die betroffene Person erheblich beeinträchtigt ist, wenn sie auf nachhaltige Weise wirtschaftlich oder persönlich dauerhaft eingeschränkt wird. Eine

blosse Belästigung reicht dafür nicht aus. Massgebend sind die konkreten Umstände des Einzelfalls. Zu berücksichtigen ist insbesondere, wie bedeutsam die fragliche Einschränkung für die betroffene Person ist, wie dauerhaft sich die Entscheidung auswirkt und ob allenfalls Alternativen möglich sind.

Gemäss Absatz 2 muss der Verantwortliche für die Datenbearbeitung der betroffenen Person auf deren Antrag hin die Möglichkeit geben, ihren Standpunkt zum Ergebnis der Entscheidung darzulegen und kann sogar verlangen, dass er von einer natürlichen Person überprüft wird. Dadurch soll unter anderem verhindert werden, dass die Datenbearbeitung auf unvollständigen, veralteten oder unzutreffenden Daten beruht. Dies liegt auch im Interesse des Verantwortlichen für die Datenbearbeitung, weil unzutreffende automatisierte Einzelentscheidungen für ihn negative Konsequenzen nach sich ziehen können.

Absatz 3 präzisiert, dass Absatz 2 nicht gilt, wenn die betroffene Person über ein Rechtsmittel gegen die Entscheidung verfügt. Die betroffene Person kann ihren Standpunkt in diesem Rahmen darlegen und die Entscheidung durch eine natürliche Person überprüfen lassen. Ihre Rechte werden also bereits gewährleistet.

Aus praktischen Gründen kann auf die Verpflichtung verzichtet werden, unaufgefordert die Logik, auf der die Entscheidung beruht, anzugeben. Sie muss jedoch auf Anfrage der betroffenen Person und im Zusammenhang mit ihrer Zugangsberechtigung (Art. 31 Abs. 1 Bst. h) mitgeteilt werden.

1.14 Artikel 21

Artikel 21 wurde komplett umformuliert, um den technischen Entwicklungen Rechnung zu tragen.

Der Verantwortliche für die Datenbearbeitung und die Auftragsbearbeiter müssen eine dem Risiko angemessene Datensicherheit gewährleisten. Diese Bestimmung materialisiert den risikobasierten Ansatz (Abs. 2). Je erheblicher die Risiken für die Datensicherheit sind, desto höher sind die Anforderungen für die zu ergreifenden Massnahmen. Es handelt sich um einen dynamischen Prozess. Die Risiken wie auch die ergriffenen Massnahmen müssen regelmässig überprüft werden.

Die Datensicherheit muss auch die Vertraulichkeit, Integrität und Verfügbarkeit der Daten gewährleisten, wozu auch die Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung gehören.

Absatz 1 wird ergänzt durch einige klassische Massnahmen wie die Pseudonymisierung und die Verschlüsselung der Personendaten. Es muss sich um organisatorische und technische Massnahmen handeln. Sie können zum Beispiel

darauf abzielen, die Nutzer auf die Risiken für die Freiheiten und die Privatsphäre zu sensibilisieren, die Nutzer vor jedem Zugang zu Daten und Bearbeitungsmitteln zu authentifizieren und ihren Zugang auf die erforderlichen Daten zu beschränken, eine Protokollierung vorzusehen, um Zugänge aufzuzeichnen und Vorfälle oder bestimmte Bearbeitungsvorgänge in automatisierten Bearbeitungssystemen zu verwalten, regelmässige Speicherungen vorzunehmen und die Kontinuität der Tätigkeit zu gewährleisten, die Daten auf gesicherte Weise zu archivieren und zu vernichten, die Integrität und die Authentizität der Daten sicherzustellen oder regelmässig die Wirksamkeit der ergriffenen Massnahmen zu testen, zu analysieren und zu bewerten.

Aufgrund der raschen Weiterentwicklung der technischen Rahmenbedingungen wird darauf verzichtet, im Gesetz technische Anforderungen festzulegen. Absatz 3 überträgt dem Staatsrat die Kompetenz, Bestimmungen zu den Mindestanforderungen an die Sicherheit von Personendaten erlassen. Der Beauftragte und die IT-Dienste können in ihrem jeweiligen Kompetenzbereich ebenfalls bewährte Vorgehensweisen empfehlen.

Die Massnahmen müssen insbesondere dem Stand der Technik, der Art und dem Umfang der Datenbearbeitung sowie den Risiken, welche die Bearbeitung für die Persönlichkeit und Grundrechte der betroffenen Personen mit sich bringt, angemessen sein und müssen es ermöglichen, Verletzungen der Datensicherheit zu vermeiden, das heisst, eine Verletzung der Sicherheit, die dazu führt, dass Daten verloren gehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden und dies ungeachtet der Absicht oder der Widerrechtlichkeit und ob die Daten übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

1.15 Artikel 22

In diesem Artikel werden die Grundsätze der Bekanntgabe von Personendaten durch eine Behörde behandelt. Um gültig zu sein, muss die Zustimmung die in Artikel 18 Absatz 4 festgelegten Kriterien erfüllen.

Artikel 22 wird durch einen neuen Absatz 1bis ergänzt, der vorsieht, dass Name, Vorname, Adresse und Geburtsdatum auf Anfrage und, wenn die gesuchstellende Person ein berechtigtes Interesse geltend macht, bekannt gegeben werden dürfen. Diese Möglichkeit der Bekanntgabe wird in Übereinstimmung mit Artikel 32 Absatz 4 nDSG hinzugefügt, der eine Möglichkeit aufnimmt, die im DSG bereits seit langem existierte. Mit dieser Bestimmung soll die Aufgabe der Behörde bezüglich der Beantwortung von Einzelanfragen vereinfacht werden. Diese muss jedoch in jedem

Fall eine Interessenabwägung vornehmen, wobei die Anforderungen angesichts der grundsätzlich begrenzten Gefährdung nicht zu hoch sein sollte.

Die materielle Tragweite der Absätze 2 und 3 bleibt unverändert. Es handelt sich lediglich um eine redaktionelle Vereinfachung.

Das Recht, Widerspruch gegen die Bekanntgabe einzulegen, wird in den Absätzen 4 und 5 hinzugefügt. Dieser Mechanismus räumt der betroffenen Person ein begrenztes Recht ein, gegen die Bekanntgabe von Daten, die normalerweise erlaubt ist, Widerspruch einzulegen. Diese Möglichkeit der Sperrung ist von besonderer Bedeutung, wenn die Behörde nicht in der Lage ist, sämtliche Gefahren einzuschätzen, die eine Bekanntgabe aufgrund von Elementen, die der Situation der betroffenen Person eigen sind, mit sich bringen könnte.

Absatz 4 sieht die Möglichkeit vor, Widerspruch gegen die Bekanntgabe bestimmter Daten einzulegen. Unter der Bekanntgabe bestimmter Daten sind entweder bestimmte Daten oder eine bestimmte Bekanntgabe bzw. eine Bekanntgabe mit einem bestimmten Zweck zu verstehen. Es genügt, wenn die betroffene Person ein legitimes Interesse glaubhaft macht. Die Anforderungen werden nicht sehr hoch sein und eine Interessenabwägung erfolgt, wenn die Behörde Gründe sieht, das Begehren im Sinne von Absatz 5 abzuweisen.

Absatz 5 legt die Bedingungen für eine Sperrung fest. Die Behörde ist berechtigt, Daten trotz einer Sperrung bekannt zu geben, wenn eine Rechtspflicht zur Bekanntgabe besteht oder die Erfüllung ihrer gesetzlichen Aufgaben sonst gefährden wäre.

1.16 Artikel 23

Dieser Artikel betrifft den besonderen Fall der Bekanntgabe von Daten durch die Einwohnerkontrolle, wenn diese systematisch geordnet sind. Für die individuelle Bekanntgabe von Daten durch die Einwohnerkontrolle gilt wie für die anderen Behörden Artikel 22. Artikel 23 ist eine *Lex Specialis*, die von Artikel 22 abweicht, wenn die Daten systematisch geordnet sind. Die individuelle Bekanntgabe von Daten durch die Einwohnerkontrolle wird weiterhin in Artikel 22 geregelt.

Absatz 1 sieht vor, dass die Einwohnerkontrolle einer privaten Person oder Organisation oder einer Behörde auf Gesuch hin systematisch geordnet Name, Vorname, Geschlecht, Adresse und Geburtsdatum bekannt geben darf. Wie in Artikel 22 muss die gesuchstellende Person ein berechtigtes Interesse geltend machen. Es wird präzisiert, dass die Daten nicht zu kommerziellen Zwecken verwendet werden dürfen, ein objektiveres Kriterium als der bisherige Wortlaut

betreffend die Bekanntgabe für schützenswerte ideelle Zwecke. Für die Einwohnerkontrolle handelt es sich in jedem Fall um eine Möglichkeit und nicht um eine Pflicht. Die Gemeinden sind für ihre Organisation zuständig und müssen festlegen, wie sie die Bekanntgabe erlauben.

Die Bekanntgabe von Daten an eine andere Behörde muss auf einer ausreichenden gesetzlichen Grundlage beruhen, im Prinzip die gesetzliche Grundlage, welche die Kompetenzen der Behörde, welche die Daten verlangt, begründet.

Die Möglichkeit, gegen diese Bekanntgabe Widerspruch einzulegen, wird in Absatz 2bis spezifisch festgehalten. Es gilt keine besondere Formvorschrift und die betroffene Person muss ihren Widerspruch nicht begründen. Die Einwohnerkontrolle könnte ein Formular zur Verfügung stellen, könnte sich aber nicht darauf berufen, um einen auf andere Weise deutlich vorgebrachten Widerspruch, zum Beispiel anhand eines Schreibens oder mündlich am Schalter, nicht zu berücksichtigen.

Eine Aufhebung des Widerspruchs scheint wenig wahrscheinlich, ausser natürlich in Fällen, in denen eine Bekanntgabe gesetzlich vorgesehen ist. Bei Bedarf kann Artikel 22 Absatz 5 analog angewendet werden.

1.17 Artikel 24

Die Bestimmung über die Bekanntgabe von Daten an Dienstleistungsbetriebe wird aufgehoben. Die klassischen Bestimmungen zur Bearbeitung durch Auftragsbearbeiter in Artikel 29 sind ausreichend. Die Anforderungen in Bezug auf die Zahlungsfähigkeit und den guten Ruf, die in Artikel 29 festgehalten wurden, finden sich teilweise in der allgemeinen Pflicht des Verantwortlichen für die Datenbearbeitung wieder, seinen Auftragsbearbeiter sorgfältig auszuwählen (*cura in eligendo*).

