Erläuternder Bericht

zum Vorentwurf des Gesetzes über die Totalrevision des Gesetzes über den Datenschutz

In Kürze

1. Das geltende Gesetz über den Datenschutz stammt vom 25. November 1994. Zur damaligen Zeit kam das *World Wide Web* eben gerade zur Welt, *Google, Facebook, Twitter* und Konsorten existierten noch nicht, die Gemeinwesen des Kantons verfügten noch nicht über E-Mail und es stand kein virtueller Schalter zum Bezug und zur Abwicklung von Verwaltungsdienstleistungen während 24 Stunden an 7 Tagen in der Woche stand zur Verfügung.

2. Im Rückblick kann man sagen, dass mit dem DSchG ein ansprechendes Schutzniveau erreicht werden konnte, dort wo 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 Datenschutzgesetze, die zu Beginn der 90-er-Jahre erlassen wurden, sind die darin enthaltenen Bestimmungen aufgrund der technischen und sozialen Entwicklungen der vergangenen 25 Jahre **teilweise veraltet**. Dies sind die Gründe für eine Modernisierung und Aktualisierung des Gesetzes.

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. Der Bund und die Mehrheit der Kantone sind nun ebenfalls daran, ihre Gesetzgebung im Bereich Datenschutz zu revidieren, um diese Ziele zu erreichen.

4. Dieser Vorentwurf zielt darauf ab, das Freiburger kantonale Recht mit diesen **neuen Standards** im Bereich des Datenschutzes in Einklang zu bringen. Er ist **stark beeinflusst** vom Projekt der Totalrevision des Bundesgesetzes über den Datenschutz, bei der ihrerseits das Ziel darin besteht, das eidgenössische Recht mit demjenigen der Konvention SEV 108+ des Europarates zum Schutz des Einzelnen bei der automatischen Verarbeitung personenbezogener Daten und den neuen Anforderungen des Rechts der Europäischen Union beim Datenschutz vereinbar zu machen. Er nimmt auch die eine oder andere interessante Regelung auf, welche die anderen Kantone in ihrer je eigenen Gesetzgebung aufgenommen haben und deren **positive Auswirkungen** von der Lehre anerkannt werden.

5. Wenngleich das Projekt zur Revision des Bundesgesetzes über den Datenschutz einen wesentlichen Einfluss auf die Erstellung dieses Vorentwurfs hatte, ist dieser nicht eine

einfache Kopie. Er nimmt auf Eigenheiten des Kantons Freiburg und auf aktuelle Entwicklungen und Projekte im Rahmen der Digitalisierung der Verwaltung Rücksicht. Hierzu können als Beispiele folgende Elemente zitiert werden:

— Spezielle Regelungen sind vorgesehen mit dem Ziel, eine **sichere und kontrollierte Externalisierung** von gewissen Formen der Datenbearbeitung an Dritte vergeben zu können, weil diese beispielsweise über bessere und passendere Fähigkeiten und Ressourcen als die entsprechenden Ämter im Kanton verfügen.

— Um die **bipartite Zusammensetzung der Behörde für Öffentlichkeit und Datenschutz** zu beachten, werden die neuen Zuständigkeiten der kantonalen Aufsichtsbehörde für Datenschutz nicht alleine in den Händen der oder des Beauftragten für den Datenschutz konzentriert, sondern zwischen dieser Person und der kantonalen Öffentlichkeits- und Datenschutzkommission aufgeteilt.

— Im Gegensatz zum Projekt zur Revision des Bundesgesetzes über den Datenschutz ist im Vorentwurf nicht vorgesehen, den Datenschutz der **juristischen Personen** aus juristischen oder praktischen Gründen aufzuheben.

6. Nichtsdestotrotz ist zu erwähnen, dass sich der Vorentwurf in einem **relativ strikten Rahmen**, der nicht viel Handlungsspielraum ermöglicht, bewegt. Abgesehen davon, dass die neuen Rechte der Personen, deren Daten verarbeitet werden, und die neuen Pflichten der Verantwortlichen für die Datenverarbeitung einen besseren Schutz gewährleisten, sollen sie im Allgemeinen auf eine Angleichung des Freiburger Rechts an die **neuen anzuwendenden Standards** im Bereich Datenschutz im Digitalisierungszeitalter hinauslaufen. Die Umsetzung dieser Standards ist insofern eine notwendige Bedingung für die erfolgreiche Umsetzung der E-Government-Strategie des Staates Freiburg, als es ohne digitales Vertrauen keine Digitalisierung geben kann.

7. Dieser Bericht ist wie folgt aufgebaut:

Die Gesetze und Reglemente werden mit ihren Abkürzungen zitiert; eine Liste befindet sich am Schluss dieses Dokumentes.

1 ALLGEMEINES

1.1 Kontext und Ursprung des Vorentwurfs

1.1.1. Im Bereich Datenschutz folgten **mehrere Generation der Gesetzgebung** aufeinander, um neue Praktiken zu entwickeln und angesichts der ständigen Weiterentwicklung der digitalen Anwendungen die erforderlichen Leitplanken für die Verarbeitung personenbezogener Daten festzulegen:
a) Die **erste Generation** dieser Gesetzgebungen erstreckt sich über die Jahre 1980 bis 2000.

Inspiriert war sie primär vom alten Übereinkommen des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 («Konvention SEV 108 »); sie zeichnet sich durch eine Herangehensweise aus, die auf den **grossen Prinzipien** - Rechtmässigkeit, Verhältnismässigkeit, Zweckbindung, Richtigkeit usw. - beruht, die dazu dienen müssen, noch **wenig verstandenen** Praktiken und Risiken einen Rahmen zu geben. In der Europäischen Union ist der erste einschlägige Bezugstext die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, die 1995 erlassen wurde. In der Schweiz verabschiedet der Bund 1992 das DSG. Einige Kantone sind dem Bund gewissermassen vorangegangen, so etwa der Kanton Bern mit seinem Gesetz über den Datenschutz (KDSG; BSG 152.04), das auf das Jahr 1986 zurück geht; die anderen folgen in den kommenden Jahren, so auch der Kanton Freiburg, dessen DSchG 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 erfahren wird. Das Datenschutzrecht beginnt sich unter der kombinierten Wirkung der Beiträge der Lehre und die darauffolgenden Gerichtsentscheide langsam **zu materialisieren**. Die grossen Prinzipien werden präzisiert und / oder vervollständigt durch **präzisere Regelungen**. Die Konvention SEV 108 entwickelt sich: Ein zusätzliches Protokoll wird 2001 angenommen, das den Mitgliedstaaten neue Pflichten auferlegt, namentlich die Stärkung der Befugnisse ihrer Aufsichtsbehörden. Während dieser Periode tritt die Eidgenossenschaft den Abkommen von **Schengen und Dublin** bei und verpflichtet sich in diesem Kontext, sich an den Rahmenbeschluss 2008/977/JI des Europarates zum Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeiten werden, zu halten. Sie revidiert dazu auch zweimal das DSG: Zum ersten Mal im Jahr 2007, mit dem Ziel, den Inhalt des Gesetzes in einigen Punkten unter Berücksichtigung gewisser Entwicklungen zu modernisieren; zum zweiten Mal im Jahr 2010, um eine Anpassung des Bundesrechts an die neuen Anforderungen der Konvention SEV 108, insbesondere an das Zusatzprotokoll, und an die Gesetzgebung der EU zu erreichen. Auf der kantonalen Ebene sind die Veränderungen unterschiedlich. Gewisse Kantone, genauso wie der Kanton Freiburg, beschränken sich strikte darauf, das übergeordnete Recht zu übernehmen. Andere Kantone hingegen gehen weiter und nehmen substanzielle Verbesserungen ihrer Gesetze zum Datenschutz vor.

c) Die **dritte Generation** beginnt 2016 mit der Übernahme der Datenschutz-Grundverordnung DSGVO der Europäischen Union und der Richtlinie (EU) 680/2016 über den Datenschutz im Bereich der Strafverfolgung; dieser ersten Serie von Gesetzestexten folgt 2018 die Promulgierung der neuen Konvention 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 durch Technik (nach Massgabe des Prinzips *privacy-by-design*) und standardmässig durch datenschutzfreundliche Voreinstellungen (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. Der Bundesrat entscheidet seinerseits, dass es nötig sei, eine Totalrevisision des DSG vorzunehmen und präsentierte in diesem Zusammenhang im September 2017 einen Gesetzesentwurf mit einer Botschaft. Im September 2018 hat die Vereinigte Bundesversammlung das SDSG verabschiedet, das eine erste Reihe von Änderungen enthält, mit denen die Schweiz sich in den festgelegten Fristen den Anforderungen des europäischen Rechts im Rahmen der Abkommen von Schengen und Dublin anpassen kann.

1.1.2. Das DSchG wurde 1994 verabschiedet und unter materiellen Gesichtspunkten **nur einmal** geändert, und zwar im Jahr 2008. Ursprünglich bestand der Revisionsentwurf aus drei Elementen (s. TGR 2008 657):
— Anpassung des kantonalen Gesetzes an die Abkommen von Schengen und Dublin und an das Zusatzprotokoll vom 8. November 2001 zur Konvention SEV 108;
— Anpassung an die übrigen Korrekturen im Bundesgesetz über den Datenschutz;
— Berücksichtigung der Erfahrungen mit dem DSchG seit dessen Inkrafttreten.

1.1.3. 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»*.

1.1.4. Anders gesagt: Das DSchG ist heute als auf **halbem Weg zwischen der ersten und der zweiten Generation** der Datenschutzgesetzgebung einzuordnen. Aus diesem Grund scheint die Durchführung **einer Totalrevision** zum jetzigen Zeitpunkt kaum vermeidbar zu sein. Sie soll dazu dienen, den Kanton Freiburg mit einem juristischen Rahmen zu versehen, der nicht nur Bürgerinnen und Bürgern einen angemessenen und kohärenten Schutz im Bereich Datenschutz bietet, sondern auch den Anforderungen und den internationalen Standards, die für die Schweiz in diesem Bereich bindend sind, entspricht.

1.2 Ablauf der Arbeiten

1.2.1. Ende Sommer 2017 hat der Bundesrat seinen Entwurf zur Totalrevision des DSG verabschiedet. In der Folge hat die Staatskanzlei die kantonale Datenschutzbeauftragte beauftragt, eine Arbeitsgruppe zu bilden, um eine Analyse der Bestimmungen der freiburgischen Gesetzgebung zum Datenschutz vorzunehmen und **die Anpassungen vorzuschlagen, die** im Lichte der Änderungen des DSG, die vom Bundesrat vorgeschlagen

wurden, und des internationalen Rechts, das in diesem Bereich in der Schweiz einen Einfluss hat, **erforderlich sind**.

1.2.2. Der Arbeitsgruppe, die von der Datenschutzbeauftragten zusammengestellt wurde, gehörten folgende Personen an: ein Vertreter jeder Direktion, ein Vertreter der richterlichen Gewalt; ein Vertreter der Staatsanwaltschaft, ein Vertreter der Polizei, zwei Vertreter des Amts für Informatik und Telekommunikation, ein Vertreter der Gemeinden und schliesslich ein Vertreter des Amtes für Gesetzgebung. Um mit der Revisionsarbeit so effizient wie möglich voranschreiten zu können, beschloss die Arbeitsgruppe einen Ausschuss aus der Beauftragten für Datenschutz und dem Vertreter des Amtes für Gesetzgebung zu bilden, der damit beauftragt wurde, die gesetzlichen Bestimmungen zu redigieren und sie der ganzen Arbeitsgruppe zur Diskussion vorzulegen. Im Laufe der Arbeit wurden weitere **Sub-Arbeitsgruppen** gebildet, um spezifischere Aspekte mit den Hauptbeteiligten diskutieren zu können, namentlich in den Bereichen der Polizei und der Technologie.

