Botschaft 2023-CE-149

26. Juni 2023

—

zum Gesetzesentwurf über die Totalrevision des Gesetzes über den Datenschutz

Inhaltsverzeichnis

—

In Kürze

1. Das geltende Gesetz über den Datenschutz (DSchG) stammt vom 25. November 1994. Zur damaligen Zeit kam das *World Wide Web* eben gerade auf, *Google, Facebook, Twitter* und Konsorten existierten noch nicht, die Gemeinwesen des Kantons verfügten noch nicht über E-Mail, und es stand noch kein virtueller Schalter zum Bezug und zur Abwicklung von Verwaltungsleistungen während 24 Stunden an 7 Tagen in der Woche zur Verfügung.
2. Im Rückblick kann man sagen, dass mit dem DSchG ein ansprechendes Schutzniveau erreicht werden konnte, in den Bereichen, für welche die Herausforderungen bei seiner Inkraftsetzung bereits bekannt waren, und dass das Gesetz eine erstaunliche Fähigkeit zur Anpassung aufwies, wenn man an die raschen Veränderungen denkt, mit denen es konfrontiert war. Aber wie andere Gesetze im Bereich Datenschutz, die zu Beginn der 90-er-Jahre angepasst wurden, sind die darin enthaltenen Bestimmungen aufgrund der technischen und sozialen Entwicklungen, die in den vergangenen 30 Jahren abliefen, teilweise veraltet. Dies ist die Begründung dafür, dass sie modernisiert und ergänzt werden müssen.
3. Dieser Modernisierungswille betrifft nicht nur den Kanton Freiburg. Vielmehr ist er vor dem Hintergrund der generellen Entwicklung in Europa und der Schweiz zu sehen, die einerseits dazu tendiert, die Rechte und die Freiheiten der betroffenen Personen angesichts von immer mehr und komplexeren Bearbeitungen ihrer Daten zu stärken, und andererseits, die Sicherheit der Infrastrukturen, der Prozesse und der Organisation, die diese Bearbeitungen unterstützen, zu verbessern. Das neue Datenschutzgesetz des Bundes wurde am 25. September 2020 verabschiedet und wird am 1. September 2023 in Kraft treten. Auf Seiten der Kantone hat die Hälfte bereits ihre eigenen Gesetze revidiert und die andere Hälfte ist daran, dies zu tun.
4. Dieser Entwurf zielt darauf ab, das Freiburger kantonale Recht mit diesen neuen Standards im Bereich des Datenschutzes in Einklang zu bringen. Er lehnt sich stark an das neue Bundesgesetz über den Datenschutz an, das seinerseits zum Ziel hat, das Bundesrecht mit dem Übereinkommen ETS 108+ des Europarates zum Schutz des Menschen bei der automatischen Bearbeitung personenbezogener Daten und den neuen Anforderungen des EU-Rechts an den Datenschutz in Einklang zu bringen.
5. Wenngleich das neue Datenschutzgesetz des Bundes einen wesentlichen Einfluss auf die Erstellung dieses Entwurfs hatte, ist dieser nicht eine einfache Kopie. Er berücksichtigt insbesondere die Besonderheiten des Kantons Freiburg sowie die Erfahrungen des Kantons mit der Digitalisierung. Als Beispiele können folgende Elemente zitiert werden:
   - Die Vorschriften zur Auslagerung der Datenbearbeitung, die im Jahr 2020 vom Gesetz zur Anpassung der kantonalen Gesetzgebung an bestimmte Aspekte der Digitalisierung eingeführt wurden, haben sich bewährt und wurden fast wortgleich in den Entwurf übernommen.
   - Um die bipartite Zusammensetzung der kantonalen Behörde für Öffentlichkeit, Datenschutz und Meditation zu berücksichtigen, werden die neuen Zuständigkeiten, die der Behörde übertragen werden, nicht allein in den Händen der oder des Beauftragten für den Datenschutz konzentriert, sondern zwischen dieser Person und der kantonalen Öffentlichkeits-, Datenschutz- und Mediationskommission aufgeteilt.
   - Im Gegensatz zum neuen Datenschutzgesetz des Bundes sieht der Entwurf aus sowohl rechtlichen als auch praktischen Gründen nicht vor, den Datenschutz für juristische Personen aufzuheben.
6. Nichtsdestotrotz ist zu erwähnen, dass sich der Entwurf in einem relativ strikten Rahmen, der nicht viel Handlungsspielraum ermöglicht, bewegt. Abgesehen davon, dass ein besserer Schutz ermöglicht werden soll, sollen die neuen Rechte der Personen, deren Daten bearbeitet werden, und die neuen Pflichten der Verantwortlichen für die Bearbeitung im Allgemeinen auf eine Angleichung des Freiburger Rechts an die neuen anzuwendenden Standards in diesem Bereich im Digitalisierungszeitalter hinauslaufen. Die Umsetzung dieser Standards ist insofern eine notwendige Bedingung für die erfolgreiche Umsetzung des E-Governments des Staates Freiburg, als es ohne digitales Vertrauen keine Digitalisierung geben kann.

1 Allgemeines

—

1.1 Hintergrund und Ursprung des Entwurfs

1.1.1. Im Bereich Datenschutz folgten mehrere Generationen der Gesetzgebung aufeinander, um die neuen Praktiken zu begleiten und angesichts der ständigen Weiterentwicklung der digitalen Anwendungen die erforderlichen Leitplanken für die Bearbeitung von Personendaten festzulegen:

a) Die erste Generation dieser Gesetzgebungen erstreckt sich über die Jahre 1980 bis 2000. Sie wurde hauptsächlich vom früheren Übereinkommen SEV 108 inspiriert und zeichnet sich durch einen Ansatz aus, der auf wichtigen Grundsätzen (Rechtmässigkeit, Verhältnismässigkeit, Zweckbestimmung, Treu und Glauben, Genauigkeit *usw.*) beruht, die dazu dienen sollen, einen Rahmen für noch wenig bekannte Praktiken und Risiken zu schaffen. In der Europäischen Union ist der erste Referenztext zu diesem Thema die alte Datenschutzrichtlinie 95/46/EG, die 1995 promulgiert wurde. In der Schweiz verabschiedete der Bund 1992 das Bundesgesetz über den Datenschutz (DSG; SR 235.1). Einige Kantone sind dem Bund vorangegangen, so etwa der Kanton Bern mit seinem Datenschutzgesetz (KDSG; BSG 152.04), das auf das Jahr 1986 zurück geht; die anderen folgen in den kommenden Jahren, so auch der Kanton Freiburg, dessen Gesetz über den Datenschutz (DSchG, SGF 17.1) aus dem Jahre 1994 datiert.

b) Die zweite Generation entwickelt sich nach und nach ab dem Jahr 2000 und erstreckt sich über eine Periode von etwa 15 Jahren, während der die Digitalisierung einen beispiellosen Aufschwung erfährt. Das Datenschutzrecht beginnt sich unter der kombinierten Wirkung der Beiträge der Lehre und die darauffolgenden Gerichtsentscheide langsam zu materialisieren. Die wichtigsten Grundsätze werden durch präzisere Regeln ergänzt. Das Übereinkommen SEV 108 entwickelt sich: Ein zusätzliches Protokoll wird 2001 angenommen und erlegt den Mitgliedstaaten neue Pflichten auf, namentlich die Stärkung der Befugnisse ihrer Datenschutzbehörden. In dieser Zeit tritt der Bund dem Schengen/Dublin-Abkommen bei und verpflichtet sich in diesem Zusammenhang zur Einhaltung des Rahmenbeschlusses 2008/977/JI. Zudem führt er zwei Revisionen des DSG durch: die erste im Jahr 2007 hatte zum Ziel, den Inhalt des Gesetzes in einigen Punkten zu modernisieren; mit der zweiten im Jahr 2010 sollte eine Anpassung des Bundesrechts an die neuen Anforderungen des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28.01.1981 (SEV 108), insbesondere an das Zusatzprotokoll, und an die Gesetzgebung der EU erreicht werden. Auf der kantonalen Ebene sind die Veränderungen unterschiedlich. Gewisse Kantone, so auch der Kanton Freiburg, beschränken sich strikte darauf, das übergeordnete Recht zu übernehmen. Andere Kantone gehen jedoch weiter und nehmen substanziellere Verbesserungen ihrer Gesetzgebung vor.

c) Die dritte Generation beginnt mit der Annahme der Datenschutz-Grundverordnung der Europäischen Union (DSGVO) 2016 und der Richtlinie zum Datenschutz im Rahmen der Strafverfolgung; dieser ersten Serie von Gesetzestexten folgt 2018 die Promulgierung des revidierten Übereinkommens SEV 108 (Übereinkommens SEV 108+). Ohne die alten Regelungen, die sich bewährten, über Bord zu werfen, befasst sich diese neuste Generation mit dem Thema Datenschutz auf eine erweiterte und dynamischere Art als die vorhergehenden und integriert darin auch die Technik und die Organisation. Man findet darin insbesondere Antworten auf die Frage, wie Informationssysteme mit der Einführung von Datenschutzgrundsätzen ab der Konzeption (nach Massgabe des Prinzips *privacy-by-design*) und standardmässig (nach Massgabe des Prinzips *privacy-by-default*) gestaltet werden müssen; ferner werden neue Rechte für die betroffenen Personen, wie etwa das Recht auf Vergessen und das Recht auf Datenübertragbarkeit, eingeführt. Vor diesem Hintergrund verabschiedet der Bund am 25. September 2020 das neue, überarbeitete Bundesgesetz über den Datenschutz (BBl 2020 7639), das am 1. September 2023 in Kraft treten wird. Es wird von allen Kantonen befolgt, die ihrerseits ihre eigenen Datenschutzgesetze überarbeiten.

1.1.2. Das 1994 verabschiedete DSchG (SGF 17.1) hat bislang zwei Revisionen von einiger Bedeutung erfahren:

Das erste Mal durch das Gesetz vom 8. Mai 2008 über den Datenschutz (Anpassung an das internationale Recht, insbesondere an das Schengen/Dublin-Abkommen; ASF 2008_053). Ursprünglich bestand der Revisionsentwurf aus drei Elementen (siehe dazu die Botschaft vom 4. Mai 2008, in TGR 2008 664):

> Anpassung des kantonalen Gesetzes an das Schengen/Dublin-Abkommen und an das Zusatzprotokoll vom 8. November 2001 zum Übereinkommen SEV 108;
> Anpassung an die übrigen Korrekturen im im Bundesgesetz über den Datenschutz;
> Berücksichtigung der Erfahrungen mit dem DSchG seit dessen Inkrafttreten.

Schliesslich hat sich die Revision insbesondere auf das erste Element beschränkt. Gemäss der Botschaft des Staatsrats zeigte es sich jedoch rasch, *«dass es nicht möglich war, alle drei Ziele innerhalb der Frist zu verwirklichen, die der Bund zur Anpassung der kantonalen Gesetze an die Abkommen von Schengen und Dublin gesetzt hatte. Daher wurde der Auftrag der Arbeitsgruppe auf den ersten Punkt beschränkt, d. h. die Anpassung des DSchG an das internationale Recht. Die beiden anderen Aspekte werden im Rahmen einer späteren Revision behandelt werden»*.

Eine zweite Anpassung erfolgte im Jahr 2020 im Rahmen des Gesetzes vom 18. Dezember 2020 zur Anpassung der kantonalen Gesetzgebung an bestimmte Aspekte der Digitalisierung (ASF 2020_195). Obwohl diese zweite Revision bereits das Ziel hatte, den gesetzlichen Rahmen an einige neue Praktiken anzupassen, konzentrierte sie sich dennoch auf die spezifische Frage der Nutzung von *Cloud Computing*. Das Ziel war nicht, das DSchG zu überarbeiten, um es mit den neuen Anforderungen, die in diesem Bereich entstanden, in Einklang zu bringen.

1.1.3. Mit anderen Worten: Das DSchG ist heute als auf halbem Weg zwischen der ersten und der zweiten Generation der Datenschutzgesetzgebung. Aus diesem Grund scheint die Durchführung einer Totalrevision zum jetzigen Zeitpunkt kaum vermeidbar zu sein. Sie soll dazu dienen, den Kanton Freiburg mit einem modernen Rechtsrahmen auszustatten, der nicht nur den Bürgerinnen und Bürgern einen angemessenen und kohärenten Datenschutz bietet, sondern auch den Anforderungen und Standards des Bundesrechts, des Europarechts und des Übereinkommens SEV 108+ des Europarats entspricht (vgl. zu den völkerrechtlichen Aspekten § 1.3.2).

1.2 Ablauf der Arbeiten

1.2.1. Im Spätsommer 2017 verabschiedete der Bundesrat seinen Entwurf für eine Totalrevision des DSG. In der Folge beauftragte die Staatskanzlei die kantonale Behörde für Öffentlichkeit und Datenschutz (ÖDSB; heute kantonale Behörde für Öffentlichkeit, Datenschutz und Mediation, ÖDSMB), eine Arbeitsgruppe einzusetzen, um die Bestimmungen der Freiburger Datenschutzgesetzgebung zu analysieren und die Anpassungen vorzuschlagen, die angesichts der vom Bundesrat vorgeschlagenen Änderungen des DSG und der neuen Normen des internationalen Rechts, die sich in diesem Bereich auf die Schweiz auswirken, erforderlich sind.

1.2.2. Die von der ehemaligen Datenschutzbeauftragten eingesetzte Arbeitsgruppe bestand aus: je einer Vertreterin oder einem Vertreter jeder Direktion, der Gerichtsbehörde, der Staatsanwaltschaft, der Polizei, des Amts für Informatik und Telekommunikation (ITA), der Gemeinden und des Amtes für Gesetzgebung (GeGA). Sie legte einen Vorentwurf des Erlasses vor, der Ende 2019 Gegenstand einer Vernehmlassung war.

1.2.3. Die Rückmeldungen aus der Vernehmlassung zeigten, dass niemand die Notwendigkeit einer Gesamtüberarbeitung des DSchG inhaltlich bestreitet. Mehrere Organe der öffentlichen Hand befürchteten jedoch, dass die Umsetzung des neuen Gesetzes viel Arbeit mit sich bringen würde, und forderten deshalb die Bereitstellung zusätzlicher Ressourcen. Einige wiesen auf den komplizierten Charakter des Entwurfs hin und forderten eine Vereinfachung, während andere wiederum die Verwendung vieler allgemeiner, vage formulierter Prinzipien bemängelten und mehr Klarheit darüber verlangten, was konkret erwartet würde. Es wurden zahlreiche gezielte Hinweise zu bestimmten Bestimmungen formuliert.

1.2.4. Im Anschluss an die Vernehmlassung wurde das Projekt freiwillig auf *Standby* gesetzt, bis der endgültige Text des DSG des Bundes bekannt war. Der Ausbruch der COVID-19-Pandemie verlängerte diesen Status insofern, als er im Zeitraum 2020-2021 zahlreiche rechtliche Ressourcen erforderte. Erst Ende 2021 wurde die mit der Revision des DSchG beauftragte Arbeitsgruppe in einer kleineren Form wieder eingesetzt, der Vertreterinnen und Vertreter der

Direktionen (FIND, RUBD und SJSD), der ÖDSMB, des ITA und der Gemeinden angehörten. Die Arbeitsgruppe wurde zudem unter die Leitung eines Mitglieds des GeGA gestellt. Die neue Arbeitsgruppe schloss ihre Arbeit im September 2022 ab.

1.2.5. Bei der Arbeit am Text berücksichtigte die Arbeitsgruppe so weit wie möglich die gezielten Bemerkungen, die bei der Vernehmlassung 2019 geäussert wurden, und versuchte, sie umzusetzen, wo dies möglich und angebracht war. Andererseits konnte sie ohne wirkliche Handlungsmöglichkeiten nur feststellen, dass die Umsetzung der neuen Datenschutzstandards logischerweise zusätzliche Anstrengungen, aber wahrscheinlich auch zusätzliche Ressourcen erfordern würde. Um der Kritik an der Kompliziertheit des Erlasses zu begegnen, nahm die Arbeitsgruppe mehrere Anpassungen vor, um scheinbar Unnötiges und Nichtnotwendiges zu entfernen und einige Formulierungen zu vereinfachen. Das Ergebnis ist nicht unbedingt ein kürzerer Text, sondern ein besser lesbarer und leichter zu handhabender Text, trotz der Materie, die zwangsläufig komplex bleibt.

1.2.6. Im September 2022 verliess die ehemalige Datenschutzbeauftragte ihre Stelle. Die ÖDSMB kündigte damals an, dass sie die Gelegenheit ergreifen werde, um eine neue Arbeitsweise, bei der die beiden Funktionen der Öffentlichkeits- und der Datenschutzbeauftragen in einer einzigen Person vereint sind, auszuprobieren. Dazu hat der Staatsrat die Öffentlichkeitsbeauftragte zur Datenschutzbeauftragten *ad interim* ernannt und eine Frist verlangt, um diese neue Zusammensetzung zu testen. Die Staatskanzlei hiess diesen Vorschlag gut und nutzte die Gelegenheit, um in der Zwischenzeit eine neue Vernehmlassung zum geänderten Text zu organisieren. Diese zweite Vernehmlassung dauerte vom 25. Oktober 2022 bis zum 27. Januar 2023.

1.2.7. Die Ergebnisse der zweiten Vernehmlassung waren im Grossen und Ganzen ähnlich wie diejenigen der ersten Vernehmlassung 2019. Obwohl die Kritik am neuen Text insgesamt abflaute, fürchten die Organe der Verwaltung weiterhin eine Arbeitsüberlastung und verlangen neue Ressourcen. Einige gezielte Bemerkungen führten zu letzten Präzisierungen und Korrekturen am Text des Erlasses und an der dazugehörigen Botschaft.

1.2.8. Es sei noch darauf hingewiesen, dass die ÖDSMB eng an allen Phasen des Projekts beteiligt war. Diese konstruktive Mitwirkung, die sehr geschätzt wurde, trug dazu bei, dass sich das Projekt unter guten Voraussetzungen entwickeln konnte, und bot dort, wo es notwendig war, die bestmöglichen Lösungen. Das Projekt stösst deshalb auf ein positives Echo seitens der Behörde.

1.3 Grundzüge des Entwurfs

1.3.1 Inhalt im Allgemeinen

1.3.1.1. Der Inhalt der beantragten Bestimmungen orientiert sich grösstenteils am neuen DSG des Bundes, das wiederum stark vom Übereinkommen SEV 108+, der DSGVO und der Richtlinie (EU) 680/2016 inspiriert ist. Diese Regelungen beeinflussten den Inhalt des Entwurfs im Wesentlichen auf drei Ebenen:

a) Der Entwurf nimmt den risikobasierten Ansatz wieder auf, der die neuen Gesetzgebungen zum Datenschutz charakterisiert. Gemäss diesem Ansatz sind die Verpflichtungen im Bereich Datenschutz bei den Verantwortlichen für die Datenbearbeitung, deren Aktivitäten ein Risiko von Grundrechtsverletzungen aufweisen, strikter als bei Personen, deren Tätigkeiten weniger riskant sind (vgl. BBl 2017 6941, 6970). Dies wird insbesondere in Artikel 11 des Entwurfs veranschaulicht.
b) Der Entwurf behält auch den technologieneutralen Charakter der vorgeschlagenen Regeln bei. Dies hinderte aber nicht daran, gewisse Praktiken der jüngeren Zeit zu reglementieren, die direkt mit der Nutzung neuer Technologien verbunden sind, wie dies etwa bei der Auslagerung gewisser Typen und Formen der Datenbearbeitung der Fall ist (Art. 18-21 des Entwurfs). Der technologieneutrale Charakter der Bestimmungen ist zwar wichtig, um zu verhindern, dass sie schnell von den Fortschritten der Technologie überholt werden, er darf aber auch nicht dazu führen, dass die Technologie ignoriert wird und das Gesetz seine Ziele nicht erreicht.
c) Die im Entwurf verwendete Terminologie wurde schliesslich modernisiert, um besser mit den Entwicklungen im Datenschutzrecht Schritt zu halten und auch die Vereinbarkeit des Gesetzes mit neuen Praktiken und den neuesten Gesetzestexten auf Bundes- und internationaler Ebene in diesem Bereich zu verbessern. Die statische Bedeutung des Begriffs «Datensammlung» wird durch den dynamischeren Begriff «Bearbeitungstätigkeit»

ersetzt. Die als sensibel bezeichneten Daten schliessen nun auch «genetische Daten» und «biometrische Daten» mit ein. Speziell neu eingeführt wurde der Begriff «Profiling».

1.3.1.2. Im Vergleich zum Entwurf des Bundesrats weist der Entwurf einen wesentlichen Unterschied auf, der besonders erwähnenswert scheint. Er sieht nicht vor, den Datenschutz juristischer Personen aufzuheben. Zwei Gründe erklären dieses Vorgehen hauptsächlich:

a) Aus streng juristischer Sicht sieht Artikel 12 Abs. 2 der Freiburger Kantonsverfassung vor, dass jede Person das Recht darauf hat, gegen die missbräuchliche Verwendung von Daten, die sie betreffen, geschützt zu werden. Die Norm entspricht Artikel 13 Abs. 2 der Bundesverfassung. Allerdings erkennen die Autoren des öffentlichen Rechts derzeit offenbar einstimmig an, dass der verfassungsrechtlich verankerte Datenschutz sowohl für natürliche als auch für juristische Personen gilt.[1] Dieser Ansicht scheint, in mehreren aktuellen Urteilen, auch das Bundesgericht zu sein[2]. Aus dieser Sicht scheint es problematisch zu sein, sich einer Gesetzesrevision zu bedienen, um den Anwendungsbereich einer Norm von Verfassungsrang einzuschränken.

b) Aus praktischer Sicht hat die Tatsache, dass der Datenschutz bei juristischen Personen wegfallen soll, gemäss Bundesrat zur Konsequenz, dass die rechtliche Grundlagen, die derzeit öffentlichen Stellen die Bearbeitung von Personendaten ermöglicht, bei den Personendaten juristischer Personen obsolet würde (s. BBl 2017 6941, S. 6972, 6981 und 7011). Für den Bundesrat ist diese Situation aus der Perspektive des Legalitätsprinzips problematisch, nach dem alles staatliche Handeln sich auf das Gesetz stützen muss (s. BBl 2017 6941, S. 7107 und 7118 f). Um Behörden die weitere Bearbeitung von Daten von juristischen Personen zu ermöglichen, hielt er es für notwendig, eine ganze Reihe von Bestimmungen im RVOG, die am Ende in sehr ähnlicher Form den Inhalt der Bestimmungen des DSG widerspiegeln, jedoch nicht für juristische Personen, einzuführen (siehe hierzu die Artikel 57h^{bis}, 57i, 57j, 57k, 57l, 57r, 57s, 57t RVOG, die vom DSG eingeführt werden). Er hat die gleiche Übung mit der Spezialgesetzgebung gemacht, wo die Regelungen, welche die Bearbeitung von Personendaten erlauben, ergänzt wurden, um auch die Bearbeitung von Daten von juristischen Personen zu erlauben (z. B.: Art. 9 BGÖ; Art. 15b RAG; Art. 5, 14a, 15 und 19 BSTatG; Art. 17a BGSA, die vom DSG eingeführt werden). Vor diesem Hintergrund scheint es, dass die Weglassung der Daten juristischer Personen zumindest im Bereich des öffentlichen Rechts eher einer Stilübung als einer echten Veränderung der Praxis gleicht. Das ist der Grund, weshalb sie im Vorentwurf nicht übernommen wurde. Andere Kantone wie die Kantone Genf oder Zürich haben die gleiche Analyse vorgenommen und darauf verzichtet, den Schutz juristischer Personen in ihren eigenen Datenschutzgesetzen zu streichen.

1.3.2 Verbindungen zum Recht der Europäischen Union und dem (modernisierten) Übereinkommen SEV 108+

1.3.2.1. Mehrere internationale Rechtstexte haben diesen Entwurf in unterschiedlichsten Massen beeinflusst. Es handelt sich hierbei um die DSGVO, die Richtlinie (EU) 2016/679 über den Datenschutz in den Bereichen Polizei und Justiz und das Übereinkommen SEV 108+.

1.3.2.2. Unter diesen Rechtstexten ist bisher nur die Richtlinie (EU) 2016/680 verbindlich für die Schweiz, weil sie eine Entwicklung des Schengen-Besitzstands darstellt (BBl 2017 6941, S. 6963 und S. 6991 ff.). Der Anwendungsbereich ist jedoch auf bestimmte Bereiche wie Justiz, Polizei oder Asyl beschränkt. Die Richtlinie (EU) 2016/680 ist weder für die Mitgliedstaaten der Europäischen Union noch für die Schweiz unmittelbar anwendbar, sie muss in internes Recht umgewandelt werden. Das bedeutet für den Kanton Freiburg, dass nicht nur sein Datenschutzrecht, sondern auch bestimmte kantonale Gesetze, die in den Geltungsbereich der Richtlinie fallen, angepasst werden müssen.

---

[1] DUBEY Jacques, *Droits fondamentaux, Band II*, Basel 2018, Nr. 1766; BIAGGINI / GIOVANNI, *BV Kommentar*, Zürich, 2. Auflage., 2017, ad Art. 13, Nr. 12; SCHWEIZER Rainer J., in Ehrenzeller Bernhard *et al.* (Hrsg.), *St.Galler Kommentar der Schweizerische Bundesverfassung*, 3. Auflage, Zürich / Basel / Genf 2014, ad Art. 13, Nr. 73; MALINVERNI / HOTTELIER, HERTIG RANDALL / FLÜCKIGER, *Droit constitutionnel suisse, Band II*, 4. Auflage, Bern 2021, Nr. 408; MÜLLER / SCHEFER, *Grundrechte in der Schweiz*, 4. Auflage, Bern 2008, S. 166; DIGGELMAN Oliver, in Waldmann Bernhard / Belser Eva Maria / Epiney Astrid (Hrsg.), Basler Kommentar Bundesverfassung, Basel 2015, ad Art. 13, Nr.33.