1.18 Artikel 25

Artikel 25 regelt die Bedingungen, zu denen Daten ins Ausland mitgeteilt werden dürfen.

Die materielle Tragweite von Artikel 1 bleibt unverändert. Es handelt sich lediglich um eine redaktionelle Vereinfachung.

Angesichts der durch das eidgenössische und europäische Recht geschaffenen Hierarchie werden die ausreichenden Garantien nun in einem eigenen Absatz (Abs. 2) behandelt.

Um gültig zu sein, muss die Zustimmung der betroffenen Person die in Artikel 18 Absatz 4 festgelegten Kriterien erfüllen. Die Anforderung einer klaren Information über die Risiken im Zusammenhang mit einem fehlenden angemessenen Schutz wird

ergänzt, um das Übereinkommen 108+ einzuhalten, obwohl diese Anforderung im nDSG überraschenderweise nicht übernommen wurde.

Steht die Bekanntgabe im Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags (Abs. 3 Bst. e), wird präzisiert, dass die Bekanntgabe nicht nur in unmittelbarem Zusammenhang mit dem Vertrag stehen muss, sondern dass der Vertrag auch den Verantwortlichen für die Datenbearbeitung und die betroffene Person oder den Verantwortlichen für die Datenbearbeitung und seinen Vertragspartner im Interesse der betroffenen Person miteinander verbinden muss. Die Formulierung entspricht jener von Artikel 14 Absatz 1 Buchstabe b nDSG.

Um sicherzustellen, dass die Bedingungen der grenzüberschreitenden Datenübermittlung erfüllt sind, kann der Verantwortliche für die Datenbearbeitung von den Behörden die Herausgabe von Unterlagen verlangen.

1.19 Artikel 26

Artikel 26 sieht die Bekanntgabe von nicht personenbezogenen Daten unter vereinfachten Bedingungen vor. Diese Ausnahme gilt nicht nur für die Bekanntgabe, sondern auch für sämtliche Bearbeitungsvorgänge. Der Wortlaut entspricht Artikel 35 nDSG.

Absatz 1 sieht fünf kumulative Bedingungen vor. Zunächst muss der Zweck der Bearbeitung Forschung, Planung oder Statistik betreffen, und darf nicht personenbezogen sein. Zweitens müssen die Daten anonymisiert werden, sobald der Bearbeitungszweck dies erlaubt. Drittens gibt die Behörde privaten Personen besonders schützenswerte Personendaten nur so bekannt, dass die betroffenen Personen nicht bestimmbar sind. Diese Bedingung gilt auch, wenn die Daten unter einem Pseudonym bekannt gegeben werden und der Schlüssel, um die Person erneut zu identifizieren, beim Übermittler der Daten (faktische Anonymisierung) bleibt, und wenn der Empfänger keine andere Möglichkeit hat, den Schlüssel zu finden oder die Personen auf eine andere Weise zu identifizieren. Viertens darf der Empfänger Dritten die Daten nur mit der Zustimmung der Behörde weitergeben, welche die Daten bekannt gegeben hat. Fünftens dürfen die Ergebnisse nur so veröffentlicht werden, dass die betroffenen Personen nicht bestimmbar sind.

Unter «anonymisieren» versteht man jeglichen Vorgang, durch den die Zuordnung von Daten zu einer konkreten Person verhindert wird oder nur noch mit unverhältnismässigem Aufwand möglich ist. In der Praxis kommt es häufig vor, dass der Forscher, der Planer oder der Statistiker zwar nicht personenbezogene Daten verwendet, sie jedoch nicht sofort anonymisiert, da er später die Möglichkeit haben

muss, die Identität einer Person ausnahmsweise zu überprüfen. In solchen Situationen muss er die Daten pseudonymisieren.

Absatz 2 wird ergänzt durch einen weiteren Grundsatz, der bei der Bearbeitung von nicht personenbezogenen Daten nicht eingehalten werden muss und zwar die Anforderung der gesetzlichen Grundlage. Diese Ergänzung wird gemacht, um die Möglichkeiten der Bearbeitung von nicht personenbezogenen Daten zu erweitern, da das Gefährdungsrisiko für die betroffenen Personen eher gering ist.

1.20 Artikel 28

Die Änderungen in Artikel 28 sind rein redaktionell und haben keine materielle Tragweite. Die in Absatz 2 vorgesehenen kumulativen Bedingungen für die Installation von Bildaufnahme- und Bildaufzeichnungsgeräten an öffentlichen Orten werden beibehalten. In diesem Sinne ist es von entscheidender Bedeutung, dass die Behörde vor jeglicher Installation ein Gesetz im formellen Sinne verabschiedet. Das GIDA bildet keine hinreichende gesetzliche Grundlage, um die Installation von Bildaufnahme- und Bildaufzeichnungsgeräten an öffentlichen Orten zu erlauben.

1.21 Artikel 28a

Gemäss Artikel 28 GIDA erfordert die Installation von Bildaufnahme- und Bildaufzeichnungsgeräten an öffentlichen Orten ein Gesetz im formellen Sinne.

Mit dem neuen Artikel 28a Absatz 1 GIDA hält der Gesetzgeber fest, dass das Erfordernis einer formellen Rechtsgrundlage für die Installation von Bildaufnahme- und Bildaufzeichnungsgeräten im kommunalen oder interkommunalen öffentlichen Raum zur Gewährleistung der öffentlichen Sicherheit durch entsprechende Bestimmungen in einem kommunalen oder interkommunalen Reglement, das vom Generalrat oder der Urversammlung angenommen und vom Staatsrat homologiert wurde, erfüllt wird.

Für den kantonalen öffentlichen Raum wird das Erfordernis einer formellen Rechtsgrundlage für die Installation von Bildaufnahme- und Bildaufzeichnungsgeräten zur Gewährleistung der öffentlichen Sicherheit durch das Gesetz über die Kantonspolizei sowie die Verordnung über Video- und Audioüberwachungsmassnahmen durch die Kantonspolizei erfüllt (Art. 28a Abs. 2 GIDA).

1.22 Artikel 28b

Gemäss der Richtlinie (EU) 2016/680 wird eine neue Bestimmung mit allgemeinen Pflichten für den Verantwortlichen für die Datenbearbeitung und den Auftragsbearbeiter hinzugefügt. Sie müssen jederzeit den Nachweis dafür erbringen können, dass sie gesetzeskonform handeln und alle geeigneten Massnahmen ergreifen, um diese Gesetzeskonformität sicherzustellen. Dies entspricht auch dem Grundsatz der Rechenschaftspflicht (*compliance*) gemäss Artikel 5 Absatz 2 DSGVO.

Um die Gesetzeskonformität sicherzustellen und den Nachweis dafür erbringen zu können, müssen sie geeignete technische und organisatorische Massnahmen umsetzen, die bei Bedarf zu überprüfen und zu aktualisieren sind.

Absatz 2 betrifft Situationen, in denen mehr als eine Behörde für die Bearbeitung zuständig ist. Die gemeinsam für die Bearbeitung Verantwortlichen müssen sich insbesondere einigen, was die Wahrnehmung der Rechte der betroffenen Person und ihre jeweiligen Pflichten bezüglich der Bereitstellung oder Lieferung von Informationen an die betroffene Person angeht. Die Anlaufstelle für die betroffene Person wird in der Vereinbarung angegeben und sie muss wissen, welche Behörde wofür zuständig ist.

1.23 Artikel 29

Artikel 29 wird umformuliert und ergänzt, um die im Falle einer Bearbeitung durch Auftragsbearbeiter einzuhaltenden Regeln festzulegen (auch Bearbeitungsdelegation genannt). Er ist in Anlehnung an Artikel 8 nDSG entstanden.

In Absatz 1 wird festgehalten, dass die Bearbeitung durch Auftragsbearbeiter zulässig ist, wenn drei Bedingungen erfüllt sind. Erstens muss sie vertraglich oder durch die Gesetzgebung vorgesehen sein. Zweitens kann der Auftragsbearbeiter nur auf Anweisung des Verantwortlichen für die Datenbearbeitung handeln und die Daten nur so bearbeiten, wie der Verantwortliche selbst es tun dürfte. In diesem Rahmen kann der Auftragsbearbeiter dieselben Rechtfertigungsgründe geltend machen wie der Verantwortliche für die Datenbearbeitung (Abs. 5). Drittens verbietet keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung. Hier ist insbesondere das Amtsgeheimnis gemeint. Dies bedeutet nicht, dass eine Bearbeitung durch Auftragsbearbeiter untersagt ist, wenn Daten durch eine Geheimhaltungspflicht geschützt sind, jedoch muss sie die Anforderungen im Zusammenhang mit dieser Geheimhaltungspflicht vollumfänglich erfüllen, um im Sinne von Artikel 29 rechtmässig zu sein.

In Absatz 2 wird ein schriftlicher Vertrag verlangt, im Gegensatz zu Artikel 8 nDSG, in dem keine Form festgehalten ist. Dies erfordert eine eigenhändige oder qualifizierte Unterschrift im Sinne von Artikel 14 OR. Ein mündlicher Vertrag wäre mit erheblichen Risiken verbunden, weshalb er ausgeschlossen ist. Es wird festgehalten, dass auch die elektronische Form annehmbar ist.

Die wichtigsten Elemente, die im Vertrag enthalten sein müssen, werden in Absatz 2 festgehalten und entsprechen den Bestimmungen der DSGVO und der Richtlinie (EU)

2016/680. Der Beauftragte kann eine Vertragsvorlage vorschlagen, um die Aufgabe der Behörden zu erleichtern.

Der Verantwortliche für die Datenbearbeitung bleibt verantwortlich für Bearbeitungen, die er an einen Auftragsbearbeiter delegiert hat. Die Pflicht eines Verantwortlichen für die Datenbearbeitung, der einen Dritten mit der Bearbeitung von Daten beauftragt, dafür zu sorgen, dass der Schutz dieser Informationen und des Bearbeitungsergebnisses gemäss diesem Gesetz gewährleistet ist, wird in Absatz 3 genauer beschrieben.