1.2.3. Die gesamte Arbeitsgruppe hat viel dazu beigetragen, das **richtige Gleichgewicht** zwischen den beiden teilweise gegensätzlichen Zielen zu finden: einerseits die **datenschutzrechtlichen Anforderungen** und die Notwendigkeit, sich so weit als möglich an die Standards der dritten Generation der Gesetzgebung dieses Bereichs anzupassen, und, andererseits, die Notwendigkeit, dass die öffentlichen Organe über einen **genügenden Spielraum** verfügen, um die ihnen durch die Verfassung und die Gesetze übertragenen Aufgaben erfolgreich und ohne unnötige Hindernisse erfüllen zu können. Gewisse Bestimmungen, die von der verkleinerten und sehr auf das erste Ziel fokussierte Arbeitsgruppe ursprünglich vorgeschlagen wurden, mussten im Lichte des zweiten Ziels weiter angepasst werden. Schliesslich befriedigt das vorgeschlagene Resultat **so weit wie möglich** sowohl die Anforderungen des Datenschutzrechts als auch des guten Funktionierens der Verwaltung.

1.3 Grundzüge des Vorentwurfs

1.3.1 Inhalt im Allgemeinen

1.3.1.1. Der Hauptinhalt des Vorentwurfs zeigt sich in **seiner Struktur**, die im Vergleich zum geltenden Gesetz praktisch unverändert bleibt. Wie Letzteres, enthält er sechs Abschnitte: Der erste Abschnitt enthält die üblichen allgemeinen Bestimmungen und eine Serie von Definitionen, die dazu dienen, Begriffen, die im Vorentwurf mehrfach auftreten, eine präzise Bedeutung zu verleihen (Art. 1 bis 4); der zweite Abschnitt legt die allgemeinen Grundsätze für die Bearbeitung von Personendaten fest sowie die präzisere Regeln für gewisse Arten von besonderen Datenbearbeitungen (Art. 5 bis 25); der dritte Abschnitt legt die Rechte dar, über welche die betroffenen Personen bei der Bearbeitung ihrer Personendaten verfügen (Art. 26 bis 36); der vierte Abschnitt beschreibt die Massnahmen, welche die für die Datenbearbeitung verantwortlichen Personen berücksichtigen und umsetzen müssen, wenn sie Personendaten bearbeiten, um sicherzustellen, dass der Schutz und die Sicherheit

gewährleistet sind (Art. 36 bis 47); der fünfte Abschnitt behandelt die von der Aufsichtsbehörde ausgeübte Aufsicht im Bereich des Datenschutzes (Art. 48 bis 64) und der sechste Abschnitt enthält die üblichen Bestimmungen des Übergangsrechts, die angeben, wie die neuen Regelungen sich ins bestehende Recht einfügen (Art. 65).

1.3.1.2. Der Inhalt der vorgeschlagenen Bestimmungen **lehnt sich zu grossen Teilen** an den Entwurf des Bundes zur Totalrevision des DSG **an**, der seinerseits wiederum an die neuen Gesetzestexte der dritten Generation, d. h. der Konvention SEV 108+ und der Verordnung (EU) 679/2016 und der Richtlinie (EU) 680/2016, angelehnt ist. Diese Regelungen beeinflussten den Inhalt des Vorentwurfs im Wesentlichen auf drei Ebenen:
a) Der Vorentwurf nimmt den **risikobasierten Ansatz** wieder auf, der die neue Gesetzgebung zum Datenschutz charakterisiert. Gemäss diesem Ansatz sind die Verpflichtungen im Bereich Datenschutz bei den Verantwortlichen für die Datenbearbeitung, deren Aktivitäten ein Schadenrisiko aufweisen, strikter als bei Personen, deren Tätigkeiten weniger riskant sind (s. BBl 2017 6941, S. 6970).
b) Der Vorentwurf bewahrt auch den **technisch neutralen Charakter** der vorgeschlagenen Regeln. Dies hindert ihn aber nicht daran, gewisse Praktiken der jüngeren Zeit zu reglementieren, die direkt mit der Nutzung neuer Technologien verbunden sind, wie dies etwa bei der Externalisierung gewisser Typen und Formen der Bearbeitung der Fall ist (Art. 20). Der technologisch neutrale Charakter der Regulierung ist gewiss wesentlich, um zu verhindern, dass sie wegen des technologischen Fortschritts schnell veraltet. Die Technologie darf aber nicht ignoriert werden, sonst werden die mit dem Gesetz verbundenen Ziele nicht erreicht.
c) Die **verwendete Terminologie** im Vorentwurf wurde modernisiert, um den Entwicklungen im Bereich des Datenschutzrechts besser gerecht zu werden und auch die Kompatibilität mit den jüngsten Gesetzestexten auf eidgenössischer und internationaler Ebene 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».

1.3.1.3. Nach dem Vorbild des Entwurfs des Bundesrates und entgegen dem Recht der EU wird im Vorprojekt ausdrücklich auf die Erwähnung eines ***«Rechts auf Vergessen»*** (s. Art. 17 Verordnung (EU) 2016/679) und auf ein allgemeines Recht auf «***Datenübertragbarkeit***» (s. Art. 20 der Verordnung (EU) 2016/679) verzichtet. Das hat folgende Gründe:
a) Die Formulierung «Recht auf Vergessen» ist täuschend, da in ihr zu Unrecht anklingt, dass ein allgemeines Recht für die betroffenen Personen darauf bestehe, aus den Datenbanken des Staates zu verschwinden. Jedenfalls könnte ein solches Recht Fall nicht anerkannt werden. Der Vorentwurf sieht dafür andere und **differenziertere** Garantien vor, die in der Praxis zu einem Recht auf Vergessen führen können (im gleichen Sinne: BBl 2017 6941, S. 7077). Es handelt sich dabei einerseits um Artikel 10, der vorsieht, dass die Personendaten, die für den Zweck der Datenbearbeitung nicht mehr nötig sind, automatisch zu löschen (oder

zu anonymisieren) sind und andererseits Artikel 30 Abs. 2 Bst. a, der es der betroffenen Person erlaubt, ihrerseits eine Löschung ihrer Daten zu verlangen, wenn sie nicht mehr von Nutzen sind. Ausserdem ermächtigt der Artikel 33 die betroffene Person, zu verlangen, dass gewisse Daten über sie nach ihrem Tod gelöscht werden.

b) Das Recht auf Übertragbarkeit der Daten erlaubt es der betroffenen Person in den Besitz ihrer persönlichen Daten (z.B. durch Download) zu gelangen, mit dem Ziel, diese Daten persönlich wieder zu verwenden oder sie an eine Drittorganisation zu transferieren. Das setzt folglich die Übertragung in strukturierter, aktueller und leicht lesbarer Form, durch was für eine Maschine auch immer, voraus. Dazu braucht es eine Standardisierung und eine Normierung der Unterstützung und Softwares, die von den Verwaltungen auf Gemeinde-, Kantons- und Bundesebene und auch im Ausland genutzt werden, wenn man das Recht auf Datenportabilität aus Europäischer Sicht berücksichtigt. Vor der Einführung eines allgemeinen Rechts auf Datenübertragbarkeit im Kanton Freiburg scheint es **angebracht zu sein**, die Ergebnisse der Entwicklung der Strategie «Digitale Schweiz» und die Erfahrungen in der Europäischen Union dazu abzuwarten (im gleichen Sinn: BBl 2017 6941, S. 6984 f.).

1.3.1.4. Im Vergleich zum Entwurf des Bundesrates weist der Vorentwurf einen wichtigen Unterschied auf, der besonders erwähnenswert scheint. Er sieht nicht vor, **den Datenschutz juristischer Personen** aufzuheben. Zwei Gründe erklären dieses Vorgehen:

a) Aus streng juristischer Sicht sieht Artikel 12 Abs. 2 der Freiburger Kantonsverfassung vor, dass jede Person das Recht darauf hat, gegen die missbräuchlich 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] Das Bundesgericht hat seinerseits die Frage noch nicht klar entschieden.[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 gesetzlichen Grundlagen, die derzeit öffentlichen Organen die Verarbeitung personenbezogener Daten ermöglichen, bei den Daten juristischer Personen obsolet würden (s. BBl 2017 6941, S. 6972, 6981 und 7011 f.). Für den Bundesrat ist diese Situation aus der Perspektive des Legalitätsprinzips

---

[1] DUBEY Jacques, *Droits fondamentaux, Band II*, Basel 2018, n° 1766; BIAGGINI / GIOVANNI, *BV Kommentar*, Zurich, 2e Auflage., 2017, ad Art. 13, n° 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 ; AUER/ MALINVERNI / HOTTELIER, *Droit constitutionnel suisse, Band II*, 3. Auflage, Bern 2013, Nr. 384 ; MÜLLER / SCHEFER, *Grundrechte in der Schweiz*, 4. Auflage, Bern 2008, S. 166 ; DIGGELMAN Oliver, in Waldmann Bernhard / Belser Eva Maria / Epiney Astrid (édit.), Basler Kommentar Bundesverfassung, Bâle 2015, *ad* art. 13, n° 33.

[2] Im Urteil BGE 137 II 371 hat das Bundesgericht erklärt, dass juristische Personen von einem Schutz der Privatsphäre profitieren, die auch den persönlichen Datenschutz einschliesst. Es hat jedoch ergänzt, dass sie nicht Träger aller in Artikel 13 BV geschützten Aspekte seien, ohne zu diesem Thema weitere Informationen zu geben (Erw. 6).

problematisch, nach dem alles staatliche Handeln sich auf das Gesetz stützen muss (s. BBl 2017 6941, S. 7101 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 für juristische Personen, einzuführen (s. die Artikel 57h^{bis}, 57i, 57j, 57k, 57l, 57r, 57s, 57t RVOG des E-DSG). Er hat die gleiche Übung mit der Spezialgesetzgebung gemacht, wo die Regelungen, welche die Bearbeitung von Personendaten erlauben, verdoppelt 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 im E-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.

1.3.2 Bezug zum Recht der Europäischen Union und der modernisierten Konvention SEV 108

1.3.2.1 Mehrere internationale Rechtstexte haben diesen Entwurf in verschiedensten Bereichen beeinflusst. Es handelt sich hierbei um die Verordnung (EU) 2016/679 über den Datenschutz, die Richtlinie (EU) 2016/680 über den Datenschutz in den Bereichen Polizei und Justiz und die Konvention 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 f. und 6991 ff.). Ihr Geltungsbereich ist jedoch auf die Bereiche Polizei und Justiz 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 bestimmte kantonale Gesetze, die in den Bereich des Geltungsbereichs der Richtlinie fallen, angepasst werden müssen.

1.3.2.3 Gemäss Bundesrat ist die Schweiz nicht unmittelbar an die Verordnung (EU) 2016/679 gebunden (s. BBl 2017 6941, S. 6963 f. und 6991 ff.). Dennoch übt sie einen nicht zu vernachlässigenden **indirekten Einfluss** aus. Denn der bedingungslose Austausch von Daten zwischen europäischen und schweizerischen Verantwortlichen für die Bearbeitung von Daten 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 Verordnung (EU) 2016/679). 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 Verantwortlichen für die Bearbeitung 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 **unhaltbar**. Zurzeit profitiert die Schweiz von einem Angemessenheitsbeschluss, der vom 26. Juli 2000 datiert (s. BBl 2017 6941, S. 6964 f.). Die Europäische Union wird demnächst eine neue Beurteilung der schweizerischen Gesetzgebung vornehmen, um deren Kompatibilität mit der Grundverordnung (EU) 2016/679 zu prüfen. Im Rahmen dieser Evaluation wird sie das Bundesrecht prüfen, aber auch das Recht zufällig ausgewählter Kantone. Es ist somit wesentlich, dass der Kanton Freiburg, wie die anderen Kantone auch, seine Gesetzgebung im Bereich Datenschutz entsprechend anpasst.