[2] BGE 144 II 77, Erw. 5; BGE 144 II 91, Erw. 4.4.

1.3.2.3. Gemäss dem Bundesrat ist die Schweiz nicht unmittelbar an die DSGVO (siehe BBl 2017 6941, S. 6963 und S. 6991 ff.) gebunden. Dennoch übt sie einen nicht zu vernachlässigenden indirekten Einfluss aus. Denn der bedingungslose Austausch von Daten zwischen europäischen und schweizerischen Verantwortlichen für die Datenbearbeitung ist an die Bedingung geknüpft, dass die Europäische Union einen Angemessenheitsbeschluss erlässt, der bescheinigt, dass die schweizerische Datenschutzgesetzgebung ein der Europäischen Gesetzgebung gleichwertiges Schutzniveau bietet (s. Art. 45 DSGVO). Liegt kein solcher Beschluss vor, so wird jeder Austausch von Daten zwischen Europa und der Schweiz von der Anwendung zusätzlicher Garantien abhängig gemacht, die mit dem europäischen Bearbeitungsverantwortlichen jedes Mal aufs Neue ausgehandelt werden müssten. Für ein Land wie das unsere, das sich im Herzen Europas befindet, wäre eine solche Situation sowohl für den öffentlichen als auch für den privaten Sektor sehr schwierig. Zurzeit profitiert die Schweiz von einem Angemessenheitsbeschluss vom 26. Juli 2000 (s. BBl 2017 6941, S. 6964). Die Europäische Union nimmt derzeit eine weitere Bewertung des Schweizer Rechts vor, um dessen Vereinbarkeit mit der DSGVO zu überprüfen. Im Rahmen dieser Bewertung prüft sie das Bundesrecht, aber auch das Recht von einigen zufällig ausgewählten Kantonen. Es ist somit wesentlich, dass der Kanton Freiburg, wie die anderen Kantone auch, seine Gesetzgebung im Bereich Datenschutz entsprechend anpasst.

1.3.2.4. Das Übereinkommen SEV 108 des Europarates stellt den ersten internationalen Rechtstext im Bereich Datenschutz dar. Er wurde am 28. Januar 1981 in Strassburg abgeschlossen und von der Schweiz am 2. Oktober 1997 mit Inkrafttreten am 1. Oktober 1998 ratifiziert. Im Jahr 2018 wurde das Übereinkommen SEV 108 mit dem Ziel vollständig modernisiert, besser auf die Herausforderungen reagieren zu können, welche die Globalisierung, technologische Entwicklungen und das Steigen des grenzüberschreitenden Datenverkehrs für den Schutz der Privatsphäre und die Grundrechte der betroffenen Person darstellen. Auch wenn es weniger detailliert und weniger dicht ist als die DSGVO und die Richtlinie (EU) 2016/680, hat das Übereinkommen SEV 108+ einen sehr ähnlichen Inhalt wie die beiden Rechtstexte. Die Bundesversammlung hat am 19. Juni 2020 den Bundesbeschluss zur Ermächtigung des Bundesrates, die revidierte Fassung des Übereinkommens SEV 108 zu ratifizieren, angenommen (BBl 2020 599). Der Ratifizierungsprozess ruht aber immer noch. Bis zum Inkrafttreten des neuen Texts gilt das Übereinkommen SEV 108 von 1981 weiterhin.

1.3.3 Rechte der betroffenen Personen

1.3.3.1. Die Frage der Rechte der betroffenen Personen wird in Abschnitt 3 des Entwurfs behandelt. Eines der Ziele des Vorentwurfes ist es, die Kontrolle und die Herrschaft der betroffenen Personen über die Informationen, die sie mit dem Gemeinwesen teilen, zu stärken. Zu diesem Zweck werden neue Rechte eingeführt, die besser an die Entwicklung der digitalen Anwendungen angepasst sind, und die Bedingungen und Modalitäten ihrer Ausübung werden erleichtert.

1.3.3.2. Zu den neu eingeführten Rechten gehören unter anderem die Folgenden:

a) Die Möglichkeit einer jeden Person, sich vorbeugend der Übermittlung von Daten zu widersetzen, die sie betreffen (Recht auf Sperrung oder auf Widerspruch). Bis jetzt ist ein solches Recht im Kanton Freiburg nur im Zusammenhang mit Daten der Einwohnerkontrolle vorgesehen (vgl. Art. 18 EKG). Das Widerspruchsrecht gehört jedoch zu den traditionellen Verteidigungsrechten im Bereich des Datenschutzes, ohne Rücksicht auf die Art der betreffenden Bearbeitung. Dies ist der Grund dafür, dass dieses in Artikel 31 des Entwurfs eingeführt wurde. Das Widerspruchsrecht ist nicht als absolut zu verstehen. Es kann nicht gegen eine gesetzlich vorgeschriebene Übermittlung von Daten geltend gemacht und nicht ins Feld geführt werden, wenn ein überwiegendes öffentliches oder privates Interesse an der Offenlegung der betreffenden Daten besteht.

b) Die Einführung eines neuen Rechts auf Einschränkung der Bearbeitung, das der betroffenen Person ermöglicht, gewisse Nutzungen ihrer Daten einzufrieren, und es dem Verantwortlichen für die Bearbeitung ermöglicht, die Daten weiterhin aufzubewahren (Ar. 33 Abs. 2 Bst. b). Das Recht auf Einschränkung der Bearbeitung stellt eine weniger radikale Alternative zum Recht auf Löschung und Berichtigung der Daten dar. Es kann namentlich eingesetzt werden, wenn die betroffene Person die Richtigkeit ihrer Daten oder die Art, in der sie bearbeitet werden, bestreitet oder ihre Löschung beantragt, während Überprüfungen erforderlich sind, um zu prüfen, ob das Gesuch begründet ist.

c) Für die automatisierte Bearbeitung von Daten in Verwaltungsverfahren werden spezifische und angemessene Verteidigungsmittel in das VRG eingeführt. Der erste Fall, der in Art. 66a VRG in Betracht gezogen wird, ist derjenige, in dem Algorithmen zur Unterstützung der Entscheidfindung eingesetzt werden, sei es, um den Sachverhalt zu erforschen oder um die rechtlichen Überlegungen zu unterstützen. Die Behörde, welche den Entscheid trifft, muss dies im Entscheid ausdrücklich erwähnen, und die betroffene Person kann gegebenenfalls verlangen, die Logik und die Kriterien der verwendeten Algorithmen zu erfahren. Der zweite in Betracht gezogene Fall ist derjenige, dass ein Entscheid ausschliesslich auf der Grundlage einer automatisierten Datenbearbeitung getroffen wird. Diese Bestimmung, die bereits im Vorentwurf enthalten war, wurde dennoch in Artikel 4a des Anhangs zum VRG über die elektronische Datenverarbeitung verschoben. Die Gründe für diese Änderung werden in den Kommentaren zu den jeweiligen Artikeln erläutert.

d) Im Vergleich zum Vorentwurf führt der Entwurf zusätzlich den Grundsatz eines Rechts auf Datenübertragbarkeit ein, ohne daraus jedoch ein subjektives Recht zu machen (Art. 32). Aufgrund der besonderen technischen Voraussetzungen, die für die Umsetzung eines solchen Rechts erforderlich sind, wird es Aufgabe der Sondergesetzgebung sein, dies vorzusehen, oder direkt den Verantwortlichen für die Bearbeitung obliegen, es in den von ihnen betriebenen Infrastrukturen und/oder Anwendungen zu konkretisieren.

1.3.3.3. Im Übrigen stellen die vorgenommenen Änderungen Verbesserungen und punktuelle Anpassungen bestehender Normen dar, mit dem Ziel, die Bedeutung zu präzisieren und die Umsetzung bestehender Regelungen zu erleichtern, namentlich das Recht auf den Zugang zu den eigenen Daten und die verschiedenen Abwehrmassnahmen, über welche die betroffene Person verfügt, um sich gegen eine unrechtmässige Datenbearbeitung zu wehren.

1.3.4 Verpflichtungen der Verantwortlichen für die Bearbeitung

1.3.4.1. Die Pflichten des Verantwortlichen für die Bearbeitung werden in Abschnitt 4 des Entwurfs festgelegt. Darin werden die organisatorischen und sicherheitsspezifischen Massnahmen bei der Bearbeitung von Personendaten durch öffentliche Stellen und die damit verbundene Verantwortung festgelegt.

1.3.4.2. Generell gesehen ist jedes Organ, das Daten auf welcher Ebene auch immer bearbeitet, für den Schutz seiner Daten verantwortlich (Art. 36). Wie es bereits heute der Fall ist, wird diese Verantwortung transparent und systematisch sichergestellt und umgesetzt: Abgesehen von einigen Ausnahmen muss jede Datenbearbeitung dem Register der Bearbeitungen gemeldet werden (Art. 38 und 39). Sie untersteht einer oder mehreren verantwortlichen Stellen, die verpflichtet sind, den Schutz und die Sicherheit der Daten durch konkrete und den Umständen angepasste Massnahmen zu gewährleisten (Art. 40). Vorschriften sind geplant, um den Fall, in dem ein Verantwortlicher für die Bearbeitung die ganze Bearbeitung oder einen Teil davon an einen Dritten weitervergibt (Art. 37).

1.3.4.3. Gegenüber der jetzigen Situation werden den Verantwortlichen für Bearbeitung neue Massnahmen auferlegt, die in den verschiedenen Phasen und auch davor umgesetzt werden sollen:

a) Der Grundsatz des Datenschutzes durch Technikgestaltung (im Englischen: «*privacy by design*») und der Grundsatz des Datenschutzes durch Voreinstellungen (im Englischen: «*privacy by default*») werden in die Sicherheitsbestimmungen aufgenommen (Art. 40). Ersteres bedeutet, dass technische und angemessene organisatorische Massnahmen ab den ersten Schritten zu einer neuen Datenbearbeitung diskutiert und umgesetzt werden müssen, damit so früh wie möglich die Rechte und Freiheiten der betroffenen Person sichergestellt werden können. Zweiteres bedeutet, dass die Personendaten mit den Default-Mitteln und gemäss den Default-Modalitäten, die standardmässig das höchstmögliche Schutzniveau sicherstellen, bearbeitet werden müssen.

b) Vor Beginn einer neuen Datenbearbeitung, bei der ein höheres Risiko für die Rechte und Freiheiten der betroffenen Person besteht, ist die oder der Verantwortliche für die Bearbeitung gehalten, vorgängig eine Datenschutz-Folgenabschätzung durchzuführen (Art. 41). Das Ziel dieser Folgenabschätzung ist doppelter Natur: Mit ihr wird angestrebt, der oder dem Verantwortlichen für die Bearbeitung dazu zu verhelfen, einerseits Datenbearbeitungen zu konstruieren, die das Privatleben respektieren, und andererseits zu beweisen, dass dabei das Datenschutzgesetz eingehalten wird.

c) Im Falle einer Verletzung der Datensicherheit ist die oder der Verantwortliche für die Bearbeitung verpflichtet, die erforderlichen Abhilfemassnahmen zu ergreifen. Je nach Situation und Schwere der Verletzung kann sie oder er verpflichtet sein, die Beauftragte oder den Beauftragten oder, falls nötig, direkt die betroffene/n Person/en zu informieren (Art. 43 und 44).

d) Jede Direktion wird verpflichtet, für sich und ihre Verwaltungseinheiten eine Ansprechperson für den Datenschutz zu ernennen (Art. 45). Diese Person wird die Aufgabe haben, einerseits das Personal für die Fragen und Herausforderungen des Datenschutzes innerhalb der Direktion zu sensibilisieren und andererseits in diesem Bereich Beratung und Unterstützung an vorderster Front zu leisten. Im Zeitalter des E-Governments und der Digitalisierung ist es von entscheidender Bedeutung, dass die Direktionen Know-how und eine gewisse Autonomie bei dieser Thematik erwerben. Dies wird auch zu einer Verringerung der Arbeitsbelastung der ÖDSMB und zu einer ausgeprägteren Konzentration auf ihre Kontroll- und Aufsichtsfunktion führen.

1.3.5 Aufsichtsbehörde für den Datenschutz

1.3.5.1. Gemäss geltendem Recht hat die Aufsichtsbehörde für den Datenschutz keine Entscheidbefugnisse in ihrem Kompetenzbereich. Sie kann nur Untersuchungen anstellen und Empfehlungen zuhanden der öffentlichen Stellen abgeben, die ihren Verpflichtungen beim Datenschutz nicht oder nicht vollständig nachkommen, und sie dazu einladen, die festgestellten Mängel zu beheben. Die Empfehlungen haben aber keinen verbindlichen Charakter. Falls das öffentliche Organ der Empfehlung nicht Folge leistet, hat die Aufsichtsbehörde aber die Möglichkeit, die Sache der Justiz zu übergeben (s. Art. 22a DSchG in der geltenden Version).

1.3.5.2. Der Entwurf stärkt die Position der Aufsichtsbehörde. Es handelt sich dabei um eine verbindliche Verpflichtung, die sich direkt aus Artikel 47 Abs. 2 der EU-Richtlinie 2016/680 und Artikel 15 Abs. 2 Bst a und d des Übereinkommens SEV 108+ ergibt. Wie die Aufsichtsbehörden des Bundes und der anderen Kantone muss auch die ÖDSMB nicht nur über Untersuchungsbefugnisse, sondern auch über Eingriffsbefugnisse verfügen, die es ihr ermöglichen, bei Nichteinhaltung der Datenschutzvorschriften gegebenenfalls Massnahmen anzuordnen.

1.3.5.3. Um jedoch zu vermeiden, dass zu viel Macht auf einer Person konzentriert wird, sieht der Entwurf eine Aufteilung der Macht zwischen der oder dem Beauftragten und der kantonalen Öffentlichkeits-, Datenschutz- und Mediationskommission vor. Die Empfehlungsbefugnis, wie sie heute im Gesetz besteht, wird somit der oder dem Beauftragten zugewiesen. Wenn sie oder er eine Verletzung des Datenschutzes feststellt, kann die oder der Beauftragte, wie bereits heute, eine Empfehlung an den Verantwortlichen für die Bearbeitung richten (Art. 57). Diese Empfehlung muss klar angeben, aus welchen Gründen die beanstandete Bearbeitung nach Auffassung der oder des Beauftragten nicht den geltenden Anforderungen entspricht und welche Art von Massnahmen der Verantwortliche für die Bearbeitung ergreifen müsste, um der Verletzung abzuhelfen. Nur wenn der Verantwortliche für die Bearbeitung sich weigert, der Empfehlung Folge zu leisten, kann die oder der Beauftragte die Kommission anrufen, damit diese einen verbindlichen Entscheid trifft (Art. 58). In diesem Fall hat der Verantwortliche für die Bearbeitung die Rechte einer Verfahrenspartei. Er hat das Recht, angehört zu werden und kann auch gegen die an ihn gerichteten Entscheide Beschwerde einlegen (Art. 59).

1.4 Änderungen nach der Vernehmlassung von 2019

Im Vergleich zum Text, der in die Vernehmlassung gegeben wurde, enthält der Entwurf nur einige inhaltliche Änderungen. Es muss gesagt werden, dass die vom übergeordneten Recht gezogene Linie den Kantonen keinen besonders grossen Spielraum lassen. Die vorgenommenen Änderungen entsprechen somit punktuellen Korrekturen, die meist durch den Wunsch nach einer Angleichung an das Bundesrecht motiviert sind.

Es gibt jedoch einige Änderungen, die besonders erwähnt werden sollen:

a) Der Grundsatz, dass die Daten direkt bei der betroffenen Person erhoben werden, wurde gestrichen, denn er entspricht nicht mehr ganz der derzeitigen Praxis (siehe Kommentar zu Art. 12 und 13 DSchG).

b) Für laufende zivilrechtliche, strafrechtliche und verwaltungsrechtliche Verfahren wurde eine neue Ausnahme vom Geltungsbereich des Gesetzes eingeführt. Im Vorentwurf wurde beantragt, auf diese allgemeine Ausnahme zugunsten von zwei gezielten Ausnahmen zu verzichten; in diesem Fall sollte vorgesehen werden, dass die

Verfahrensregeln vorgehen und dass die ÖDSMB nicht zuständig ist, aber die Gerichtsbehörde und das Kantonsgericht waren nicht für dieses Lösung, denn sie waren der Meinung, dass sie nur schwer lesbar sei (s. Kommentar zu Artikel 3).

c) Die Vorschriften für Pilotprojekte wurden völlig neu gestaltet (siehe Kommentar zu Art. 22 DSchG und Kommentar zu den Art. 35-35b E-GovG).

d) Das Recht der betroffenen Person, über den Verbleib ihrer Daten nach ihrem Tod zu bestimmen, wurde gestrichen, denn es kann in Praxis kaum angewendet werden (siehe Kommentar zu Art. 27-30 DSchG).

e) Der Entwurf legt die Grundlagen zur Einführung eines Rechts auf Datenübertragbarkeit fest, aber ohne daraus direkt ein justiziables Recht zu machen (siehe Kommentar zu Art. 32 DSchG).

f) Die Vorschriften zu automatisierten Einzelentscheiden wurden vom DSchG ins VRG verschoben (siehe Kommentar zu den Anpassungen des VRG).

g) Die Pflicht, eine Ansprechperson für den Datenschutz zu ernennen, obliegt nicht mehr jedem Verantwortlichen für die Bearbeitung, sondern den Direktionen (siehe Kommentar zu Art. 46 DSchG).

h) Auf Anfrage der ÖDSMB sind die Funktionen der oder des Öffentlichkeitsbeauftragten und der oder des Datenschutzbeauftragten nicht mehr getrennt, sondern werden in einer Person zusammengelegt, welche die Funktion Öffentlichkeitsbeauftragte und Datenschutzbeauftragte innehat.

i) Nach dem Vorbild des Bundes und der anderen Kantone und gemäss den Vorschriften der Europäischen Union wird die oder der Öffentlichkeits- und Datenschutzbeauftragte nicht mehr auf unbestimmte Zeit angestellt, sondern für einen Zeitraum von fünf Jahren ernannt, der verlängert werden kann (siehe Kommentar zu Art. 51 DSchG). Zudem wurde die Aufgabenteilung zwischen der oder dem Beauftragten und der kantonalen Öffentlichkeits-, Datenschutz- und Mediationskommission überprüft und geklärt (Kommentar zu Art. 48 ff. DSchG).

1.5 Folgen des Entwurfs

a) Veränderungen im Verwaltungshandeln

1.5.1. Die Stärkung der Rechte der betroffenen Person und der Pflichten der oder des Verantwortlichen für die Bearbeitung wird sich zwangsläufig auf die Funktionsweise der Organe der Gemeinwesen auswirken. Die tatsächlichen Auswirkungen der vorgenommenen Änderungen auf das Verhalten der betroffenen Personen und der Organe der Verwaltung sind im aktuellen Stadium jedoch schwierig vorherzusehen. Wenn man den ersten Rückmeldungen über das Inkrafttreten der DSGVO und der Richtlinie (EU) 2016/680 in der Europäischen Union Glauben schenkt, scheint eine echte Umwälzung der Verwaltungspraxis dennoch unwahrscheinlich.

1.5.2. Im Gegensatz zu dem, was nach dem Inkrafttreten des DSchG im Jahr 1995 eintrat, werden die Organe des Gemeinwesens nicht gründlich überprüfen müssen, wie sie funktionieren, um sich den neuen Anforderungen im Datenschutz anzupassen. Die Mehrheit unter ihnen ist bereits seit Langem für Fragen des Datenschutzes sensibilisiert. Die erforderlichen Anpassungen dürften für die Mehrheit von ihnen also, auch in Anbetracht der 30 Jahre Erfahrung in diesem Bereich, nur zu punktuellen Veränderungen führen. Weiter gilt, dass, gemäss dem risikobasierten Ansatz, vor allem die Verantwortlichen für die Bearbeitung, die regelmässig grosse Mengen von Daten bearbeiten, am meisten davon betroffen sind. Jedoch haben gerade Letztere seit dem Inkrafttreten des Gesetzes 1995 gezwungenermassen verstärkt Erfahrung in diesem Bereich erworben.

b) Finanzielle und personelle Konsequenzen

1.5.3. Da der Entwurf im Wesentlichen eine Anpassung an übergeordnetes Recht vornimmt, die ohnehin zwingend ist, führt er von sich aus kaum zu neuen Ausgaben. Aber Tatsache ist, dass die verschiedenen Organe des Staates wohl punktuell auf ihre verfügbaren Ressourcen zurückgreifen müssen, insbesondere, wenn es darum geht, eine Datenschutz-Folgenabschätzung durchzuführen oder sicherzustellen, dass eine korrekte Nachbearbeitung eines Sicherheitsvorfalls erfolgt. Auf Verwaltungsebene wird vor allem die Verpflichtung der Direktionen, mindestens eine Ansprechperson für den Datenschutz zu ernennen, die deutlichste neue Belastung darstellen. Die zusätzliche

Arbeitsbelastung beläuft sich auf 0,25 VZÄ pro Direktion plus Staatskanzlei, d. h. insgesamt 2 VZÄ. Im Entwurf wird zusätzlich die Möglichkeit vorbehalten, dass der Staatsrat die Ernennung von Ansprechpersonen in den Ämtern und in den Anstalten vorsieht, die in diesem Bereich besonderen Bedarf haben. Aber da es sich nur um eine Möglichkeit handelt, hat sie keine finanziellen Folgen, solange sie nicht genutzt wird. Die Einführung der Ansprechpersonen für Datenschutz führt so zu einer neuen Ausgabe von 345 000 Franken pro Jahr. Es wird beantragt, dass diese neue Aufgabe an diejenige der Begleitung der Informationssicherheit, ein Thema, das mit dem Datenschutz verbunden ist, gekoppelt wird.

1.5.4. Aus technischer Sicht ist anzumerken, dass der Kanton Freiburg im Rahmen seiner Strategie Freiburg 4.0 den Weg der Digitalisierung eingeschlagen hat. In diesem Zusammenhang wurden bereits einige Initiativen gestartet, um die Verwaltung, Zentralisierung und Standardisierung bestimmter Datenkategorien so gut wie möglich zu beherrschen (siehe hierzu z. B. das Projekt des kantonalen Bezugssystems). Die Gesetzesrevision bringt in Verbindung mit der Umsetzung der Strategie Freiburg 4.0 unweigerlich neue technische Anforderungen mit sich. Diese Anforderungen stehen jedoch voll und ganz im Einklang mit den derzeit verfolgten Zielen der Standardisierung und Konzentration von IT-Architekturen, die zu einer grundlegenden Überarbeitung der Informationsverarbeitung innerhalb des Staates führen. Es ist daher normal, den Datenschutz damit in Verbindung zu bringen, obwohl er nicht die erste Ursache dafür ist. Um den neuen Bedürfnissen und den neuen Pflichten der Verwaltung gerecht zu werden, wird es in einigen Bereichen notwendig sein, die Prozesse zu automatisieren, um die manuelle Bearbeitung zu verringern. Die Umsetzung dieser automatisierten Prozesse wird einige Anstrengungen und auch eine gewisse Anpassungszeit erfordern. So müssen namentlich die notwendigen Umgebungen für die Ausführung der Anfragen aufgebaut oder parametrisiert werden. Dies kann nur unter Berücksichtigung der verwaltungsinternen Haushaltszyklen und auch der Tatsache geschehen, dass einige Systeme veraltet sind und ersetzt werden müssen. In diesem Zusammenhang ist mittel- bis langfristig mit Kosten zu rechnen, die indirekt durch die Anwendung des Gesetzes verursacht werden, die aber auch und vor allem den Kosten entsprechen, die mit einer guten Verwaltung der elektronischen Ressourcen und Infrastrukturen des Staates verbunden sind. Diese Kosten zu beziffern, ist daher weder machbar noch wirklich relevant.

1.5.5. Der Entwurf führt neue Aufgaben für die ÖDSMB und insbesondere für die oder den Öffentlichkeits- und Datenschutzbeauftragte/n ein. Diese neuen Aufgaben kommen zu einer allgemeinen Zunahme der Arbeitsbelastung hinzu, welche die Behörde bereits seit mehreren Jahren im Rahmen der Digitalisierung des Staates bewältigen muss, an der sie entweder direkt durch die Mitwirkung in mehreren Arbeitsgruppen oder indirekt durch ihre Beratung sowie im Rahmen von Vernehmlassungen von Gesetzen beteiligt ist. Seit ihrer Gründung im Jahr 1994 sind die Personalressourcen der ÖDSMB für den Datenschutz jedoch nur leicht gestiegen. 2009 wurden der ÖDSMB 0,5 VZÄ für eine Juristenstelle bewilligt, und im Jahr 2020 wurde die Stelle der oder des Datenschutzbeauftragten um 0,3 VZÄ von 0,5 auf 0,8 VZÄ aufgestockt. Die ÖDSMB verfügt zudem über eine Verwaltungsmitarbeiterin (0,8 VZÄ) und eine juristische Praktikantenstelle zu 100 %. Diese Dotation wurde während der Versuchsphase, in der die Öffentlichkeitsbeauftragte gleichzeitig zur Datenschutzbeauftragten ad interim ernannt wurde (s. § 1.2.6), leicht umgestaltet. Da die Beauftragte 0,8 VZÄ arbeitete, war es möglich, die restlichen 0,5 VZÄ für die Beauftragte in 0,5 VZÄ für eine Juristin oder einen Juristen umzuwandeln und so eine 100 %-Stelle zu erhalten. Ausserdem leiht die Staatskanzlei der Behörde derzeit 0,6 VZÄ für eine Juristin oder einen Juristen und 1 VZÄ für eine juristische Praktikantenstelle. Sicherlich wird die Umstellung auf das neue Gesetz zu einem höheren Personalbedarf der Behörde führen, doch lässt sich dieser Anstieg derzeit nur schwer beziffern. In jedem Fall ist für diese Legislaturperiode bereits ein neues, zusätzliches VZÄ vorgesehen. Da diese Erhöhung eine Folge der Umsetzung völkerrechtlicher Verpflichtungen ist, die für die Schweiz bindend sind, handelt es sich nicht um eine neue, sondern um eine gebundene Ausgabe; sie wird bei der Berechnung des Finanzreferendums nicht berücksichtigt.