Absatz 4 sieht vor, dass eine Übertragung der Datenbearbeitung an einen Dritten nur mit vorgängiger Genehmigung des Verantwortlichen für die Datenbearbeitung möglich ist. Hier geht es um Fälle, in denen der vom Verantwortlichen für die Datenbearbeitung bezeichnete Auftragsbearbeiter die Datenbearbeitung ebenfalls ganz oder teilweise einem Dritten übertragen möchte. Die Genehmigung kann beim Abschluss des Vertrags mit dem Auftragsbearbeiter oder bei Hinzukommen eines neuen Auftragsbearbeiters allgemein oder spezifisch erteilt werden. Wenn möglich ist die zweite Variante vorzuziehen.

Gemäss Absatz 6 muss der Auftragsbearbeiter ein Verzeichnis sämtlicher im Auftrag des Verantwortlichen für die Datenbearbeitung verrichteten Bearbeitungstätigkeiten führen. Dieses ist nicht zu verwechseln mit dem in Artikel 30 vorgesehenen öffentlichen Register. Das Verzeichnis des Auftragsbearbeiters muss es dem Verantwortlichen für die Datenbearbeitung und der Aufsichtsbehörde ermöglichen, Zugang zu allen erforderlichen Informationen zu erhalten, um zu überprüfen, dass der Auftragsbearbeiter seine Datenschutzpflichten einhält.

1.24 Artikel 30

Die Pflicht für jede Behörde, ihr eigenes Register mit der Datensammlung zu führen und den Beauftragten zu informieren, wenn dieses besonders schützenswerte Daten enthält, wird ersetzt durch die Pflicht, die Bearbeitungen gemäss Artikel 11 Absatz 4 nDSG dem Beauftragten zu melden. Da es kein kantonales Register mehr gibt, wird die Überschrift von Artikel 30 entsprechend angepasst.

Konkret wird das Register vom Beauftragten geführt, der für das reibungslose technische Funktionieren und seine Öffentlichkeit zuständig ist. Die Bereitstellung eines einzigen Registers erleichtert den Zugang zu Informationen, da der Rechtssuchende für sämtliche Behörden nur noch ein einziges Register konsultieren muss. Jede Behörde bleibt jedoch selbst verantwortlich für den Inhalt des Registers, den sie in Bezug auf die von ihr vorgenommenen Bearbeitungen zu vervollständigen

hat. Diese Pflicht gilt nicht für die Auftragsbearbeiter, die ein Verzeichnis gemäss Artikel 29 Absatz 6 führen müssen, das jedoch nicht dem öffentlichen Register entspricht, von dem hier die Rede ist.

Der Grundsatz ist in Absatz 1 festgehalten und der Inhalt des Registers in Absatz 2. Es muss für jede Bearbeitungstätigkeit mindestens Informationen über die für die Bearbeitung zuständige Behörde und eine Kontaktperson, die gesetzliche Grundlage, den Zweck, die betroffenen Personen oder die Kategorien der betroffenen Personen, die bearbeiteten Daten oder Datenkategorien, gegebenenfalls die Datenempfänger, die Aufbewahrungsdauer oder mindestens die Kriterien für die Festlegung dieser Dauer sowie die Massnahmen zur Gewährleistung der Datensicherheit enthalten.

Absatz 3 ermöglicht es dem Staatsrat, für bestimmte Bearbeitungstätigkeiten Ausnahmen von der Registrierungspflicht vorzusehen. Daher ist es nicht nötig, im Gesetz spezifische Ausnahmen vorzusehen. Hier ist eine sehr punktuelle Bearbeitung oder eine Bearbeitung durch eine Behörde mit begrenzten Mitteln und betreffend eine begrenzte Anzahl Personen denkbar, unter der Voraussetzung, dass die fraglichen Bearbeitungen kein Risiko für die betroffene Person darstellen. Die Ausnahme betreffend Bearbeitungen, die ausschliesslich der Erfüllung von Aufgaben der Verwaltung dienen und keine Wirkung nach aussen haben, wird in das Reglement aufgenommen. Dies ist nicht der Fall für die Ausnahme betreffend Bearbeitungen, die regelmässig veröffentlicht werden, welche aufgehoben wird. Andernfalls wäre das Risiko, den Nutzen eines einzigen Registers aufs Spiel zu setzen, zu gross. Der Staatsrat kann anstelle der vollständigen Befreiung auch eine vereinfachte Erklärung vorsehen. Die Erklärung muss jedoch die Regel bleiben.

1.25 Artikel 30a

In Artikel 30a wird die Pflicht eingeführt, jede Verletzung der Datensicherheit zu melden, wie es in Artikel 22 nDSG und in den europäischen Rechtstexten vorgesehen ist.

Absatz 1 sieht vor, dass der Verantwortliche für die Datenbearbeitung dem Beauftragten so rasch als möglich jede Verletzung der Datensicherheit, die ein erhöhtes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann, meldet.

Der Begriff «Verletzung der Datensicherheit» wird in Artikel 3 definiert und beinhaltet jegliche Verletzung der Sicherheit, die ungeachtet der Absicht oder der Widerrechtlichkeit dazu führt, dass Personendaten verloren gehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich

gemacht werden. Die Verletzung kann durch Dritte erfolgen, aber auch durch Mitarbeiter, die ihre Kompetenzen überschreiten oder fahrlässig handeln. Durch eine Verletzung der Datensicherheit kann die betroffene Person die Kontrolle über ihre Daten verlieren, oder diese Daten werden missbraucht. Darüber hinaus kann sie auch zu einer Verletzung der Persönlichkeit der betroffenen Person führen, zum Beispiel indem geheime Informationen über sie bekannt werden.

Eine Verletzung der Datensicherheit gilt als Persönlichkeitsverletzung. Auf diese Gefährdungen kann die betroffene Person nur reagieren, wenn sie von der Verletzung der Datensicherheit weiss. Daher muss der Verantwortliche für die Datenbearbeitung eine unbefugte Bearbeitung melden, wobei die Meldung zunächst an den Beauftragten geht und nur unter den Voraussetzungen von Absatz 4 an die betroffene Person.

Die Meldung hat ab dem Zeitpunkt der Kenntnisnahme so rasch als möglich zu erfolgen. Der Verantwortliche für die Datenbearbeitung muss schnell handeln, grundsätzlich innerhalb von drei Tagen, aber die Bestimmung gibt einen gewissen Ermessensspielraum. Massgebend ist dabei unter anderem das Ausmass der Gefährdung der betroffenen Person. Je erheblicher die Gefährdung, je grösser die Anzahl der betroffenen Personen, umso schneller muss gehandelt werden.

Nicht jede Verletzung der Datensicherheit rechtfertigt eine Meldung. Im Gegenteil: Eine Meldung ist nur nötig, wenn die Verletzung der Datensicherheit voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt. Dies soll verhindern, dass unbedeutende Verletzungen gemeldet werden. Der vorübergehende Verlust von verschlüsselten Daten, ohne dass der Entschlüsselungsschlüssel exponiert gewesen wäre oder hätte entdeckt werden können, oder der Zugang zu öffentlichen Daten über einen anderen Kanal müssen grundsätzlich nicht gemeldet werden.

Der Verantwortliche für die Datenbearbeitung muss die möglichen Folgen einer Verletzung für die betroffene Person in jedem Fall beurteilen und festhalten, weshalb er der Ansicht ist, dass die Verletzung nicht gemeldet werden muss.

Absatz 2 enthält die Mindestanforderungen an eine Meldung an den Beauftragten. Der Verantwortliche für die Datenbearbeitung muss zunächst die Art der Verletzung der Datensicherheit nennen, soweit ihm dies möglich ist. Dabei lassen sich vier Arten der Verletzung unterscheiden: die Vernichtung oder Löschung, der Verlust, die Veränderung und die Bekanntgabe von Daten an Unbefugte. Ebenfalls muss er die Folgen der Verletzung der Datensicherheit soweit als möglich umschreiben. Hierbei stehen die Folgen für die betroffene Person im Vordergrund; gemeint sind nicht

diejenigen für den Verantwortlichen für die Datenbearbeitung selbst. Schliesslich muss der Verantwortliche für die Datenbearbeitung angeben, welche Massnahmen er aufgrund der Verletzung ergriffen hat beziehungsweise welche Massnahmen er für die Zukunft vorschlägt. Dabei geht es um Massnahmen, welche die Verletzung beseitigen oder deren Folgen mildern. Insgesamt soll die Meldung dem Beauftragten erlauben, möglichst zeitnah und wirksam zu intervenieren. Wenn nicht alle Informationen unmittelbar zur Verfügung stehen, darf der Verantwortliche für die Datenbearbeitung die Meldung nicht verzögern, sondern muss unverzüglich alle Informationen mitteilen, über die er verfügt, und diese später ergänzen oder berichtigen.

Um die Übermittlung dieser Informationen zu vereinfachen, kann der Beauftragte eine Formularvorlage oder eine gesicherte Online-Kommunikation vorsehen.

In Absatz 3 geht es um den Fall, in dem die Verletzung der Datensicherheit beim Auftragsbearbeiter auftritt. In diesem Fall muss er den Verantwortlichen für die Datenbearbeitung so rasch als möglich jede unbefugte Datenbearbeitung zu melden. Es obliegt dann dem Verantwortlichen für die Datenbearbeitung, anschliessend eine Risikoabschätzung vorzunehmen und darüber zu entscheiden, inwieweit eine Meldepflicht gegenüber dem Beauftragten und der betroffenen Person besteht. Der Auftragsbearbeiter muss über jede Verletzung der Datensicherheit informieren und nicht nur über solche, die einer Meldung bedürfen. Obwohl diese Pflicht im Gesetz festgehalten ist, wird empfohlen, diese in den Verträgen mit den Auftragsbearbeitern ausdrücklich zu erwähnen.

Absatz 4 sieht in zwei spezifischen Fällen eine Information der betroffenen Person vor: wenn es die Umstände erfordern oder es der Beauftragte verlangt. Im ersten Fall geht es insbesondere um Situationen, in denen die betroffenen Personen dank der Meldung Massnahmen ergreifen können, um die Risiken für ihre Persönlichkeit oder ihre Grundrechte zu verringern, zum Beispiel indem sie ihre Zugangsdaten oder Passwörter ändern, oder auch weil ein bedeutendes Risiko besteht, dass die Daten öffentlich zugänglich gemacht werden. Im zweiten Fall kann der Beauftragte die Meldung an die betroffenen Personen verlangen, weil er entweder, im Gegensatz zum Verantwortlichen für die Datenbearbeitung, der Meinung ist, dass diese Massnahmen ergreifen könnten, oder weil es ein anderes wichtiges Interesse gibt, sie zu informieren.