1.3.2.4 Die Konvention SEV 108 des Europäischen Rates stellt den **ersten Text internationalen Rechts** im Bereich Datenschutz dar. Er ist am Oktober1985 in Kraft getreten und wurde von der Schweiz am 2. Oktober 1997 mit Inkrafttreten am 1. Februar 1998 ratifiziert. Im Jahr 2018 wurde die Konvention SEV 108 mit dem Ziel **vollständig modernisiert**, besser auf die Herausforderungen reagieren zu können, welche die Globalisierung, technologische Entwicklungen und die Zunahme des grenzüberschreitenden Datenverkehrs für den Schutz der Privatsphäre und die Grundrechte der betroffenen Personen darstellen. Auch wenn sie weniger detailliert und weniger dicht ist als die Verordnung (EU) 2016/679 und die Richtlinie (EU) 2016/680, hat die Konvention SEV 108+ einen sehr ähnlichen Inhalt wie die beiden Rechtstexte. Für den Bundesrat stellt die Ratifikation der modernisierten Konvention SEV 108 **eine wichtige Etappe** im Prozess dar, der darauf abzielt, den Datenschutzes in der Schweiz zu stärken (s. BBl 2017 6941, S. 6994 f. und 7186). Im Falle einer Ratifizierung **wäre** der Kanton Freiburg **gezwungen**, sein Recht entsprechend anzupassen. Der Vorentwurf **antizipiert** die entsprechende Ratifikation insofern, als sie zum jetzigen Zeitpunkt mehr als sicher erscheint.

1.3.3 Recht der betroffenen Personen

1.3.2.1. Die Frage rund um die Rechte der betroffenen Personen wird im Kapitel 3 des Vorentwurfs behandelt. Eines der Ziele des Vorentwurfes ist, den betroffenen Personen mehr Kontrolle und die Überwachung der Informationen einzuräumen, welche sie mit der öffentlichen Hand teilen. 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.

1.3.2.2. Neue Rechte werden eingeführt, insbesondere:
a) Die Möglichkeit einer jeden Person, sich vorbeugend der Kommunikation von sie betreffenden Daten an Dritte zu widersetzen (**Recht auf Sperrung**). Heute ist ein solches Recht im Kanton Freiburg nur im Zusammenhang mit Daten der Einwohnerkontrolle vorgesehen (s. Art. 18 EKG). Das Recht auf Sperrung gehört jedoch in Europa und der Schweiz seit langem zu den traditionellen Verteidigungsrechten im Bereich des Datenschutzes, unabhängig vom Typ der jeweiligen Bearbeitung der Daten. Dies ist der Grund dafür, dass dieses in Artikel 29 des Vorentwurfs eingeführt wurde. Das Recht auf Sperrung ist jedoch 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 öffentliches oder überwiegendes 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 vorübergehend zu verhindern, und es dem Verantwortlichen der Bearbeitung gleichwohl ermöglicht, die Daten weiterhin aufzubewahren (Art. 33 Abs. 1 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 Abklärungen erforderlich sind, um zu überprüfen, ob das Gesuch begründet ist.
c) Spezifische und angepasste Verteidigungsmittel werden in Artikel 31 des Vorentwurfs zugunsten von Personen anerkannt, die einer **Entscheidung unterliegen, die ausschliesslich auf einer automatisierten Datenverarbeitung** beruht (z. B. basierend auf einem Algorithmus). In diesem Fall muss die betroffene Person immer informiert werden, dass es sich um eine ausschliesslich von einer Maschine getroffene Entscheidung handelt. Sie hat auch das Recht, die Logik und die Kriterien derselben zu kennen und gegebenenfalls zu verlangen, dass die Entscheidung von einer menschlichen Person überprüft wird.
d) Eine neue Bestimmung wird in Artikel 33 vorgeschlagen, mit der jeder Person die Möglichkeit geboten wird, in einem bestimmten Rahmen über das Schicksal ihrer personenbezogenen Daten **nach dem Tod** zu entscheiden.

1.3.2.3. 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 Zugang zu den eigenen Daten und die verschiedenen Abwehrmassnahmen, über welche die betroffene Person verfügt, um sich gegen eine unrechtmässige Bearbeitung ihrer Daten zu wehren.

1.3.4 Verpflichtung der Verantwortlichen für die Bearbeitung

1.3.4.1. Die Verpflichtungen des Verantwortlichen der Datenbearbeitung werden in Kapitel 4 des Vorentwurfs definiert. 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 ist jedes Organ, das Daten auf welchem Niveau auch immer bearbeitet, für den Schutz seiner Daten verantwortlich (Art. 37). Wie es bereits heute der Fall ist, wird diese Verantwortung **transparent und systematisch** sichergestellt und umgesetzt: Jede Bearbeitung von Daten innerhalb des Staates steht unter der Verantwortung einer oder eines Verantwortlichen für die Datenbearbeitung, die oder der dazu verpflichtet ist, sie im

Register der Bearbeitungstätigkeiten anzumelden (Art. 38-40) und den Schutz der Daten und die Datensicherheit durch möglichst konkrete und den Umständen anzupassende Massnahmen sicherzustellen (Art. 41).

1.3.4.3. Gegenüber der jetzigen Situation werden den Verantwortlichen für die Datenbearbeitung **neue Massnahmen** auferlegt, die in den verschiedenen Phasen und auch davor umgesetzt werden sollen:
a) Die Konzepte des Datenschutzes durch T**echnik** (im Englischen: «*privacy by design*») und **standardmässig, durch datenschutzfreundliche Voreinstellungen** (im Englischen: «*privacy by default*») werden explizit zitiert. Ersteres bedeutet, dass technische und angepasste organisatorische Massnahmen ab den ersten Schritten der Entwicklung zu entsprechenden Datenbearbeitungen diskutiert und umgesetzt werden müssen, damit so früh wie möglich die Rechte und Freiheiten der betroffenen Personen sichergestellt werden können (Art. 42 Abs. 1). Zweites impliziert, dass die Personendaten mit den Mitteln und gemäss den Modalitäten, die standardmässig das höchstmögliche Schutzniveau sicherstellen, bearbeitet werden müssen (Art. 42 Abs. 2).
b) Vor Beginn einer neuen Datenbearbeitung, bei der ein höheres Risiko für die Rechte und Freiheiten der betroffenen Personen besteht, ist die oder der Verantwortliche für die Datenbearbeitung gehalten, vorgängig eine **Datenschutz-Folgenabschätzung** durchzuführen (Art. 43). Das Ziel dieser Folgenabschätzung ist doppelter Natur: Mit ihr wird angestrebt, den für die Datenbearbeitung zuständigen Verantwortlichen dazu zu verhelfen, einerseits Datenbearbeitungen zu tätigen, die die Privatsphäre respektieren, und andererseits die Einhaltung des Datenschutzgesetzes nachzuweisen.
c) Im Falle eines Verstosses gegen den Datenschutz muss die oder der Verantwortliche für die Bearbeitung den **Verstoss** so bald wie möglich der Behörde für Öffentlichkeit und Datenschutz und in schwereren Fällen direkt der betroffenen Person (Art. 45 und 46) **melden**.
d) Öffentliche Stellen, die regelmässig und systematisch Personendaten bearbeiten, müssen eine **Ansprechperson für Datenschutz** (Art. 47) ernennen. Diese Person hat die Aufgabe, die Verantwortlichen für die Datenbearbeitung juristisch in deren Tätigkeit zu begleiten, und, falls nötig, die Verbindung zur Behörde für Öffentlichkeit und Datenschutz herzustellen. Die Ansprechperson für Datenschutz übernimmt jedoch **keinerlei persönliche Verantwortung** für die Bearbeitung, die sie begleitet.

1.3.5 Aufsichtsbehörden im Bereich Datenschutz

1.3.5.1 Gemäss geltendem Recht hat die Aufsichtsbehörde für 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, indem sie sie dazu einlädt, die festgestellten Mängel zu beheben. Die Empfehlungen haben aber keinen verbindlichen Charakter. Falls die öffentliche Stelle der Empfehlung nicht Folge leistet, hat die

Aufsichtsbehörde aber die Möglichkeit, die Sache gerichtlich beurteilen zu lassen (s. Art. 22a DSchG).

1.3.5.2 Der Vorentwurf **stärkt die Position** der Aufsichtsbehörde. Es handelt sich dabei um eine klare Verpflichtung, die sich unmittelbar aus Artikel 47 Abs.2 der Richtlinie (EU) 2016/680 und Art. 15 § 2 Buchstaben a) und d) der Vereinbarung SEV 108+ ergibt. Genau gleich wie die Aufsichtsbehörden beim Datenschutz in Europa, der Eidgenossenschaft und anderen Kantonen muss die Behörde für Öffentlichkeit und Datenschutz nicht nur über ein Recht zur Untersuchung verfügen, sondern auch über die Möglichkeit zu **intervenieren**, was es ihr, falls die Vorschriften des Datenschutzes nicht eingehalten werden, ermöglicht, erforderlichenfalls Massnahmen zu ergreifen.

1.3.5.3 Um auf jeden Fall zu verhindern, dass sich **eine zu grosse Macht** in den Händen einer Person **konzentriert**, sieht der Vorentwurf vor, dass die oder der Beauftragte für den Datenschutz nur über eine **Weisungsbefugnis** verfügt, die es ihr oder ihm ermöglicht, von den Verantwortlichen für die Datenbearbeitung, die ihrer Verpflichtung nicht nachkommen, zu verlangen, die erforderlichen Massnahmen zu ergreifen, damit das Gesetz eingehalten wird (Art. 57). Die Kompetenz, eine **verbindliche Entscheidung** in Sachen Datenschutz auszusprechen, kommt schliesslich der kantonalen Öffentlichkeits- und Datenschutzkommission zu (Art. 58). Letztere ist ein **multidisziplinär zusammengesetztes Gremium**, das vom Grossen Rat gewählt wird und dem eine Juristin/ein Jurist, eine Fachperson aus dem Gesundheitswesen, eine Spezialistin/ein Spezialist der Informations- und Kommunikationstechnologien und eine Fachperson aus dem Medienbereich angehören.

1.4 Folgen des Vorentwurfs

a) Veränderungen im Verwaltungshandeln

1.4.1 Die Stärkung der Rechte der betroffenen Personen und die Verpflichtungen zulasten der Verantwortlichen für die Bearbeitung wird sich zwangsläufig auf die Funktionsweise der öffentlichen Stellen **auswirken**. Die tatsächlichen Auswirkungen dieser Änderungen auf das Verhalten der betroffenen Personen und auf die öffentlichen Stellen ist im aktuellen Stadium jedoch schwierig vorherzusehen. Wenn man den ersten Reaktionen seit dem Inkrafttreten der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 Glauben schenken darf, ist **eine eigentliche Umwälzung** bei den Verwaltungspraktiken jedoch eher **unwahrscheinlich**.