1.5.6. Insgesamt können die neu und direkt auf das neue Gesetz zurückzuführenden Kosten somit auf die Schaffung von 2 neuen VZÄ geschätzt werden. Über einen Zeitraum von fünf Jahren ergibt sich daraus eine Ausgabe von rund 1 725 000 Franken. Dieses Gesetz unterliegt somit weder dem fakultativen noch dem obligatorischen Finanzreferendum.

1.6 Übereinstimmung mit übergeordnetem Recht und nachhaltige Entwicklung

1.6.1. Der Entwurf aktualisiert die Rahmenbedingungen des Rechts auf Datenschutz, das in Artikel 12 Abs. 2 der Verfassung des Kantons Freiburg vom 16. Mai 2004 garantiert wird. Es stellt auch sicher, dass die Verpflichtungen, welche die Schweiz im Rahmen der Abkommen von Schengen und Dublin mit der Europäischen Union eingegangen ist, eingehalten werden, und erfüllt die Anforderungen des Übereinkommens SEV 108+, das der Bund bereits ratifiziert hat. Das Projekt hat somit genau das Ziel, die Gesetzgebung des Kantons Freiburg mit dem übergeordneten Recht in Einklang zu bringen.

1.6.2. Der Entwurf wurde einer umfassenden Analyse nach der Methode Kompass 21 unterzogen, um die Stärken und Schwächen des Entwurfs in den drei Dimensionen der nachhaltigen Entwicklung (Wirtschaft, Umwelt und Gesellschaft) zu ermitteln. Diese Analyse ergab, dass der Entwurf eine weitgehend positive gesellschaftliche Auswirkung haben wird, da er einen beruhigenden Rahmen für die Bearbeitung personenbezogener Daten durch Verwaltungsorgane schafft. Auch aus wirtschaftlicher Sicht sind die Auswirkungen insgesamt positiv. Es ist richtig, dass die Anforderungen des Datenschutzes kurzfristig den Fortschritt einiger Projekte bremsen können. Diese Bemühungen, die Teil einer guten Regierungsführung sind, werden jedoch mittel- und langfristig belohnt, da sie zu robusten und nachhaltigen Infrastrukturen und Anwendungen führen. Zudem wird die Harmonisierung des kantonalen Rechts mit den Gesetzen des Bundes, der anderen Kantone und der EU den Austausch zwischen dem Kanton Freiburg und der Aussenwelt erleichtern. Damit das künftige Gesetz seine Ziele erreichen kann, hat die Analyse jedoch einen hohen Bedarf an Begleitung aufgezeigt, der durch die Dichte und Komplexität des Gesetzestextes induziert wird. Die Schaffung eines Netzwerks von Ansprechpersonen für den Datenschutz innerhalb der Verwaltung und die Durchführung von Schulungen wurde als eines der Schlüsselelemente angesehen, die für den Erfolg des Entwurfs notwendig sind. Diese Begleitung wird es mittelfristig ermöglichen, den Bedarf an bestehender Unterstützung innerhalb der Direktionen zu ermitteln, um diese Umsetzung zu gewährleisten.

2 Kommentar zu den einzelnen Bestimmungen

—

2.1 Abschnitt 1, Allgemeine Bestimmungen

Art. 1, Zweck

Die kontinuierliche Zunahme der Zahl der Datenbearbeitungen und die Verbesserung der Mittel in diesem Bereich haben zu tiefgreifenden Veränderungen in der Rechtsordnung mehrerer Grundrechte geführt, zu denen in erster Linie die persönliche Freiheit und der Schutz der Privatsphäre gehören. Aber auch andere Rechte sind direkt betroffen, so etwa die Meinungsäusserungsfreiheit, die Meinungsfreiheit und die Vereinsfreiheit. Das Bundesgericht hat vor diesem Hintergrund die Existenz eines neuen Grundrechts auf informationelle Selbstbestimmung anerkannt, das die Funktion hat, der betroffenen Person eine bessere Kontrolle über die sie betreffenden Informationen zu gewähren[3]. Aus diesem Grund sieht der Entwurf wie das geltende Gesetz vor, dass die *Grundrechte* der betroffenen Person geschützt werden, ohne indes zu präzisieren, welche das genau sind.

Art. 2, Persönlicher Geltungsbereich

1. Der persönliche Geltungsbereich des Entwurfs basiert im Wesentlichen auf dem geltenden Gesetz. Er deckt ab:
    a) alle Organe, die der Legislative, Exekutive und Judikative auf kantonaler, kommunaler und interkommunaler Ebene unterstehen, einschliesslich anderer Personen des öffentlichen Rechts wie öffentlich-rechtliche Anstalten (mit oder ohne Rechtspersönlichkeit) oder öffentlich-rechtliche Gesellschaften in Form einer Aktiengesellschaft. Hierunter fallen auch besondere Einrichtungen wie der Justizrat.

—

[3] Namentlich: BGE 145 IV 42, Erw. 4.2; BGE 144 I 126 Erw. 4; BGE 143 I 253 Erw. 4.

b) bestimmte natürliche oder juristische Privatpersonen, wenn sie mit der Erfüllung öffentlicher Aufgaben betraut sind. Die Formel entspricht der in Artikel 2 Bst. *d* VRG verwendeten. Das Gesetz ist jedoch nur auf den Teil ihrer Tätigkeit anwendbar, der mit der betreffenden öffentlichen Aufgabe zusammenhängt. Als Institutionen werden beispielsweise der Freiburger Tourismusverband oder die Freiburger Krebsliga, für den Betrieb des kantonalen Krebsregisters verstanden.

2. Wie bereits unter dem geltenden Gesetz wird in Absatz 2 die Frage der anerkannten Kirchen behandelt. Gemäss dem KSG sind Pfarreien und Kirchgemeinden, kirchliche Körperschaften und kirchenrechtliche Personen juristische Personen des öffentlichen Rechts. Aus diesem Grund fallen sie in den Anwendungsbereich der kantonalen Datenschutzgesetzgebung. Der Entwurf behält für die Kirchen jedoch die Möglichkeit vor, ihre eigenen Bestimmungen zu erlassen und eine eigene Aufsichtsbehörde für den Datenschutz einzusetzen. Unter diesen Bedingungen können sie beantragen, aus dem Geltungsbereich des kantonalen Gesetzes herausgenommen zu werden und sich selbst zu verwalten.

Art. 3, Materieller Geltungsbereich

1. Der materielle Geltungsbereich des Gesetzes ist absichtlich so weit wie möglich gehalten (s. Abs. 1). Gewisse Arten von Bearbeitungen fallen jedoch nicht darunter. Das betrifft insbesondere:

   a) *Datenbearbeitungen im Rahmen von laufenden Zivil-, Straf- und Verwaltungsverfahren.* Im Vorentwurf war ursprünglich vorgesehen, dass dieser Grund für eine Ausnahme zugunsten von zwei gezielteren Ausnahmen aufgegeben wird. Während der Dauer des Verfahrens wären die Anforderungen nach diesem Gesetz auf Eis gelegt worden, und die ÖDSMB wär für unzuständig erklärt worden. Damit konnte sichergestellt werden, dass die Vorschriften über die Datensicherheit weiterhin gegolten hätten. Aber die richterliche Gewalt und das Kantonsgericht waren von dieser Lösung, die von den Standards von anderen Datenschutzgesetzen in der Schweiz abweicht, nicht überzeugt. Deshalb wurde die Ausnahme bei den laufenden rechtlichen Verfahren wieder eingeführt. Dieser Grund für eine Ausnahme betrifft ausschliesslich die Bearbeitungen von Daten zu einem hängigen Verfahren. Die gerichtlichen Organe bleiben damit für die übrigen Bearbeitungen, die sie ausführen (Personalmanagement, Korrespondenz ausserhalb der Verfahren, Kommunikation mit der übrigen Verwaltung usw.) oder wenn das Verfahren beendet ist, dem Datenschutzgesetz unterstellt. Im Verwaltungsrecht gilt die Ausnahme nicht für erstinstanzliche Verwaltungsverfahren, die vollständig dem Datenschutzgesetz unterstellt bleiben. Nur die Verfahren vor den Verwaltungsgerichtsbehörden im Sinn von Artikel 3 VRG fallen unter diesen Grund für eine Ausnahme.

   b) *Datenbearbeitungen, die für den ausschliesslich persönlichen Gebrauch durchgeführt werden.* Dieser Grund für eine Ausnahme stand nicht im Vorentwurf. Er betrifft die Datenbearbeitungen, die von einer Person im Dienst des Staats ausschliesslich für den persönlichen Gebrauch durchgeführt werden. Die Einführung dieser Ausnahme, die man in Artikel 2 Abs. 2 Bst. a n-DSG und in verschiedenen kantonalen Gesetzen findet, wurde im Vernehmlassungsverfahren ausdrücklich gefordert. Sie hat aber nur beschränkte Wirkung, denn sie kann nicht mehr geltend gemacht werden, sobald die fraglichen Daten amtlich verwendet, mit einer Drittperson geteilt oder auf einem geteilten Server zur Verfügung gestellt werden. Konkret beschränkt sich diese Ausnahme auf die persönlichen Überlegungen, die eine Einzelperson anstellt, um sich in einer Angelegenheit ihre eigene Meinung zu bilden, und die sie nicht teilt.

   c) *Datenbearbeitungen, die von öffentlichen Organen im wirtschaftlichen Wettbewerb mit Personen des Privatrechts durchgeführt werden.* Diese Ausnahme ist nötig, damit keine Wettbewerbsverzerrung geschaffen wird. Die betreffenden Datenbearbeitungen unterstehen dem Teil des Bundesgesetzes über den Datenschutz, der Privatpersonen vorbehalten ist. Der Geltungsbereich dieser Ausnahme ist jedoch begrenzt. Darauf berufen können sich nur öffentliche Organe, die Aktivitäten in einer Situation des wirtschaftlichen Wettbewerbs ausüben und soweit sie nicht als von der öffentlichen Hand eingesetzte Organe handeln. Das ist beispielsweise grundsätzlich bei der Kantonalbank der Fall, ausser bei den Tätigkeiten, bei denen sie ein öffentlich-rechtliches Monopol hat (z. B. Art. 7 Abs. 1 FKBG). Im Gegensatz zum Vorentwurf verzichtet der Entwurf darauf, die Überwachung dieser Art von Bearbeitungen der ÖDSMB zu übertragen, wie das namentlich im Kanton Bern der Fall (s. Art. 4 Abs. 2 Bst. a, 2. Satz KDSG/BE). Einerseits hat der

Eidgenössische Datenschutzbeauftragte in der Vernehmlassung geltend gemacht, dass er nicht für diese Lösung ist, denn er ist der Meinung, dass sie in seine eigenen Kompetenzen eingreift. Andererseits ist es besser, wenn sich die Behörde auf ihre Hauptaufgabe konzentriert, da sie über beschränkte Ressourcen verfügt.

2. Gegenüber dem Vorentwurf entfällt die feste Ausnahme bei den Verhandlungen des Grossen Rates, der Gemeindeversammlungen, der Generalräte sowie der Bürgerversammlungen und ihrer Kommissionen (Art. 2 Abs. 2 DSchG). Diese Ausnahme wurde früher mit dem Grundsatz der Geheimhaltung begründet, der innerhalb des Staates herrschte, und dem daraus resultierenden Wunsch, die Möglichkeit einer Person zu blockieren, ihr Recht auf Zugang zu ihren eigenen Daten auszuüben, wenn diese von solchen Organen bearbeitet wurden. Dieses Prinzip wurde jedoch seither weitgehend durchbrochen, insbesondere durch die Verabschiedung des InfoG im Jahr 2009, mit dem das Öffentlichkeitsprinzip eingeführt wurde.[4] Im Weiteren wurde diese Regelung in der Lehre kritisiert und überlebte nur in einer Minderheit von Kantonen (GE, VD, NW und BE). Die Aufhebung scheint daher für die betroffenen Organe durchaus machbar zu sein. Im Übrigen wurde sie im Rahmen der Vernehmlassung nicht angefochten. Was die Anwendung des Rechts auf Zugang zu den eigenen Daten und anderer damit verbundener Rechte in diesem Bereich betrifft, so wird es weiterhin möglich sein, in gerechtfertigten Fällen die Ausübung dieser Rechte einzuschränken oder zu verweigern, jedoch nur in begründeten Fällen und auf der Grundlage einer ordnungsgemässen Interessenabwägung.

Art. 4, Definitionen

Fast alle Definitionen in diesem Artikel wurden wörtlich oder fast wörtlich aus dem neuen DSG des Bundes übernommen. Wir können uns daher generell auf die Erläuterungen zu diesem Thema in der Botschaft des Bundesrats berufen (siehe BBI 2017 6941, S. 7019 ff.) und dazu die folgenden Präzisierungen anbringen:

> Der Begriff Abrufverfahren, den man in Artikel 14 Abs. 4 des Entwurfs wiederfindet, wird in den Definitionen eingeführt (Bst. e). Diese besondere Form der Datenbekanntgabe wurde bisher lediglich in einem Erlass des Staatsrats beschrieben. Angesichts seiner Bedeutung schien es angebracht, diese Definition auf Gesetzesebene einzuführen.

> Nach dem Vorbild des neuen Bundesgesetzes (Art. 5 Bst. f DSG) und des EU-Rechts (Art. 3 Abs. 4 der EU-Richtlinie 2016/680 und Art. 4 Abs. 4 DSGVO) führt der Entwurf den Begriff des Profilings ein. Dabei handelt es sich um einen automatisierten Bearbeitungstyp von Daten, der als besonders eindringlich zu betrachten ist. Er besteht darin, absichtlich bestimmte persönliche Merkmale hervorzuheben oder vorherzusagen, die für eine Person bedeutend sind, namentlich mit dem Zweck, der betreffenden Person eine Sonderbehandlung zuteilwerden zu lassen. Aus diesem Grund unterliegt das Profiling denselben Bedingungen wie die Bearbeitung besonders schützenswerter Daten.

> Gemäss den Änderungen, die bei der Verabschiedung des Gesetzes vom 18. Dezember 2020 zur Anpassung der kantonalen Gesetzgebung an bestimmte Aspekte der Digitalisierung (AS 2020_195) eingeführt wurden, enthält der Entwurf eine Definition der Auslagerung der Datenbearbeitung. Diese Definition unterstützt die Artikel 18 – 21, in denen die Bedingungen aufgeführt sind, unter denen eine Auslagerung zulässig ist. Gegenüber der Definition, die 2021 eingeführt wurde, wird die neue Definition in zwei Punkten genauer. Erstens gibt sie an, dass die Auslagerung eine Form der qualifizierten Auftragsbearbeitung ist. Dadurch ist es gerechtfertigt, dass sie besonderen Vorschriften unterworfen wird. Zweitens wird im Entwurf wortwörtlich festgehalten, dass die Auslagerung die Zuhilfenahme von Informatikinstrumenten in der Cloud (*cloud computing*) betrifft, damit klar zwischen Auslagerung und Weitervergabe unterschieden werden kann.

> Wie das neue DSG und das Übereinkommen SEV 108+ verzichtet der Entwurf auf den Begriff der «*Datensammlung*»~~,~~ der angesichts des allgegenwärtigen Charakters der Daten veraltet ist. Er wird generell ersetzt durch den weiteren und dynamischeren Begriff der «*Bearbeitungstätigkeit*». Aus diesem Grund wird der

[4] MAURER-LAMBROU Urs / KUNZ Simon, op. zit., Nr. 23; ebenfalls: ZUFFEREY Jean-Baptiste, *Les règles de la procédure administrative face à la protection des données – Combat ou complémentarité?*, in FZR, Spezialnummer: «Le droit en mouvement, 2002 169, S. 176.

«Verantwortliche der Datensammlung», der im Art. 4 Bst. g des geltenden Gesetzes erwähnt wird, zum «Verantwortlichen für die Bearbeitung (Bst. h) und der Begriff Register der Datensammlungen, den man derzeit in Art. 21 DSchG findet, im Entwurf zum «Bearbeitungsregister» (Art. 38 des Entwurfs) umbenannt (Bst. j). Insgesamt bleiben diese Änderungen jedoch in erster Linie terminologischer Art und dürften keine besonderen praktischen Auswirkungen haben.

> Angesichts seiner zentralen Rolle bei der Durchsetzung des Datenschutzes wird vorgeschlagen, eine Definition des « Bearbeitungregisters» (Bst. j) zu geben. Dieses stellt zugleich ein Werkzeug zur Sicherung der Transparenz und der Governance dar. Das bedeutet insbesondere, dass die oder der Verantwortliche für die Bearbeitung in der Lage sein muss, für jede Bearbeitung zu bestimmen, wer die Daten bearbeitet, welche Kategorien von Personen betroffen sind, welche Daten zu welchem Zweck und auf welche Weise bearbeitet werden, wer Zugang zu diesen Daten hat, wie lange sie aufbewahrt werden, welche Sicherheitsmassnahmen ergriffen wurden usw.

> Im Gegensatz zum Vorentwurf führt der Entwurf eine Definition der «*Verletzung der Sicherheit von* Personendaten» ein (Bst. k) und passt sich damit an Artikel 5 Bst. h des neuen DSG und an das EU-Recht an (Art. 3 Ziff. 12 der Richtlinie (EU) 2016/680 und Art. 4 Ziff. 11 DSGVO). Diese Definition unterstützt die Artikel 43 und 44 des Entwurfs des DSchG, in denen die Massnahmen aufgeführt sind, die zu ergreifen sind, wenn ein solches Ereignis eintritt.

Im Vergleich zum Vorentwurf verzichtet der Entwurf auf die Definition von Personenidentifikatoren und damit auf eine gesetzliche Regelung dieser Thematik. Seit der im Bundesrecht vorgesehenen Liberalisierung der AHV-Nummer und der Schaffung des im E-GovG vorgesehenen kantonalen Personenidentifikators (KPI) scheint die Notwendigkeit, dieses Thema gesetzlich zu regeln, nicht mehr erwiesen zu sein.

2.2 Abschnitt 2, Grundsätze für die Bearbeitung von Personendaten

2.2.1 Abschnitt 2.1: Allgemeine Bedingungen für die Rechtmässigkeit der Bearbeitung

Art. 5, Gesetzliche Grundlage

1. Die Bearbeitung von Personendaten durch öffentliche Organe ist eine staatliche Tätigkeit, die dem Legalitätsprinzip unterliegt (Abs. 1). Die Frage, wie präzise die gesetzliche Bestimmung sein muss und auf welcher Ebene sie liegen sollte, hängt davon ab, wie gross das Risiko der Verletzung der Rechte von Personen durch die geplante Bearbeitung ist.
2. In Anlehnung an die Praxis des Bundes und anderer Kantone stellt der Entwurf höhere Anforderungen an die Rechtmässigkeit der Bearbeitung von Personendaten, die ein erhöhtes Risiko für die Rechte von Personen darstellen (besonders schützenswerte Daten, Profiling, Schaffung besonderer Risiken). Diese Art der Bearbeitung ist generell nur dann zulässig, wenn eine Rechtsgrundlage im formellen Sinne dies ausdrücklich erlaubt (Abs. 2 Bst. a und Abs. 3). Auf Gemeindeebene entspricht dies einem allgemeinverbindlichen Reglement. Für die Bearbeitung besonders schützenswerter Daten kann jedoch in bestimmten Situationen eine indirekte gesetzliche Grundlage ausreichen, wenn die Bearbeitung für die Erfüllung einer in einem Gesetz im formellen Sinne vorgesehenen Aufgabe unerlässlich ist und sich daraus keine besonderen Risiken für die betroffenen Personen ergeben (Abs. 2 Bst. b). Diese Regel ergibt sich aus der Tatsache, dass der Gesetzgeber nicht immer alle Datenbearbeitungen, die der Erfüllung einer bestimmten Aufgabe zugrunde liegen, im Voraus vorhersehen kann.
3. Die kantonale Aufsichtsbehörde hat bisher immer eine formalrechtliche Grundlage für diese Arten der Bearbeitung verlangt, auch wenn es keine solche ausdrückliche Anforderung im Gesetz gibt. Angesichts der guten Akzeptanz dieser Praxis innerhalb der Verwaltung dürfte diese Änderung keinen erheblichen praktischen Einfluss haben. Es ist jedoch zu überprüfen, ob diese Vorschrift bei den laufenden Bearbeitungen eingehalten wird. Eine Übergangsfrist von zwei Jahren ist speziell für diesen Zweck vorgesehen (vgl. Art. 65 des Entwurfs).
4. Das Amt für Gesetzgebung hat ein Dokument verfasst, das den Juristinnen und Juristen ein Instrument und eine Methode zum Verfassen der nötigen gesetzlichen Grundlage für die Bearbeitung der Personendaten geben soll. Dieses Dokument kann auf der Website des Amtes für Gesetzgebung abgerufen werden

(https://www.fr.ch/cha/sleg). Insofern, als es sich um ein Dokument des Amts für Gesetzgebung handelt, ist der Inhalt für die ÖDSMB natürlich nicht verbindlich. Es bildet einfach eine Redaktionshilfe.

5. Ausnahmsweise ist eine gesetzliche Grundlage nicht nötig, wenn eine Datenbearbeitung, insbesondere eine Bekanntgabe, unerlässlich ist, um die erheblichen Interessen der betroffenen Person oder einer oder eines Dritten, wie das Leben oder die körperliche Integrität, zu wahren (Abs. 4). Es handelt sich um eine Ausnahme, deren Geltungsbereich jedoch sehr eng gefasst ist, deren Nutzung sollte sich in der Praxis auf die Bereiche medizinische oder allenfalls polizeiliche Notfälle beschränken.

Art. 6, Einwilligung

1. Die Einwilligung der betroffenen Person ist der wichtigste aussergesetzliche Rechtfertigungsgrund im Datenschutzrecht. Grundsätzlich werden die Rechte der betroffenen Person nicht verletzt, wenn sie einwilligt, dass ihre Personendaten für Zwecke, die sie selbst gewählt hat, gesammelt und bearbeitet werden. Im öffentlichen Recht kann die Einwilligung im Allgemeinen nur in einem konkreten Fall erfolgen und vermag den Erlass einer gesetzlichen Grundlage nicht zu ersetzen (Abs. 1).
2. In Absatz 2 werden die Bedingungen für die Gültigkeit der Einwilligung festgelegt. Um gültig zu sein, muss die Einwilligung zunächst einmal frei und aufgeklärt erfolgen. Das bedeutet zum einen, dass die einwilligende Person ordnungsgemäss, transparent und verständlich über den Zweck und die Modalitäten der Bearbeitung informiert worden sein muss, und zum anderen, dass die Person weiterhin die Möglichkeit hat, die Einwilligung ohne Nachteile zu verweigern. Bei der Bearbeitung besonders schützenswerter Daten und bei Profiling-Aktivitäten muss die Einwilligung-ausdrücklich erfolgen. Dies ist insbesondere dann der Fall, wenn die betroffene Person einer ordnungsgemässen Einwilligungserklärung zustimmt. Diese Art von Erklärungen findet man bereits für bestimmte Leistungen, die im virtuellen Schalter angeboten werden. Dies schliesst Einwilligungen durch schlüssige Handlungen aus. Im Vergleich zum Vorentwurf fügt der Entwurf hinzu, dass die Einwilligung vermutet wird, wenn die Person ihre Daten selbst frei zugänglich gemacht hat. Dieser Zusatz findet sich im Bundesrecht (vgl. Art. 17 Abs. 2 Bst. c DSG / Art. 34 Abs. 4 Bst. b des neuen DSG) und in fast allen kantonalen Gesetzen. Er betrifft beispielsweise die Daten, welche die betroffene Person auf LinkedIn gepostet hat und die von der Anstellungsbehörde im Rahmen einer Bewerbung bearbeitet werden können.
3. In den Absätzen 3–5 werden verschiedene Bedingungen festgelegt, welche die Verantwortlichen für die Bearbeitung, die sich auf die Einwilligung der betroffenen Person stützen, erfüllen müssen. Die Tatsache, dass die Freiwilligkeit einer Datenbearbeitung, die nicht im Gesetz vorgesehen ist, erwähnt werden muss (Abs. 3), ist eine Konkretisierung der freien und aufgeklärten Einwilligung. Die Aufbewahrung eines Mittels, welches das Vorhandensein der Einwilligung nachweisen kann (Abs. 4), ist aus Beweisgründen erforderlich. Der Widerruf der Einwilligung (Abs. 5) geht Hand in Hand mit der Möglichkeit, die Einwilligung zu erteilen.

Art. 7, Zweckbindung

1. Der Grundsatz der Zweckbindung ist charakteristisch für das Datenschutzrecht. Er ist in zwei Teile gegliedert: *a*) Festlegung eines Zwecks vor der Bearbeitung (Grundsatz der Zweckbestimmung) und *b*) Verwendung der Daten für diesen Zweck oder zumindest für einen Zweck, der mit diesem Zweck vereinbar ist (Grundsatz der Vereinbarkeit des Zwecks). Zusammen schränken die Grundsätze der Bestimmtheit und der Vereinbarkeit die Möglichkeiten der Wiederverwendung von Daten ein, indem sie insbesondere ausschliessen, dass Daten unbegrenzt beschafft und «im Hinblick auf ...» gespeichert werden.
2. Das Prinzip der Zweckbindung ist jedoch nicht unumstösslich. Die betroffene Person kann einer Änderung des Zwecks ihrer Daten rechtswirksam zustimmen, wenn sie ein Interesse daran hat (Abs. 2). Grundsätzlich kann ein Gesetz auch vom Zweckbindungsgrundsatz abweichen, indem es die Weiterverwendung von Daten zu anderen Zwecken als den ursprünglich vorgesehenen vorsieht.
3. Im Vergleich zum Vorentwurf wurde im Entwurf die Anforderung gestrichen, dass die vorgesehene Zweckbindung legitim sein muss. Es ist absolut möglich, aufgrund von Legalitätsprinzipien und des Grundsatzes von Treu und Glauben und auch des Willkürverbots zu demselben Ergebnis zu gelangen.