Die Meldung muss schriftlich erfolgen (per Post oder per E-Mail, je nach Umständen). Wenn es nicht möglich oder zu schwierig ist, nur die betroffenen Personen zu informieren, zum Beispiel, weil es (noch) nicht möglich ist, diese genau zu

identifizieren, kann eine Meldung an eine grössere Anzahl Personen zugelassen werden, wenn dabei mindestens die betroffenen Personen informiert werden. In besonderen Fällen kann gemäss Absatz 5 Buchstabe c auch eine öffentliche Bekanntmachung anstelle einer individuellen Information vorgenommen werden.

Gemäss Absatz 5 kann der Verantwortliche für die Datenbearbeitung die Information an die betroffene Person in bestimmten Fällen einschränken, aufschieben oder darauf verzichten. Dies gilt nicht für die Meldung an den Beauftragten. Im Rahmen des Möglichen ist es besser, eine Meldung aufzuschieben, als darauf zu verzichten.

In Buchstabe a geht es um den Fall, in dem ein überwiegendes öffentliches Interesse, insbesondere die innere oder äussere Sicherheit des Staates, gegen die Meldung spricht oder diese eine Ermittlung, eine Untersuchung oder ein behördliches oder gerichtliches Verfahren gefährden könnte.

Nach Buchstabe b ist die Einschränkung ebenfalls zulässig, wenn die Information unmöglich ist oder einen unverhältnismässigen Aufwand erfordert. Eine Information ist unmöglich, wenn der Verantwortliche für die Datenbearbeitung gar nicht weiss, welche Personen von der Verletzung der Datensicherheit betroffen sind, beispielsweise, weil die Logfiles, aus denen dies ersichtlich wäre, nicht mehr vorhanden sind. Ein unverhältnismässiger Aufwand würde beispielsweise auch vorliegen, wenn bei einer grossen Anzahl Betroffener diese einzeln informiert werden müssten und die dadurch verursachten Kosten im Verhältnis zum Informationsgewinn für die betroffene Person unverhältnismässig erschienen. Diese Ausnahme sollte nicht angewandt werden, wenn die betroffenen Personen nützliche Massnahmen ergreifen können oder wenn eine öffentliche Bekanntgabe im Sinne von Buchstabe c möglich wäre.

Gemäss Buchstabe c kann der Verantwortliche für die Datenbearbeitung eine öffentliche Bekanntmachung wählen, wenn die betroffenen Personen dadurch auf vergleichbare Weise informiert werden. Dies ist der Fall, wenn die Information der betroffenen Person durch eine individuelle Information nicht substantiell verbessert wird und die betroffenen Personen Zugang zur öffentlichen Bekanntmachung hat.

Gemäss Buchstabe d muss der Verantwortliche für die Datenbearbeitung die Interessen eines Dritten berücksichtigen, wenn diese im Vergleich zur Information der betroffenen Person überwiegen. Um sich auf diese Ausnahme zu berufen, muss der Verantwortliche für die Datenbearbeitung eine Interessenabwägung vornehmen. Die Information darf nur in seltenen Fällen mit der Begründung eingeschränkt werden, dass das Interesse eines Dritten überwiegt.

1.26 Artikel 30b

Die Pflicht, eine Datenschutz-Folgenabschätzung vorzunehmen, entspricht den Anforderungen des europäischen Rechts und richtet sich nach den Artikeln 20 und 21 nDSG. Gemäss dem Grundsatz des Datenschutzes durch Technik handelt es sich um ein Instrument, mit dem die Risiken gewisser Bearbeitungen vorgängig erkannt und bewertet werden sollen. Da dieses Instrument neu ist, muss der Beauftragte die Behörden anleiten, indem er insbesondere Kriterien und Beispiele von Bearbeitungen liefert, die ein hohes Risiko mit sich bringen, oder eine Mustervorlage zur Verfügung stellt, um die Erstellung einer Datenschutz-Folgenabschätzung zu erleichtern. Andernfalls können sich die Behörden auch von der Projektmanagementmethode Hermes inspirieren lassen, die auf Bundesebene rege genutzt wird.

Nach Absatz 1 muss der Verantwortliche für die Datenbearbeitung eine Datenschutz-Folgenabschätzung durchführen, wenn die vorgesehene Datenbearbeitung voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt. Er kann eine gemeinsame Abschätzung erstellen, wenn er mehrere ähnliche Bearbeitungsvorgänge plant (gemeinsames Ziel). Entsprechend ist es nicht notwendig, jeden geplanten Bearbeitungsschritt einzeln zu prüfen, sondern die Abschätzung kann alle Vorgänge umfassen.

Der Verantwortliche für die Datenbearbeitung ist demnach verpflichtet, eine Prognose darüber abzugeben, welche Folgen die geplante Datenbearbeitung für die betroffene Person hat. Massgebend ist hierfür insbesondere, auf welche Weise und in welchem Umfang sich eine Bearbeitung auf die Persönlichkeit oder die Grundrechte der betroffenen Person auswirkt

Gemäss Absatz 2 ergibt sich ein hohes Risiko aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung. Je umfangreicher die Bearbeitung, je sensibler die bearbeiteten Daten, je umfassender der Bearbeitungszweck, umso eher ist ein hohes Risiko anzunehmen. Ein solches Risiko liegt vor, wenn in umfangreicher Form besonders schützenswerte Personendaten bearbeitet werden, wie dies beispielsweise bei medizinischen Forschungsprojekten (Bst. a), bei einem Profiling (Bst. b) oder bei der Überwachung umfangreicher öffentlicher Bereiche (Bst. c) der Fall sein kann.

Um zu beurteilen, ob es sich um ein hohes Risiko handelt, kann sich der Verantwortliche für die Datenbearbeitung auf die neun Kriterien der Artikel-29-

Datenschutzgruppe[8] stützen: Bewerten oder Einstufen (darunter das Erstellen von Profilen und Prognosen), automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung, systematische Überwachung, besonders schützenswerte oder personenbezogene Daten, Datenbearbeitung in grossem Umfang (Zahl betroffener Personen, verarbeitete Datenmenge, Dauer und geografisches Ausmass der Bearbeitungstätigkeit), Abgleichen oder Zusammenführen von Datensätzen, Daten zu schutzbedürftigen Betroffenen, innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen, Fälle, in denen die Verarbeitung an sich die betroffenen Personen an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung beziehungsweise Durchführung eines Vertrags hindert.

In Absatz 3 wird der Inhalt der Datenschutz-Folgenabschätzung ausgeführt. Zunächst muss die geplante Bearbeitung beschrieben werden (Vorgehen, eingesetzte Technologien, Zweck, Aufbewahrungsdauer), dann aufgezeigt werden, welche Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person die fraglichen Bearbeitungsvorgänge mit sich bringen können. Es handelt sich hier um eine Vertiefung der Risikobewertung, die bereits im Hinblick auf die Notwendigkeit einer Datenschutz-Folgenabschätzung vorzunehmen ist. So ist darzustellen, in welcher Hinsicht von der fraglichen Datenbearbeitung ein hohes Risiko ausgeht und wie dieses Risiko zu bewerten ist. Schliesslich muss die Datenschutz-Folgenabschätzung erläutern, mit welchen vorgesehenen Massnahmen diese Risiken bewältigt werden sollen (Pseudonymisierung, Datenminimierung, besondere Sicherheitsmassnahmen, Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen) oder was die Restrisiken sind. Schliesslich können auch die Interessen der betroffenen Person und des Verantwortlichen für die Datenbearbeitung berücksichtigt werden.

In Absatz 4 ist vorgesehen, dass der Verantwortliche für die Datenbearbeitung den Beauftragten vor der Bearbeitung informieren muss, wenn sich aus der Datenschutz-Folgenabschätzung ergibt, dass die geplante Bearbeitung trotz der geplanten Massnahmen ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person hätte. Diese Verpflichtung ist eingeschränkter als jene gemäss DSGVO oder SDSG, in denen verlangt wird, dass der Beauftragte jedes Mal

[8] Artikel-29-Datenschutzgruppe, «Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“» angenommen am 4. April 2017 und zuletzt überarbeitet und angenommen am 4. Oktober 2017 (WP 248 Rev. 01), S. 4.

konsultiert wird, wenn die geplante Bearbeitung ein hohes Risiko zur Folge hätte, wenn das Bundesorgan keine Massnahmen zur Abschwächung treffen würde.

Durch die Information kann der Beauftragte seine Beratungs- und Präventionsfunktion ausüben. Innerhalb von zwei Monaten kann er Einwände gegen die geplante Bearbeitung anbringen und geeignete Massnahmen vorschlagen. Nachdem er über eine Datenschutz-Folgenabschätzung benachrichtigt worden ist, überprüft der Beauftragte, ob die vorgeschlagenen Massnahmen zum Schutz der Grundrechte und der Persönlichkeit der betroffenen Person ausreichend sind. Kommt er zum Schluss, dass die geplante Bearbeitung in der vorgeschlagenen Form gegen die Bestimmungen des GIDA verstossen würde, schlägt er dem Verantwortlichen für die Datenbearbeitung geeignete Massnahmen vor, um die festgestellten Risiken einzudämmen. Erhält der Verantwortliche innerhalb der Zweimonatsfrist keine Nachricht vom Beauftragten, kann er grundsätzlich davon ausgehen, dass der Beauftragte keine Einwände gegen die vorgeschlagenen Massnahmen hat.

Dem Beauftragten bleibt es indes unbenommen, zu einem späteren Zeitpunkt eine Untersuchung zu eröffnen, wenn die Voraussetzungen nach Artikel 37 erfüllt sind. Dies kann insbesondere der Fall sein, wenn im Rahmen der Datenschutz-Folgenabschätzung die Risiken nicht korrekt eingeschätzt wurden und sich dementsprechend auch die fraglichen Massnahmen nicht als zielgenau oder als nicht ausreichend erweisen.