1.4.2 Im Gegensatz zu dem, was nach dem Inkrafttreten des DSchG im Jahr 1995 eintrat, werden die Organe des Gemeinwesens ihre Funktionsweise nicht umfassend überprüfen müssen, um sich den neuen Anforderungen im Bereich 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 25 Jahre Erfahrung in diesem Bereich, nur zu **punktuellen Veränderungen** führen. Weiter dürften gemäss dem **risikobasierten Ansatz** vor allem die Verantwortlichen für die Bearbeitung, die regelmässig grosse Mengen von Daten bearbeiten, am meisten davon

betroffen sein. Jedoch sind es gerade Letztere, welche üblicherweise über die hierfür erforderlichen technischen und personellen Ressourcen verfügen.

b) Finanzielle und personelle Konsequenzen

1.4.3 Soweit der Vorentwurf im Wesentlichen zu einer **Anpassung an übergeordnetes Recht** führt, was ohnehin zwingend ist, hat er als solcher keine direkten finanziellen und personellen Folgen. Aber Tatsache ist, dass die verschiedenen Organe des Staates wohl punktuell **auf ihre verfügbaren Ressourcen zurückgreifen** müssen, um sich an die neuen Anforderungen des Vorentwurfs anzupassen, namentlich wenn es darum geht, eine Datenschutz-Folgenabschätzen zu erstellen oder eine korrekte Nachbearbeitung eines Zwischenfalls im Bereich des Datenschutzes sicherzustellen. Im Weiteren bedeutet die gesetzliche Formalisierung der Rolle der **Ansprechperson für Datenschutz** für die betroffenen Verwaltungseinheiten, dass diese in ihren Einheiten die erforderlichen Ressourcen finden, um dieser Aufgabe nachzukommen.

1.4.4 Aus technischer Sicht ist zu beachten, dass der Kanton Freiburg im Rahmen seiner Strategie «Verwaltung 4.0» den Weg der Digitalisierung eingeschlagen hat. In diesem Zusammenhang wurden bereits einige Initiativen ins Leben gerufen, um die Verwaltung, Zentralisierung und Standardisierung bestimmter Datenkategorien besser zu managen (siehe die Projekte des kantonalen Bezugssystems für Referenzdaten). Die Revision des Gesetzes im Zusammenhang mit der Umsetzung seiner Strategie «Verwaltung 4.0» wird unweigerlich zu **neuen technischen Anforderungen** führen, insbesondere hinsichtlich der Rückverfolgbarkeit der Daten. Diese Anforderungen stehen jedoch in vollem Einklang mit den Zielen der Standardisierung und Konzentration der derzeit am Werk befindlichen IT-Landschaften, die zu einer tiefgreifenden Überarbeitung der Informationsverarbeitung innerhalb des Staates führen. Es ist daher völlig normal, den **Datenschutz einzubeziehen**. Um einer möglichen Zunahme der Rückverfolgbarkeitsgesuche gerecht zu werden, müssen in einigen Bereichen Prozesse automatisiert werden, um die manuelle Verarbeitung zu reduzieren und die gesetzlichen Fristanforderungen einzuhalten. Die Implementierung dieser automatisierten Prozesse erfordert **Aufwand und auch Anpassungszeit**. Es wird in der Tat notwendig sein, die erforderlichen Umgebungen (Ereignisprotokollierung, Protokollierung von Verbindungen, Aufzeichnung des Datenverbrauchs usw.) für die Beantwortung von Gesuchen zu erstellen oder zu parametrisieren. Dies kann nur unter Berücksichtigung der verwaltungsinternen Budgetzyklen und der Veralterung einiger Systeme erfolgen, die ersetzt werden müssen. In diesem Zusammenhang werden mittel- bis langfristig indirekt mit der Anwendung des Gesetzes verbundene Kosten erwartet, die zum gegenwärtigen Zeitpunkt schwer quantifizierbar sind.

1.4.5 Wie der Bundesrat in seiner Botschaft zur Totalrevision des DSG (vgl. BBl 2017 6941, S. 7170 f.) ausgeführt hat, werden die vorgenommenen Änderungen insbesondere im Bereich der Überwachung erhebliche Auswirkungen haben. Weil der Vorentwurf eine ganze Reihe

neuer Aufgaben für die ÖDSB sowie für die oder den Datenschutzbeauftragte/-n vorsieht (Unterstützung der für die Verarbeitung Verantwortlichen bei den von ihnen durchzuführenden Risiko- und Folgenabschätzungen und im Rahmen von Meldungen von Bearbeitungstätigkeiten, Kontrolle der eingerichteten technischen und organisatorischen Prozesse und IT-Plattformen, Management von Sicherheitslücken, Sensibilisierung der kantonalen und kommunalen Stellen für den Datenschutz, Ermittlungsverfahren und Verkündung von Entscheidungen). Diese neuen Aufgaben kommen zu der **zusätzlichen Arbeitsbelastung** hinzu, mit der die Behörde im Rahmen der Digitalisierung des Staates, in dem sie unmittelbar tätig ist, bereits seit mehreren Jahren konfrontiert ist, indem sie in mehreren Arbeitsgruppen zu verschiedenen Projekten in diesem Bereich teilnimmt, entweder indirekt durch die zahlreichen Beratungen in diesem Bereich sowie im Rahmen von Vernehmlassungen im Bereich der Gesetzgebung. Seit ihrer Schaffung im Jahr 1994 wurden die für den Datenschutz aufgewendeten Personalressourcen der ÖDSB jedoch nur einmal im Jahr 2009 aufgestockt, indem 0,5 VZÄ für eine Juristenstelle gewährt wurden. Diese neue Stelle kam zu derjenigen der/des Datenschutzbeauftragten, die auf den 1. Januar 2020 von 0,5 auf 0,8 VZÄ aufgestockt wird, hinzu. Bisher ist die Behörde von einer **chronischen Arbeitsüberlastung** betroffen, die es nicht nur äußerst schwierig macht, ihre Aufgaben täglich auszuführen, sondern manchmal auch zu Verzögerungen bei der Realisierung bestimmter wichtiger IT-Projekte führt. Aus diesem Grund ist eine Aufstockung der **ÖDSB-Personalressourcen** zum gegenwärtigen Zeitpunkt unvermeidlich. Der genaue Ressourcenbedarf wird in Zusammenarbeit mit dem Amt für Personal und Organisation im Rahmen der Umsetzung des Gesetzes genauer analysiert.

In diesem Zusammenhang ist darauf hinzuweisen, dass die Bereitstellung ausreichender Mittel für die Aufsichtsbehörde ein wichtiges Element sowohl für den Angemessenheitsbeschluss und die Umsetzung des Schengen - Besitzstands als auch für die künftige Ratifizierung durch die Schweiz Konvention SEV 108+ (Artikel 42 Ziffer 4 der Richtlinie (EU) 2016/680, Artikel 52 Ziffer 4 der Verordnung (EU) 2016/679 und Artikel 15 Ziffer 6 des aktualisierten Übereinkommens SEV 108+). Die folgende Tabelle zeigt die derzeitige Personalbesetzung der ÖDSB und die Besetzung, die sie für erforderlich hält, um die ihr gesetzlich übertragenen Aufgaben erfüllen zu können.

In diesem Zusammenhang ist darauf hinzuweisen, dass die Bereitstellung ausreichender Mittel für die Aufsichtsbehörde ein wichtiges Element sowohl für den Angemessenheitsbeschluss und die Umsetzung des Schengen - Besitzstands als auch für die künftige Ratifizierung durch die Schweiz Konvention SEV 108+ (Artikel 42 Ziffer 4 der Richtlinie (EU) 2016/680, Artikel 52 Ziffer 4 der Verordnung (EU) 2016/679 und Artikel 15 Ziffer 6 des aktualisierten Übereinkommens SEV 108+).

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 rechtlichen Ordnung 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 Vorentwurf wie das geltende Gesetz vor, dass die ***Grundrechte*** der betroffenen Personen garantiert werden, ohne indes zu präzisieren, welche das genau sind.

Art. 2, Persönlicher Geltungsbereich

1. Der persönliche Geltungsbereich des Vorentwurfs basiert im Wesentlichen auf dem geltenden Gesetz.

a) Er gilt zunächst für alle Organe, die auf kantonaler, kommunaler und interkommunaler Ebene der Zuständigkeit **des Gesetzgebers, der Exekutive und der Judikative** unterliegen, einschliesslich der öffentlich-rechtlichen Anstalten (mit oder ohne Rechtspersönlichkeit) und der Körperschaften kantonalen öffentlichen Rechts (z. B. Baulandumlegungsgenossenschaften, Bodenverbesserungskörperschaften, öffentlich-rechtlich Gesellschaften, die in Form einer Aktiengesellschaft oder einer Genossenschaft gegründet wurden), hinzuzufügen sind auch spezielle Institutionen wie die Kantonalbank oder der Justizrat.
b) Er gilt auch für gewisse natürliche und juristische Privatpersonen, wenn sie beauftragt sind, **öffentliche Aufgaben zu erfüllen**. Die Formel verwendet diejenige in Art. 2 Bst. d VRG. Das Gesetz gilt nur für den Teil ihrer Tätigkeit, der zur fraglichen öffentlichen Aufgabe gehört. Personen, die öffentlich-rechtliche Aufgaben wahrnehmen sind etwa Notare, in öffentlichen Spitälern angestellte Ärzte. Zu den angesprochenen Instituten kann man den Freiburger Tourismusverband oder GastroFribourg im Bereich der Ausbildung künftiger Gastwirtinnen und Gastwirte zählen.
c) Gemäss Artikel 3 Abs. 2 des KSG sind die **Pfarreien, Kirchgemeinden und andere kirchliche Institutionen** Körperschaften des öffentlichen Rechts. Aus diesem Grund sind sie ebenfalls Teil des Geltungsbereichs des geltenden Gesetzes. Der Vorentwurf ermöglicht indessen der Kirche, ihre eigenen einschlägigen Bestimmungen anzupassen und ihre eigenen Aufsichtsbehörden einzurichten (s. Art. 2 Abs. 1 Bst. c und Art. 48 Abs. 3). In diesen Fällen

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

wird die kantonale Aufsichtsbehörde für Datenschutz die **Oberaufsicht** über die kirchliche Aufsichtsbehörde für Datenschutz übernehmen.

2. Zusätzlich zu den Fällen nach Absatz 1 führt der Vorentwurf in Absatz 2 die Möglichkeit für die kantonale Aufsichtsbehörde für Datenschutz ein, im Rahmen einer Zusammenarbeitsvereinbarung mit der oder dem Eidgenössischen Datenschutzbeauftragten (EDÖB) oder mit einer anderen Aufsichtsbehörde im Bereich des Datenschutzes **bei anderen Institutionen mit Sitz im Kanton** tätig zu werden. So könnte die oder der EDÖB im Falle eines Verdachts der Verletzung der Datenschutzbestimmungen durch ein Unternehmen des Kantons Freiburg die kantonalen Behörde ersuchen, vor Ort Untersuchungen beim Unternehmen aufzunehmen, insbesondere wenn das Unternehmen enge Beziehungen zum Staat oder zu einer Gemeinde pflegt. Die grosse Nähe der kantonalen Behörde und ihre sehr gute Kenntnis der Lage vor Ort dürfte in diesem Fall den Austausch und die Möglichkeiten zur Lösungsfindung vereinfachen. Zu bemerken ist auch, dass die **Stärkung der Zusammenarbeit** zwischen den verschiedenen Datenschutzaufsichtsbehörden eines der Ziele der gesamten Revision des Datenschutzes darstellt (s. Art. 60 ff. der Verordnung (EU) 2016/679; Art. 50 der Richtlinie (EU) 2026/680 und Art. 17 der Konvention SEV 108+).

Art. 3, Materieller Anwendungsbereich

1. Im Landesrecht wird der Datenschutz in **allgemeiner Form** in einem Rahmengesetz über den Datenschutz und in **spezifischer Form** in verschiedenen sektoriellen Reglementierungen geregelt, die dazu dienen, gewisse fachlich spezifische Sachverhalte zu normieren. Per definitionem regelt die Spezialgesetzgebung die Frage des Datenschutzes im betreffenden Bereich, in dem die Institution datenbearbeitend tätig ist, nicht **abschliessend,** sondern nur **ergänzend**.