Art. 8, Verhältnismässigkeit

1. Der Grundsatz der Verhältnismässigkeit ist ein Schlüsselinstrument der gesamten Rechtsordnung. Im Allgemeinen fordert er, dass die Mittel, die von der öffentlichen Hand eingesetzt werden, um ein bestimmtes Ziel zu erreichen, nicht übermässig sein und nicht unangemessen in die Rechte und Freiheiten des Einzelnen eingreifen dürfen.
2. Im Datenschutzrecht bedeutet der Grundsatz der Verhältnismässigkeit, dass nur solche Daten bearbeitet werden dürfen, die geeignet und erforderlich sind, um den Zweck der Bearbeitung zu erreichen. Ausserdem muss ein vernünftiges Verhältnis zwischen den Zweckbindungen und den eingesetzten Mitteln bestehen. Die Grundsätze der Datenvermeidung und -minimierung sind zwei eigene Ausprägungen des Verhältnismässigkeitsprinzips im Datenschutzrecht. Aus dem ersten folgt, dass, wenn der Zweck der Bearbeitung ohne die Erhebung neuer Daten erreicht werden kann, diese Option bevorzugt werden sollte. Die zweite besagt, dass nur die für den Zweck relevanten und unbedingt notwendigen Daten bearbeitet werden dürfen, während andere ausgeschlossen sind. Grundsätzlich sollten diese beiden Leitlinien bereits bei der Entwicklung neuer Bearbeitungen beachtet werden. Sie sind eng mit den Grundsätzen des Datenschutzes durch Technikgestaltung und des Datenschutzes durch Voreinstellungen verknüpft (vgl. Art. 40 des Entwurfs).

Art. 9, Richtigkeit

Unter Richtigkeit, wie sie hier verwendet wird, ist eine relative Richtigkeit zu verstehen: In der Praxis ist klar, dass die Daten, die von den verschiedenen Gemeinwesen gespeichert werden, nicht laufend auf dem neuesten Stand sein können. Obgleich es ein mehr oder weniger konstantes Ziel bleiben muss, ist die Pflicht der Richtigkeit und der Aktualisierung der Daten vor allem eine Pflicht der Mittel und nicht des Ergebnisses. Ihr Umfang hängt von den Umständen des jeweiligen Falls, vom Zweck der Bearbeitung, der Natur der bearbeiteten Daten und ihrem mehr oder weniger besonders schützenswerten Charakter ab.

Art. 10, Aufbewahrungsfrist

1. Die Aufbewahrung der Daten darf die erforderliche Dauer für die Zwecke, für die sie gespeichert worden sind, nicht überschreiten. Ist der Zweck der Datenbearbeitung erreicht, dürfen sie nicht weiter gespeichert bleiben, sondern müssen gelöscht (oder anonymisiert) werden. Dies hat für die Verantwortlichen für die Bearbeitung zur Folge, dass sie in regelmässigen Abständen prüfen müssen, ob die Daten in ihrem Besitz für die angestrebten Zwecke noch relevant sind. Ein Vorbehalt existiert aber für Daten, die archivwürdig sind. Diese Daten dürfen nicht gelöscht werden, sondern müssen dem Archiv abgeliefert werden[5]. Zusätzliche Details zu diesem Thema finden sich in den Artikeln 23 und 24 des Entwurfs.
2. Gemäss Absatz 2 müssen Personendaten, die im Bereich der Forschung, der Planung oder der Statistik einen besonderen Wert haben, nicht in der gleichen Art gelöscht werden und können länger aufbewahrt werden, sofern Massnahmen zum Schutz der Rechte der betroffenen Personen ergriffen werden.

Art. 11, Besondere Sorgfaltspflicht

Die besondere Sorgfaltspflicht, die angesichts der Bearbeitung von Daten mit grösseren Risiken für die Rechte von Personen gefordert wird, ist bereits im Text des aktuellen Gesetzes enthalten. Es ist eine Freiburger Spezialität, die in keinem anderen Datenschutzgesetz in der Schweiz vorkommt. Auch wenn in der Vorschrift nicht konkret definiert wird, welche Massnahmen ergriffen werden müssen, blieb sie erhalten, da sie eine Konkretisierung des risikobasierten Ansatzes darstellt, mit dem erreicht werden soll, dass die grossen Anstrengungen, die im Bereich Datenschutz unternommen werden sollen, da erfolgen, wo das Risikopotenzial am grössten ist. Das heisst für die Praxis, dass technische und/oder organisatorische Massnahmen situationsspezifisch und risikoadäquat ergriffen werden sollen.

[5] Zur Wirkung dieses Vorbehalts: BGE 148 I 233, Erw. 4–6.

2.2.2 Abschnitt 2.2: Zusätzliche Bedingungen für bestimmte Formen der Bearbeitung

Art. 12 und 13, Beschaffen von Daten

1. Wie bei jeder Bearbeitung muss auch für das Beschaffen von Daten ein Rechtfertigungsgrund vorliegen. Da diese Anforderung jedoch bereits aus den Artikeln 5 und 6 hervorgeht, verzichtet der Entwurf darauf, sie hier ein zweites Mal zu wiederholen. Aus diesem Grund wurde Artikel 12 Abs. 1 des Vorentwurfs gestrichen.
2. Im Vergleich zum Vorentwurf wird im Entwurf auch der Grundsatz gestrichen, dass die Daten direkt bei der betroffenen Person erhoben werden. Während dieser Grundsatz Anfang der 1990-er-Jahre, als das DSchG ausgearbeitet wurde, galt und auch heute noch in mehreren Tätigkeitsbereichen der Verwaltung anwendbar ist, werden bestimmte Datenkategorien künftig einmal beschafft und dann den Verwaltungseinheiten zur Verfügung gestellt, die sie zur Erfüllung ihrer Aufgaben benötigen. Dies entspricht dem *Once-Only-Prinzip*, das der Bund und die Kantone derzeit entwickeln. Angesichts dieser Entwicklung erschien es unangemessen, diesen Grundsatz im Gesetz beizubehalten.
3. Mit dem Ziel, die Transparenz und Wiedererkennbarkeit der Datenbearbeitung zu verbessern, führt der Entwurf im Weiteren eine Pflicht für die Verantwortlichen ein, die betroffenen Personen über die Datenbeschaffung zu informieren (Art. 12). Diese Regel stellt heute einen einhellig anerkannten Standard im Datenschutz dar, der sich im Bundesrecht (vgl. Art. 19 des neuen DSG) und in anderen kantonalen Gesetzen wiederfindet. Die zu liefernden Informationen müssen es der betroffenen Person ermöglichen, rasch zu verstehen, wer Daten in ihrer Sache bearbeitet, zu welchem Zweck dies erfolgt, wem die Daten im Prinzip bekanntgegeben werden könnten und welches ihre Rechte sind. Daten, die freiwillig gewonnen werden – z. B. mit einem Fragebogen – müssen als solche ausgewiesen werden. Der Schuldner der Informationspflicht ist immer die Stelle, welche die Daten beschafft, nicht diejenige, die sie bekannt gibt. Die Stelle, welche die Daten bekannt gibt, muss sicherstellen, dass die Bekanntgabe rechtmässig ist, ist aber nicht verpflichtet, die betroffene Person über die Bekanntgabe ihrer Daten zu informieren. Artikel 31 Abs. 3 des Entwurfs bleibt aber vorbehalten, wenn die Person ihr Recht auf Einsprache ausübt.
4. Es wird nicht weiter präzisiert, welche Form die Information annehmen muss. Die oder der Verantwortliche für die Bearbeitung hat dafür zu sorgen, dass die betroffene Person über ein einfach zugängliches Mittel effektiv von der Datensammlung Kenntnis nehmen kann, aber nicht, dass sie sich tatsächlich danach erkundigt. Ein direkter Kontakt mit der betroffenen Person ist nicht erforderlich. Eine standardisierte Information, z. B. mit einer Datenschutzerklärung, die an ein Formular angehängt oder auf einer Webseite abrufbar ist, kann genügen.
5. Die Informationspflicht ist nicht als absolut zu verstehen: die oder der Verantwortliche für die Bearbeitung kann unter den verschiedenen Bedingungen nach Artikel 13 von der Informationspflicht befreit werden. Der Ausnahmegrund, der am häufigsten zutreffen wird, ist dann logischerweise die Erfüllung einer gesetzlichen Aufgabe. In diesem Fall wird die Informationspflicht mit der Veröffentlichung des Gesetzes erfüllt. Die Informationspflicht kann auch unter denselben Bedingungen eingeschränkt oder verzögert werden, wie sie für das Auskunftsrecht in Artikel 29 Abs. 1 vorgesehen sind (vgl. Art. 13 Abs. 2).

Art. 14–17, Gewöhnliche und grenzüberschreitende Datenbekanntgabe

1. Die Bekanntgabe von Daten dient dazu, Personendaten zugänglich zu machen, z. B. indem ihre Einsichtnahme gestattet wird, sie weitergegeben, verbreitet oder veröffentlicht werden. Dieses Konzept umfasst sowohl die regelmässige Bekanntgabe als auch die Bekanntgabe im Einzelfall. Die Bedingungen der Rechtmässigkeit sind jedoch nicht dieselben, sondern hängen davon ab, in welchem Fall man sich befindet:
    a) Nach Artikel 14 Abs. 1 des Entwurfs muss die systematische Bekanntgabe, d. h. die Bekanntgabe eines Datentyps, der regelmässig an die gleichen Empfänger gerichtet wird, in einer gesetzlichen Grundlage im Sinne von Artikel 5 des Entwurfs vorgesehen sein.
    b) Nach Artikel 14 Abs. 2 müssen Datenbekanntgaben, die im Einzelfall stattfinden, nicht zwingend in einer gesetzlichen Bestimmung vorgesehen werden. Sie können auch stattfinden, wenn sie einem der Gründe nach den Buchstaben *a* bis *c* entsprechen.

2. Im Entwurf wird eine dritte Kategorie der Bekanntgabe von Daten geregelt: die Bekanntgabe im Abrufverfahren (Art. 14 Abs. 4). Die Bekanntgabe im Abrufverfahren ist ein automatisierter Datenbekanntgabemodus, bei dem die Empfängerin oder der Empfänger der Daten aufgrund einer Bewilligung des Verantwortlichen der Datensammlung selber und ohne vorherige Kontrolle über den Zeitpunkt und den Umfang der Bekanntgabe entscheidet. Angesichts der Besonderheiten dieser Art von Bekanntgabe ist es sowohl aus Gründen der Transparenz als auch der Governance und der Sicherheit gerechtfertigt, sie eigens zu erwähnen, um sie von anderen Formen der Bekanntgabe zu unterscheiden. Diese Forderung ist nicht neu. Sie wurde aus Artikel 10 Abs. 2 des geltenden Gesetzes übernommen.

3. Bei der grenzüberschreitenden Bekanntgabe von Daten gelten zusätzliche Anforderungen (Art. 15):

   a) Übermittlungen von Personendaten an Staaten im Ausland sind grundsätzlich nur zulässig, wenn der Empfängerstaat ein als angemessen erachtetes Datenschutzniveau bietet. Um festzustellen, ob ein Staat ein angemessenes Schutzniveau bietet, kann die vom Bundesrat gemäss Artikel 16 Abs. 1 des neuen DSG erstellte Liste herangezogen werden.

   b) Wenn der Empfängerstaat ein Drittstaat ist, der kein angemessenes Schutzniveau bietet, oder wenn diesbezüglich Zweifel bestehen, bleibt eine grenzüberschreitende Bekanntgabe von Daten trotzdem möglich, wenn andere ausreichende Garantien vorhanden sind oder wenn es einen Rechtfertigungsgrund für die Bekanntgabe gibt (Abs. 2). Im Vergleich zum Vorentwurf und zum geltenden Gesetz wurde die Liste der ausreichenden Garantien durch die Erwähnung technischer und/oder organisatorischer Massnahmen neben der vertraglichen Massnahmen genauer. In der Praxis kann es je nach Fall notwendig sein, mehrere Arten von Massnahmen miteinander zu verknüpfen.

   Diese besonderen Vorschriften gelten aber nur für Bekanntgabe von Personendaten natürlicher Personen. Der Ausschluss juristischer Personen ist nötig, damit sichergestellt wird, dass der Kanton Freiburg beim Austausch mit dem Ausland keine Nachteile gegenüber Staaten erleidet, welche die juristischen Personen vom Geltungsbereich ihres Datenschutzgesetzes ausgenommen haben.

   3.1. Im Vergleich zum Vorentwurf verzichtet der Entwurf auf die Beibehaltung einer besonderen Bestimmung über die Befugnisse der ÖDSMB im Zusammenhang mit der grenzüberschreitenden Bekanntgabe von Daten. Dieser Artikel überschnitt sich unnötigerweise mit Abschnitt 5 des Gesetzes, der den Befugnissen der Behörde gewidmet ist. Daraus ergibt sich kein inhaltlicher Unterschied. Die Pflicht, der oder dem Beauftragten über die gegebenen Garantien zu informieren, und die Möglichkeit dieses Organs, sich über die Gründe nach den Buchstaben b–e zu erkundigen, wurden beibehalten (vgl. Art. 15 Abs. 3).

   3.2. Veröffentlichungen von Personendaten im Internet oder auf anderen Plattformen, die der Information der allgemeinen Öffentlichkeit dienen, sind nicht mit einer grenzüberschreitenden Bekanntgabe gleichzusetzen (Art. 15 Abs. 4), selbst wenn diese Informationen auch im Ausland abgerufen werden können. Diese Regel ist gerechtfertigt, um die Anwendung unverhältnismässiger Vorschriften in Situationen zu vermeiden, für die dies nicht nötig ist. Nichtsdestotrotz versteht es sich von selbst, dass solche Veröffentlichungen einer Datenbearbeitung entsprechen und den allgemeinen Regelungen des DSchG entsprechen müssen.

4. Die Einschränkungen der Bekanntgabe von Personendaten, die in Artikel 16 des Entwurfs formuliert werden, bleiben gegenüber der geltenden Gesetzgebung unverändert (vgl. Art. 11 DSchG). Die Rechtmässigkeit der Bekanntgabe hängt nicht nur von der Einhaltung der generellen Prinzipien des Datenschutzes ab, sondern auch davon, dass es keine Einschränkungen im Sinne dieses Artikels gibt. Die Regelung gilt ebenso sehr für die normale Datenbekanntgabe wie für die Bekanntgabe ins Ausland.

5. In Artikel 17 des Entwurfs werden gewisse gesetzliche Bestimmungen aus anderen Gesetzgebungen, die teilweise von den gesetzlichen Bestimmungen des DSchG abweichen können, ausdrücklich vorbehalten. Beispielsweise sind die Vorschriften über die Bekanntgabe von Daten der Einwohnerkontrolle in Artikel 17 EKG für sich selbst ausreichend und erfordern nicht, dass die betroffene Person zusätzlich um ihre Zustimmung gebeten wird, wie es in Artikel 14 Abs. 3 des Entwurfs verlangt werden könnte. Natürlich können auch andere

Gesetze vom DSchG abweichen, aber die hier genannten sind zwei Beispiele, die aufgrund ihrer Bedeutung klar sind.

Art. 18–21, Auslagerung

1. Die Artikel 18–21 übernehmen fast wortgleich die gesetzlichen Grundlagen für die Auslagerung der Datenbearbeitung, die mit dem Gesetz vom 18. Dezember 2020 zur Anpassung der kantonalen Gesetzgebung an bestimmte Aspekte der Digitalisierung (ASF 2020_195) eingeführt wurden. Zur Erinnerung: Diese gesetzlichen Grundlagen wurden nach einem Pilotprojekt, das von 2018 bis 2020 durchgeführt wurde, eingeführt (ASF 2018_112). Seit ihrem Inkrafttreten am 1. März 2021 haben sie einen klaren und nützlichen Rahmen für die Nutzung der *Cloud (Cloud-Dienste*) durch die kantonalen Behörden geschaffen. Sie haben die Entwicklung harmonisierter und kohärenter Praktiken sowohl auf technischer als auch auf vertraglicher Ebene ermöglicht.

2. Derzeit verfügen nur einige Kantone über besondere Vorschriften über die Nutzung von *cloud computing* (Glarus, Luzern, Schwyz, Zürich). Auf Bundesebene und in den übrigen Kantonen wird *cloud computing* im Allgemeinen einer einfachen Auftragsbearbeitung gleichgestellt und folglich den entsprechenden Vorschriften unterstellt (s. Art. 37 des Entwurfs). Aber da diese Regeln ziemlich bescheiden sind und den Besonderheiten des *cloud computing* nicht Rechnung tragen (allgegenwärtige Lokalisierung der Daten, im Allgemeinen dauerhafte Natur der Auftragsbearbeitung, besondere vertragliche Aspekte, geteilte Kontrolle über die Daten und geteilte Verantwortung für sie, ausländische Gesetzgebung …), sind sie nicht wirklich angemessen, um die Nutzung dieser Technologie zu regeln. Ausserdem ist Rechtmässigkeit der Zuhilfenahme des *cloud computing,* die sich auf die Vorschriften im Bereich der Auftragsbearbeitung stützt, bis heute nicht einstimmig anerkannt. Eine Beschwerde zu diesem Thema, die von einer Privatperson gegen die Bundeskanzlei eingereicht wurde, ist derzeit vor dem Bundesverwaltungsgericht hängig[6]. Diese Situation schafft eine grosse rechtliche Unsicherheit, die auf den Verantwortlichen für die Bearbeitung lastet, da sie nicht wissen, ob sie riskieren, dass sie bei der Zuhilfenahme einer Cloud-Lösung haftbar werden. Aus diesem Grund hat der Staatsrat beschlossen, die Nutzung des *cloud computing* im Kanton Freiburg mit Vorschriften zu regeln, die diese Nutzung nicht nur bewilligen, sondern auch die technischen und rechtlichen Voraussetzungen festlegen. Die Auslagerung mit einer Cloud-Lösung wird also als qualifizierte Art der Auftragsbearbeitung betrachtet; sie entspricht einer Reihe von Sondervorschriften, mit denen man diese Technologie so gut wie möglich in den Griff bekommen will.

3. Artikel 18 bildet die gesetzliche Grundlage dafür, dass Gemeinwesen die Bearbeitung ihrer personenbezogenen Daten auslagern können (Abs. 1). Er legt einen geografischen Perimeter für die zugelassenen Bearbeitungsorte fest. Nur das Hoheitsgebiet der Schweiz oder eines Staates, dessen Datenschutzgesetzgebung nach Artikel 15 Abs. 1 als angemessen gilt, kommt für eine Auslagerung in Frage (Abs. 2). Der Vorbehalt von Artikel 54 KV/FR ist für den Fall vorgesehen, dass die Auslagerung der Bearbeitung einer vollständigen Übertragung einer staatlichen Aufgabe gleichkäme (z. B. wenn ein von einem externen Anbieter bereitgestellter *Cloud-Dienst* selbst einen Entscheid fällen würde, ohne dass die Verwaltung eingreift). Diese Art von Situation wird von diesem Artikel nicht abgedeckt und würde nach der Verfassung den Erlass einer speziellen gesetzlichen Grundlage erfordern (Abs. 3). Die Forderung nach einem Bericht über die Auslagerung, der alle zwei Jahre der Finanz- und Geschäftsprüfungskommission vorzulegen ist, wurde vom Grossen Rat während der parlamentarischen Debatten über das Gesetz zur Anpassung der Gesetzgebung an bestimmte Aspekte der Digitalisierung ausdrücklich gefordert (Abs. 4). Sie wurde unverändert in den Entwurf übernommen.

4. Die Vorschriften über die Verantwortung werden in Artikel 19 festgelegt.

   4.1. Das Grundprinzip ist, dass das Organ, das seine Datenbearbeitung auf die Infrastruktur eines Auftragsbearbeiters auslagert, weiterhin verantwortlich für die Aufbewahrung, Nutzung und Vertraulichkeit seiner Daten bleibt (Abs. 1). Die Bestimmung nennt eine Reihe wichtiger Punkte, die es zu beachten gilt. Insbesondere muss die Stelle, welche die Bearbeitung ihrer Daten auslagert, ihren Auftragsbearbeiter

[6] https://www.bvger.ch/bvger/de/home/medien/medienmitteilungen-2022/public-clouds.html. Letzte Überprüfung erfolgte am 15. März 2023.

sorgfältig auswählen, ihn mithilfe eines hinreichend genauen Vertrags über die auszuführenden Aufgaben unterrichten und die Einhaltung der Vertragsbestandteile überwachen.

4.2. Als Beispiel kann hier eine *Checkliste* der verschiedenen Elemente angeführt werden, die ein Auslagerungs-Vertrag je nach den Umständen enthalten sollte:

a) den Gegenstand, die Art und den Zweck der Bearbeitung;

b) die Kategorien der bearbeiteten Daten und deren Vertraulichkeitsstufe;

c) den Standort der Server, auf denen die Daten gehostet werden;

d) die Massnahmen, die ergriffen wurden, um die Sicherheit und Vertraulichkeit der Daten zu gewährleisten;

e) die Personen oder Kategorien von Personen, die Zugang zu den betreffenden Daten oder Anwendungen haben;

f) die Rechte und Kontrollmöglichkeiten;

g) das Verbot für den Auftragsbearbeiter, das Bearbeiten von Daten ohne vorherige Zustimmung der verantwortlichen Behörde weiter zu vergeben, und die Unterzeichnung eines Auslagerungs-Vertrags, der die gleichen Anforderungen stellt wie der Vertrag zwischen der verantwortlichen Behörde und dem Auftragsbearbeiter;

h) die Meldepflichten des Auftragsbearbeiters im Falle eines Datenvorfalls, -verlusts oder -diebstahls oder bei Anfragen ausländischer Behörden;

i) die Möglichkeiten, die betreffenden Daten und Anwendungen während der Laufzeit des Vertrags wiederherzustellen;

j) die Prozesse, die bei Beendigung des Vertrags einzuhalten sind, insbesondere die Rückgabe von Daten und deren Vernichtung beim Auftragsbearbeiter;

k) soweit möglich, die Anwendbarkeit des Schweizer Rechts und die Bestimmung eines Gerichtsstands in der Schweiz im Falle von Streitigkeiten.

Diese Elemente können sich jedoch im Laufe der Zeit und je nach Art der Auslagerung ändern.

4.3. Gegenüber dem geltenden Gesetz werden künftig in Artikel 19 Abs. 1 Bst. b Ziff. 4 die Rechte und die Möglichkeiten zur Kontrolle über den Auftragsbearbeiter erwähnt, ohne dass genau gesagt wird, wem diese Rechte zukommen sollen. Es handelt sich also nicht mehr nur um die Rechte der Aufsichtsbehörde, wie dies im geltenden Gesetz vorgesehen wird, sondern auch des Verantwortlichen für die Bearbeitung. Je nach Auftragsbearbeiter können verschiedene Kontrollmöglichkeiten ins Auge gefasst werden. In der Praxis stimmen nur wenige Auftragsbearbeiter einer Inspektion am Standort ihrer Infrastrukturen zu. Einerseits setzt diese Lösung sie dem Risiko einer Verletzung der Geschäftsgeheimnisse aus. Andererseits kann sie je nach Grösse des Auftragsbearbeiters wenig Aufschluss geben. Oft wird in den Cloud-Verträgen vorgesehen, dass sich der Auftragsbearbeiter regelmässig einem Audit unterzieht, das von einer Firma, die auf diese Art Audits spezialisiert ist und über eingehende Kenntnisse und Mittel verfügt, durchgeführt wird. Die Ergebnisse des Audits werden dann dem Verantwortlichen für die Bearbeitung übermittelt. Es versteht sich von selbst, dass auch die Aufsichtsbehörde Zugang zu ihnen hat.

4.4. Innerhalb der Kantonsverwaltung sorgen das fachlich zuständige Organ und das ITA gemeinsam dafür, dass die Bestimmungen bei einer Auslagerung eingehalten werden (Abs. 2). Diese Vorgehensweise ermöglicht die Entwicklung einer kohärenten und möglichst einheitlichen Praxis. Das ITA achtet darauf, dass der Auslagerungsvertrag alle notwendigen Klauseln enthält, um die Sicherheit und den Schutz der ausgelagerten Personendaten zu gewährleisten. Die Bestimmung behält jedoch den Fall von öffentlichen Organen vor, die ihre Informatik autonom verwalten, wie zum Beispiel die Universität, das Amt für

Verkehr und Schifffahrt oder das Freiburger Spital. Diese Organe sind allein für die Auslagerung ihrer Daten und IT-Werkzeuge verantwortlich.

4.5. Einige *Cloud*-Computing-*Lösungen* sind nicht auf ein einzelnes Organ eines Gemeinwesens beschränkt, sondern können sich auf mehrere oder sogar alle Organe erstrecken. Es ist dann offensichtlich, dass nicht jedes betroffene öffentliche Organ persönlich sicherstellen kann, dass der Auftragsbearbeiter seine Verpflichtungen einhält. In diesem Fall bezeichnet der Staatsrat ein hauptsächlich verantwortliches Organ (Abs. 3). Es handelt sich grundsätzlich um das Organ, das die Lösung einführt und deren Nutzung innerhalb des Staats durchsetzt. Es wird damit zum Verantwortlichen für die Lösung für die ganze Verwaltung. Es haftet allgemein dafür, dass es mit den Anforderungen des Datenschutzes übereinstimmt; es muss die Bedienungsanleitungen und in erster Linie einen Support zu seinem Betrieb für die übrigen Benutzerinnen und Benutzer beim Staat liefern und ist auch hauptsächliche Ansprechperson für den Lieferanten bei der Verwaltung. Die übrigen benutzenden Organe sind nur für die Bearbeitungshandlungen, die sie mit der Lösung selber durchführen verantwortlich. Bei einem Problem, das sie nicht selbst lösen können, müssen sie sich an das hauptsächlich verantwortliche Organ wenden, das sich wiederum wenn nötig an den Lieferanten der Lösung wenden wird. Wenn das hauptsächlich verantwortliche Amt nicht das ITA ist, gilt Artikel 19 Abs. 2 zusammen mit Artikel 19 Abs. 3 weiterhin. Die Umsetzung und die Kontrolle der Vorschriften über die Auslagerung werden gemeinsam vom hauptsächlich verantwortlichen Organ und vom ITA übernommen. Wenn das ITA das hauptsächlich verantwortliche Organ ist, wird Artikel 19 Abs. 2 logischerweise gegenstandslos. Als Beispiel für eine Lösung, für die diese Bestimmung gilt, kann man die Suite M365, die von Microsoft geliefert wird, anführen. Sie wurde vom ITA für alle Dienststellen der Verwaltung installiert. Das ITA wurde als hauptsächlich dafür verantwortliches Organ bezeichnet.