1.27 Artikel 30c

Jede Behörde, die dem GIDA unterstellt ist, muss einen Datenschutzdelegierten bestimmen. Der Begriff *délégué à la protection des données* (auf Deutsch: Datenschutzdelegierter) wurde auf Französisch von der Richtlinie (EU) 2016/680 übernommen, obwohl im nDSG und im SDSG die Rede von *conseiller à la protection des données* ist (auf Deutsch Datenschutzberater respektive Datenschutzverantwortlicher). Es handelt sich nur um einen terminologischen Unterschied.

Der Datenschutzdelegierte ist für betroffene Personen und Aufsichtsbehörden für Datenschutz und Öffentlichkeit die Hauptkontaktperson. Er überwacht die Einhaltung der Datenschutzvorschriften innerhalb einer Behörde und berät den Verantwortlichen für die Datenbearbeitung in Datenschutzbelangen. Der Verantwortliche für die Datenbearbeitung trägt jedoch bei Verletzungen der Rechtsvorschriften allein die Verantwortung.

Es kann ein Mitarbeiter oder eine Drittperson ernannt werden. Der Delegierte muss seine Funktion unabhängig ausüben, er ist gegenüber dem Verantwortlichen nicht weisungsgebunden, um seinen Beratungstätigkeiten korrekt nachzugehen. Nimmt die Behörde Dienstleistungen eines Dritten in Anspruch, so muss dies über einen Mandatsvertrag geschehen.

Absatz 2 Buchstabe a sieht vor, dass der Delegierte über die erforderlichen Fachkenntnisse verfügt, um diese Aufgabe zu übernehmen. So ist für diese Tätigkeit Fachwissen sowohl im Bereich der Datenschutzgesetzgebung als auch über technische Standards zur Datensicherheit erforderlich.

Die andere Bedingung besteht darin (Abs. 2 Bst. b), keine Tätigkeiten zu übernehmen, die mit seinen Aufgaben unvereinbar sind. Er darf beispielsweise keine Funktionen in den Bereichen Personalführung oder Informationssystemverwaltung haben.

1.28 Artikel 31

Dieser Artikel wird ergänzt, um den Ablauf der Gesuche um Zugang zu Personendaten zu klären. Dabei werden teilweise die Inhalte der bisherigen Artikel 48 und 51 übernommen, wobei nur die Frage des Zugangs zu Personendaten berücksichtigt wird. Der Zugang zu amtlichen Dokumenten wird im entsprechenden Kapitel behandelt.

In Absatz 1 ist nunmehr nicht nur das Recht vorgesehen, die Bestätigung der Bearbeitung mit bestimmten Informationen zu verlangen, sondern insbesondere, diese unter Vorbehalt der Ausnahmen gemäss Artikel 32 zu erhalten.

Der Zugang zu den Daten umfasst für die betroffene Person das Recht, folgende Informationen zu erhalten: die Identität und die Kontaktangaben des Verantwortlichen für die Datenbearbeitung; die gesetzliche Grundlage für die Bearbeitung und den Bearbeitungszweck; welche Daten bearbeitet werden; alle Angaben über die Herkunft der Daten; die Datenempfänger oder die Kategorien der Datenempfänger; die Aufbewahrungsdauer oder mindestens die Kriterien für die Festlegung dieser Dauer; das Vorhandensein einer automatisierten Einzelentscheidung sowie die Logik, auf die sich diese Entscheidung stützt.

Es steht dem Verantwortlichen für die Datenbearbeitung frei, die Empfänger oder die Kategorien der Empfänger anzugeben. Wenn er die Identität der Empfänger nicht offenlegen möchte, kann er sich damit begnügen, die Kategorie anzugeben. Die Auftragsbearbeiter gehören zu den Empfängern.

Wenn es nicht möglich ist, Aufbewahrungsdauer der Daten mitzuteilen, kann der Verantwortliche für die Datenbearbeitung die Kriterien für die Festlegung dieser Dauer angeben.

Im Falle einer automatisierten Einzelentscheidung muss vorgängig informiert werden (Art. 20). Es wird nicht verlangt, die Logik, auf die sich diese Entscheidung stützt, im Vorfeld zu erklären. Im Fall eines Gesuchs um Zugang muss jedoch nicht nur das Vorhandensein, sondern auch die Grundlage dieser Entscheidung mitgeteilt werden (Art. 31 Abs. 1 Bst. h). Dabei müssen nicht unbedingt die Algorithmen mitgeteilt werden, die Grundlage der Entscheidung sind, weil es sich dabei oft um Geschäftsgeheimnisse handelt. Vielmehr müssen die Grundannahmen der Algorithmus-Logik genannt werden, auf der die automatisierte Einzelentscheidung beruht. Zum Beispiel können Details über die wichtigsten Eigenschaften, die bei der Entscheidung berücksichtigt wurden, die Informationsquelle und deren Relevanz sowie die durchgeführten Tests, um sicherzustellen, dass die Entscheidungen gerecht, effizient und unparteiisch sind, weitergegeben werden.

Absätze 3 und 4 betreffen Formfragen und wurden aus dem bisherigen Artikel 48 Absätze 1 und 3 übernommen. Absatz 5 nimmt die Frist ins Gesetz auf, die bisher im Ausführungsreglement enthalten war. Absatz 6 wird eingeführt, um die Behandlung des Gesuchs um Zugang zu Daten mit dem Zugang zu amtlichen Dokumenten (Art. 12b Abs. 2) zu vereinheitlichen.

Absatz 7 entspricht grösstenteils dem bisherigen Artikel 51. Ein Dritter ist insbesondere betroffen, wenn seine Personendaten im Rahmen eines Gesuchs um Zugang offenbart werden können. Dieser Zugang muss der Persönlichkeit des Dritten schaden. Es ist vorzuziehen, die Personendaten Dritter zu schwärzen.

1.29 Artikel 32

Hier wird nur die Einschränkung des Zugangsrechts behandelt. Die Überschrift des Artikels wird entsprechend angepasst.

Es ist möglich, das Recht auf Einsichtnahme einzuschränken, wenn es sich um eine notwendige und verhältnismässige Massnahme handelt, um behördliche oder gerichtliche Untersuchungen, Ermittlungen und Verfahren nicht zu behindern, die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung nicht zu gefährden und um die öffentliche Sicherheit oder die Rechte und Freiheiten anderer zu schützen. Die Bekanntgabe von Auskünften oder das Recht auf Einsichtnahme kann auch aufgeschoben werden, obwohl dies im Gesetz nicht ausdrücklich vorgesehen ist.

Absatz 2 wird hinzugefügt, um auszuführen, dass eine Beschränkung oder Verweigerung des Zugangs vom Verantwortlichen für die Datenbearbeitung begründet werden muss. Dies soll der betroffenen Person ermöglichen, die Einschränkung oder Verweigerung zu verstehen und allenfalls anzufechten. Die Einschränkung oder Verweigerung kann natürlich vorübergehend sein. Sowohl auf europäischer als auch auf nationaler Ebene geht es bei den jüngsten Entwicklungen im Datenschutz insbesondere darum, die Rechte der betroffenen Personen zu stärken. Die entsprechenden Rechtsmittel sind in Artikel 52 vorgesehen.

1.30 Artikel 33

Die betroffene Person hat nicht nur ein Zugangsrecht zu ihren Daten, sondern auch das Recht, diese berichtigen oder vernichten zu lassen, wenn sie falsch sind. Ein Zugangsrecht wäre nicht sehr sinnvoll, wenn es nicht dazu führen würde, dass die betroffene Person sowohl die durchgeführten Datenbearbeitungen als auch die Daten an sich überprüfen und anfechten könnte.

Die Änderungen in Absatz 1 sind hauptsächlich redaktionell, materiell ändert sich nichts. Absatz 2 ist unverändert.

Absatz 3 wird dahingehend geändert, dass die betroffene Person verlangen kann, dass erwähnt wird, dass die Daten umstritten sind und gemäss Artikel 22 Absatz 4 Einsprache eingelegt wurde, sofern der Verantwortliche für die Datenbearbeitung den Beweis der Genauigkeit der strittigen Daten nicht umgehend erbringen kann. Die provisorische Löschung gemäss bisherigem Absatz 3 wird gestrichen.

In bestimmten Fällen, die unter Absatz 3bis Buchstaben a bis d aufgelistet sind, kann der Verantwortliche für die Datenbearbeitung die Bearbeitung beschränken, anstatt die Daten zu löschen oder zu vernichten.

In einem neuen Absatz 3ter ist zudem vorgesehen, dass der Verantwortliche für die Datenbearbeitung den Empfänger unverzüglich darüber informiert, wenn ungenaue Daten weitergegeben oder Daten widerrechtlich weitergegeben wurden. Der Empfänger muss die fraglichen Daten berichtigen oder löschen. Die Pflicht gilt nicht uneingeschränkt, aber die Behörde muss dennoch einen vernünftigen Aufwand betreiben, um die Empfänger auszumachen und zu informieren.

In Absatz 3quater ist die Möglichkeit vorgesehen, dass der Verantwortliche für die Datenbearbeitung die Rechte gemäss Absatz 1 nicht erfüllt, wenn es gerechtfertigte Gründe für die Bearbeitung gibt, die Vorrang vor den Interessen und Grundrechten der betroffenen Person haben.

1.31 Artikel 34

Die Einsprache gegen die Bekanntgabe, was dem ehemaligen Begriff «Sperrung» entspricht, ist nun unter Artikel 22 Absätze 4 und 5 zu finden. Dazu kommt gemäss Artikel 9 Absatz 1 Buchstabe d des Übereinkommens 108+ ein allgemeineres Recht, sich gegen jede Datenbearbeitung zu stellen. Entsprechend wurden der Randtitel sowie der Inhalt von Artikel 34 komplett geändert.

In Artikel 34 ist vorgesehen, dass die betroffene Person, die ein schutzwürdiges Interesse glaubhaft macht, jederzeit dagegen Einsprache erheben kann, dass Personendaten über sie bearbeitet werden. Es obliegt der betroffenen Person, für ihre Einsprache ein schutzwürdiges Interesse geltend zu machen.

Unmittelbar nach Erhalt eines Gesuchs um Ausübung des Einspracherechts muss der Verantwortliche für die Datenbearbeitung die Bearbeitung einschränken, solange geprüft wird, ob das von der betroffenen Person geltend gemachte schutzwürdige Interesse die Fortführung der Bearbeitung überwiegt. Die betroffene Person muss über den Entscheid des Verantwortlichen für die Datenbearbeitung informiert werden. Dieser muss bei Ablehnung in der Lage sein zu beweisen, dass kein schutzwürdiges Interesse vorliegt.