2. Um beim Datenschutz das **Auftreten von Lücken zu verhindern**, sieht der Vorentwurf vor, dass das Gesetz in jedem Fall mindestens **ergänzend** zur Spezialgesetzgebung anwendbar ist (Abs. 2). Das bedeutet, dass die spezialgesetzlichen Regelungen weiter dazu dienen könnten, die generellen Regelungen zu ergänzen oder in den Bereichen, mit denen sie sich befassen, sogar von ihnen abzuweichen, aber dass die generellen Regelungen immer auf Situationen und Fragen anwendbar bleiben, die nicht in der Spezialgesetzgebung behandelt werden. Diese Regelung lehnt sich an § 2 Abs. 3 des kantonalen Gesetzes von Basel-Stadt über die Information und den Datenschutz vom 9. Juni 2010 (Gesetz über die Information und den Datenschutz [IDG]; 153.260) an.

3. Infolge dieser Änderung sieht der Vorentwurf **keine feste Ausnahme** im Bereich der materiellen Anwendung des Gesetzes vor (Vergleich: Art. 2 Abs. 2 DSchG). Daraus resultiert namentlich:
a) Die feste Ausnahme bei **den Verhandlungen** des Grossen Rates, der Gemeindeversammlungen oder der Generalräte, der Bürgerversammlungen und ihrer Kommissionen (Art. 2 Abs. 2 Bst. a) entfällt. Die entsprechende Ausnahme wurde damals mit dem **Grundsatz der**

Geheimhaltung, der im Staat vorherrschte, begründet. Dieser Grundsatz wurde jedoch seither weitgehend ausgehebelt, namentlich mit der Annahme des Gesetzes vom 9. September 2009 über die Information und den Zugang zu Dokumenten (InfoG; RSF 17.5), das den **Grundsatz der Transparenz** einführte.[4] Im Weiteren wurde diese Regelung in der Lehre kritisiert und überlebte nur in einer Minderheit von Kantonen (GE, VD, NE und JU; OW, NW, GL und BE). Die Aufhebung scheint daher für die betroffenen Organe durchaus sinnvoll zu sein. Was die Anwendung im Bereich des Zugangs zu den eigenen Daten und andere damit verbundene Rechte betrifft, ist es **in berechtigten Fällen** immer noch möglich, ihre Ausübung einzuschränken oder zu verweigern, jedoch auf der Grundlage einer ordentlichen und begründeten Interessenabwägung.
b) Die feste Ausnahme bei den laufenden Zivil-, Straf- und Verwaltungs**verfahren** (Art. 2 Abs. 2 Bst. b) wird durch zwei **zielgerichtetere** Ausnahmen ersetzt, die das korrekte Funktionieren der Justiz und die Rechte der betroffenen Personen in diesem Bereich gewährleisten. Die erste Ausnahme hat zum Ziel, **eine gleichzeitige Anwendung** der Regelungen des Gesetzes über den Datenschutz und der Verfahrensgarantien in den Prozessordnungen **zu verhindern**; sie sieht vor, dass die Rechte und Ansprüche der betroffenen Personen im Rahmen der laufenden Verfahren ausschliesslich dem anwendbaren Verfahrensrecht unterliegen (Art. 32). Die zweite Ausnahme wurde mit dem Ziel eingeführt, **die Unabhängigkeit der Justiz** zu garantieren; sie erklärt, dass die Aufsichtsbehörde für Datenschutz **nicht zuständig** sei, die richtige Anwendung des Gesetzes bei Datenbearbeitungen zu kontrollieren, die von öffentlichen Stellen in Ausübung ihrer richterlichen Funktionen durchgeführt werden (Art. 62).

4. Um keine Wettbewerbsverzerrungen zu verursachen, sieht der Absatz 3 gleich wie im geltenden Gesetz (Art. 2 Abs. 2 Bst. c DSchG) vor, dass die kantonalen Bestimmungen im Zusammenhang mit dem Datenschutz bei Organen im öffentlichen Bereich nicht anwendbar sind, wenn sie Tätigkeiten in einer **Situation des wirtschaftlichen Wettbewerbs** ausüben und nicht als eine mit hoheitlicher Gewalt ausgestattete Einrichtung handeln. Im Gegensatz zum geltenden Gesetz sieht der Vorentwurf vor, dass die Aufsicht in diesem Fall bei der Kantonalen Aufsichtsbehörde für Datenschutz und nicht beim der oder dem Beauftragten für Datenschutz des Bundes verbleibt. Auf diese Weise **wird verhindert**, dass beim Datenschutz ein einziges und gleiches Organ simultan **zwei verschiedenen Behörden** unterstellt ist. Man findet die gleiche Regelung namentlich in Artikel 4 Abs. 2 Bst. a, 2. Satz des bernischen Datenschutzgesetzes vom 19. Februar 1986 (KDSG; BSG 152.04).

Art. 4, Definitionen

Die Mehrheit der in diesem Artikel enthaltenen Definitionen wurde **wörtlich oder fast wörtlich** aus dem Entwurf zur Totalrevision des Bundesgesetzes über den Datenschutz

[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.

übernommen. Wir können uns daher generell auf die diesbezüglichen Erläuterungen in der Botschaft des Bundesrats berufen (s. BBI 2017 6941, S. 7019 ff.) und dazu die folgenden Präzisierungen anbringen:

a) Im Vergleich mit dem Totalrevisions-Entwurf des Bundes führt der Vorentwurf zusätzlich den Begriff «***gemeinsamer Personenidentifikator***» ein (Bst. d). Es handelt sich um eine Art von Superdaten, die eine bestimmte Gesamtheit von Attributen zu Personen zusammenfassen und eine oft komplexe und detaillierte Darstellung der Person ermöglichen. Eine kürzlich erschienene Studie, die im Auftrag des Bundesamtes für Justiz (BJ) und des EDÖB erstellt wurde, zeigte, dass bei Abwesenheit oder Fehlen von angemessenen Schutzmassnahmen die Nutzung solcher Identifikatoren **reelle Risiken** für die Rechte der betroffenen Personen darstellen können. Tatsächlich ermöglichen sie es, dass Daten, die in verschiedenen Registern gehalten werden, von nicht befugten Personen oder Hackern schneller und einfacher verknüpft werden können, was es ermöglicht, ein detailliertes Profil einer Person zu erstellen.[5] Dieses Risiko steigt mit einer zunehmenden Anzahl von Institutionen, die auf denselben Identifikator Zugriff haben, namentlich weil die angewendeten Sicherheitsstandards zwischen den verschiedenen Organen, die ihn nutzen (Kantonsverwaltung, Gemeindeverwaltung, Schule, Spitäler usw.), variieren können. Dies ist der Grund dafür, dass im Vorentwurf die Schaffung solcher Identifikatoren der Einhaltung spezifischer Regeln unterworfen wird (Art. 5 Abs. 1). Wie aus der gegebenen Definition ersichtlich ist, finden diese Regelungen bislang nur bei gemeinsamen Personenidentifikatoren, die **von mehreren Institutionen geteilt werden**, Anwendung (so etwa der kantonale Personenidentifikator im Sinne von Art. 14 E-GovSchG). Diese Präzisierung zielt darauf ab, sektorielle Kennungen auszuschliessen, die nur für einen Zweck gebraucht werden können und die es ermöglichen, Personen, die mit diesem Organ in Kontakt stehen, leichter zu klassifizieren. Die vorgeschlagene Definition ist eine Adaption von Art. 4 Bst. i des «Loi sur l'information du public, l'accès aux documents et la protection des données personnelles» des Kantons Genf vom 5. Oktober 2001 (LIPAD; RSG A 2 08).

b) Auch wenn die aktuelle Definition der Bedeutung von « ***Datenbearbeitung***» bewusst beispielhaft und **sehr breit** angelegt ist, um alle Operationen mit Personendaten abdecken zu können, wurde sie doch mit den Konzepten der **Datenverknüpfung** und der **Externalisierung** ergänzt (Bst. e). In Anbetracht des Umfangs, den diese Bearbeitungsarten in der Informationsgesellschaft mit sich bringen, ist es wichtig, in Erinnerung zu rufen, dass es sich um **vollständige** Datenbearbeitungen handelt, die den Anforderungen dieses Gesetzes unterworfen sind. Unter der dem Verknüpfen von Daten versteht man eine Operation, die dazu dient, neue Informationen zu generieren, indem existierende Daten, die in verschiedenen definierten Datenquellen vorhanden sind, miteinander verknüpft werden (s. für ein Freiburger Beispiel Artikel 137 Abs. 3 DStG). Was die Externalisierung betrifft, bezieht

[5] BASIN David, *Risk Analysis on Different Usages of the Swiss AHV Number – Evaluation on behalf of the Federal Office of Justice and the Federal Data Protection and Information Commissioner*, Zürich 2017. Dokument einsehbar unter folgendem Link:
https://www.bj.admin.ch/bj/de/home/publiservice/publikationen/externe/2017-09-27.html.

sich der Begriff auf die Inanspruchnahme eines Dritten zur Bearbeitung oder das Hosting der Daten. Sie umfasst insbesondere den Einsatz von Lösungen für das ***Cloud Computing***. Im Gegenzug verzichtet der Vorentwurf auf die Definition **der Bekanntgabe von Daten**. Soweit es sich um einen Bearbeitungstyp unter anderen handelt, macht es keinen Sinn, diese Definition, die man im Übrigen weder in der Konvention SEV 108+ noch in der übrigen Gesetzgebung der EU vorfindet, weiter aufrecht zu erhalten.

c) Wie im Entwurf des Bundesrates (Art. 4 Bst. f E-DSG) und gemäss den Anforderungen der EU-Gesetzgebung (Art. 3 Ziffer 4 der Richtlinie (EU) 2016/680 und Art. 4 Ziffer. 4 der Verordnung (EU) 2016/679) führt der Vorentwurf den Begriff des **Profiling** ein. Dabei handelt es sich um einen Bearbeitungstyp, der als besonders einschneidend zu bezeichnen ist. Er besteht darin, absichtlich bestimmte persönliche Merkmale hervorzuheben oder vorherzusagen, die für ein Individuum bedeutend sind, namentlich mit dem Zweck, der betreffenden Person eine Sonderbehandlung zuteilwerden zu lassen. Dies ist der Grund dafür, dass das Profiling den gleichen Bedingungen unterworfen wird wie die Bearbeitung **besonders schützenswerter Personendaten**.

d) Analog zum Entwurf des Bundesrates und der Konvention SEV 108+ fällt im Vorentwurf der Begriff der **«*Datensammlung***» weg, da dieser angesichts der allgegenwärtigen Natur der Daten veraltet ist. Er wird generell ersetzt durch den weiter gefassten und dynamischeren Ausdruck der «***Bearbeitungstätigkeiten***». Aus diesem Grund wird der Begriff Register der Datensammlungen, den man derzeit in Art. 21 DSchG findet, im Vorentwurf zum «Register der Bearbeitungstätigkeiten» (Art. 40), und der «Verantwortliche der Datensammlung», der im Art. 4 Bst. g des DSchG erwähnt wird, wird im Vorentwurf zum «Verantwortlichen für die Bearbeitung» (Art. 4 Bst. g). Insgesamt gesehen sind diese Änderungen vor allem **terminologischer Art** und sollten keine besonderen spezifischen praktischen Auswirkungen haben.

e) Der Vorentwurf verzichtet auf die Definition von «***Verletzung der Datensicherheit***», so wie sie im Entwurf des Bundesrats (Art. 22 E-DSG) und im Europäischen Recht (Art. 3 Ziffer 11 der Richtlinie (EU) 2016/680 und Art. 4 Ziff. 11 der Verordnung (EU) 2016/679) figuriert. In Anbetracht ihres Inhalts ist eine solche rechtliche Definition **überflüssig**. Aufgrund ihres vagen und allgemeinen Charakters bietet sie keine sinnvolle Klärung, die über die normale Bedeutung hinausgeht. In diesem Kontext scheint es besser, die Präzisierung des Begriffs der Rechtsprechungspraxis oder der Lehre zu überlassen.

f) Angesichts der zentralen Rolle der Umsetzung des Datenschutzes wird vorgeschlagen, eine Definition für «***Register der Bearbeitungstätigkeiten***» aufzunehmen. Dieses stellt zugleich ein Werkzeug zur Sicherung der **Transparenz** und der **Governance** dar. Dies setzt namentlich voraus, dass die oder der Verantwortliche für die Datenbearbeitung in der Lage ist, für jeden Vorgang, in dem Daten bearbeitet werden, das Folgende festzulegen: welche Personenkategorien betroffen sind, welche Daten bearbeitet werden, mit welchem Zweck und gemäss welcher Modalitäten bearbeitet wird, wer Zugriff auf die Daten hat, wie lange sie aufbewahrt werden, welche Sicherheitsmassnahmen ergriffen werden usw.