5. Die Sicherheitsmassnahmen, die bei einer Auslagerung getroffen werden müssen, werden in Artikel 20 allgemein geregelt. Das Gesetz nennt jedoch absichtlich keine spezifischen Massnahmen, da diese von Fall zu Fall im Auslagerungsvertrag vorgesehen werden müssen. Dies ist aus zwei Gründen gerechtfertigt. Zum einen entspricht nicht jede Art von Datenbearbeitung, die ausgelagert werden kann, notwendigerweise denselben Sicherheitsbedürfnissen. Andererseits muss das Gesetz technologisch neutral bleiben, um die Nutzung zusätzlicher oder zukünftiger Techniken und Technologien nicht zu behindern. Auch wenn die einzurichtenden Sicherheitsmassnahmen in der Regel mehrere unterschiedliche Ziele verfolgen, erinnert Absatz 2 an die Notwendigkeit, dem Schutz der betroffenen Personen und ihren Grundrechten einen besonderen Stellenwert einzuräumen. Um der Gefahr vorzubeugen, dass der Staat bei einer Fehlfunktion, die beim *Cloud-Anbieter* auftritt, völlig lahmgelegt wird, schreibt das Gesetz schliesslich die Einführung von Ersatzmechanismen für den Fall eines Zwischenfalls vor, wenn die betroffenen Daten für das Funktionieren des Staates unerlässlich sind (Abs. 3). Diese Mechanismen sollten dazu dienen, die Folgen eines Versagens des *Cloud-Anbieters*, das zu einem Verlust oder einer längeren Nichtverfügbarkeit von Daten führt, so weit wie möglich zu minimieren. Da solche unangenehme Folgen auch bedeutende Auswirkungen für die betroffene Person haben können, ist es gerechtfertigt, eine solche Vorschrift auch im Datenschutzgesetz einzuführen.

6. Die Auslagerung von besonders schützenswerten und geheimen Daten wird in Artikel 21 des Entwurfs behandelt.

6.1. Die vorgeschriebenen Massnahmen greifen die Empfehlungen der Konferenz der Datenschutzbeauftragten (PRIVATIM) auf. Diese sehen die Einführung zusätzlicher Sicherheitsmassnahmen vor:

> Die Daten sind zu verschlüsseln, und die Verschlüsselung hat durch das öffentliche Organ zu erfolgen. Die Schlüssel dürfen nur für das öffentliche Organ verfügbar sein. Sie sind vor Verlust, Entwendung sowie unrechtmässiger Bearbeitung und Kenntnisnahme zu schützen (Abs. 1).

> ur wenn sich daraus keine untragbaren Risiken für die Grundrechte der betroffenen Personen ergeben (was vom öffentlichen Organ nachvollziehbar darzulegen ist), kann eine Verschlüsselung beim Cloud-Anbieter geprüft werden. Hierbei muss die Ebene, auf welcher die Verschlüsselung erfolgt (Applikation, Datenbank oder Festplatte), berücksichtigt werden. Die Schlüssel können beim Cloud-Anbieter aufbewahrt werden, wenn dieser sich vertraglich verpflichtet, sie nur mit der ausdrücklichen

Zustimmung des öffentlichen Organs zu verwenden. Zugriffe sind zu protokollieren. Ausserdem muss der Cloud-Anbieter die Schlüssel vor Verlust, Entwendung sowie unrechtmässiger Bearbeitung und Kenntnisnahme schützen und sicherstellen, dass die Daten beim Verschlüsselungsvorgang nicht kompromittiert werden können (Abs. 2).

> Bei Geheimnissen sind die Anforderungen im Grossen und Ganzen dieselben. In diesem Fall muss jedoch zusätzlich darauf geachtet werden, dass der Anbieter des *Cloud-Dienstes* als Hilfsperson des Geheimnisträgers bezeichnet werden kann (Abs. 3). Diese Bezeichnung, die aus dem Strafrecht stammt, wird in Artikel 321 StGB für das Berufsgeheimnis vorgesehen und im Verlauf des Jahres in Artikel 320 StGB für das Amtsgeheimnis eingeführt[7]. Sie gilt für Berufsleute, die einer Person, die dem Geheimnis unterstellt ist, bei der Erfüllung ihrer Aufgaben helfen. Die Weitergabe von Informationen an eine Hilfsperson ist nicht strafbar. In einem Entscheid zum Anwaltsgeheimnis urteilte das Bundesgericht, dass ein Lieferant einer Cloud-Dienstleistung als Hilfsperson des Anwalts betrachtet werden kann.[8]

6.2. Die vorgesehene Bestimmung überträgt diese Anforderungen auf Gesetzesebene in eine Sprache, die technologieneutral ist.

Art. 22, Pilotprojekte

1. Die Bestimmung über Pilotprojekte wurde in einigen Punkten angepasst. Ihr Inhalt wurde zwischen dem E-GovG für allgemeine Pilotprojekte und dem DSchG für Pilotprojekte, die bestimmte heiklere Datenbearbeitungen beinhalten, aufgeteilt. Wenn diese Datenbearbeitungen im Rahmen eines Pilotprojekts stattfinden, kann ihre Bearbeitung vorübergehend auf einer Verordnung des Staatsrats anstatt auf einem vom Grossen Rat verabschiedeten Gesetz beruhen.

2. Die Grundvoraussetzungen für die Durchführung eines Pilotprojekts werden in den Artikeln 35-35b E-GovG beschrieben. Insbesondere bedarf es einer zu erfüllenden Aufgabe, eines Experimentierbedarfs, der Notwendigkeit einer Versuchsphase, der Zusammenstellung eines vollständigen Dossiers, der Verabschiedung einer zeitlich begrenzten Versuchsverordnung durch den Staatsrat und eines Berichts über die rückblickende Bewertung. Artikel 21 des Entwurfs fügt besondere Bedingungen für Pilotprojekte bei, welche die Bearbeitung besonders schützenswerter Daten oder andere Arten der Bearbeitung mit einem höheren Risiko der Verletzung von Grundrechten beinhalten. Einerseits müssen die Unterlagen des Pilotprojekts und der Evaluierungsbericht, mit dem die Pilotphase abgeschlossen wird, obligatorisch einen Teil enthalten, der sich mit Bearbeitung der Personendaten und deren Schutz befasst (Abs. 2). Bei der Zusammenstellung der Unterlagen müssen die Risiken, die das Pilotprojekt mit sich bringt, und die Massnahmen, die ergriffen werden müssen, um sie zu vermindern, identifiziert werden. Am Ende des Pilotprojekts, bei der Evaluierung muss rückwirkend untersucht werden, ob die identifizierten Risiken mit den ergriffenen Massnahmen genügend in den Griff zu bekommen waren, ob andere Risiken aufgetaucht sind, die nicht identifiziert worden waren, ob diese Risiken in den Griff zu bekommen waren, und ganz allgemein muss eine Bilanz der Restrisiken und der Vorteile, die beim Projekt festgestellt werden konnten, gezogen werden. Andererseits muss die Aufsichtsbehörde bei der Zusammenstellung der Unterlagen und der rückwirkenden Evaluierung obligatorisch angehört werden (Abs. 3). Die Behörde erhält beide Dokumente vor ihrer Überweisung an den Staatsrat und wird um Stellungnahme gebeten. Ihre Stellungnahme wird anschliessend dem Staatsrat mitgeteilt.

3. Es versteht sich von selbst, dass die Aufsichtsbehörde ausserhalb dieser beiden Phasen weiterhin jede Möglichkeit hat, während der Pilotphase einzugreifen. In der Praxis wird sogar ein einmaliger oder sogar regelmässiger Austausch innerhalb der Grenzen der Ressourcen der Behörde gefördert.

---

[7] Änderung von Artikel 320 StGB, die beim Erlass des Bundesgesetzes vom 18. Dezember 2020 über die Informartionssicherheit beim Bund (ISG) eingeführt wurde, in: AS 2020 232.

[8] BGE 145 II 229, Erw. 7.3.

Art. 23, Archivierung

Wenn die Personendaten, die von den öffentlichen Behörden bearbeitet werden, Archivwürdigkeit haben, unterstehen die der Gesetzgebung über die Archivierung. Sie dürfen weder gelöscht noch vernichtet werden (s. Kommentar zu Artikel 10). Damit die Verpflichtung, Daten, die keinem Zweck mehr dienen, zu vernichten, einen Sinn behält, sollten Mechanismen, mit denen die Archivwürdigkeit eines Dokuments innert vernünftiger Frist bestimmt werden kann, geschaffen werden.

Art. 24, Löschen und Vernichten

1. Die Personendaten, die bei einem öffentlichen Organ aufbewahrt werden, müssen gelöscht oder vernichtet werden, wenn ihre Aufbewahrung keinen Zweck mehr hat; vorbehalten bleiben die Daten welche als archivwürdig identifiziert wurden. Die aufbewahrten Personendaten müssen also periodisch überprüft werden.
2. Während der Dauer der Unterstützungsnutzung eines öffentlichen Organs – oder solange dieses unter der Kontrolle der Verwaltung steht – müssen die Personendaten, die dort gespeichert sind, gelöscht werden (Abs. 1). Im Moment des Rezyklierens oder des Ersetzens von Informatikmaterial muss die oder der Verantwortliche für die Datenbearbeitung sich versichern, dass kein Risiko für besonders schützenswerte Personendaten existiert, die gelöscht wurden, aber durch unbefugte Dritte wiedergefunden und ausgewertet werden können. Falls dies der Fall ist, muss der Datenträger – z. B. die Harddisk – physisch vernichtet werden (Abs. 2). Die Vernichtung der Medien liegt in der Verantwortung des ITA.

Art. 25, Videoüberwachung

Kein Kommentar.

2.2.3 Abschnitt 2.3. Bearbeitung von Daten für nicht personenbezogene Zwecke

Art. 26, Vorschriften

Die Lockerung der Datenschutzanforderungen bei der Bearbeitung für nicht personenbezogene Zwecke ist dadurch gerechtfertigt, dass diese Bearbeitung wesentlich weniger riskant ist, da sie eben nicht personenbezogen ist und bestimmte spezifische Anforderungen erfüllt werden. Darüber hinaus berücksichtigen diese Vorschriften das öffentliche Interesse an Forschung, Planung und Statistik.

2.3 Abschnitt 3, Rechte der betroffenen Person

Art. 27–30, Auskunftsrecht

1. Das Auskunftsrecht (Art. 27) ist und bleibt die zentrale Einrichtung des Datenschutzrechts. Ohne Auskunftsrecht wäre die betroffene Person nicht in der Lage, ihre Rechte in diesem Bereich auszuüben. Nur die- oder derjenige, die oder der Kenntnis einer Datenbearbeitung hat, die sie oder ihn betrifft, ist gegebenenfalls in der Lage, den Zweck der Bearbeitung zu überprüfen oder die Berichtigung oder Löschung unrichtiger oder nicht mit dem Zweck des Bearbeitungsvorgangs zusammenhängender Daten zu verlangen. Schuldner des Auskunftsrechts ist immer die oder der Verantwortliche für die Bearbeitung im Sinne von Artikel 4 Abs. 1 Bst. h. Die Tatsache, dass diese oder dieser die Bearbeitung einer oder einem Dritten überträgt, ändert daran nichts (Abs. 3).
2. Das Auskunftsrecht ist die konkreteste Ausprägung des Grundrechts auf Datenschutz. Es ist im Besitz jeder Person, die Gegenstand einer Datenbearbeitung ist, und ist nicht von einem bestimmten Interesse abhängig. Dies bedeutet, dass keinerlei Einschränkungen aufgrund von Nationalität, Wohnort oder Alter oder auch verbunden mit der Persönlichkeit der Antragstellerin oder des Antragsstellers oder der Nutzung, die sie oder er mit ihren oder seinen Daten vorhat, gegeben sind. Die Antragstellerin oder der Antragsteller muss den Antrag im Weiteren auch nicht begründen. Die einzige Pflicht, die ihr oder ihm obliegt, ist die Angabe ihrer oder seiner Identität, damit ihr oder ihm effektiv die eigenen Daten zugestellt werden (Art. 28 Abs. 1). Zur Erinnerung: Es gibt eine besondere Vorschrift über das Auskunftsrecht in Artikel 60 Abs. 3 GesG. Für die Anträge auf Auskunft bei Gesundheitsfachpersonen kann die oder der Verantwortliche für die Bearbeitung (im Grunde genommen die behandelnde Ärztin oder der behandelnde Arzt) der betroffenen Person vorschlagen, dass sie ihre Daten in Anwesenheit einer Expertin oder eines Experten ihrer oder seiner Wahl einsehen könne. Es handelt sich hierbei jedoch nur um einen Vorschlag, den die betroffene Person akzeptieren oder ablehnen kann.

3. Das Auskunftsrecht ist nicht als absolut zu verstehen. Artikel 29 des Entwurfs zeigt die Bedingungen auf, gemäss denen es eingeschränkt werden kann. Die Berufung auf einen Grund für die Einschränkung des Auskunftsrechts muss jedoch die Ausnahme bleiben. Sie kann nur sehr eingeschränkt nach einer Interessenabwägung und in Übereinstimmung mit dem Verhältnismässigkeitsprinzip stattfinden. Im Vergleich zum Vorentwurf sieht der Entwurf zwei zusätzliche Gründe für Einschränkungen vor. Der erste, das Gesetz, wird insofern als Hinweis erwähnt, als ein Gesetz allgemein stets von einem anderen Gesetz abweichen kann. Der zweite, die Berufung auf die Missbräuchlichkeit des Gesuchs ist eine Angleichung an das Bundesrecht und das Recht der anderen Kantone. Er entspricht einer Konkretisierung des Rechtsmissbrauchs. In der Praxis wird er jedoch nur restriktiv geltend gemacht werden können, wenn der Missbrauch offensichtlich ist.
4. Artikel 30 gehört nicht direkt zum Auskunftsrecht der betroffenen Person, sondern legt verschiedene Grundsätze für die Einsichtnahme in einige ihrer Daten nach dem Tod fest. Auch wenn man über ihre Platzierung streiten kann, kann sie dennoch aus didaktischen und auch systematischen Gründen gerechtfertigt sein. In jedem Fall ist das wesentliche Element, das aus dieser Bestimmung hervorgeht, die Interessenabwägung, die bei der Entscheidung über die Weitergabe von Daten der Verstorbenen oder des Verstorbenen an Dritte vorgenommen werden muss.

Art. 31, Einsprache gegen die Bekanntgabe von Personendaten

1. Das Recht auf Einsprache (oder Recht auf Sperrung) ermöglicht es der betroffenen Person, sich im Voraus der Bekanntgabe gewisser sie betreffender Daten zu widersetzen. Es ist Teil der Forderungen, die das Datenschutzrecht den betroffenen Personen allgemein, unabhängig von der Art der betroffenen Daten, zuerkennt (s. Art. 20 DSG und 37 n-DSG; siehe auch Art. 21 DSGVO; Art. 9 § 1 Bst. d Übereinkommen SEV 108+).
2. Nach geltendem Recht ist das Recht auf Sperrung nur für Daten aus dem Einwohnerregister in Artikel 18 EKG vorgesehen. Im Jahr 2003 fällte die damalige Eidgenössische Datenschutzkommission ein Urteil, das den Kanton Freiburg betraf und in dem sie feststellte, dass die Beschränkung des Rechts auf Einsprache nur auf bestimmte Datenkategorien gegen das Datenschutzrecht verstösst (Urteil der damaligen Eidgenössischen Datenschutzkommission vom 22. Mai 2003, in VPB 68.69). Der Entwurf sieht folglich die Einführung eines erweiterten Rechts auf Einsprache vor, das unabhängig von den fraglichen Datenarten gegeben ist.
3. Das Recht auf Einsprache gilt weder generell noch absolut. Erstens darf es sich nur auf Daten, die zuvor von der betroffenen Person festgelegt wurden, beziehen (Abs. 1 *in fine*). Es gibt also kein generelles Recht auf Sperrung aller Daten einer Person. Zweitens kann die Sperrung von Daten unter den Bedingungen nach Absatz 2 Bst. a–c aufgehoben werden. Das ist jedes Mal der Fall, wenn die Bekanntgabe ausdrücklich gesetzlich vorgesehen ist (Bst. a), wenn die Erfüllung der Aufgaben des öffentlichen Organs ohne Bekanntgabe der Daten gefährdet ist (Bst. b) oder wenn sie dazu führen würde, dass eine Drittperson ihre legitimen Interessen nicht verteidigen kann, obwohl keine rechtlichen Hindernisse für die Bekanntgabe existieren (Bst. c). In letzterem Fall muss die Behörde, an die ein Gesuch um Bekanntgabe gerichtet wurde, einen Entscheid treffen: Entweder verweigert sie der Person, welche das Gesuch gestellt hat, die Bekanntgabe oder sie hebt das Recht der betroffenen Person auf Einsprache auf. Da diese Wahl notwendigerweise rechtliche Folgen für beide Parteien hat, muss die Behörde einen Entscheid, der mit Beschwerde angefochten werden kann, erlassen (Abs. 3).
4. Absatz 4 behält die Regeln über die Informationspflicht der Behörden und den Zugang zu amtlichen Dokumenten im InfoG vor. Standardmässig kann das Recht auf Sperrung im Sinne des DSchG allein keinen Grund für eine Einschränkung angesichts der Anforderungen der Transparenz der Verwaltung darstellen. Im Falle einer aktiven Bekanntgabe der Behörden oder eines Gesuchs um Zugang zu einem amtlichen Dokument, das Personendaten enthält, für welche die betroffene Person ihr Recht auf Sperrung geltend gemacht hat, muss das Zugangsgesuch gemäss den Vorschriften der Artikel 11 und 26 ff. InfoG bearbeitet werden.

Art. 32 Datenübertragbarkeit

1. Das Recht auf Datenübertragbarkeit war absichtlich nicht Teil des Vorentwurfs, da es als verfrüht und wenig geeignet für die Bearbeitung von Daten im öffentlichen Bereich angesehen wurde. Dennoch wurde es in den Entwurf aufgenommen, um über eine umfassende Datenschutzgesetzgebung zu verfügen und um möglichen neuen Entwicklungen vorzugreifen.
2. So wie es formuliert ist, ist das Recht auf Datenübertragbarkeit jedoch nicht direkt justiziabel, sondern bedarf der Konkretisierung in der Spezialgesetzgebung oder muss vom Verantwortlichen für die Bearbeitung freiwillig angeboten werden. Der Grund dafür ist, dass nicht alle Datenbanken auf Anfrage eine automatisierte Extraktion eines Teils ihres Inhalts ermöglichen. Um ein solches Ergebnis zu erzielen, bedarf es einer Reihe von technischen Voraussetzungen. Die Daten müssen strukturiert und in geeigneten Formaten gespeichert sein. Diese Voraussetzungen sind jedoch nicht für alle Datenbanken gegeben. Aus diesem Grund beschränkt sich Artikel 32 darauf, einen Rahmen für das Recht auf Datenübertragbarkeit festzulegen.

Art. 33, Abwehrklagen

1. Absatz 1 nennt die drei traditionellen Abwehrmittel gegen eine unrechtmässige Datenbearbeitung. Es handelt sich um die gleichen Mittel, die im Zivilrecht im Bereich des Persönlichkeitsschutzes vorgesehen sind.
2. Der Ausdruck «wer ein schutzwürdiges Interesse hat» am Anfang des Satzes übernimmt den Ausdruck von Artikel 41 des neuen DSG. Er bezieht sich nicht nur auf die Person, die von der tatsächlichen Bearbeitung ihrer Daten direkt betroffen ist. Neben dem letztgenannten Anspruch können darüber hinaus auch bestimmte Vereine und Verbände berechtigt sein, sich auf einen Anspruch nach Art. 30 Abs. 1 zu berufen, wenn sie zur Wahrung ihrer eigenen Interessen oder der Interessen ihrer Mitglieder handeln («egoistische Verbandsbeschwerde»; französisch «recours égoïste»). Bei der Frage, ob eine Person über ein schutzwürdiges Interesse verfügt, das es ihr ermöglicht, sich einer Datenbearbeitung zu widersetzen, kann auf die Rechtsprechung des Bundesgerichts zurückgegriffen werden (insb. BGE 147 I 280, Erw. 6.2).
3. In Absatz 2 werden verschiedene datenschutzrechtliche Mittel vorgesehen, die im Einzelfall in Anspruch genommen werden können, um einen Verstoss durch rechtswidrige Datenbearbeitung zu beheben. Die Person kann im Einzelnen verlangen, dass unnütze oder unrichtige Daten gelöscht oder berichtigt werden müssen; sie kann auch die Hinzufügung eines Vermerks des strittigen Charakters gewisser Daten verlangen, wenn weder ihre Richtigkeit noch ihre Unrichtigkeit festgestellt werden kann. Weiter können die Bekanntgabe an Dritte oder die Veröffentlichung der Löschung, der Berichtigung der Personendaten oder der Hinzufügung der Erwähnung ihres strittigen Charakters verlangt werden. Neu gegenüber dem geltenden Recht ist die Einführung eines neuen Rechts auf Einschränkung der Bearbeitung. Die Einschränkung der Bearbeitung ist weniger radikal als die Berichtigung oder das Löschen von Daten und ermöglicht es, die mit bestimmten Daten verbundenen Bearbeitungsmöglichkeiten vorübergehend einzufrieren, in der Regel bis zur Klärung entweder der Richtigkeit oder der Rechtmässigkeit der angefochtenen Bearbeitung. Während der Massnahme kann – bzw. muss – der Verantwortliche für die Bearbeitung die betreffenden Daten weiterhin unverändert aufbewahren, darf sie aber nicht mehr für neue Zwecke bearbeiten.
4. In Absatz 3 wird auf den Grundsatz der Integrität der Archivbestände und der öffentlich zugänglichen Bestände, auch wenn sie Personendaten enthalten, hingewiesen. Diese Bestände und ihr Inhalt dürfen weder vernichtet noch berichtigt werden. In gewissen Situationen kann der Zugang zu ihnen beschränkt werden, und/oder es kann eine Notiz, in der die betroffene Person Daten über sie ablehnt oder ergänzt, angefügt werden.

Art. 34, Verfahren und Rechtsmittel

Seit der Revision des DSchG im Jahr 2008 müssen alle Entscheide, die von öffentlichen Organen in Anwendung dieses Abschnitts getroffen werden, systematisch an die Aufsichtsbehörde weitergeleitet werden. Dies ermöglicht es ihr, die Einhaltung der Gesetze zu überprüfen und gegebenenfalls Beschwerde zu erheben. Dieses System kann jedoch zu einem Eingriff in die Grundrechte der betroffenen Personen führen, wenn diese eine solche Mitteilung nicht wünschen. Aus diesem Grund führt der Entwurf im Vergleich zum geltenden Gesetz die Möglichkeit ein, dass die Betroffenen die Mitteilung von Entscheiden, die sie betreffen, ablehnen können.

Art. 35, Schadenersatz und Genugtuung

Die Verletzung der Bestimmungen des Gesetzes über den Datenschutz kann im Sinne von Artikel 6 Abs. 1 HGG eine rechtswidrige Handlung darstellen. Sie kann unter den im Gesetz festgelegten Bedingungen zu einer Entschädigung führen.

2.4 Abschnitt 4, Durchführung des Datenschutzes

Art. 36 und 37, Verantwortung

1. In Artikel 36 wird der Grundsatz festgelegt, dass das öffentliche Organ, das personenbezogene Daten bearbeitet, für den Schutz und die Sicherheit dieser Daten verantwortlich ist (Abs. 1). Diese Vorschrift und ihre Folgen werden wird an anderen Stellen des DSchG, wie in anderen Erlassarten näher erläutert.
2. Die Verantwortung für eine Datenbearbeitung kann jedoch auf verschiedene Akteure aufgeteilt werden (Abs. 2), die dann gemeinsam verantwortlich sind. Unter solchen Umständen ist es wichtig, dass die Aufteilung der Verantwortung zwischen den beteiligten Akteuren ausreichend definiert ist (z. B.: Umfang, Datenkategorien, Arten der Bearbeitung *usw.*). Dies kann entweder mit der Erklärung nach Artikel 38 geschehen oder sich aus einer oder mehreren gesetzlichen Bestimmungen ergeben. In jedem Fall hat die interne Verteilung der Zuständigkeiten keinen Einfluss auf die Situation der betroffenen Personen, die weiterhin berechtigt sind, alle ihre Rechte und Ansprüche gegenüber dem Staat geltend zu machen.
3. In Artikel 37 werden die Haftungsfragen geregelt, wenn eine öffentliche Einrichtung einen Auftragsbearbeiter beauftragt. Im Vergleich zum Vorentwurf hat die Bestimmung eine Anpassung an das Bundesrecht erfahren. Die in der Schweiz üblichen Bedingungen für diesen Bereich sind darin enthalten. In Absatz 5 wurde eine Präzisierung hinzugefügt. Sie besagt, dass es, sofern nichts anderes bestimmt ist, keine Auftragsbearbeitungen zwischen mehreren Organen, die derselben Körperschaft angehören, geben darf. In diesem Fall wird die Anwendung der Vorschriften über die gemeinsame Verantwortung vorgezogen. Dies hat keine Auswirkungen auf die betroffenen Personen, da die Verantwortung ohnehin beim Staat bleibt. Dadurch wird jedoch vermieden, dass komplizierte und wenig hilfreiche Rechtskonstrukte ausgearbeitet werden müssen.
4. Da die Auslagerung von Daten im Entwurf eine qualifizierte Form der Auftragsbearbeitung darstellt, gelangen in diesem Fall die zusätzlichen Regelungen der Artikel 18–21 zur Anwendung. Die Grundregeln nach Artikel 37 gelten, aber so lange, als sie den besonderen Regeln über die Auslagerung nicht widersprechen.