Das Gesuch um Einsprache gegen eine Bearbeitung ist keiner Formvorschrift unterworfen.

1.32 Artikel 35

Im Allgemeinen mussten Status und Rolle der Aufsichtsbehörde überdacht werden, um ihre Unabhängigkeit zu stärken und ihr die Möglichkeit zu geben, gegenüber den Verantwortlichen für die Datenbearbeitung infolge einer Untersuchung von Amtes wegen oder auf Anzeige verbindliche Entscheide zu fällen.

Es wird also eine zweiteilige Struktur beibehalten, die sich aus einem Datenschutz- und Öffentlichkeitsbeauftragten (der Beauftragte) und einer kantonalen Datenschutz- und Öffentlichkeitskommission (die Kommission) zusammensetzt. Eine solche Struktur ist in den lateinischen Kantonen verbreitet. Sie unterscheidet sich vom Bundesmodell, das keine Datenschutzkommission vorsieht. Im Gegensatz zur bisherigen Organisation und ausgehend vom Modell in den Kantonen Jura und Neuenburg sind die beiden Behörden nun unabhängig voneinander. Einerseits mussten die Verfahren vereinfacht und andererseits gewährleistet werden, dass der Beauftragte seine Rolle als Berater und Mediator wahrnehmen kann. Wenn er der Entscheidungsbehörde (die Kommission) angegliedert ist oder von ihr abhängt, verliert er die notwendige Unabhängigkeit, um die Behörden zu beraten. Die Grösse

des Kantons lässt es auch nicht zu, im Büro des Beauftragten ausreichend Personal zu beschäftigen, sodass sich einige mit der Beratung beschäftigen und andere Entscheide fällen könnten, wie es auf Bundesebene möglich ist. Überschrift 4 wird entsprechend angepasst. Der Beauftragte hat hauptsächlich Aufgaben im Bereich Beratung und Mediation, während die Kommission die erstinstanzliche Entscheidungsbehörde ist. Die Kommission ist eine unabhängige Justizbehörde und kein politisches Organ. Die beiden Behörden üben ihre Aufsicht auch in den Gemeinden weiter aus.

Absatz 2 sieht vor, dass der Beauftragte sowie der Kommissionspräsident und die Kommissionsmitglieder vom Grossen Rat ernannt werden. Dieser Wahlmodus entspricht den Bestimmungen des nDSG (Art. 39) und soll die Unabhängigkeit der Aufsichtsbehörde gegenüber dem Staatsrat und der Verwaltung gewährleisten. Es handelt sich um eine Ernennung und die Details der Funktion müssen im GIDA, allenfalls in der ARGIDA, geregelt werden, aber nicht in Form eines privaten Mandatsvertrags.

Der Beauftragte sowie der Kommissionspräsident und die Kommissionsmitglieder sind natürlich an das Amtsgeheimnis gebunden. Das Amtsgeheimnis umfasst alle vertraulichen Informationen, von denen sie bei der Ausübung ihrer Aufgaben und Befugnisse Kenntnis erhalten, auch nach Beendigung der Tätigkeit. Diese Pflicht gilt auch für die Meldung durch natürliche Personen von Verletzungen des vorliegenden Gesetzes.

Der Beauftragte sowie der Kommissionspräsident und die Kommissionsmitglieder üben ihre Funktionen unabhängig und unparteiisch aus. Die Aufsichtsbehörden müssen sowohl funktionell, institutionell, personell als auch materiell unabhängig sein[9]. Gemäss Absatz 3 dürfen sie weder Anweisungen von einer Behörde oder Dritten erhalten noch einholen. Sie dürfen weder direkt noch indirekt von aussen beeinflusst werden. Die beiden Organe sind auch voneinander unabhängig und erfüllen ihre jeweilige Aufgabe selbstständig. Der Beauftragte gehört weder der Kommission an noch erhält er von ihr Anweisungen. Damit wird bezweckt, dass er über ausreichend Spielraum verfügt, Probleme des Ausstands vermieden werden und ein pragmatischer, flexibler und bürgernaher Ansatz verfolgt werden kann, wie in verschiedenen anderen Schweizer Kantonen. Die Behörden sind verpflichtet, mit dem Beauftragten und der Kommission zusammenzuarbeiten.

[9] Siehe insbesondere «Unabhängigkeit der kantonalen Aufsichtsbehörde für Datenschutz», Rechtsgutachten im Auftrag der Sicherheits- und Justizdirektion des Kantons Freiburg durch Bernhard Waldmann und André Spielmann, Februar 2010.

Im Hinblick auf die Selbstständigkeit und Unabhängigkeit müssen sie über die notwendigen Mittel und insbesondere je ein eigenes Budget verfügen. Über den Parlamentsdienst legen sie dem Grossen Jahr zudem jedes Jahr ihren Budgetentwurf vor (Abs. 4). Sowohl der Beauftragte als auch die Kommission sind dem kantonalen Finanzinspektorat unterstellt.

Sowohl der Beauftragte als auch die Kommission müssen nach Absatz 5 jährlich einen Tätigkeitsbericht verfassen. Dieser muss bis am 31. März eingereicht werden. Er wird an den Staatsrat und den Grossen Rat gerichtet und veröffentlicht. Dies ist nicht nur wichtig, um die Tätigkeit der Aufsichtsbehörde zu kontrollieren, sondern insbesondere auch, um zur Sensibilisierung der Behörden und der Öffentlichkeit beizutragen. Im Bericht können die Art der gemeldeten Verletzungen sowie die Art der vorgesehenen Sanktionen aufgelistet werden.

1.33 Artikel 36

In Absatz 1 wird die Mandatsdauer des Beauftragten festgehalten, die weiterhin vier Jahre beträgt. Die Verlängerung wird auf drei Mandate beschränkt (maximal zwölf Jahre). Die Amtsdauer des Beauftragten beginnt am 1. Januar nach Beginn der Legislaturperiode des Grossen Rates.

Im bisherigen Gesetz war die Mandatsdauer des Beauftragten nicht beschränkt. Dieser Grundsatz wird in Übereinstimmung mit dem nDSG und dem europäischen Recht geändert. Durch diese Massnahme soll die Unabhängigkeit des Beauftragten als Behörde gestärkt werden. Er soll nicht aus Furcht, nicht wiedergewählt zu werden, in der Erfüllung des gesetzlichen Auftrags zurückgehalten werden.

Der Beauftragte kann unter Einhaltung einer Frist von sechs Monaten verlangen, von seiner Funktion befreit zu werden. Bei einem Rücktritt weniger als sechs Monate vor der neuen Legislaturperiode kann auf der Grundlage von Artikel 36a ausnahmsweise eine Person bestimmt werden, die das Amt interimistisch ausübt. Um seine Unabhängigkeit zu gewährleisten, wird in Absatz 2 ausgeführt, dass er nur in sehr begrenzten Fällen von seiner Funktion enthoben werden kann. Dies trifft zu, wenn er entweder dauerhaft unfähig ist, seine Aufgaben auszuführen, oder bei der Ausübung seiner Funktion einen schwerwiegenden Fehler begangen hat, zum Beispiel eine strafbare Handlung im Zusammenhang mit seiner Tätigkeit oder die seine Glaubwürdigkeit in Zweifel ziehen würde. Die Entscheidung, den Beauftragten von seiner Funktion zu entheben, wird auf Vormeinung der Kommission vom Grossen Rat als Ernennungsbehörde getroffen. Diese Möglichkeiten müssen sehr restriktiv ausgelegt werden und dürfen keinesfalls dazu dienen, ihn an der Ausübung seiner gesetzlichen Aufgaben zu hindern.

Gemäss Absatz 3 verfügt der Beauftragte über ein ständiges Sekretariat und stellt sein Personal an. In Artikel 35 Absatz 3 wird festgehalten, dass er über ein eigenes Budget verfügt. Das Budget muss alle Ausgaben umfassen (Löhne, Sozialabgaben, Mieten, Bibliothek und Informatikmaterial, Weiterbildung, Mandate Dritter usw.). Der Beauftragte ist administrativ dem Parlamentsdienst angegliedert. Dieser hat jedoch keine Weisungsbefugnis gegenüber dem Beauftragten. Es handelt sich um eine rein administrative Angliederung, durch welche die Unabhängigkeit des Beauftragten nicht in Frage gestellt wird.

In Absatz 4 wird der Grundsatz festgehalten, dass der Beauftragte weder eine zusätzliche Erwerbstätigkeit ausüben noch ein Amt der Eidgenossenschaft oder eines Kantons bekleiden und auch nicht als Mitglied der Geschäftsleitung, des Verwaltungsrats, der Aufsichtsstelle oder der Revisionsstelle eines Handelsunternehmens tätig sein darf und zwar unabhängig davon, ob die Tätigkeit bezahlt ist oder nicht. Er darf also auch nicht Mitglied des Staatsrats oder des Grossen Rates sein. Der Begriff «Kanton» ist in einem weiten Sinne zu verstehen und umfasst auch die Gemeinden, Bezirke, Kreise und Körperschaften des öffentlichen Rechts. Unter Vorbehalt von Interessenkonflikten gilt das Verbot der Nebenbeschäftigung nicht für das Personal.

Ausnahmsweise kann das Büro des Grossen Rates dem Beauftragten gestatten, eine Nebenbeschäftigung auszuüben, wenn dadurch die Ausübung der Funktion sowie seine Unabhängigkeit und sein Ansehen nicht beeinträchtigt werden. Dies könnte zum Beispiel bei einer beschränkten akademischen Tätigkeit der Fall sein. Der Entscheid muss im Amtsblatt veröffentlicht werden.

Absatz 4 gilt nicht für die Kommission. Sie ist dennoch verpflichtet, darauf zu achten, dass es zu keinen Interessenkonflikten kommt.

In Absatz 5 wird ausgeführt, dass schriftliche Unterlagen und andere Dokumente, die der Beauftragte im Rahmen seiner Tätigkeit erstellt, dem Staat gehören.

1.34 Artikel 36a

In dieser neuen Bestimmung geht es um die dauerhafte und vorübergehende Verhinderung des Beauftragten. Gemäss Absatz 1 kann das Büro des Grossen Rates bei dauerhafter Verhinderung des Beauftragten auf Vormeinung der Kommission eine Person bezeichnen, die das Amt interimistisch ausübt. Der Beauftragte *ad interim* übt das Amt so lange aus, wie die Verhinderung dauert.