2.2 Abschnitt 2, Grundsätze für das Bearbeiten von Personendaten

2.2.1 Abschnitt 2.1, Allgemeine Bedingungen *der Rechtmässigkeit der Bearbeitung*

Art. 5, Gesetzliche Grundlage

1. Die Bearbeitung von Personendaten durch öffentliche Organe stellt einen Akt staatlichen Handelns dar und ist dem **Legalitätsprinzip** unterworfen. Grundsätzlich ermächtigt nur eine Rechtsgrundlage ein Organ zur Bearbeitung von Personendaten.

2. Die Antwort auf die Frage nach dem Präzisionsgrad der gesetzlichen Bestimmung und auf welchem Niveau sie zu situieren ist, hängt ab von der Gefahr, dass Rechte der vom Bearbeitungsvorgang betroffenen Personen verletzt werden.

3. Der Vorentwurf passt sich an die Praxis des Bundes und aller schweizerischen Kantone an und stellt **strengere Anforderungen an die Rechtmässigkeit der Bearbeitung von Personendaten, die ein erhöhtes Risiko** für die persönlichen Rechte **darstellt** (besonders schützenswerte oder heikle Daten, Profiling, Abrufverfahren, Erstellung von gemeinsamen Personenidentifikatoren usw.). Dieser Bearbeitungstyp ist nur dann rechtmässig, wenn er in einem Gesetz im formalen Sinne explizit bewilligt wird (direkte gesetzliche Grundlage) oder wenn es für die Erfüllung einer Aufgabe, die in einem Gesetz im formalen Sinne klar definiert wird, unerlässlich ist (indirekte gesetzliche Grundlage).

4. Angesichts der Praxis der Aufsichtsbehörde, die für sich bis jetzt immer in Anspruch nahm, dass für diese Bearbeitungstypen eine formale gesetzliche Grundlage erforderlich sei, auch ohne eine solche ausdrückliche Anforderung im Gesetz, und angesichts dessen, dass die Praxis in der öffentlichen Verwaltung gut aufgenommen wird, sollte diese Änderung in der Praxis keine nennenswerten Einflüsse haben. Es ist jedoch zu überprüfen, ob bei den laufenden Bearbeitungen diese Vorschrift eingehalten wird.

5. Ausnahmsweise ist eine gesetzliche Grundlage nicht nötig, wenn eine Datenbearbeitung, insbesondere eine Datenübertragung, unerlässlich ist, um die erheblichen Interessen der betroffenen Person oder eines oder einer 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 und möglicherweise sogar polizeiliche Notfälle beschränken.

Art. 6, Zustimmung

1. Die Zustimmung der betroffenen Person stellt im Datenschutzrecht die wichtigste **aussergesetzliche Begründung** dar. Grundsätzlich liegt keine Verletzung der Rechte der betroffenen Person vor, wenn Letztere einwilligt, dass ihre persönlichen sie betreffenden Daten gesammelt und zu gewissen Zwecken bearbeitet werden. Damit die Zustimmung gültig ist, muss sie **aufgeklärt, frei und explizit** (Abs. 1) erfolgen. Das bedeutet einerseits, dass die Person, die zustimmt, richtig und in transparenter und verständlicher Art darüber

informiert worden sein muss, was das Ziel und die Modalitäten der Datenbearbeitung sind, und andererseits, dass die Person auch nicht zur Einwilligung einer Datenbearbeitung gezwungen wird, die vom Gesetz nicht vorgesehen ist. Die Zustimmung muss im Übrigen von einer positiven Handlung der betroffenen Person begleitet sein, was eine «*standardmässige*» Zustimmung ausschliesst. Ob eine Einwilligung vorliegt, hat der Verantwortliche für die Datenbearbeitung zu prüfen, der auch festhalten sollte, dass die Person in die Bearbeitung ihrer spezifischen Daten eingewilligt hat.

2. Es ist jedoch zu beachten, dass die Auswirkung der Zustimmung **im öffentlichen Recht** grundsätzlich **geringer** ist als im Privatrecht. In der Beziehung der öffentlichen Verwaltung zu den Bürgerinnen und Bürgern bleibt die wichtigste unterstützende Tatsache aber vor allem die der Rechtmässigkeit der Datenbearbeitung[6]. Die Datensammlung durch eine öffentliche Stelle, die vom Gesetz nicht verlangt wird, müsste aus diesem Grund für Spezialfälle und begründete Fälle reserviert bleiben. Im Weiteren müsste die Bürgerin und der Bürger nach Möglichkeit immer **über eine Alternative** zur Zustimmung verfügen können und dürfen, jedenfalls nicht benachteiligt werden, wenn sie oder er sich weigert, sie zu erteilen. Dies ist der Grund dafür, dass der Vorentwurf präzisiert, dass jedes Gesuch um Zustimmung zur Datenbearbeitung, die im Gesetz nicht vorgesehen ist, von einem sehr klaren und sichtbaren Hinweis auf deren **fakultativem Charakter** begleitet sein muss (Abs. 2).

Art. 7, Zweckbindung

1. Das Prinzip der Zweckbindung beinhaltet drei Bereiche (Abs. 1):
a) Erstens impliziert es, dass die Personendaten nicht gesammelt und bearbeitet werden dürfen, ohne dass dafür im **Vorhinein** ein Zweck **definiert** worden ist, d. h. er darf weder vage, ungenau noch unbestimmt sein (**Zweckbindungsprinzip**).
b) Zweitens erfordert dies, dass der Zweck und die Methoden der Bearbeitung sowie die Kategorien der bearbeiteten Daten nach dem Grundsatz von Treu und Glauben für die betroffenen Personen insgesamt erkennbar sein müssen.
c) Schliesslich müssen die vorgesehenen Bearbeitungen eine **rechtmässige** Zweckbindung verfolgen, was Bearbeitungen ausschliesst, die nicht auf seriösen, objektiven Motiven beruhen, die keinen Sinn machen und mit denen kein Zweck verfolgt wird. Es handelt sich hierbei deshalb um eine Konkretisierung des verfasssungsmässigen Prinzips des **Verbots der Willkür** im Datenschutzrecht.

2. Das Prinzip der Zweckbindung steht in engem Zusammenhang mit der anerkannten Befugnis der Person, die sie betreffenden Informationen **zu beherrschen**. Die betroffene Person kann diese Befugnis nutzen, indem sie einer Nutzung der Daten zu neuen Zwecken zustimmt. Die Möglichkeit wird besonders interessant im Rahmen der Umsetzung der **E-Government**-Strategie des Staates Freiburg, welche die Möglichkeit für die Bürgerinnen und

[6] FASNACHT Tobias, *Die Einwilligung im Datenschutzrecht: Vorgaben einer völker- und verfassungsrechtlich konformen Ausgestaltung der datenschutzrechtlichen Einwilligung im schweizerischen Recht*, Dissertation Freiburg, Zürich/Basel/Genf 2017, S. 91.

Bürger vorsieht, sich für die Verwendung ihrer Daten zu entscheiden, um Dienstleistungen gemäss deren Wünschen in Anspruch nehmen zu können.

Art. 8, Verhältnismässigkeit

1. Ein zentrales Element des Datenschutzrechts stellt das Prinzip der Verhältnismässigkeit dar, das in **jeder Phase** der Datenbearbeitung, von der Phase der Sammlung bis zu derjenigen der Löschung oder Archivierung, wichtig ist. Es betrifft nicht nur **die Daten**, sondern auch **die Wahl der Mittel und der Methoden** zu deren Bearbeitung.

2. Das Prinzip der Verhältnismässigkeit impliziert, dass die bearbeiteten Daten und Bearbeitungsmethoden im Verhältnis zum Zweck der Bearbeitung **nicht übermässig sein dürfen**. Dies bedeutet einerseits, dass nur die Daten bearbeitet werden dürfen, die objektiv erforderlich sind, um den definierten Zweck zu erreichen (**Prinzip der Datenminimierung)**. In Übereinstimmung mit dieser Regel ist es nicht erlaubt, Personendaten zu bearbeiten, die für den zu verfolgenden Zweck nicht relevant sind (z. B. die AHV-Nr. um Parkplatzgebühren zu entrichten). Andererseits müssen die gewählten Bearbeitungsmethoden **möglichst wenig invasiv und eingreifend** in die Rechte der betroffenen Personen sein.

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 öffentlichen Stellen gespeichert werden, **nicht** unter allen Umständen **mit der Realität übereinstimmen**. Obgleich es ein mehr oder weniger konstantes Ziel bleiben muss, ist die Verpflichtung zur Gewährleistung der Richtigkeit und zur Aktualisierung der Daten vor allem eine Verpflichtung 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 heiklen Charakter ab.

Art. 10, Aufbewahrungsfrist

1. Die Datenaufbewahrung darf **die erforderliche Dauer für die Zwecke, für die sie gespeichert worden sind,** nicht überschreiten. Ist der Zweck der Datensammlung erreicht, dürfen sie nicht weiter aufbewahrt oder gespeichert bleiben, sondern müssen gelöscht oder anonymisiert werden. Dies hat für die Verantwortlichen der Datensammlung zur Folge, dass sie in regelmässigen Abständen prüfen müssen, ob die Daten in ihrem Besitz für die angestrebten Zwecke noch relevant sind. Angesichts der technologischen Entwicklungen und der bestehenden fast unbeschränkten Datenspeicherkapazitäten macht der Vorentwurf aus dieser Regel ein Prinzip der Rechtmässigkeit der Bearbeitung.

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 die Rechte der betroffenen Personen geschützt

sind. Die Vorschriften über die Archivierung bleiben vorbehalten (s. Art. 22 des Vorentwurfs).

Art. 11, Besondere Sorgfaltspflicht

Die besondere Sorgfaltspflicht, die für eine Datenbearbeitung, welche für die persönlichen Rechte erhebliche Risiken birgt, verlangt wird, ist eine **freiburgische Spezialität,** die in keinem anderen Datenschutzgesetz in der Schweiz existiert. 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 situationsgerecht ergriffen werden sollen.

2.2.2 Abschnitt 2.2, Zusätzliche Bedingungen für bestimmte Formen der Bearbeitung

Art. 12–14, Beschaffen von Daten

1. Das Beschaffen von Daten ist die Phase, die der Speicherung von Daten in einem Register der Verwaltung unmittelbar vorangeht. Die so erhobenen Daten werden in der Folge für eine mehr oder weniger lange Dauer gespeichert und können derweil im Rahmen von Prüfungen, Mitteilungen oder Entscheidungen genutzt werden. Das **einfache Faktum,** personenbezogene **Daten zu sammeln** und diese zu speichern, stellt bereits einen **Eingriff** in die Privatsphäre der Personen dar, unabhängig von der Tatsache, ob die gesammelten Daten in der Folge genutzt werden oder nicht.[7] Deshalb muss jede Sammlung von Daten durch ein Organ des Staates für die betroffene Person **kenntlich gemacht** werden und auf **einer gesetzlichen Grundlage oder einem anderen berechtigten Anliegen** basieren, das in einem Gesetz vorgesehen ist (Art. 12 Abs. 1).