Art. 38-39, Bearbeitungsregister und Anmeldung der Bearbeitungen

1. Die Anmeldung der Bearbeitungen und das Bearbeitungsregister sind die beiden Governance-Instrumente im Bereich des Datenschutzes, mit denen die Transparenz und die Kontrolle bei der Datenbearbeitung der öffentlichen Organe sichergestellt werden. Selbst wenn Entwicklungen wahrscheinlich sind, muss man von der Idee ausgehen, dass diese Funktion weiterhin vom Register der Datensammlungen, das von der ÖDSMB geführt wird, wahrgenommen wird.
2. Der Ersatz des Ausdrucks «Datensammlung» durch «Bearbeitungstätigkeit» entspricht einer terminologischen Anpassung und dürfte nicht zu grösseren praktischen Änderungen führen. Insbesondere ist nicht davon die Rede, dass jede Bearbeitung einzeln gemeldet werden muss. Der Audruck Datensammlung wird als überholt betrachtet, denn die Daten, die es für die Erfüllung einer Aufgabe braucht, werden heute nicht mehr notwendigerweise in einem abgegrenzten Raum gespeichert, sondern können an verschiedenen Orten gelagert werden, obwohl sie derselben Tätigkeit dienen. Deswegen haben der eidgenössische Gesetzgeber, das Übereinkommen SEV 108 und die neuen kantonalen Gesetze den Ausdruck «Datensammlung» durch «Bearbeitungstätigkeit» ersetzt. Das soll aber nicht heissen, dass die beiden Ausdrücke zu 100 % deckungsgleich sind und dass die genau dieselbe Realität abbilden. Obwohl es deswegen nicht mehr Anmeldungen geben dürfte, die Anmeldung der Bearbeitungen macht es nötig, dass künftig nicht an den Ort der Aufbewahrung, sondern an die zu erfüllende Tätigkeit gedacht werden muss (im Allgemeinen, diejenige, die im Gesetz vorgesehen wird). Es kann also gewisse Unterschiede geben.

3. In Artikel 38 wird die Liste der Informationen erwähnt, welche die oder der Verantwortliche für die Bearbeitung zum Zeitpunkt liefern muss, wenn sie oder er mit der Bearbeitung beginnt. In Artikel 39 wird eine gewisse Anzahl von Ausnahmen von der Meldepflicht festgelegt. Diese Bestimmungen stimmen weitgehend mit denjenigen des geltenden DSchG überein.
4. Das Bearbeitungsregister wird von der ÖDSMB geführt.[9] Es ist öffentlich und kann kostenlos eingesehen werden. Im Entwurf wird jedoch darauf verzichtet, festzulegen, dass es online veröffentlicht werden muss, da dies bereits der aktuellen Praxis entspricht und man sich nicht vorstellen kann, dass es anders sein könnte. Auch wird darauf verzichtet, klarzustellen, dass die Gemeinden neben der Meldung an die ÖDSMB auch eine Liste ihrer Bearbeitungen führen müssen.
5. Im Vorentwurf war vorgesehen, dass eine Datenbearbeitung zwingend bei der Aufsichtsbehörde angemeldet werden muss, bevor sie beginnen kann (vgl. Art. 38 Abs. 1 VE-DSchG). Diese Verpflichtung wurde aufgegeben, da sie in der Praxis nicht durchführbar ist. Sie hätte auch eine völlig einzigartige Massnahme in der Schweiz dargestellt.

Art. 40, Organisatorische und technische Massnahmen

1. Artikel 40, in dem auf die einzurichtenden organisatorischen und technischen Massnahmen eingegangen wird, wurde im Entwurf mit Artikel 42 des Vorentwurfs zusammengefasst, in dem der Grundsatz des Datenschutzes durch Technikgestaltung (*Privacy by design*) und der Grundsatz des Datenschutzes durch Voreinstellungen (*Privacy by default*) eingeführt werden. Letztere widmen sich einem proaktiven Ansatz zum Schutz der Privatsphäre während des gesamten Datenbearbeitungsprozesses.
2. Die Verantwortlichen für die Bearbeitung müssen während des gesamten Lebenszyklus der Daten die organisatorischen und technischen Massnahmen ergreifen, die ihrer Situation, den von ihnen durchgeführten Verarbeitungen und der Art der von ihnen bearbeiteten Daten angemessen sind. Dabei sind verschiedene Kriterien zu berücksichtigen. Dazu gehören nicht nur die Vertraulichkeit, sondern auch die Verfügbarkeit, Authentizität, Integrität, Nachvollziehbarkeit und Dauerhaftigkeit. Genauere Angaben dazu werden sich in der Gesetzgebung über die Informationssicherheit, die derzeit vorbereitet und auf die insbesondere in Absatz 2 verwiesen wird, finden.
3. In Übereinstimmung mit dem risikobasierten Ansatz werden im Gesetz keine spezifischen Massnahmen vorgelegt, die implementiert werden müssen, sondern das Prinzip der «Accountability», das man in den meisten modernen Gesetzen zum Datenschutz wiederfindet (Art. 4 § 4 der Richtlinie (EU) 2016/680; Art. 5 § 2 DSGVO und Art. 10 § 1 des Übereinkommens SEV 108+), wird übernommen. Dieser neue Grundsatz, der schwer ins Deutsche zu übersetzen ist, bedeutet für die Verantwortlichen zwei Dinge:
    a) Wirksame, geeignete und den Umständen angemessene Massnahmen umsetzen, um den Schutz und die Sicherheit der von ihnen bearbeiteten personenbezogenen Daten zu gewährleisten. Neben der Einführung technischer Lösungen kann es sich dabei auch um Sensibilisierungs- und Schulungsmassnahmen, Massnahmen zum Schutz der Räumlichkeiten oder Mechanismen zur Begrenzung der Folgen eines Verlusts oder Diebstahls von festen oder mobilen Geräten handeln.
    b) In der Lage sein, das Vorhandensein und die Umsetzung dieser Massnahmen anhand einer geeigneten Dokumentation nachzuweisen (vgl. Abs. 4). Das Ausmass der Dokumentationspflicht hängt von den Umständen ab. Es kann im Detail die folgenden Formen annehmen: einfache, regelmässig aktualisierte Liste von Massnahmen, Charta, Politik, ISDS-Konzept, Nutzungsreglement usw.

Art. 41 und 42, Datenschutz-Folgenabschätzung

1. Die Datenschutz-Folgenabschätzung ist ein wichtiges Instrument, um das Verantwortungsbewusstsein der Urheber der Bearbeitung zu wecken: Sie unterstützt sie nicht nur dabei, Datenbearbeitungen, die das Privatleben respektieren, zu erstellen, sondern auch dabei, aufzuzeigen, dass sie gemäss dem Gesetz über den Datenschutz

[9] Das Register der Datensammlungen (frz. ReFi) ist online wie folgt verfügbar: https://www.fr.ch/de/oedsb/institutionen-und-politische-rechte/transparenz-und-datenschutz/register-der-datensammlungen.

handeln. Die Folgenabschätzung muss vom Verantwortlichen für die Bearbeitung vor der Umsetzung der Datenbearbeitung durchgeführt werden. Schliesslich muss sie regelmässig evaluiert werden, damit sichergestellt ist, dass sie im Rahmen des Bearbeitungszyklus aktuell bleibt.

2. Nach dem Vorbild der Vorschriften im europäischen Recht (Art. 27 § 1 Richtlinie (EU) 2016/680 und Art. 35 § 1 Verordnung (EU), Übereinkommen SEV 108+ [Art. 10 § 2]) und im Entwurf zur Totalrevision des DSG (Art. 22) ist die Folgenabschätzung für die Bearbeitung von Daten obligatorisch, die voraussichtlich zu einem erhöhten Risiko für die Rechte und Freiheiten der betroffenen Person führen (Art. 41 Abs. 1). Das Risiko muss von Fall zu Fall auf Schwere und Wahrscheinlichkeit geprüft werden. Das Gesetz liefert eine beispielhafte Liste von Fällen, für die eine solche Abschätzung obligatorisch ist (Abs. 2). Der Mindestinhalt einer Folgenabschätzung wird in Artikel 41 Abs. 3 beschrieben. Sie soll ohne übertriebene Formalismen und unter Beachtung der Verhältnismässigkeit durchgeführt werden.

3. Wenn die Folgenabschätzung ergibt, dass die geplante Verarbeitung ein hohes Risiko für die Rechte der betroffenen Personen darstellt und daher besondere Schutzmassnahmen erforderlich sind, muss der Verantwortliche die Aufsichtsbehörde anhören, bevor er mit der Bearbeitung beginnen darf (Art. 42 Abs. 1). Die Aufsichtsbehörde kann ihm ihre möglichen Einwände und Empfehlungen zu der geplanten Bearbeitung mitteilen (Abs. 2). Gemäss dem Entwurf hat die Behörde zwei Monate Zeit, um ihre Stellungnahme abzugeben; diese Frist kann um einen Monat verlängert werden. Ohne Rückmeldung von der Behörde kann der Verantwortliche für die Bearbeitung davon ausgehen, dass die Behörde auf eine Stellungnahme verzichtet und sie oder er daher mit der Bearbeitung beginnen kann. Dies hindert die Behörde jedoch nicht daran, zu einem späteren Zeitpunkt einzugreifen.

4. Die oder der Verantwortliche für die Bearbeitung ist frei, die Empfehlungen der Aufsichtsbehörde in die Praxis umzusetzen, sie oder er muss sie aber in jedem Fall spätestens zum Zeitpunkt der Aufnahme der Bearbeitung über die getroffenen Massnahmen informieren (Abs. 3). Wenn die oder der Verantwortliche für die Bearbeitung beschliesst, den Empfehlungen der Behörde nicht zu folgen, und die Behörde der Ansicht ist, dass die Bearbeitung nicht den Anforderungen des Datenschutzes entspricht, dann kann sie von allen ihr gemäss Artikel 56 ff. zur Verfügung stehenden Befugnissen Gebrauch machen. Die gleichen Regeln gelten auch auf Bundesebene.

Art. 43 und 44, Verletzungen der Datensicherheit

1. Die zu ergreifenden Massnahmen bei einem Zwischenfall, der eine Verletzung der Vertraulichkeit, der Verfügbarkeit oder der Integrität der Daten zur Folge hat, decken drei Bereiche ab: a) Identifizierung der Verletzung und Korrektur (Art. 43 Abs. 1); *b)* Aufzeichnung der Verletzung in einem schriftlichen Dokument (Art. 43 Abs. 2) und c) wenn nötig Meldung der Verletzung an die oder den Datenschutzbeauftragten oder an die betroffene Person (Art. 43 Abs. 3 und Art. 44).

2. Im Gesetz wird nicht verlangt, dass jeder Zwischenfall im Bereich des Datenschutzes systematisch der oder dem Datenschutzbeauftragten gemeldet werden muss. Dies gilt nur für die Zwischenfälle, mit denen ein erhöhtes Risiko für die Rechte der betroffenen Personen verbunden ist. Damit ein hohes Risiko erkannt wird, muss wahrscheinlich ein Schaden, z. B. Diebstahl, Identitätsdiebstahl oder auch Diskriminierung, eintreten. Es ist hingegen nicht notwendig, dass eine Mindestzahl von Personen betroffen ist.[10] Im Gesetz wird darauf verzichtet, die Frist festzulegen, innerhalb derer die Mitteilung erfolgen muss. Diese sollte jedoch so kurz wie möglich gehalten werden. Sie sollte grundsätzlich nicht länger als 72 Stunden dauern (Vgl.: Art. 30 § 1 Richtlinie (EU) 2016/680; Art. 33 § 1 DSGVO).

3. Wenn dies aus Gründen der Transparenz erforderlich ist und/oder um den betroffenen Personen die Möglichkeit zu geben, nützliche Massnahmen zur Wahrung ihrer Interessen zu ergreifen (z. B. Änderung des Passworts, Sperrung eines Zugangs oder Kontaktaufnahme mit der Behörde), müssen die betroffenen Personen persönlich über die Verletzung benachrichtigt werden (Art. 44 Abs. 1). Im Falle von Untätigkeit des Verantwortlichen für

[10] MÉTILLE / MEYER, *Annonce des violations de la sécurité des données: une nouvelle obligation de la nLPD*, in: SZW 2021 23, S. 26.

die Bearbeitung kann das Bekanntmachen von der oder vom Datenschutzbeauftragten verordnet werden (Art. 44 Abs. 4). Ausnahmsweise kann aber die Pflicht zur Meldung an die betroffenen Personen aufgeschoben oder eingeschränkt werden. Es ist auch möglich, unter den üblichen Bedingungen darauf zu verzichten (Abs. 2). Die Ausnahmegründe gelten hingegen nie für die Meldung an die Datenschutzbeauftragte oder den Datenschutzbeauftragten, wenn die Voraussetzungen für eine Meldung erfüllt sind. Für Fälle von Verstössen, die eine grosse Anzahl von Personen betreffen, ist im Entwurf die Möglichkeit einer öffentlichen Bekanntmachung in der Regel in einem Medium vorgesehen (Abs. 3). In einem solchen Fall wird dafür gesorgt, dass die betroffenen Personen die Möglichkeit haben, über eine Webseite präzisere und persönlichere Informationen zu erhalten oder es wird eine geeignete Kontaktmöglichkeit zur Verfügung gestellt.

4. Gemäss Art. 43 Abs. 4 muss jede Verletzung der Datensicherheit, die bei einem Auftragsbearbeiter auftritt, der oder dem Verantwortlichen für die Bearbeitung gemeldet werden (Ausnahmen können jedoch Bagatellfälle sein, die offensichtlich kein Risiko für die betroffene Person oder die betroffenen Personen darstellen). Wenn die für die Datenbearbeitung verantwortliche Person über eine solche Verletzung benachrichtigt wird, entscheidet sie oder er gemäss den oben genannten Regeln, ob die Verletzung der oder dem Datenschutzbeauftragten und den betroffenen Personen gemeldet werden soll.

Art. 45 Ansprechperson für Datenschutz

1. Die Pflicht, eine Ansprechperson für den Datenschutz zu ernennen, entspringt der Absicht, das Verständnis und die Anwendung des Datenschutzrechts innerhalb der kantonalen Verwaltung angesichts seines transversalen und ubiquitären Charakters zu professionalisieren.
2. Ein typisches Profil ist nicht festgelegt, zunächst scheinen Grundkenntnisse der Datenschutzgesetzgebung und ein gewisses Interesse für Fragen der Informatik unabdinglich zu sein. So kann diese Funktion von Juristen, Wirtschaftswissenschaftlern, Personen aus dem IT-Bereich oder anderen Führungskräften aus der Verwaltung besetzt werden. Aufgrund der Neuartigkeit dieses Profils wird es zu Beginn vor allem darauf ankommen, dass die benannten Personen bereit sind, sich in diesem Bereich aus- und weiterzubilden und Interesse an der Materie haben. Im Gegenzug wird es Aufgabe der Verwaltung sein, diesen Personen die Möglichkeit zu geben, sich weiterzubilden.
3. Im Gegensatz zum Vorentwurf wird im Entwurf nicht mehr vorgeschrieben, dass die Ämter Ansprechpersonen benennen müssen, sondern diese Verpflichtung auf die Ebene der Direktionen verlagert. Der Staatsrat kann jedoch weitere kantonale Organe verpflichten, eine solche Rolle bei einem Amt zu bezeichnen, wenn ein besonderer Bedarf besteht (Abs. 5). Ziel ist es, ein Kompetenzzentrum an vorderster Front aufzubauen, das in der Lage ist, die wichtigsten Datenschutzfragen innerhalb der Verwaltung zu lösen. Die bezeichneten Personen werden in einem Netzwerk zusammengeführt, in dem sie Schulungen erhalten und Wissen und Erfahrungen im Zusammenhang mit dem Datenschutz austauschen können (Abs. 4). Wenn nötig, können sie auch bei der oder dem Beauftragten um Unterstützung und Rat nachsuchen.
4. Die Ansprechpersonen übernehmen in erster Linie eine beratende und unterstützende Funktion. Sie sind keine Aufsichtsbehörde, sondern werden hauptsächlich auf Antrag der Verantwortlichen für die Bearbeitung selbst tätig oder wenn ein Fall dies erfordert (z. B., wenn sie von einer Verletzung erfahren). Doch auch wenn es gesetzlich nicht vorgeschrieben ist, hindert sie nichts daran, proaktiv zu handeln. Sie sind jedoch nie persönlich anstelle der Verantwortlichen für die Bearbeitung für die Einhaltung der Vorschriften verantwortlich. Bei all ihren Einsätzen ist ihre Rolle lediglich beratender Natur.
5. Die den Ansprechpersonen zuerkannte Autonomie (Abs. 3) ist eine notwendige Voraussetzung für die Ausübung ihrer Funktion. Um ihre Rolle effektiv erfüllen zu können, müssen diese Personen in der Lage sein, ohne hierarchische Einschränkungen oder Angst vor Nachteilen klar Stellung zu den Bearbeitungen zu beziehen, bei denen sie einschreiten.

2.5 Abschnitt 5, Aufsicht

2.5.1 Abschnitt 5.1: Aufsichtsbehörde für Datenschutz

Art. 46, Aufsichtsbehörde

Die Bezeichnung einer Aufsichtsbehörde ist eine zwingende Bedingung für ein System der Kontrolle des Datenschutzes in einer demokratischen Gesellschaft. Auf kantonaler Ebene ist diese Funktion der kantonalen Behörde für Öffentlichkeit, Datenschutz und Mediation (ÖDSMB; Aufsichtsbehörde) zugeordnet. Im Vergleich zum geltenden Gesetz wird im Entwurf darauf verzichtet, die Möglichkeit vorzusehen, dass Gemeinden ihre eigene Aufsichtsbehörde bilden können. Abgesehen davon, dass diese Möglichkeit derzeit von keiner Gemeinde genutzt wird, hat sich in der Praxis gezeigt, dass sie zahlreiche Schwierigkeiten mit sich bringt. Diese Änderung stiess bei den Gemeinden auf keinerlei Widerstand.

Art. 47, Organisation

1. Der Entwurf ändert die aktuelle Struktur der Aufsichtsbehörde teilweise. Wie heute besteht die Aufsichtsbehörde aus einer von Grossen Rat gewählten Kommission, welche den Personen, die mit der Öffentlichkeit, dem Datenschutz und der Mediation beauftragt sind, übergeordnet ist. Dieses System ermöglicht es, die Legitimität einer vom Grossen Rat gewählten Kommission mit der Professionalität und der Verfügbarkeit von Fachleuten aus den jeweiligen Bereichen zu verbinden. Es wird nicht geändert.
2. Im Vergleich mit der jetzigen Situation wird im Entwurf beantragt, die Trennung zwischen Öffentlichkeitsbeauftragter oder Öffentlichkeitsbeauftragtem und Datenschutzbeauftragter oder Datenschutzbeauftragtem aufzugeben und anstatt dessen die Stelle einer oder eines Öffentlichkeits- und Datenschutzbeauftragten zu schaffen. Von einer Lösung mit zwei Beauftragten geht man über zu einer Lösung mit nur noch einer oder einem Beauftragten, die oder der in den Bereichen der Öffentlichkeit und des Datenschutzes tätig ist. Mit der Wahl, die beiden Funktionen zu trennen, sollte ursprünglich jedem Bereich die gleiche Bedeutung zugemessen werden, obwohl sie bisweilen gegensätzlichen Interessen entsprechen. Im Grossen und Ganzen hat dieses System immer gut funktioniert, und der Staatsrat hatte nicht geplant, es zu ändern. Nach dem Weggang der ehemaligen Datenschutzbeauftragten kündigte die ÖDSMB aber an, dass sie eine neue Arbeitsweise mit einer Person, die gleichzeitig die Funktion der oder des Öffentlichkeitsbeauftragten und der oder des Datenschutzbeauftragten ausüben sollte, testen wolle, namentlich um die Effizienz der Arbeitsweise der Behörde zu erhöhen. Die derzeitige Öffentlichkeitsbeauftragte wurde dazu zur Datenschutzbeauftragten *ad interim* ernannt. Nach einer dreimonatigen Versuchsphase, erklärte die ÖDSMB, dass sie mit dieser Änderung zufrieden ist, und hat darum ersucht, sie im Rahmen der Revision des jetzigen Gesetzes dauerhaft zu verankern. Zu diesem Zweck wurden mehrere Bestimmungen des DSchG und des InfoG geändert.

Art. 48, Status

1. Die Aufsichtsbehörde geniesst innerhalb der Verwaltung einen Sonderstatus. Die Garantie der Unabhängigkeit, die ihr zuerkannt wird (Abs. 1), ist eine grundlegende Anforderung, die bereits im geltenden Gesetz (Art. 29 Abs. 3 DSG) enthalten ist und die sich generell in den schweizerischen und europäischen Datenschutzvorschriften wiederfindet (vgl. Art. 26 Abs. 3 DSG und Art. 43 Abs. des neuen DSG, Art. 42 der Richtlinie (EU) 2016/680; Art. 52 der DSGVO; Art. 15 § 5 der Übereinkommen SEV 108+). Sie setzt angemessene organisatorische Garantien für die Stellung der Aufsichtsbehörde innerhalb der Verwaltung, die Ressourcen, über die sie verfügt, und die Bezeichnung und die rechtliche Stellung der oder des Beauftragten voraus.
2. Um ihre Unabhängigkeit zu gewährleisten, ist die Aufsichtsbehörde keiner Direktion direkt unterstellt, sondern nur administrativ einer von ihnen zugeordnet (Abs. 2). Sie darf daher bei der Ausübung ihres Amtes keine Anweisungen entgegennehmen. Diese Stellung bedeutet jedoch nicht, dass die Behörde «ausserhalb des Staates» stünde, wie eine Privatperson oder eine private Organisation, und dass sie sich vollständig selbst verwalten könnte. Die Aufsichtsbehörde erfüllt ihre Aufgaben in den Räumlichkeiten und mit den Mitteln, die der Staat ihr

zur Verfügung stellt. Wie jede Verwaltungseinheit unterliegt sie den Vorschriften über die Nutzung dieser Räumlichkeiten und Mittel.

3. Der der Behörde jedes Jahr zugewiesene Haushaltsrahmen verleiht ihr eine sehr grosse Autonomie bei der Ausführung und Verwaltung des Haushalts. Sie ermöglicht es der Behörde, frei über die Verwendung der erhaltenen Mittel zu entscheiden, sofern diese mit der Erfüllung ihrer Aufgaben und/oder ihrem Betrieb in Zusammenhang stehen. Gemäss den allgemeinen Vorschriften, die für die Verwaltungseinheiten gelten, kann die Behörde Material erwerben, das sie für nützlich hält, sich für Schulungen anmelden, Sensibilisierungskampagnen zu Fragen des Datenschutzes, der Transparenz oder der Mediation finanzieren oder Stellungnahmen oder Gutachten von Fachleuten in Auftrag geben. Innerhalb des erhaltenen Finanzrahmens muss sie keine vorherige Genehmigung einholen, um eine Ausgabe zu tätigen. Die Behörde kann an der Aufstellung ihres eigenen Voranschlags mitwirken und dem Staatsrat einen Voranschlagsantrag unterbreiten. Dieser Antrag wird dann von der Person, welche die Direktion, der die Behörde administrativ zugewiesen ist, leitet, vorgelegt, die ihren Standpunkt bei der Präsentation vor dem Staatsrat geltend machen kann (vgl. Art. 61 Abs. 1 Bst. a SVOG).

Art. 49 und 50, Kantonale Öffentlichkeits-, Datenschutz- und Mediationskommission

1. Die Zusammensetzung und Organisation der kantonalen Öffentlichkeits-, Datenschutz- und Mediationskommission wird in Artikel 49 geregelt. Sie ist ein multidisziplinäres Organ, das mehrere Berufsbilder und so viele Fähigkeiten, wie sie für ein möglichst breites Verständnis der mit den Tätigkeitsbereichen der Aufsichtsbehörde zusammenhängenden Herausforderungen erforderlich sind, vereint. Die Mitglieder der Kommission werden auf Vorschlag des Staatsrats vom Grossen Rat gewählt (Abs. 1). Diese Lösung, die sich seit dem Inkrafttreten des geltenden Gesetzes bewährt hat, stellt einerseits die Unabhängigkeit der Aufsichtsbehörde gegenüber der kantonalen Exekutive und der Verwaltung, die von ihr abhängt, sicher und sorgt andererseits dafür, dass die Mitglieder vor allem aufgrund der erforderlichen Kompetenzen gewählt werden. Gegenüber der jetzigen Situation wird die Zusammensetzung der Kommission leicht geändert, um darin auch juristische, Informatik- und Datensicherheitskompetenz einzubinden (Abs. 2). Diese Zusammensetzung entspricht der derzeit bestehenden, auch wenn das Gesetz es nicht ausdrücklich vorsieht.

2. Die Befugnisse der Kommission werden in Artikel 50 geregelt. Dabei handelt es sich um die Leitungsfunktionen der Behörde, die einer stärkeren Legitimation bedürfen. Ausserdem legt die Kommission über den Staatsrat dem Grossen Rat jedes Jahr den Tätigkeitsbericht der Behörde vor. Die Möglichkeit der Aufsichtsbehörde, die Öffentlichkeit über ihre Feststellungen zu informieren, wenn das allgemeine Interesse dieses rechtfertigt, ist eine Folge ihrer Unabhängigkeit.