In Absatz 2 ist vorgesehen, dass das Büro des Grossen Rates bei vorübergehender Verhinderung des Beauftragten auf Vormeinung der Kommission eine Person bezeichnen kann, die diese Funktion *ad hoc* übernimmt.

In beiden Fällen bezieht sich die Vormeinung der Kommission nur auf die Verhinderung des Beauftragten.

1.35 Artikel 37

Der Beauftragte hat vorwiegend Beratungs-, Sensibilisierungs- und Mediationsaufgaben. Er kann auch Empfehlungen abgeben und von seinem umfassenden Recht Gebrauch machen, die Kommission anzurufen oder gegen deren Entscheide Beschwerde einzulegen.

Absatz 1 wird vervollständigt, damit der Beauftrage eine Untersuchung gegen eine Behörde einleiten kann, wenn es Hinweise darauf gibt, dass eine Bearbeitung den Bestimmungen des Datenschutzes zuwiderlaufen könnte (Bst. a). Der Beauftragte kann von Amtes wegen oder auf Anzeige hin handeln, was ebenfalls von Buchstabe c abgedeckt ist. Der Beauftragte kann eine Angelegenheit auch jederzeit der Kommission zum Entscheid vorlegen, der durch Sanktionen gemäss Artikel 292 StGB begleitet werden kann (Bst. d) und sein Beschwerderecht gemäss Artikel 53 ausüben (Bst. e). Buchstabe c wird ergänzt, damit der Beauftragte eine Anzeige nicht nur behandeln, sondern den Urheber der Anzeige auch über die darauf gestützten Schritte und das Ergebnis einer allfälligen Untersuchung informieren kann. Der Urheber der Anzeige hat keine Parteistellung. Buchstabe f wird dahingehend ergänzt, dass der Beauftragte nicht nur die in Artikel 25 Absatz 3 erwähnten Garantien genehmigen, sondern allgemein überprüfen kann, ob die grenzüberschreitende Bekanntgabe von Daten im Einklang mit dem gesetzlichen Rahmen geschieht. Auch wenn Buchstabe b nicht geändert wurde, muss ergänzt werden, dass die Arbeit des Beauftragten die Sensibilisierung der Öffentlichkeit auf den Datenschutz beinhaltet, wie in Artikel 15 Absatz 2 Buchstabe e des Übereinkommens 108+ verlangt wird.

Er muss auch geeignete Massnahmen vorschlagen, wenn er im Fall einer Datenschutz-Folgenabschätzung aufgrund einer Bearbeitung konsultiert wird, die ein erhöhtes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person darstellen würde (Bst. j).

Im Rahmen seiner Beratungstätigkeit muss der Beauftragte zu gesetzgeberischen Entwürfen, die mit dem Datenschutz und dem Öffentlichkeitsprinzip in Verbindung stehen, oder in anderen gesetzlich vorgesehenen Fälle, seine Meinung abgeben (Bst. h). Das bedeutet, dass ihm jeder betroffene Gesetzesentwurf übermittelt werden

muss. Er kann sich natürlich auch zu einem Gesetzesentwurf äussern, ohne dazu offiziell aufgefordert worden zu sein.

Infolge der Einführung eines Registers über die Bearbeitungstätigkeiten auf kantonaler Ebene und der Pflicht, Verletzungen der Datensicherheit zu melden, muss der Beauftragte diese Register gemäss den Artikeln 30 und 30a (Bst. i) führen.

Es wird auch daran erinnert, dass der Beauftragte seinen Tätigkeitsbericht gemäss Artikel 35 Absatz 4 veröffentlichen muss (l).

Der Beauftragte ist nicht nur dazu befugt, sondern muss von Amtes wegen einschreiten, um für die Einhaltung des vorliegenden Gesetzes zu sorgen. Diesbezüglich verfügt er über volle Untersuchungsbefugnisse. Gemäss Absatz 2 kann er Akten verlangen, Auskünfte einholen und sich Datenbearbeitungen vorführen lassen. Die betroffenen Behörden sind verpflichtet, bei der Ermittlung der Sachverhalte mitzuarbeiten. Nachdem er mit dem Vorgesetzten der kontrollierten Behörde Kontakt aufgenommen hat, hat er insbesondere Zugang zu allen Auskünften, Dokumenten, Registern und notwendigen Daten, Räumlichkeiten und Anlagen und kann Zeugen anhören sowie Gutachten anordnen. Anders gesagt hat er jederzeit Zugang zu den Räumlichkeiten, in denen sich Datensammlungen befinden, kann sich diese und die Datenbearbeitungen vorführen lassen, das Personal befragen sowie Auskünfte und Akten verlangen. In diesem Rahmen kann ihm das Amtsgeheimnis nicht entgegengehalten werden.

Die Pflicht gemäss bisherigem Absatz 4, der Kommission Bericht zu erstatten, wird gestrichen, um die Unabhängigkeit der beiden Behörden zu gewährleisten.

1.36 Artikel 37a

In dieser Bestimmung geht es um die Unabhängigkeit und die Organisation des Beauftragten, insbesondere, dass der Beauftragte keine Anweisungen von einer Behörde oder Dritten erhält (Abs. 1) und sich selbst organisiert (Abs. 2). Dazu werden ihm vom Kanton Wallis ständige Räumlichkeiten zur Verfügung gestellt (Abs. 3).

Sowohl der Beauftragte als auch seine Mitarbeitenden unterstehen dem Gesetz über das Personal des Staates Wallis (Abs. 4). Der Beauftragte ist allerdings dem vorgesehenen Personalcontrolling nicht unterstellt, um jede Beeinträchtigung seiner Unabhängigkeit zu verhindern.

1.37 Artikel 37b

Die Zusammenarbeit zwischen den kantonalen, eidgenössischen und ausländischen Datenschutzbehörden ist in Artikel 37b vorgesehen.

Der Grundsatz ist in Absatz 1 festgehalten. Die Absätze 2 bis 4 entsprechen weitgehend dem Inhalt von Artikel 26 SDSG in Bezug auf die Amtshilfe zwischen dem Beauftragten und ausländischen Behörden. Die vorgesehenen Bedingungen dürften bezüglich der Zusammenarbeit mit den schweizerischen Datenschutzbehörden (kantonal und eidgenössisch) keine Probleme bereiten.

1.38 Artikel 38

Die Kommission besteht weiterhin aus fünf Mitgliedern, neu ist aber in Absatz 1 vorgesehen, dass mindestens zwei Juristen und ein Informatikspezialist Mitglied sein müssen. Die Kommission wird vom Grossen Rat ernannt und funktioniert als unabhängige Justizbehörde. Sie ist kein politisches Organ.

Die Mandatsdauer von vier Jahren ist erneuerbar. Da es sich um eine Kollegialbehörde handelt, scheint es nicht nötig zu sein, die Dauer zu begrenzen. Es wird nur daran erinnert, dass die übrigen Tätigkeiten der Kommissionsmitglieder mit ihrer Funktion vereinbar sein müssen. Da es sich um eine sehr eingeschränkte Funktion handelt, wäre es nicht zielführend, jede andere Tätigkeit auszuschliessen.

Das Sekretariat wird künftig nicht mehr durch den Beauftragten sichergestellt, da die beiden Behörden voneinander unabhängig sind. Es wird vorgeschlagen, die Kommission als Justizorgan administrativ dem Parlamentsdienst anzugliedern, von dem sie bei Bedarf auch logistisch unterstützt werden kann. Ihre Unabhängigkeit wird dadurch nicht in Frage gestellt. In Anbetracht der vermutlich geringen und unregelmässigen Tätigkeit ist ein unabhängiges Sekretariat nicht gerechtfertigt.

Absatz 2 sieht vor, dass die Kommission mindestens einmal jährlich und zusätzlich je nach zu behandelnden Fällen zusammentritt. Sie kann in Anwesenheit von mindestens drei Mitgliedern gültig beraten. Bei Bedarf kann die Kommission externe Experten hinzuziehen (Abs. 3). In Anbetracht der Häufigkeit, mit der die Kommission zusammentritt, ist es nicht notwendig, dass sie über ständige Räumlichkeiten verfügt.

Zudem regelt der Grosse Rat die Organisation und die Funktionsweise der Kommission sowie die Entschädigung ihrer Mitglieder (Abs. 4). Er muss ihr Organisationsreglement veröffentlichen.

1.39 Artikel 39

Die Kommission ist die erstinstanzliche Entscheidungsbehörde, wenn ein Streitfall nicht durch Mediation gelöst werden kann. Gemäss Absatz 1 entscheidet sie nur über die Fälle, in denen sie angerufen wird. Sie kann nicht von Amtes wegen handeln, sie kann jedoch vom Beauftragten, einer Behörde oder einer betroffenen Person angerufen werden.

Die Kommission verfügt über dieselben Untersuchungsbefugnisse wie der Beauftragte. Das heisst, dass sie Akten verlangen, Auskünfte einholen und sich Datenbearbeitungen vorführen lassen kann. Die betroffenen Behörden sind verpflichtet, bei der Ermittlung der Sachverhalte mitzuarbeiten. Nachdem sie mit dem Vorgesetzten der kontrollierten Behörde Kontakt aufgenommen hat, hat sie insbesondere jederzeit Zugang zu den Räumlichkeiten, in denen sich Datensammlungen befinden, kann sich diese und die Datenbearbeitungen vorführen lassen, das Personal befragen sowie Auskünfte und Akten verlangen. In diesem Rahmen kann ihr das Amtsgeheimnis nicht entgegengehalten werden.

Absatz 3 betrifft die Befugnisse der Kommission. Sie kann insbesondere die Behörde informieren, anordnen, dass die Bearbeitungen mit dem Gesetz in Übereinstimmung gebracht werden, eine Bearbeitung teilweise oder vollständig auszusetzen oder abzubrechen, die Daten vollständig oder teilweise zu löschen oder zu vernichten sowie eine Bearbeitung einschränken oder verbieten.

Absatz 4 weist schliesslich darauf hin, dass sie ihren Tätigkeitsbericht in Übereinstimmung mit Artikel 35 Absatz 4 veröffentlicht muss. Die Kompetenz, sich zu Gesetzesentwürfen zu äussern, wurde gestrichen, da diese nun dem Beauftragten obliegt. Dadurch kann verhindert werden, dass die Kommission zu stark beansprucht wird.