2. Um sich bezüglich der Qualität der gewonnenen Daten zu versichern, aber auch, um der betroffenen Person zu ermöglichen, von ihren damit im Zusammenhang stehenden Rechten Gebrauch zu machen, muss sie in den Prozess der Datengewinnung so weit wie möglich **einbezogen** werden. Der Vorentwurf enthält in diesem Sinne die Regelung, die vorsieht, dass die Datengewinnung so weit wie möglich **direkt** bei der betroffenen Person erfolgt. Dabei handelt es sich allerdings nicht um eine absolute Regel. Eine gewisse Anzahl Daten sind für das Gemeinwesen *via* andere Mittel sofort verfügbar, namentlich über Datenbankschnittstellen und Abrufverfahren (s. Art. 15 Abs. 2 des Vorentwurfs). In diesen Fällen wird die mangelnde Beteiligung der betroffenen Person bei der Datenbeschaffung im Allgemeinen teilweise durch den Erlass geeigneter Rechtsgrundlagen ausgeglichen.

[7] ATF 143 I 253, Erw. 3.2.

3. Mit dem Ziel, die **Transparenz** und **Erkennbarkeit** der Datenbearbeitung zu verbessern, führt der Vorentwurf im Weiteren eine Verpflichtung für die Verantwortlichen von Datenbearbeitungen ein, **die betroffenen Personen** über die Datenbeschaffung **zu informieren** (Art. 13). Dieses Prinzip stellt heutzutage im Bereich des Datenschutzes einen **einstimmig anerkannten Standard** dar, den man bereits im geltenden Bundesgesetz über den Datenschutz vorfindet (Art. 18 und 18a DSG) und der im Totalrevisionsprojekt des Bundesrats wiederaufgenommen wurde (Art. 17 E-DSG). Sie existiert auch in der Gesetzgebung der EU (Art. 13 der Richtlinie (EU) 2016/680 und Art. 13 und 14 der Verordnung (EU) 2016/679, ebenso wie in Art. 8 der Konvention SEV 108+). Die zu liefernden Informationen müssen es der betroffenen Person ermöglichen, rasch zu verstehen, wer Daten über sie bearbeitet, einschliesslich der untergeordneten Auftragsbearbeiter, 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. Es wird nicht weiter präzisiert, **welche Form** die Information annehmen muss. Die oder der Verantwortliche für die Bearbeitung hat darüber zu wachen, dass die betroffene Person über ein einfach zugängliches Mittel effektiv von der Datengewinnung Kenntnis nehmen kann, aber nicht, dass sie sich tatsächlich danach erkundigt. Eine **standardisierte Information**, z. B. mittels einer Datenschutzerklärung, die an ein Formular angehängt oder auf einer Webseite abrufbar ist, kann genügen.

4. Die Informationspflicht ist **nicht als absolut** zu verstehen: Die oder der Verantwortliche für die Bearbeitung kann von der Pflicht zur Information befreit werden, falls die betroffene Person bereits informiert wurde oder falls die Datengewinnung bei einem Dritten erfolgt und die Gewinnung im Gesetz vorgesehen ist oder falls die Informationspflicht unmöglich zu respektieren ist oder überproportionale Anstrengungen dazu erforderlich sind (Art. 14 Abs. 1). Die Informationspflicht kann auch **beschränkt oder hinausgeschoben** werden, zu denselben Bedingungen, die für das Zugangsrecht gelten (Art. 14 Abs. 2).

Art. 15–19, Standardisierte und grenzüberschreitende Datenbekanntgabe

1. Eine Datenbekanntgabe dient dazu, Personendaten **verfügbar** zu machen, z. B. indem sie konsultiert werden können, indem sie übermittelt, verbreitet oder veröffentlicht werden. Dieses Konzept umfasst sowohl die regelmässige Bekanntgabe von Personendaten als auch die Bekanntgabe im konkreten Fall. Die **Bedingungen der Rechtmässigkeit** sind jedoch nicht gleich, je nachdem, ob man sich im einen oder anderen Fall befindet (Art. 15 Abs. 1):
a) Die **systematischen** Bekanntgaben, d. h. die Bekanntgabe eines Datentyps, der regelmässig an die gleichen Empfänger gerichtet wird, müssen im Sinne von Art. 5 des Vorentwurfs in einer **gesetzlicher Grundlage** vorgesehen sein;
b) Die einmaligen Bekanntgaben von Daten müssen **im Einzelfall** nicht in einer gesetzlichen Regelung vorgesehen werden, aber sie müssen einer der Bedingungen in Artikel 15, Abs. 1, Bst. a-c genügen.

2. Der Vorentwurf regelt eine dritte Kategorie der Datenbekanntgabe: die **Bekanntgabe im Abrufverfahren** (Art. 15 Abs. 2). Wie dies derzeit der Fall ist (Art. 10 Abs. 2 DSchG), erfordert dieser Typ der Bekanntgabe den Erlass der gesetzlichen Grundlage *ad hoc*. In diesem Punkt unterscheidet sich der Vorentwurf vom DSG-Totalrevisionsprojekt des Bundesrates, das vorschlägt, diese Anforderung, die sich derzeit im Art. 19 Abs. 3 des DSG befindet, zu löschen. Gemäss Bundesrat sind die mit der Datenbekanntgabe im Abrufverfahren verbundenen Anforderungen zu entfernen, da sie in der Informationsgesellschaft **überholt** sind (BBI 2017 6941, S. 7083). Dieser Ansicht kann **jedoch nicht gefolgt werden**. Eine Bekanntgabe im Abrufverfahren ist ein automatisierter Zugangsmodus, bei dem der Empfänger der Daten aufgrund einer Genehmigung des Verantwortlichen für die Bearbeitung von sich aus, ohne vorherige Prüfung über Zeitpunkt und Umfang der Bekanntgabe im Rahmen der ihm erteilten Genehmigung entscheidet. Anders formuliert, handelt es sich hier um einen Bearbeitungstyp, der simultan die Charakteristika einer Sammlung und einer Datenkommunikation gemäss dem **Selbstbedienung**sprinzip aufweist. In diesem Kontext erscheint es aus Gründen der Transparenz, der Governance und der Sicherheit gerechtfertigt zu sein, **Leitplanken** vorzusehen.

3. In Übereinstimmung mit dem EU-Recht (Art. 45 ff. der Verordnung (EU) 2016/679) und der Konvention SEV 108+ (Art. 14)) gelten weitere Anforderungen im Rahmen von Datenbekanntgaben **ins Ausland,** namentlich mit dem Ziel, die **freie Zirkulation von Daten** zwischen den Mitgliedstaaten zu ermöglichen (Art. 16):
a) Gemäss der Grundregel in diesem Bereich (Art. 16 Abs. 1) gilt für die Übermittlung von Personendaten an Drittstaaten, dass diese im Prinzip nur dann erlaubt ist, wenn der Empfängerstaat über ein **angemessenes Datenschutzniveau** verfügt. Um zu wissen, ob ein Staat über ein genügendes oder nicht genügendes Datenschutzniveau verfügt, wird es möglich sein, sich an die vom Bundesrat gemäss Artikel 13 Abs. 1 E-DSG geführte und aktualisierte Liste zu halten. Es ist darauf hinzuweisen, dass der Inhalt dieser Liste, auch wenn sie regelmässig aktualisiert wird, **nicht immer vollständig sein muss**. Auch muss die Absenz eines Drittstaates auf dieser Liste nicht bedeuten, dass dieser nicht über ein angemessenes Schutzniveau verfügt, sondern allenfalls vom Bundesrat noch nicht beurteilt worden ist (s. BBI 2017 6941, S. 7039).
b) Wenn der Empfängerstaat kein angemessenes Schutzniveau bietet, oder im Fall von Zweifeln in dieser Sache, bleibt eine grenzüberschreitende Datenbekanntgabe im Rahmen **anderer genügender Garantien**, oder wenn ein anderer **gerechtfertigter Grund** für die Bekanntgabe besteht, trotz Allem möglich (Abs. 2). Die Liste der Garantien und Rechtfertigungsgründe, um dem Fehlen ausreichender Rechtsvorschriften abzuhelfen, bleibt gegenüber der geltenden Gesetzgebung **weitgehend unverändert** und erfordert keine spezifischen Kommentare.

3.1 Wie beim Beschaffen von Daten (s. Art. 13 des Vorentwurfs) verpflichtet Artikel 16 Abs. 3 die Verantwortliche oder den Verantwortlichen für die Datenbearbeitung, die **betroffene Person** über die Daten, die sie oder er ans Ausland bekanntgibt, zu informieren.

3.2 Im Vorentwurf wird vorgesehen, dass die **Publikation von Personendaten auf dem Internet** oder auf anderen Plattformen, die der allgemeinen Information der Öffentlichkeit dienen, nicht als Bekanntgabe von Daten ins Ausland (Art. 16 Abs. 4) gilt, auch wenn diese Informationen im Ausland eingesehen werden können. Diese Regelung ist deshalb gerechtfertigt, um die Anwendung **unverhältnismässiger** Regeln 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 Datenschutzgesetzes entsprechen müssen.

3.3 In Übereinstimmung mit Artikel 49 Abs. 1 der Verordnung (EU) 2016/679 und Artikel 12 Ziffern 5 und 6 der Konvention SEV 108+ verleiht der Vorentwurf der Datenschutzaufsichtsbehörde spezifische Kompetenzen im Zusammenhang mit dem grenzüberschreitenden Datenfluss. Zunächst unterstellt er die Verantwortlichen für die Datenbearbeitung der **Pflicht,** die Aufsichtsbehörde über die Datenbekanntgaben in Staaten **zu informieren**, die nicht im Besitz eines Angemessenheitsbeschlusses sind. Schliesslich räumt er Letzterer eine **Befugnis zum Einschreiten** ein, falls die Rechte der betroffenen Personen ungenügend geschützt werden (Art. 17). Die Kompetenzen der Aufsichtsbehörde werden in Artikel 56 ff. des Vorentwurfs aufgelistet.

4. Die **Einschränkungen** der Bekanntgabe von Personendaten, die in Artikel 18 des Vorentwurfs formuliert werden, bleiben gegenüber der geltenden Gesetzgebung **unverändert** (Art. 11 DSchG). Die Rechtmässigkeit einer Bekanntgabe hängt nicht nur von der Respektierung der generellen Prinzipien des Datenschutzes ab, sondern auch von der Abwesenheit von Einschränkungen im Sinne dieses Artikels. Die Regelung gilt ebenso für die normale Datenbekanntgabe wie für die Bekanntgabe ins Ausland.

5. In Artikel 19 des Vorentwurfs **werden** gewisse gesetzliche Bestimmungen aus anderen Gesetzgebungen, die teilweise von den gesetzlichen Bestimmungen des Datenschutzgesetzes **abweichen können, ausdrücklich vorbehalten**.

Art. 20, Auslagerung

1. Im Bereich der Informationssysteme ist die Auslagerung gewisser Dienstleistungen an Drittanbieter sowohl für die Privatunternehmen als auch für die öffentlichen Verwaltungen zur unumgänglichen Praxis geworden. Die Unternehmen im Sektor Informations- und Kommunikationstechnologien verfügen über hochspezialisierte Ressourcen und Kompetenzen bei der Qualität der Leistungen, der Leistungsfähigkeit, der Innovationskapazität und der Sicherheit, die über das, was der Staat in diesem Bereich bieten kann, hinausgehen.