3. Im Entwurf ist vorgesehen, dass das Verfahren zur Ernennung der oder des Beauftragten von der Kommission in Zusammenarbeit mit der Direktion, der die Behörde zugewiesen ist, durchgeführt wird. Es ist aber Aufgabe der Kommission, eine Stellungnahme zuhanden des Staatsrats abzugeben. Diese Art der Ernennung entspricht den Anforderungen des übergeordneten Rechts, die den Mitgliedstaaten in dieser Hinsicht einen relativ grossen Ermessensspielraum belassen. Nach europäischem Recht ist es vor allem wichtig, dass das Verfahren zur Ernennung der Mitglieder der Behörde transparent ist. Dieses kann jedoch sowohl vom Parlament als auch von der Regierung, dem Staatsoberhaupt oder einer unabhängigen Stelle durchgeführt werden (vgl. Erg. zu Art. 43 Richtlinie EU/2016/680; 53 DSGVO). In der Schweiz folgt die Ernennung des oder der Beauftragten mehreren unterschiedlichen Schemata. In einigen Kantonen wird sie oder er vom Parlament auf der Grundlage eines Antrags des Staatsrats (z. B.: BE; BL; GE; GL; LU; SO), einer Kommission (AI; BS) oder direkt (VS; ZH) ernannt. In anderen Kantonen ernennt die Regierung die Beauftragte oder den Beauftragten (AG; AR; GR; NE und JU; SG; SH; TI; UR; VD, ZG).

4. Aufgrund der Zusammensetzung der Behörde, die sowohl eine Fachkommission als auch eine Beauftragte oder einen Beauftragten umfasst, unterscheidet sich die Situation in Freiburg von derjenigen in anderen Kantonen. Da die Kommission bereits vom Grossen Rat ernannt wird, erscheint es nicht schlüssig, auch die Ernennung der oder des Beauftragten, die oder der das operative Organ der Behörde ist, der Zuständigkeit des Grossen Rates zu unterstellen. In diesem Fall ist eine Ernennung durch den Staatsrat durchaus angemessen. Zum einen entspricht

diese Lösung dem europäischen Recht. Zum anderen ist dies auch die Lösung, die in fast der Hälfte der Kantone in der Schweiz zur Anwendung gelangt.

5. Letztlich bietet die vorgeschlagene Regelung viele Vorteile. Sie bietet der Kommission die volle Legitimität einer Wahl durch den Grossen Rat und garantiert der oder dem Beauftragten, dass eine unabhängige Behörde in den Auswahlprozess eingreift. Diese innerhalb der Verwaltung völlig einzigartige Regelung unterstreicht den Sonderstatus der Behörde und ihrer Mitglieder. Sie geht weit über die im europäischen Recht vorgesehene Mindestregelung hinaus. Auch im interkantonalen Vergleich gewährt sie mindestens gleich viel, wenn nicht mehr Schutz als die meisten bestehenden Regelungen.

Art. 51–54, Beauftragte/r

1. Die oder der Beauftragte ist das operative Organ der Behörde im Bereich des Datenschutzes. Damit sie oder er ihre oder seine Aufgaben effizient erfüllen kann, hat sie oder er aufgrund des Gesetzes einen besonderen Status.

2. Gemäss Artikel 51 wird die oder der Beauftragte vom Staatsrat für einen Zeitraum von fünf Jahren ernannt, der erneuert werden kann. Die Wahl einer befristeten Anstellung lehnt sich an das Bundesrecht (vgl. Art. 44 des neuen DSG) und das EU-Recht (vgl. Art. 44 Abs. 1 Bst. e der EU-Richtlinie 2016/680; Art. 54 Abs. 1 Bst. e DSGVO) an. Sie findet sich scheinbar bis heute auch bei allen Kantonen, die ihr eigenes Gesetz bereits überarbeitet haben. Sie ist das Gegenstück zur Sonderregelung, welche die Beauftragte oder den Beauftragten während der Amtszeit schützt. In Artikel 52 wird vorgesehen, dass das Arbeitsverhältnis der oder des Beauftragten während dieser Zeit nur bei grobem Fehlerverhalten oder grober Fahrlässigkeit oder bei längerer Arbeitsunfähigkeit gekündigt werden kann (Abs. 3). Der Entscheid, die Beauftragte oder den Beauftragten des Amts zu entheben, wird vom Staatsrat auf eigene Initiative oder auf Initiative der Kommission getroffen. In beiden Fällen verlangt der Staatsrat die Stellungnahme der Kommission (Abs. 4). Dieser in der Verwaltung einzigartige Status soll es der oder dem Beauftragten ermöglichen, ihre oder seine Aufgaben effizient und unabhängig zu erfüllen. Am Ende der Anstellungsperiode, d. h. alle fünf Jahre, wird das Arbeitsverhältnis der oder des Datenschutzbeauftragten grundsätzlich stillschweigend erneuert (Art. 52 Abs. 1). Der Staatsrat kann jedoch per Entscheid beschliessen, das Arbeitsverhältnis nicht zu erneuern. In diesem Fall muss er aber die Stellungnahme der Kommission einholen. Der Entscheid, dass das Arbeitsverhältnis nicht erneuert wird, muss der oder dem Beauftragten sechs Monate vor Ablauf der Amtsperiode zukommen. Dieser Entscheid muss dann mindestens sechs Monate vor Ende der Amtszeit bei der oder dem Beauftragten eintreffen. Er muss ausreichend begründet sein und kann angefochten werden. In Artikel 53 werden die Regeln festgelegt, die im Falle einer Verhinderung der oder des Beauftragten zu befolgen sind. Soweit im Entwurf oder in der dazugehörigen Ausführungsverordnung nichts Gegenteiliges vorgesehen wird, gilt die Gesetzgebung über das Staatspersonal für das Arbeitsverhältnis der oder des Beauftragten (Art. 51 Abs. 4).

3. Die Liste der Aufgaben der oder des Datenschutzbeauftragten ist in Artikel 54 aufgeführt. Die Erweiterung dieser Liste im Vergleich zum aktuellen Gesetz ist zum Teil auf die neuen Aufgaben im Bereich des Datenschutzes zurückzuführen, zum Teil aber auch auf den Wunsch, die Aufgaben zwischen der Kommission und der oder dem Beauftragten für den Datenschutz besser zu verteilen.

Art. 55, Selbstkontrolle der Aufsichtsbehörde

Mit dieser Bestimmung wird die Aufsichtsbehörde verpflichtet, mit geeigneten Kontrollmassnahmen sicherzustellen, dass bei ihrer Tätigkeit die Organisation und die Sicherheit von Personendaten sowie die Einhaltung und die richtige Anwendung der Bestimmungen im Bereich des Datenschutzes gegeben sind.

2.5.2 Abschnitt 5.2: Kontroll- und Eingriffsbefugnis der Aufsichtsbehörde

Art. 56-59, Kontrolle durch die Beauftragte oder den Beauftragten

1. Gemäss den Anforderungen des übergeordneten Rechts verstärkt der Entwurf die Eingriffsmöglichkeiten der Aufsichtsbehörde und passt sie den neuen Standards der Datenschutzgesetzgebung an.

2. Die Eingriffsmöglichkeiten der Aufsichtsbehörde können in zwei Kategorien aufgeteilt werden: diejenigen, die direkt der oder dem Beauftragten zur Verfügung stehen und diejenigen, für welche die Kommission zuständig ist:

   2.1. Die oder der Beauftragte ist die zuständige Stelle, um eine Untersuchung bei einem Verantwortlichen für die Bearbeitung oder gegenüber einer externen Auftragsbearbeiterin oder einem externen Auftragsbearbeiter durchzuführen, um zu prüfen, ob sie oder er die Bestimmungen zum Datenschutz einhält (Art. 56 Abs. 1). Sie oder er kann von Amtes wegen oder aufgrund einer Anzeige einer oder eines Dritten einschreiten. Im Rahmen der Untersuchungen verfügt die oder der Datenschutzbeauftragte über einen unbeschränkten Zugang zu allen erforderlichen Informationen zur Erfüllung ihrer oder seiner Aufgaben; sie oder er kann insbesondere die Herausgabe von Akten verlangen oder Anhörungen durchführen oder eine Inspektion vor Ort vornehmen (Abs. 2). Geheimhaltungspflichten können ihr oder ihm nicht entgegengehalten werden (Abs. 3); das Berufsgeheimnis bleibt vorbehalten. Betroffene Personen, die der Behörde eine problematische Situation melden, haben im Verfahren keine Parteistellung. Sie werden jedoch über die Folgen, die ihrer Anzeige gegeben werden, und in geeigneter Form über das Ergebnis einer etwaigen Untersuchung informiert. In besonders schweren oder hartnäckigen Fällen hat die oder der Beauftragte die Möglichkeit, eine Empfehlung auszusprechen, in der sie oder er den Verantwortlichen für die Bearbeitung auffordert, innerhalb einer bestimmten Frist für die Einhaltung der Vorschriften zu sorgen (Art. 57). Die Empfehlung muss hinreichend präzise sein, damit der Verantwortliche für die Bearbeitung versteht, was ihm vorgeworfen wird und welche Art von Massnahmen ergriffen werden müssen, um Abhilfe zu schaffen. Innerhalb der gesetzten Frist legt die Empfängerin oder der Empfänger eine Bestimmung darüber vor, welche Folge sie oder er der Empfehlung geben will. Wird die Empfehlung ganz oder teilweise abgelehnt, so kann die oder der Beauftragte die Kommission anrufen.

   2.2. Als ein vom Grossen Rat gewähltes Kollegialorgan ist die kantonale Öffentlichkeits-, Datenschutz- und Mediationskommission das zuständige Organ, um verbindliche Entscheide gegenüber den Verantwortlichen für die Bearbeitung zu treffen (Art. 58). Die Kommission kann nur tätig werden, um einen Entscheid zu fällen, wenn sie von der oder dem Datenschutzbeauftragten nach einer erfolglosen Empfehlung angerufen wird; Fälle einer schweren und unmittelbaren Bedrohung (Abs. 3) bleiben vorbehalten. Die Kommission kann verschiedene Massnahmen anordnen, diese reichen von der Aussetzung, der Änderung bis zur Einstellung der Bearbeitung oder bis zur Vernichtung der bereits gesammelten Daten. In ihren Entscheiden beachtet die Kommission das Prinzip der Verhältnismässigkeit. Die oder der Datenschutzbeauftragte wirkt mit beratender Stimme am Verfahren vor der Kommission mit. Sie oder er kann mit der Untersuchung des Falles beauftragt werden (Abs. 4). Die Tatsache, dass die oder der Beauftragte bereits eine Empfehlung in derselben Sache abgegeben hat, stellt keinen Befangenheitsgrund dar, der sie oder ihn daran hindert, den Fall für die Kommission zu untersuchen. Zu beachten ist, dass das Aussprechen einer Empfehlung oder eines Entscheids nie Selbstzweck ist. Wenn der Verantwortliche für die Bearbeitung das Problem im Rahmen des Verfahrens vor der oder dem Beauftragten oder vor der Kommission behebt, können beide den Fall abschreiben und auf einen Entscheid verzichten (Art. 57 Abs. 5 und 58 Abs. 5). Die Kommission hat auch die Möglichkeit, sich mit einer Verwarnung zu begnügen.

3. Artikel 59 erinnert daran, dass sowohl die oder der Beauftragte als auch die Kommission bei ihren Interventionen die Regelungen des VRG einzuhalten haben. Neben dem ausdrücklich erwähnten Anspruch des betroffenen Organs auf rechtliches Gehör umfasst dies die Einhaltung der Grundsätze der Gesetzmässigkeit, der Gleichbehandlung, der Verhältnismässigkeit, des guten Glaubens und des Willkürverbots, das Recht auf einen ausreichend begründeten Entscheid oder die Vertretungsregeln.

Art. 60, Zusammenarbeit mit anderen Datenschutzbehörden

Die Bestimmung legt die Regeln fest, die zu befolgen sind, wenn die Aufsichtsbehörde mit anderen Datenschutzbehörden zusammenarbeitet und in diesem Rahmen Personendaten oder allenfalls Daten, die einem Geheimnis unterliegen, austauschen muss (Amtshilfe). Sie betrifft jedoch nicht die verschiedenen Formen der

informellen Zusammenarbeit, die sich nicht auf einzelne Fälle beziehen (Organisation von Veranstaltungen, Weiterbildungen, Seminare *usw.*).

2.6 Abschnitt 6, Übergangsbestimmungen

Art. 61, Ausführungsreglement

Die Bestimmung sieht eine Kompetenzdelegation zugunsten des Staatsrats vor, damit dieser den Entwurf in verschiedenen Aspekten ergänzt, wenn dafür Bedarf besteht.

Art. 62, Übergangsrecht

1. Der Übergang zum neuen Recht, namentlich die Verschärfung der Anforderungen an die Sicherheit bei den Verantwortlichen für die Bearbeitung kann kaum ohne eine gewisse Anpassungszeit erfolgen. Es ist auch nicht möglich, die Gesamtheit der neuen Anforderungen ausnahmslos auf alle Bearbeitungen anzuwenden, insbesondere, wenn diese zu einem Zeitpunkt angefangen haben, zu dem noch die alten Anforderungen galten. Das ist der Grund dafür, dass im Entwurf gewisse Ausnahmebewilligungen und Fristen vorgesehen werden, damit die Verantwortlichen für die Bearbeitung ihre Arbeit an die neuen Bestimmungen anpassen können.
2. Es ist eine allgemeine Frist von zwei Jahren vorgesehen, um den Verantwortlichen für die Bearbeitung die Möglichkeit zu geben, die neuen Anforderungen des DSchG zu erfüllen; die Meldungen von Verletzungen der Datensicherheit müssen der Aufsichtsbehörde oder den betroffenen Personen bereits ab Inkrafttreten des neuen Gesetzes gemacht werden (Abs. 1).
3. Sofern der Zweck der Bearbeitung unverändert bleibt und keine neue Datenerhebungen, die eine solche Abschätzung rechtfertigen könnten, stattfinden, gelten die Verpflichtungen zur Durchführung einer Datenschutz-Folgenabschätzung nicht für Bearbeitungen, die unter dem alten Recht begonnen wurden und nach dem Inkrafttreten des neuen Rechts fortbestehen (Abs. 2). Die Durchführung einer Folgenabschätzung stellt eine grosse Arbeitsbelastung dar. Von der Verwaltung zu verlangen, eine solche Verpflichtung nachzuholen, wenn die betreffenden Bearbeitungen unter anderen Vorschriften begonnen haben, wäre unfair und unverhältnismässig.
4. Eine Sonderregelung ist für Bearbeitungen vorgesehen, die unter dem alten Recht begonnen haben und zum Zeitpunkt des Inkrafttretens des neuen Gesetzes beendet sind (Abs. 3). Sie werden weiterhin den Anforderungen des DSchG von 1994 unterliegen. Sofern es technisch machbar ist, dürfen sich die betroffenen Personen hingegen ab dem Inkrafttreten des Gesetzes auf die neuen Rechte in Abschnitt 3 des Gesetzes berufen (erweitertes Auskunftsrecht, Widerspruchsrecht).
5. Um gemäss der Richtlinie (EU) 2016/680, die für die Schweiz ab dem 1. August 2018 verbindlich ist (s. BBI 2017 6565, S. 6783), zu handeln, müssen die Verantwortlichen für die Bearbeitung, für welche die Richtlinie gilt, alles daransetzen, sicherzustellen, dass sie mit dem Inkrafttreten des neuen Gesetzes der Pflicht, die betroffene Person über die Erhebung ihrer Daten zu informieren, und den Verpflichtungen im Zusammenhang mit der Umsetzung des Gesetzes gemäss Abschnitt 4 des Entwurfs nachkommen (Abs. 4).

Art. 63, Anpassung der Gesetzgebung

Artikel 5 des Entwurfs ändert teilweise die Anforderungen an die Art und Weise, wie gesetzliche Grundlagen zum Datenschutz zu verfassen sind. Artikel 63 räumt den Direktionen eine Frist von zwei Jahren ab Inkrafttreten des neuen Gesetzes ein, um allfällige Anpassungen in ihrem Gesetzesportfolio vorzunehmen. Ursprünglich war eine Frist von einem Jahr vorgesehen. Die Rückmeldungen bei der Vernehmlassung haben aber gezeigt, dass diese Frist nicht lange genug war, namentlich angesichts der Langsamkeit des Gesetzgebungsverfahrens.

Art. 64, Dienstverhältnis der oder des Beauftragten

Da die Funktionen der oder des Öffentlichkeitsbeauftragten und der oder des Datenschutzbeauftragten zusammengelegt werden (s. Kommentar zu Art. 47) und zu einer befristeten Anstellung (s. Kommentar zu Art. 51) übergegangen wird, muss das Dienstverhältnis der oder des Beauftragten angepasst werden. Auch wenn der Wechsel von einem unbefristeten Vertrag zu einem befristeten Vertrag für die amtierende Person auf den ersten Blick ungünstiger scheint, gibt es für sie tatsächlich keine Verschlechterung. Die oder der Beauftragte kommt in den Genuss eines erhöhten Schutzes während der Dauer des Dienstverhältnisses (fünf Jahre) und fällt alle fünf Jahre in

ein Verhältnis zurück, das ungefähr dem für alle Staatsangestellten geltenden entspricht, aber mehr Schutz bietet. Der Entscheid, den Auftrag der oder des Beauftragten nicht zu erneuern, muss sich auf triftige Gründe stützen und der oder dem Beauftragten sechs Monate vor Ablauf seines Auftrags zukommen; ausserdem braucht es dazu unbedingt die Stellungnahme der Kommission (s. Art. 52 Abs. 1). Zudem wird der Staatsrat dafür sorgen, dass im Ausführungsreglement eine Bestimmung aufgenommen wird, in der das Gehalt der oder des Beauftragten bei Krankheit und Unfall während des Dienstverhältnisses während sichergestellt wird; das Gehalt wird in der Schutzfrist von 730 Tagen gemäss Gesetzgebung über das Staatspersonals weitergezahlt (s. Art. 110 Abs. 4 StPG).

2.7 Änderung anderer Gesetze

2.7.1 Anpassung des StatG

Die Änderungen an den Artikeln 5 Abs. 1 und 16 Abs. 2 und 3 haben im Wesentlichen zum Ziel, auf die neue Version des Gesetzes über den Datenschutz, das vom Grossen Rat verabschiedet wird, zu verweisen. Im Entwurf wird aber beantragt, dass ein Schreibfehler, der sich in Artikel 16 Abs. 3 eingeschlichen hat, korrigiert werden soll. Nicht der Zugang zu den Daten, sondern deren Veröffentlichung ist verboten, wenn sie eine Identifikation oder einen Rückschluss auf die persönliche Situation einzelner Personen erlauben. Dass es sich um einen Schreibfehler handelt, geht sehr klar aus der Botschaft des Staatsrats vom 25. Oktober 2005, die den Entwurf des Gesetzes über die kantonale Statistik begleitete, hervor[11].

2.7.2 Anpassung des SVOG

Auf Ersuchen der ÖDSMB und nach dem Vorbild des Bundes (vgl. Art. 57h und 57hbis RVOG) wird im Entwurf vorgeschlagen, im SVOG einen neuen Artikel 58a einzuführen, der es den Verwaltungsorganen ermöglicht, ein Geschäftsverwaltungssystem zu führen, das Personendaten, einschliesslich besonders schützenswerter Daten, enthalten kann. Diese Bestimmung soll nicht die verschiedenen Regeln ersetzen, die für die Datenverarbeitung in der Spezialgesetzgebung gefordert werden, sondern eine Rechtsgrundlage für die Aufzeichnung und Speicherung von Daten bieten, die auf der elektronischen Infrastruktur der Verwaltung erhoben werden.

2.7.3 Anpassung des JG

Art. 46a und 71a

1. Im Entwurf wird die Einführung einer Ansprechperson für Datenschutz beim Kantonsgericht (Art. 46a) und bei der Staatsanwaltschaft (71a) vorgesehen.
2. Diese zwei Einheiten fallen unter die Richtlinie (EU) 2016/680 über den Datenschutz im Bereich der Polizei und der Justiz. Diese Richtlinien stellt für die Schweiz eine Entwicklung des Schengen-Besitzstands dar (s. § 1.3.2.2). Gemäss Artikel 32 der Richtlinie muss eine Ansprechperson für Datenschutz bezeichnet werden. Die zu bezeichnende Person muss genügende Kenntnisse der Gesetzgebung über den Datenschutz und eine Stellung, die sicherstellt, dass ihre Stellungnahmen beachtet werden, haben. Wie in Artikel 45 DSchG muss die Ansprechperson für Datenschutz in der Lage sein, ihr Amt selbständig auszuüben. Sie ist jedoch nicht befugt, sich in eine laufende richterliche Angelegenheit einzumischen. Das Amt der Ansprechperson für Datenschutz kann mit einem anderen Amt im Dienst der betreffenden Einheiten kumuliert werden.

Art. 140

Die Änderung von Artikel 140 Abs. 1 Bst. B nimmt eine Anpassung der neuen Gesetzgebung über Informationssicherheit vorweg. Die Änderung von Artikel 140 Abs. 1 Bst. c stellt eine kosmetische Änderung des Gesetzes dar. Sie hätte im Prinzip zum Zeitpunkt des Erlasses des ArchG eingeführt werden müssen.

2.7.4 Anpassung des GG

Artikel 102a übernimmt Artikel 58a SVOG für die Gemeinden.

---

[11] TGR 2006 S. 13.

2.7.5 Anpassung des VRG

Art. 66a

Ohne den Ermessensspielraum der Behörde zu ersetzen, können die Algorithmen manchmal als Entscheidhilfe in einem Verfahren dienen. Aus Gründen der Transparenz und Loyalität wird in Artikel 66a vorgesehen, dass der Einsatz dieser Art von Werkzeugen systematisch im getroffenen Entscheid erwähnt werden muss und es dem Adressaten des Entscheids ermöglicht wird, angemessene Informationen über deren Funktionsweise zu erhalten.

Art. A-4a

1. Im Vergleich zum Vorentwurf wurde die Bestimmung über automatisierte Einzelentscheide vom DSchG ins VRG verschoben. Der Grund dafür ist, dass es sich hierbei in erster Linie um eine Verfahrensregel handelt. Der Kanton ist jedoch nur für das Verwaltungsverfahren zuständig. Zivil- und Strafverfahren fallen dagegen in die ausschliessliche Zuständigkeit des Bundes, der diese Materie umfassend in der Zivilprozessordnung vom 19. Dezember 2008 (ZPO; SR 272) und der Strafprozessordnung vom 5. Oktober 2007 (StPO; SR 312.0) geregelt hat. Eine kantonale Verfahrensregel – selbst wenn sie im DSchG steht – kann sich daher nicht auf diese beiden Verfahrensarten auswirken. Da das Kantonsgericht zum jetzigen Zeitpunkt die Verwendung von automatisierten Einzelentscheiden in Gerichtsverfahren ausschliesst und keine Nützlichkeit einer solchen Vorschrift, die für es gilt, sieht[12], wurde die Bestimmung in Anhang I über das elektronische Verfahren platziert, da dieser Anhang nur für Verwaltungsbehörden der ersten Instanz gilt.
2. Die Besonderheit automatisierter Einzelentscheide besteht darin, dass sie ausschliesslich auf der Grundlage einer automatisierten Datenverarbeitung getroffen werden. Es gibt also keinen Menschen, der an der Entscheidfindung teilnimmt. Die Bereiche, die sich für diese Art von Entscheiden eignen, sind jedoch bis heute noch sehr begrenzt, da nur sehr kurze und rudimentäre Subsumtionsoperationen von einer Maschine durchgeführt werden können. Trotz allem besteht ein gewisses Potenzial im Bereich der Massenverwaltung, wenn regelmässig Tausende relativ ähnliche Entscheide auf der Grundlage einfacher Rechenoperationen getroffen werden. Zum Beispiel können Ordnungsbussen für Geschwindigkeitsüberschreitungen eines Tages sicher vollautomatisch ausgestellt werden. Schliesslich ist auch denkbar, dass bestimmte wenig komplexe Genehmigungen in Zukunft auf diese Weise erteilt werden können.
3. Da die Algorithmen, die diesen Entscheiden zugrunde liegen, nicht unfehlbar sind und sich irren können, ist es wichtig, dieses Risiko durch geeignete Verfahrensgarantien auszugleichen. Ein Einzelentscheid, der ausschliesslich auf der Grundlage einer automatisierten Datenbearbeitung getroffen wird, muss zwingend durch einen ausdrücklichen Hinweis als solcher dargestellt werden (Abs. 1). Auf Anfrage des Adressaten des Entscheids muss die Verwaltung ihm ausserdem die Logik und die Kriterien der Bearbeitung, die zum Entscheid führte, mitteilen. Diese Garantie ist erforderlich, um es der betroffenen Person zu ermöglichen, die Richtigkeit des Entscheids zu bewerten, bevor er gegebenenfalls angefochten wird. Eine schnelle und kostenlose aussergerichtliche Überprüfung von Bearbeitungsvorgängen im Zusammenhang mit einem automatisierten Entscheid kann beantragt werden, wenn klar ersichtlich ist, dass der Entscheid mit einem offensichtlichen, nicht rechtlichen Mangel behaftet ist, der vollständig der Maschine zuzuschreiben ist. Aus verfahrensrechtlicher Sicht gelten für den Antrag auf Überprüfung die gleichen Regeln wie bei einer Einsprache nach Art. 103 VRG. Eine Überprüfung kann jedoch nicht beantragt werden, wenn die Behörde nicht verpflichtet ist, eine Partei vor ihrem Entscheid anzuhören. Die Vorschrift verweist auf Artikel 58 VRG.

2.7.6 Anpassung des VidG

Die Installation eines flächendeckenden Überwachungssystems, das grosse Teile des öffentlichen Grunds abdeckt, stellt einen schweren Eingriff in die Rechte und Freiheiten der betroffenen Personen dar. Das ist der Grund dafür, dass, nebst anderen Bedingungen, in jedem Fall eine Datenschutz-Folgenabschätzung gemäss den Artikeln 41 und 42 des DSchG-Entwurfs erforderlich ist (Art. 4 Abs. 3 und 5 Abs. 1 Bst. c). Das Gesetz definiert nicht, ab wann ein Überwachungssystem grosse Teile des öffentlichen Bereichs erfasst. Die Regelung wird jedoch aus Artikel 22 Abs. 2

[12] Vgl. Stellungnahme des Kantonsgerichts vom 17. Mai 2022 als Antwort auf eine Frage.