1.40 Artikel 52

Die Verfahrensbestimmungen und die Rechtsmittel wurden aufgrund der neuen Definition der Aufsichtsbehörden vollständig überarbeitet. Das Gesuch um Zugang, das bisher unter den Artikeln 48 bis 50 geregelt war, wird neu unter den Artikeln 12 ff. für die amtlichen Dokumente und 31 ff. für die Personendaten behandelt.

Absatz 1 verpflichtet die Behörde, die einem Gesuch nicht Folge leisten will, die betroffenen Personen darüber zu informieren und sie über die Möglichkeit der Eröffnung eines Mediationsverfahrens beim Beauftragten gemäss Artikel 49 in Kenntnis zu setzen. Die bisherige Frist für die Eröffnung einer Mediation ist nicht mehr notwendig, da die Behörde keinen Entscheid mehr fällen muss.

1.41 Artikel 53

Um eine Überlastung der Kommission zu verhindern, muss die Mediation gefördert werden. Der Beauftragte muss betreffend Durchführung weitgehend frei sein und es wird darauf verzichtet, verbindliche Verfahrensregeln vorzusehen.

Sobald es zu Meinungsverschiedenheiten infolge eines auf das GIDA gestützten Gesuchs kommt, soll die Möglichkeit einer Mediation bestehen (Abs. 1bis). Sowohl

die Behörde, die gesuchstellende Person als auch der betroffene Dritte kann beim Beauftragten eine Mediation verlangen.

Das Verfahren muss einfach sein, damit der Beauftragte jedoch effizient arbeiten kann, muss wenigstens ein schriftliches und kurz begründetes Gesuch mit allen sachdienlichen Unterlagen eingereicht werden.

Der Beauftragte ist frei, die Mediation den Umständen entsprechend so durchzuführen, wie er es für richtig hält. In Absatz 2ter wird ausgeführt, dass er eine Mediationsverhandlung mit allen Parteien durchführen kann. Eine solche Verhandlung ist nicht obligatorisch, insbesondere wenn die Lage juristisch klar ist und der Beauftragte auf der Grundlage der Informationen in seinem Besitz bereits eine Empfehlung formulieren kann.

Wird eine Verhandlung einberufen, können die Parteien in Begleitung ihres Vertreters an der Mediation teilnehmen. Es ist nicht notwendig, dass der Beauftragte ein Protokoll der Mediationsverhandlung erstellt, ausser zur Feststellung der Abwesenheit einer Partei. Kommt bei der Mediation eine Vereinbarung zustande, ist dies ausreichend und der Beauftragte muss keine Empfehlung abgeben. Wird keine Vereinbarung erzielt, gibt der Beauftragte Empfehlungen ab, die innerhalb von 10 Tagen ab Scheitern der Mediation vorliegen muss. Diese Frist kann im gegenseitigen Einverständnis ausgesetzt werden. Wenn eine der Parteien nicht erscheint, gilt die Mediation als gescheitert und die Kosten können auf die abwesende Partei überwälzt werden.

1.42 Artikel 54a

Gemäss Absatz 1 hat die Behörde, die gesuchstellende Person oder der betroffene Dritte klassischerweise die Möglichkeit, die Kommission anzurufen, wenn die Mediation scheitert. Die Mediation wird als gescheitert betrachtet, wenn keine Vereinbarung erzielt wird und die Behörde der Empfehlung des Beauftragten nicht Folge leistet oder wenn die gesuchstellende Person oder der betroffene Dritte mit der Empfehlung des Beauftragten nicht zufrieden ist (unabhängig davon, ob sie von der Behörde befolgt wird oder nicht) oder wenn die Vereinbarung nicht eingehalten wird.

Eine direkte Anrufung der Kommission durch eine Behörde oder eine betroffene Person ohne vorgängige Mediation ist nicht vorgesehen. Der Beauftragte muss die Kommission jedoch auch spontan anrufen können, unabhängig von der Ansicht der Mediationsparteien oder ohne Mediation, damit das GIDA korrekt umgesetzt wird. Dadurch kann beispielsweise über einen Fall von allgemeinem Interesse entschieden

werden, auch wenn die Parteien kein direktes Interesse daran haben oder wenn eine Behörde eine Empfehlung des Beauftragten nicht befolgt.

Beim Verfahren vor der Kommission müssen die Verfahrensregeln eingehalten werden und den Parteien, auch dem Beauftragten, muss ein Anhörungsrecht gewährt werden (Abs. 2).

Die Konsultation oder Anrufung des Beauftragten soll die Arbeit der Kommission erleichtern, da sie dadurch ein möglichst vollständiges Dossier vorliegen hat. Es ist grundlegend, dass die Kommission vonseiten des Beauftragten so viele Elemente wie möglich erhält. Der Beauftragte kann sich dabei auf seine praktischen Kenntnisse des Bereichs stützen, wodurch vermieden werden kann, dass die Kommission zu viel Zeit damit verliert, sich in die Dossiers einzuarbeiten. Um die Unabhängigkeit der Kommission zu wahren, bleibt sie jedoch frei, alle Untersuchungshandlungen vorzunehmen, die ihr nützlich erscheinen.

1.43 Artikel 56

Absatz 1 wird angepasst, da künftig nur die Entscheide der Kommission mit Beschwerde beim Kantonsgericht angefochten werden können.

Absatz 2 wird vervollständigt und gewährt dem Beauftragten das Recht, bei sämtlichen rechtsprechenden Behörden auf kantonaler oder eidgenössischer Ebene Beschwerde gegen jeden Entscheid der Kommission oder einer Behörde, die das vorliegende Gesetz anwendet, einzulegen. Dies entspricht der Unabhängigkeit des Beauftragten.

In Absatz 3 wird der Zweck des bisherigen Absatzes 1 übernommen und daran erinnert, dass das Verfahren ergänzend im Gesetz über das Verwaltungsverfahren und die Verwaltungsrechtspflege (VVRG) geregelt wird.

In Absatz 4 sind die Verfahrensregeln in Zusammenhang mit einem Gesuch um Ausstand des Beauftragten oder eines Kommissionsmitglieds geregelt. Das Gesamtgericht des Kantonsgerichts ist zuständig, sich zu einem solchen Ausstandsgesuch zu äussern. Wenn das Kantonsgericht beim Ausstandsverfahren Partei ist, hat der Grosse Rat das Gesuch um Ausstand zu prüfen.

1.44 Artikel 56a

Im Rahmen der Umsetzung der Richtlinie (EU) 2016/680 müssen einige bestimmte Rechte gewährt werden. Es ist nicht gerechtfertigt, deswegen das im GIDA vorgesehene System komplett zu ändern. Deshalb werden eine neue Überschrift 6a (Bestimmung über den Datenschutz im Rahmen der Anwendung des Schengen-Besitzstands in Strafsachen) sowie ein neuer Artikel 56a eingeführt.

Dieser gilt nur für im Rahmen der Anwendung des Schengen-Besitzstands in Strafsachen bearbeitete Daten.

Gemäss Absatz 1 Buchstabe a hat die betroffene Person ausschliesslich im Rahmen der Anwendung des Schengen-Besitzstands in Strafsachen das Recht, den Beauftragten anzurufen, damit dieser alle notwendigen Überprüfungen vornehmen kann, wenn bestimmte Rechte verzögert, eingeschränkt oder verweigert werden.

Unter Absatz 1 Buchstabe b wird ein zweites besonderes Recht hinzugefügt. Es handelt sich um das Recht der betroffenen Person, direkt beim Kantonsgericht Beschwerde gegen einen Entscheid einer Behörde, die das GIDA anwendet, einzulegen, wenn dies im Rahmen der Anwendung des Schengen-Besitzstands in Strafsachen geschieht. Dieses Beschwerderecht ist von Artikel 54 der Richtlinie (EU) 2016/680 vorgegeben.

1.45 Artikel T1-1

Im neuen Artikel T1-1 geht es um die Bearbeitung der Daten juristischer Personen. Wie im Kommentar zu Artikel 3 Absatz 3 erwähnt, fällt der Schutz der Daten juristischer Personen nicht mehr unter das vorliegende Gesetz, um den auf nationaler und internationaler Ebene getroffenen Entscheidungen zu entsprechen. Sämtliche Rechtserlasse des Kantons Wallis müssen diesem Umstand Rechnung tragen. Die gesetzlichen Grundlagen, die bisher die Bearbeitung der Daten von natürlichen und juristischen Personen zuliessen, gelten nur noch für natürliche Personen. Die verschiedenen kantonalen Gesetzesbestimmungen müssen angepasst werden, um eine Verletzung der Persönlichkeitsrechte und der Grundrechte von juristischen Personen zu begründen. In dieser Bestimmung ist eine Übergangsfrist von fünf Jahren vorgesehen, um diese Änderungen vorzunehmen.

2. Änderung anderer Erlasse

Die Richtlinie (EU) 2016/680 hat zu einer Änderung des Schweizerischen Strafgesetzbuches geführt. Zur Umsetzung der Anforderungen der Richtlinie (EU) 2016/680 wurden einige Bestimmungen zum Datenschutz, die beim Datenaustausch im Rahmen der polizeilichen Zusammenarbeit anwendbar sind, in das Strafgesetzbuch aufgenommen. Mit Ausnahme einiger spezifischer Bestimmungen gelten diese auch für die kantonalen Behörden.

Die Änderungen anderer Erlasse bedürfen keiner besonderen Kommentare.

Die übrigen Änderungen des geltenden Rechts, die im Gesetzesentwurf erwähnt sind, wurden vom letzten Entwurf übernommen, bei dem es nur um die Anpassung des

GIDA an die Richtlinie (EU) 2016/680 ging. Es wurde nicht überprüft, ob die Änderungen des geltenden Rechts vollständig sind.

3. Finanzielle und personelle Auswirkungen

Die anfänglichen Gesamtkosten, gestützt auf die Standards der Kantonsverwaltung, können auf 350’000 bis 400’000 Franken geschätzt werden. Sie umfassen die Stellen des Beauftragten und des Sekretärs, die Mietkosten für die Räumlichkeiten sowie verschiedene Kosten.

Zudem ist eine Stelle für einen Datenschutzdelegierten (Jurist), eine unabhängige Person vorzusehen. Dabei kann es sich um eine interne Vollzeitstelle oder ein Mandat handeln. Die jährlichen Kosten dürften sich auf 200’000 Franken belaufen.

* * *