Bst. *b* des neuen DSG übernommen, so dass zur Beantwortung dieser Frage die Kommentare und die Rechtsprechung zu dieser Bestimmung herangezogen werden können.

2.7.7 Anpassung des InfoG

Art. 33 und 39

Die Änderungen an Artikel 33 Abs. 1 und 2 und 39 sind eine Folge der Zusammenlegung der Funktionen der oder des Öffentlichkeitsbeauftragte und der oder des Datenschutzbeauftragten.

Art. 40

Die Änderung von Absatz 1 Bst. b ist eine Folge der Zusammenlegung der Funktionen der oder des Öffentlichkeitsbeauftragten und der oder des Datenschutzbeauftragten. Dies ist auch bei der Streichung von Absatz 1 Bst. b^{bis} der Fall, da die Frage der Ernennung und des Status des oder der Beauftragten bereits im DSchG geregelt ist.

Art. 41

Absatz 1 wird aufgehoben, denn die Frage der Anstellung der oder des Datenschutz- und Öffentlichkeitsbeauftragten wird im DSchG geregelt. Absatz 2 wird in der Folge angepasst.

Art. 42a

S. Kommentar zu Artikel 64 DSchG.

2.7.8 Anpassung des MedG

Art. 5, 6 Abs. 2 Bst. b, 8 und 9

Immer mit dem Ziel, die rechtliche Regelung für die drei Mitglieder der ÖDSMB zu vereinheitlichen, werden die Artikel 5 und 6 Abs. 2 Bst. b geändert und die Artikel 8 und 9 gestrichen, da sich ihr Inhalt bereits in der Regelung für die Öffentlichkeits- und Datenschutzbeauftragte oder den Öffentlichkeits- und Datenschutzbeauftragten wiederfindet.

Art. 27

S. Kommentar zu Artikel 64 DSchG.

2.7.9 Anpassung des E-GovG

Art. 30

Siehe Kommentar zu Artikel 19 Abs. 2 und 3 DSchG.

Art. 35-35b

1. Der Übergang zum E-Government ist ein komplexer Prozess, der manchmal Lernphasen erfordert, bevor man sich endgültig für die gewünschte Lösung entscheidet[13]. Diese Lernphasen können es erforderlich machen, vorübergehend von einer bestehenden Regelung abzuweichen, bevor gegebenenfalls ihre Aufhebung oder endgültige Änderung vorgeschlagen wird. Nach dem geltenden Recht erlaubt ein Pilotprojekt lediglich eine Ausnahme von der Verpflichtung, sich auf eine gesetzliche Grundlage im formellen Sinne zu stützen, um besonders schützenswerte Personendaten zu bearbeiten. Mit der vorgeschlagenen Änderung wird es künftig möglich sein, vorübergehend von anderen Arten von Normen abzuweichen, wenn diese Verweise auf einen analogen Gegenstand oder ein analoges Verfahren enthalten, die ein Hindernis für die Digitalisierung darstellen könnten.
2. Die Durchführung eines Pilotprojekts unterliegt strengen inhaltlichen und formalen Bedingungen, die auf die Artikel 35-35b aufgeteilt werden. Inhaltlich muss ein Pilotprojekt notwendigerweise der Erfüllung öffentlicher Aufgaben dienen oder ein ausgewiesenes öffentliches Interesse verfolgen, die Sicherheit von Personen muss durch geeignete Massnahmen gewährleistet werden, und es muss ein anerkannter Experimentierbedarf bestehen, der die Durchführung eines Pilotprojekts vor der Verabschiedung der endgültigen gesetzlichen Grundlagen

[13] MONTAVON Michael, *De la planification à la codification de la cyberadministration*, in: SJZ/RSJ 16-17/2022 803-812.

rechtfertigt. Formal muss ein Pilotprojekt einem klar festgelegten Protokoll folgen, das aus mehreren Schritten besteht. Es sollte grundsätzlich nicht länger als fünf Jahre dauern und erfordert zwingend die vorherige Erstellung eines umfassenden Dossiers, einen Evaluierungsbericht am Ende der Pilotphase und die Beteiligung verschiedener Akteure in den verschiedenen Phasen des Projektverlaufs. Vor allem aber muss ein Pilotprojekt mit einer (experimentellen) Verordnung vorgesehen werden, deren Dauer und Anwendungsbereich begrenzt sind, um eine ausreichende Publizität und Betreuung des Projekts zu gewährleisten. Erst nach Abschluss des Pilotprojekts wird dem Grossen Rat allenfalls schliesslich ein Gesetzesentwurf vorgelegt. Der Vorteil dieses Verfahrens ist, dass es die Sicherheit und Genauigkeit des Gesetzes erhöht, da die vorgeschlagenen Normen empirisch und nicht nur auf der Grundlage von Annahmen entwickelt werden konnten. Deren Qualität wird dadurch gesteigert.

3. Artikel 35 Abs. 3 enthält einen ausdrücklichen Verweis auf Artikel 22 DSchG, der sich mit Pilotprojekten befasst, welche die Bearbeitung besonders schützenswerter Personendaten, die Durchführung von Profiling-Aktivitäten oder andere Arten der Bearbeitung, die ein hohes Risiko für die Rechte der betroffenen Personen darstellen können, beinhalten (Abs. 6). Es geht also darum, diese beiden Bestimmungen zu koordinieren. Für diese Projektkategorie gelten die allgemeinen Regelungen des E-GovG, die für alle Pilotprojekte gelten, und die zusätzlichen Regelungen des DSchG, die für Pilotprojekte gelten, die sich mit besonderen Datenbearbeitungen befassen. Konkret beziehen sich diese zusätzlichen Regelungen auf die Einbeziehung der ÖDSMB in die verschiedenen Phasen des Projekts.
4. Die Verwaltung greift bei der Erfüllung bestimmter Aufgaben manchmal auf Dritte zurück. Dies kann auch im Bereich des E-Government der Fall sein, wo öffentlich-private Partnerschaften geeignete Lösungen darstellen können. Gemäss Artikel 54 der KV muss jedoch jede Übertragung öffentlicher Aufgaben an Dritte in einem Gesetz vorgesehen werden. Sollte die Durchführung eines Pilotprojekts die Inanspruchnahme von Dritten erfordern, so würde Artikel 35b Abs. 2 während der gesamten Dauer des Pilotprojekts, aber nicht darüber hinaus, die erforderliche gesetzliche Grundlage bilden (Abs. 1).
5. Gemäss Artikel 35b Abs. 2 wird die Möglichkeit, einen Pilotversuch durchzuführen, auf die Gemeinden, in ihren Zuständigkeitsbereichen, ausgeweitet.

2.7.10 Anpassung des SchG

Artikel 43 Abs. 3a bildet die gesetzliche Grundlage für die Übermittlung bestimmter Daten von Schülerinnen und Schülern, Lehrkräften und Verwaltungspersonal an die Föderation der Identitätsdienste im Bildungsraum Schweiz (Edulog), um insbesondere auf Online-Lehrmittel zugreifen zu können. Edulog verwendet die AHVN13 ausschliesslich zur Föderierung und Deföderierung einer Identität. Ein technischer Identifikator wird nach dem Zufallsprinzip zugewiesen, und die AHVN wird nie registriert.

Mit der Änderung von Artikel 43 Abs. 4 wird allein das Ziel verfolgt, auf die neue Version des Gesetzes, die vom Grossen Rat verabschiedet wird, zu verweisen.

2.7.11 Anpassung des MSG

Gleicher Kommentar wie beim SchG zur Änderung von Artikel 43.

2.7.12 Anpassung des FHG

Das Softwarepaket SAP (im Folgenden: das integrierte Finanzmanagementsystem) wird von den Dienststellen und Anstalten des Staates seit vielen Jahren eingesetzt. Haushaltsführung und Buchhaltung laufen grundsätzlich über dieses Tool, das den verschiedenen Verwaltungseinheiten von der Finanzverwaltung zur Verfügung gestellt wird. Die Nutzung dieses Systems verläuft zur vollen Zufriedenheit. Um den Anforderungen des Datenschutzes zu genügen (Erfordernis einer formellen gesetzlichen Grundlage), verankert der vorliegende Entwurf die Verwendung eines solchen Softwarepakets in der Gesetzgebung über den Finanzhaushalt des Staates.

Kapitel 6a

Die Bestimmungen über das integrierte Finanzmanagementsystem sollen in einem neuen Unterkapitel 6a des FHG eingefügt werden, im Anschluss an die organisatorischen Bestimmungen. Die drei Artikel dieses Unterkapitels enthalten die grundlegenden datenschutzrechtlich erforderlichen Bestimmungen. Darin wird angegeben, welche Kategorien von Daten bearbeitet werden, zu welchem Zweck und nach welchen besonderen Modalitäten. Sie beschreiben auch, wie und unter welchen Voraussetzungen auf das integrierte Finanzmanagementsystem zugegriffen werden kann. Hinsichtlich der Aufteilung der Verantwortlichkeiten und der zu treffenden Sicherheitsmassnahmen verweist der Gesetzesentwurf auf die Ausführungsbestimmungen.

Art. 47a

1. Diese Bestimmung beschreibt den Verwendungszweck des integrierten Finanzmanagementsystems für die Dienststellen und Anstalten des Staates sowie den Inhalt dieses Informationssystems.
2. Der Zweck wird in Absatz 1 beschrieben. Es geht dabei um die Haushaltsführung und die operative Führung sowie um die Finanzplanung und die Budgetkontrolle.
3. Die Angabe der Zwecke, die mit der Nutzung des integrierten Finanzmanagementsystems verfolgt werden, ist abschliessend und entspricht der aktuellen Praxis. Mit der Verwendung des Ausdrucks «namentlich» im Gesetzentwurf soll lediglich ein unnötig schwerfälliges Verfahren vermieden werden für den unwahrscheinlichen Fall, dass die Liste in Zukunft durch eine damit zusammenhängende neue Aufgabe ergänzt werden müsste, die derzeit nicht in Betracht gezogen wird.
4. Absatz 2 legt die Kategorien von Daten fest, die mithilfe des integrierten Finanzmanagementsystems bearbeitet werden. Es handelt sich um folgende Elemente:
    a) Identität und Adresse der natürlichen und juristischen Personen, die finanzielle Beziehungen zum Staat unterhalten;
    b) Angaben zu Finanzinformationen der natürlichen und juristischen Personen nach Buchstabe a) und über ihre Finanztransaktionen mit dem Staat.
5. Die Identität der natürlichen Personen umfasst Informationen über Namen, Vornamen, Adressen, Kontaktdaten, Geburts- und gegebenenfalls Todesdatum, Nationalität, Heimatort, Geschlecht, AHV-Nummer, Korrespondenzsprache, Bankverbindungsdaten (IBAN), AHV-Nummer, kantonaler Personenidentifikator (KPI) und weitere Identifikatoren, die für die Verwaltung des Dossiers der betroffenen Person in finanzieller Hinsicht erforderlich sind (Symic [im Migrationswesen verwendete Nummer], PID Gelan [Persönliche Nummer des Bewirtschafters in der EDV-Gesamtlösung Landwirtschaft und Natur], RegEdu-Nr. [im Bildungswesen verwendete Nummer], usw.
6. Die Identität juristischer Personen umfasst die Daten über den Namen, die Rechtsform, die Adresse, die Kontaktdaten, das Datum der Gründung und gegebenenfalls der Liquidation, die Korrespondenzsprache, die Bankverbindung (IBAN), die Mehrwertsteuer-, UID- (Unternehmensidentifikationsnummer), BUR- (Betriebs- und Unternehmensregister) und KPI-Nummer sowie weitere Identifikatoren, die für die Verwaltung des Dossiers der betreffenden juristischen Person in finanzieller Hinsicht erforderlich sind.
7. Auch hier soll mit dem Ausdruck «namentlich» das Verfahren nicht unnötig schwerfällig gemacht werden, falls es in Zukunft hypothetisch notwendig sein sollte, die Liste der Kategorien von bearbeiteten Daten zu ergänzen. Zurzeit werden nur die Daten der zwei im Entwurf genannten Kategorien im Finanzmanagementsystem bearbeitet.
8. In Übereinstimmung mit dem Datenschutzrecht wird in Absatz 3 erwähnt, dass mit dem integrierten Finanzmanagementsystem besonders schützenswerte Personendaten bearbeitet werden können. Einige Dienststellen und Anstalten des Staates, die die Software für ihre Rechnungsstellung verwenden, sind in «sensiblen» Bereichen im datenschutzrechtlichen Sinne tätig, wie etwa in den Bereichen Polizei, Sozialwesen usw. Absatz 3 verleiht solchen Datenbearbeitungen eine formelle gesetzliche Grundlage. In diesem Zusammenhang ist es wichtig zu erwähnen, dass die technischen und organisatorischen Massnahmen zur

Gewährleistung der Sicherheit der Datenverarbeitung bereits ergriffen wurden. Das System ist nämlich «siloartig» aufgebaut, so dass jede Benutzerin oder jeder Benutzer nur Zugang zu den Daten hat, die sie oder ihn betreffen und die sie oder er für die Ausübung ihrer oder seiner Aufgaben benötigt. In diesem Zusammenhang stellt Absatz 3 klar, dass die Verarbeitung sensibler Daten durch das integrierte Finanzmanagementsystem nur dann zulässig ist, wenn die Erfüllung der in Absatz 1 genannten «finanziellen» Aufgaben davon abhängt.

Artikel 47b

1. In Absatz 1 wird angegeben, welche Organe das integrierte Finanzmanagementsystem nutzen können. Es sind dies hauptsächlich die Verwaltungseinheiten des Staats, das heisst die Dienststellen und Anstalten. Diese Stellen können das integrierte Finanzmanagementsystem nutzen, müssen aber nicht. In der Praxis sind allerdings nur wenige Einheiten berechtigt, das System nicht für ihre Buchhaltung zu verwenden, so etwa beispielsweise die Hochschulen und Universitäten. Was die Gemeinden betrifft, so können sie insofern Zugriff auf das integrierte Finanzmanagementsystem haben, als sie ihr Kontokorrent über Platcom (Kommunikationsplattform zwischen Staat und Gemeinden) einsehen können müssen. Dazu ist zu sagen, dass die Gemeinden nur Zugang zu Daten haben, die sie im Zusammenhang mit ihrer Haushaltsführung und Buchhaltung direkt betreffen.
2. Die Absätze 2 und 3 spezifizieren den Datenfluss: Die Dienststellen und Anstalten nutzen das integrierte Finanzmanagementsystem für ihre Buchhaltung und Rechnungsstellung sowie für die Transaktionen im Zusammenhang mit der Finanzplanung und dem Voranschlagsverfahren. Die Finanzverwaltung kann im Rahmen der ihr durch die Gesetzgebung über den Finanzhaushalt des Staates übertragenen Befugnisse (Zahlungseingang von Rechnungen und Zahlungsausstände/Finanzplanung und Voranschlagsverfahren) auf alle in der Software enthaltenen Daten zugreifen. Für Abteilungen, die besonders sensible Personendaten bearbeiten, werden besondere Massnahmen getroffen.
3. In Übereinstimmung mit den datenschutzrechtlichen Vorgaben wird in Absatz 4 die Möglichkeit, das integrierte Finanzmanagementsystem mit anderen Informationssystemen zu verknüpfen, gesetzlich verankert. Es ist nicht sinnvoll, die betreffenden Systeme aufzuzählen und im Gesetz festzuschreiben. Der Bereich ist nämlich ausgesprochen entwicklungsfreudig, und es wäre nicht effizient, das FHG bei jeder neuen Schnittstelle oder bei jeder Aufhebung einer bestehenden Schnittstelle ändern zu müssen. Um das Risiko eines Missbrauchs auszuschliessen, ist Absatz 4 restriktiv formuliert. Die Verknüpfungen müssen dem in der Datenschutzgesetzgebung verankerten Grundsatz der Zweckbindung entsprechen und sind nur zwecks staatlicher Haushaltführung und Buchhaltung erlaubt.
4. Das integrierte Finanzmanagementsystem verfügt bereits heute über Schnittstellen zu anderen Informationssystemen, wie z.B. zum Schulverwaltungs-Informationssystem (HAE), zu egov oder auch e-kogu (System, das im Bereich der ausserkantonalen Spitalaufenthalte eingesetzt wird). Es wird demnächst mit dem Kantonalen Bezugssystem über die Plattform Fripers (Plattform des kantonalen Einwohnerregisters) verbunden, gemäss dem Verfahren und den Modalitäten nach den Bestimmungen über das Kantonale Bezugssystem.
5. Nach Absatz 5 kann über ein Abrufverfahren auf die Daten des integrierten Finanzmanagementsystem zugegriffen werden. Für diese Art von Zugriff gelten datenschutzrechtliche Sonderregeln, das heisst er muss mit einem Benutzerreglement formalisiert werden, insbesondere mit der Bestimmung, wer Zugriff auf welche Daten hat, und Angaben zur Abfragehäufigkeit, zum Authentifikationsverfahren, zu den weiteren Sicherheitsmassnahmen sowie zu den Kontrollmassnahmen (Art. 21 Abs. 3 des Reglements vom 29. Juni 1999 über die Sicherheit der Personendaten; SGF 17.15). Wie für die Datenverknüpfung muss der Bearbeitungszweck in Übereinstimmung mit der Finanzhaushaltsgesetzgebung stehen.
6. Absatz 6 regelt die Datenweitergabe an andere Behörden oder Dritte. Für eine solche Datenbearbeitung gelten dieselben Vorgaben wie für die Datenverknüpfung oder das Abrufverfahren. Sie ist nur für die im FHR genannten Daten und für einen gesetzeskonformen Zweck zulässig. In Betracht kommt dabei beispielsweise die Übermittlung von Daten über die Erhebung von Grundbuchgebühren an Gemeinden, um ihnen die Erhebung von Gemeinde-Zusatzabgaben zu ermöglichen, oder von Daten, die es für die Erhebung der Hundesteuer braucht. Die Nutzerinnen und Nutzer können sich auf keinen Fall auf diese Bestimmung berufen, um Daten zu einem

Zweck an Dritte weiterzugeben, der nicht mit der Finanzverwaltung und Buchhaltung des Staates in Verbindung steht.

Artikel 47c

1. Um der Weiterentwicklung der Informatiksicherheit Rechnung zu tragen, überträgt der Gesetzesentwurf dem Staatsrat die Kompetenz, die organisatorischen und technischen Sicherheitsmassnahmen festzulegen, die zur Gewährleistung der Sicherheit der Daten bei der Nutzung des integrierten Finanzmanagementsystems ergriffen werden müssen.
2. Wie schon erwähnt, wird das integrierte Finanzmanagementsystem den Dienststellen und Anstalten des Staates von der Finanzverwaltung zur Verfügung gestellt. Demnach wird dieses Tool von sehr vielen Einheiten genutzt werden. Es ist wichtig, dass die Verantwortlichkeiten der verschiedenen Beteiligten klar festgelegt werden. Da es sich in diesem Fall um eine hauptsächlich organisatorische Frage handelt, überträgt der Entwurf dem Staatsrat auch die Aufgabe, die Verantwortlichkeiten zwischen den verschiedenen betroffenen Stellen aufzuteilen.
3. Der Entwurf präzisiert jedoch, dass die Einzelheiten der umzusetzenden Sicherheitsmassnahmen und der Aufteilung der Verantwortlichkeiten in Vereinbarungen zwischen der Finanzverwaltung und den das integrierte Finanzmanagementsystem nutzenden Stellen geregelt werden können und die Vereinbarungen gegebenenfalls an die kantonale Behörde für Öffentlichkeit, Datenschutz und Mediation weitergeleitet werden müssen, damit diese entsprechend darüber informiert ist.

2.7.13 Anpassung des GesG

Gemäss der Änderung an Artikel 60 Abs. 3 des GesG darf der Zugang zu den eigenen Personendaten im Gesundheitsbereich nicht mehr an die Bedingung der Anwesenheit einer Fachperson aus dem Gesundheitswesen geknüpft werden; diese Art des Zugangs kann der betroffenen Person nur vorgeschlagen werden. Diese Änderung geht in die Richtung eines grösseren Respekts vor der Autonomie der betroffenen Person und ihres Rechts auf informationelle Selbstbestimmung.

3 Liste der wichtigsten Abkürzungen

—

3.1 Erlasse

Alte EU-Richtlinie 95/46/CE: Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr

Übereinkommen SEV Nr. 108: Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 (SR 0.235.1)

ArchG: Gesetz vom 10. September 2015 über die Archivierung und das Staatsarchiv (SGF 17.6)

BGÖ: Bundesgesetz vom 17. Dezember 2004 über das Öffentlichkeitsprinzip in der Verwaltung (SR 152.3)

BGSA: Bundesgesetz vom 17. Juni 2005 über Massnahmen zur Bekämpfung der Schwarzarbeit (SGF 822.41)

BStatG: Bundesstatistikgesetz vom 9. Oktober 1992 (SR 431.01)

DSchG: Gesetz vom 25. November 1994 über den Datenschutz (SGF 17.1)

DSG, 1. Änderung: Änderung des Bundesgesetzes über den Datenschutz vom 24. März 2006 (AS 2007 4983)

DSG, 2. Änderung: Bundesgesetzes über die Umsetzung des Rahmenbeschlusses 2008/977 /JI über den Schutz von Personendaten im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen (AS 2010 3387)

DSG: Bundesgesetz vom 19. Juni 1992 über den Datenschutz (SR 235.1)

DSGVO: Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr sowie zur Aufhebung der Richtlinie 95/46/EG (Datenschutzgrundverordnung, DSGVO)

E-GovG: E-Government-Gesetz vom 18. Dezember 2020 (SGF 184.1)

EKG: Gesetz vom 23. Mai 1986 über die Einwohnerkontrolle (SGF 114.21.1)

EU-Rahmenbeschluss 2008/977/JAI: Rahmenbeschluss (EU) 2008/977/JAI über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden vom 27. November 2008 (Amtsblatt der Europäischen Union (L 350/60)

EU-Richtlinie 2016/680: Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2017 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

FHG: Gesetz vom 25. November 1994 über den Finanzhaushalt des Staates (SGF 610.1)

FKBG: Gesetz vom 22. November 1988 über die Freiburger Kantonalbank (SGF 961.1)

GesG: Gesundheitsgesetz vom 16. November 1999 (SGF 821.0.1)

GG: Gesetz vom 25. September 1980 über die Gemeinden (SGF 140.1)

HGG: Gesetz vom 16. September 1986 über die Haftung der Gemeinwesen und ihrer Amtsträger (SGF 16.1)

InfoG: Gesetz vom 9. September 2009 über die Information und den Zugang zu Dokumenten (SGF 17.5)

ISR: Reglement über Informationssicherheit (in Vorbereitung)

JG: Justizgesetz vom 31. Mai 2010 (SGF 130.1)

KSG: Gesetz vom 26. September 1990 über die Beziehungen zwischen den Kirchen und dem Staat (SGF 190.1)

LSR: Bundesgesetz vom 16. Dezember 2005 über die Zulassung und Beaufsichtigung der Revisorinnen und Revisoren (SR 221.302)

MedG: Gesetz vom 25. Juni 2015 über die Mediation für Verwaltungsangelegenheiten (SGF 181.1)

MSG: Gesetz vom 11. Dezember 2018 über den Mittelschulunterricht (SGF 412.0.1)

Neues DSG: Neues Bundesgesetz vom 25. September 2020 über den Datenschutz (BBI 2020 7397; geplantes Inkrafttreten im September 2023)

RAG: Bundesgesetz vom 16. Dezember 2005 über die Zulassung und Beaufsichtigung der Revisorinnen und Revisoren (SR 221.302)

RVOG: Regierungs- und Verwaltungsorganisationsgesetz vom 21. März 1997 des Bundes (SR 172.010)

SchG: Gesetz vom 9. September 2014 über die obligatorische Schule (SGF 411.0.1)

StatG: Gesetz vom 7. Februar 2006 über die kantonale Statistik (SGF 110.1)

StPO: Schweizerische Strafprozessordnung vom 5. Oktober 2007 (SR 312.0)

SVOG: Gesetz vom 16. Oktober 2001 über die Organisation des Staatsrates und der Verwaltung (SGF 122.0.1)

Übereinkommen (EU) SEV Nr. 108+: Modernisiertes Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 17. und 18. Mai 2018

VE-DSchG: Vorentwurf der Revision des kantonalen Datenschutzgesetzes vom 27. November 2019

VidG: Gesetz vom 7. Dezember 2010 über die Videoüberwachung (SGF 17.3)

VRG: Gesetz vom 23. Mai 1991 über die Verwaltungsrechtspflege des Kantons Freiburg vom 23. Mai 1991 (VRG; SGF 150.1)

ZPO: Schweizerische Zivilprozessordnung vom 19. Dezember 2008 (SR 272)

3.2 Andere Abkürzungen

Abs.: Absatz

AHVN: Alters- und Hinterlassenenversicherung-Nummer

Art.: Artikel

ASF: Amtliche Sammlung des Kantons Freiburg

Aufl.: Auflage

BBl: Bundesblatt

BGE: Bundesgerichtsentscheid

BSG: Bernische Systematische Gesetzessammlung

Bst.: Buchstabe

EU: Europäische Union

s.: siehe

SGF: Systematische Gesetzessammlung des Kantons Freiburg

SJZ: Schweizerische Juristen-Zeitung

SR: Systematische Sammlung des Bundesrechts

SZW: Schweizerische Zeitschrift für Wirtschafts- und Finanzmarktrecht

TGR: Amtliches Tagblatt der Sitzungen des Grossen Rates

Vgl.: Vergleiche

VPB: Verwaltungspraxis der Bundesbehörden

VZÄ: Vollzeitäquivalent

Ziff.: Ziffer