2. Mit dem Pilotprojekt, das vom ITA betreffend Auslagerung gewisser Daten in die *Cloud* durchgeführt wurde[8], konnten die technischen Möglichkeiten in diesem Bereich erforscht

[8] Cf. Verordnung über die Bewilligung für das Amt für Informatik und Telekommunikation zur Auslagerung der Bearbeitung gewisser Daten in die «Cloud» (Pilotprojekte) (RSG 17.42).

und auch gewisse Sicherheitsaspekte vertieft werden, damit man sich versichern konnte, dass diese Art Lösung mit den gesetzlichen Anforderungen beim Datenschutz vereinbar ist. Der Auswertungsbericht des ITA kommt zum Schluss, dass die Rückmeldungen zur Bewertung überzeugend genug sind, um den Erlass der nötigen gesetzlichen Grundlagen ins Auge zu fassen und so die Möglichkeiten des Einsatzes von Cloud-Computing-Lösungen auszuweiten. In dieser Bestimmung werden die Lehren aus der Pilotphase berücksichtigt. Sie ist so formuliert, dass die Zuhilfenahme dieser Art von Lösungen in einem begrenzten und gesicherten Rahmen, der den höchsten Standards in diesem Bereich entspricht, bewilligt wird. Mit dieser Bestimmung wird der Beizug der *Cloud-Computing*-Lösungen in einem begrenzten und gesicherten Rahmen, der den höchsten Standards in diesem Bereich entspricht, bewilligt. Es sei vermerkt, dass diese Öffnung einem der Ziele des «Massnahmenkatalogs zur Cloud Computing Strategie der Schweizer Behörden 2012-2020» (Stossrichtung S2: Anpassung der rechtlichen Grundlagen) entspricht[9].

3. Besondere Anforderungen werden festgelegt, damit die öffentlichen Organe gleichzeitig die Kontrolle über ihre ausgelagerten Daten behalten und den Schutz der Rechte der Personen gewährleisten können. Vor allem wird in Absatz 1 darauf hingewiesen, die Leistungserbringerin oder der Leistungserbringer als Autragsbearbeiterin oder Auftragsbearbeiter betrachtet wird; das bedeutet, dass das Organ, das die Daten auslagert, vollständig für das Bearbeiten verantwortlich bleibt. Es muss deshalb alle nötigen Massnahmen und Vorsichtsmassnahmen ergreifen, damit die Auslagerung reibungslos vonstattengeht. Ausserdem muss sich das auslagernde Organ versichern, dass die Daten immer an Orten in der Schweiz oder auf dem Gebiet eines Staates, der über eine dem DSchG gleichwertige Gesetzgebung verfügt, gehostet werden (Abs. 2). Damit sind hier insbesondere die Mitgliedstaaten der Europäischen Union gemeint, die seit dem Inkrafttreten des Allgemeinen Reglements (EU) 2016/679 über den Datenschutz die weltweit restriktivste Gesetzgebung beim Datenschutz haben.

4. Es sei darauf hingewiesen, dass diese Anforderungen, zu denen noch diejenigen von Artikel 37 des Vorentwurfs (Bearbeiten im Auftrag) kommen, grösstenteils die Empfehlungen der Konferenz der schweizerischen Datenschutzbeauftragten zur Auslagerung übernehmen[10].

5. Gemäss Absatz 4 führt der Staatsrat auf dem Verordnungs- oder Reglementsweg die besonderen Anforderungen aus, mit denen das höchstmögliche Schutzniveau, namentlich bei der Wahl und bei der Kontrolle der Auftragsbearbeiterin oder des Auftragsbearbeiters, eingehalten werden sollen. Im Bestreben nach Transparenz veröffentlicht er ebenfalls eine Liste der Auftragsbearbeiter, an die er Auslagerungen vergibt.

---

[9] https://www.egovernment.ch/de/umsetzung/e-government-schweiz-2008-2015/cloud-computing-schweiz/

[10] privatim-Merkblatt «*Cloud-spezifische Risiken und Massnahmen*» (das Dokument kann unter dem folgenden Link heruntergeladen werden: http://http://www.privatim.ch/de/privatim-merkblatt-cloud-spezifische-risiken-und-massnahmen/).

Art. 21, Pilotversuche

1. Dieser Artikel lehnt sich an den Artikel 17a des DSG an, der in Artikel 31 E-DSG übernommen wurde, und besteht derzeit in ähnlicher Form in Artikel 21 E-GovSchG. Ein Pilotversuch, in dem Personendaten bearbeitet werden, stellt eine **Datenbearbeitung** im Sinne der Gesetzgebung über den Datenschutz dar. Das ist der Grund dafür, dass der Vorentwurf den Weg wählt, diese Norm ins DSchG zu verschieben.

2. Die Umsetzung der Pilotversuche ist den **Grundbedingungen** unterworfen, die in Absatz 1 beschrieben werden. Die erste unter ihnen lautet dahingehend, dass nur die Versuche zugelassen werden, die der Erfüllung einer öffentlichen Aufgabe dienen, die ein klares öffentliches Interesse verfolgen oder die im Rahmen eines strategischen Projekts stattfinden, das von mehreren schweizerischen Verwaltungen gemeinsam verfolgt wird (Bst. a). Zudem müssen **die Risiken** für Bürgerinnen und Bürger so weit wie möglich **reduziert** werden (Bst. b). Über die technischen und organisatorischen Massnahmen hinaus kann der Staatsrat sie z. B. auf ein Gebiet beschränken, nur gewissen Organen erlauben oder auf gewisse Daten und gewisse Bereiche beschränken. Schliesslich sei daran erinnert, dass ein Pilotversuch der Verwaltung die Möglichkeit gibt, ein System vor der Definition und der Umsetzung eines gesetzlichen Rahmens, der für die eigentliche Nutzung nötig ist, **zu testen und zu prüfen**. Ihre Aufgabe besteht jedoch nicht darin, die Anwendung eines endgültigen Systems zu ermöglichen, noch bevor die notwendigen Rechtsgrundlagen vorhanden sind (Bst. c).

3. Gemäss Artikel 54 Abs. 1 KV können die Organe des Gemeinwesens die Erfüllung öffentlicher Aufgaben an Dritte delegieren, wenn ein Gesetz im formellen Sinne dies vorsieht. Für den Fall, dass die Durchführung eines Pilotversuchs dazu führt, dass Bearbeitungen an Dritte übergeben werden, dient der Artikel 21 Abs. 4 als notwendige Rechtsgrundlage für die Delegation für die Dauer des Pilotversuchs.

Art. 22, Archivierung

Die Organe des Gemeinwesens führen die Archivierung von Personendaten gemäss dem ArchG durch. Die Personendaten, die keine Archivwürdigkeit haben, werden grundsätzlich gelöscht oder vernichtet.

Art. 23, Löschen und Vernichten

1. Der Artikel 10 des Vorentwurfs erhebt die Verpflichtung zur Vernichtung nicht mehr benötigter Daten zu einer Bedingung für die Rechtmässigkeit des Bearbeitungsprozesses. Diese Bestimmung zeigt **die Art auf**, wie diese Verpflichtung erfüllt werden muss.

2. Während der Dauer der Nutzung eines Datenträgers durch ein öffentliches Organs – oder solange dieses unter der Kontrolle der Verwaltung steht – müssen die Personendaten, die daselbst gespeichert sind und die keinen Nutzen mehr haben, regelmässig gelöscht oder vernichtet 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 zwar retgelöscht wurden, aber durch unbefugte Dritte wiedergefunden und ausgewertet werden können. Falls dies der Fall ist, muss der Datenträger - grundsätzlich die Harddisk - physisch zerstört werden (Abs. 2).

Art. 24, Videoüberwachung

Kein Kommentar.

2.2.3 Abschnitt 2.3, Bearbeitung von Daten für nicht personenbezogene Zwecke

Art. 25, Vorschriften

Die Reduzierung der Datenschutzanforderungen für die Bearbeitung zu anderen als zu personenbezogenen Zwecken ist gerechtfertigt, da diese Bearbeitung wesentlich **weniger riskant** ist, gerade weil sie sich **nicht auf Personen** bezieht und bestimmte spezifische Anforderungen erfüllt sind. Im Übrigen tragen diese Anforderungen dem öffentlichen Interesse Rechnung, etwa wo es um die Forschung, die Planung und die Statistik geht.

2.3 Abschnitt 3, Recht der betroffenen Personen

Art. 26 bis 28, Auskunftsrecht

1. Das Auskunftsrecht (Art. 26) 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 der- oder diejenige, die Kenntnis einer Datenbearbeitung hat, die sie oder ihn betrifft, ist gegebenenfalls in der Lage, den Zweck des Bearbeitungsvorgangs zu überprüfen oder die Berichtigung oder Löschung unrichtiger oder nicht mit dem Zweck des Verarbeitungsvorgangs zusammenhängender Daten zu verlangen. Der Schuldner des Auskunftsrechts ist immer die oder der **Verantwortliche für die Datenbearbeitung**, und zwar im Sinn von Artikel 4 Abs. 1 Bst. g. Die Tatsache, dass diese oder dieser die Bearbeitung einem Dritten anvertraut, ändert nichts an dieser Tatsache (Abs. 3).

2. Als Grundpfeiler des Datenschutzrechts ist das Auskunftsrecht ein Recht aller betroffenen Personen und als solches **von keinem Partikularinteresse** abhängig. Das bedeutet, dass keinerlei Einschränkungen aufgrund von Nationalität, Wohnort oder Alter oder auch verbunden mit der Persönlichkeit des Antragsstellers oder der Nutzung, die er mit seinen Daten vorhat, gegeben sind. Die Antragstellerin oder der Antragsteller muss den Antrag im Weiteren auch nicht **begründen**. Die einzige Verpflichtung, die ihr oder ihm obliegt, ist die Angabe ihrer oder seiner Identität, damit ihr oder ihm effektiv die eigenen Daten zugestellt werden (Art. 27 Abs. 1). Für die Anträge auf Auskunft zu **medizinischen Daten** kann die oder der Verantwortliche für die Datenbearbeitung (in der Regel die behandelnde Ärztin oder der behandelnde Arzt) der betroffenen Person vorschlagen, dass sie ihre Daten in Anwesenheit eines Experten ihrer Wahl einsehen könne. Es handelt sich hierbei jedoch nur um einen

Vorschlag, den die betroffene Person akzeptieren oder zurückweisen kann (s. Art. 60 Abs. 3 GesG).

3. Das Auskunftsrecht ist **nicht als absolut zu verstehen**. Artikel 28 des Vorentwurfs zeigt die Bedingungen auf, gemäss denen es eingeschränkt werden kann. Die Berufung auf ein eingeschränktes Auskunftsrecht muss jedoch die Ausnahme bleiben. Sie kann nur in sehr eingeschränkter Form und nach einer Interessenabwägung und in Übereinstimmung mit dem Verhältnismässigkeitsprinzip stattfinden.

Art. 29, Widerspruch gegen die Bekanntgabe von Personendaten

1. Das Recht auf Einsprache oder auf Widerspruch ermöglicht es der betroffenen Person, sich im Voraus der Offenlegung gewisser sie betreffender Daten zu widersetzen. Es ist Teil der Ansprüche, die das Datenschutzrecht betroffenen Personen **allgemein und unabhängig von der Art der betroffenen Daten** einräumt (s. Art. 21 Verordnung (EU) 2016/679; Art. 9 Ziffer 1 Bst. d Konvention SEV 108+; Art. 20 DSG und Art. 33 E-DSG).
2. Unter den Kantonen anerkennt nur der Kanton Uri ein solches Recht nicht. Die Kantone Aargau und Freiburg beschränken diese Möglichkeit auf die Daten des Einwohnerkontrollwesens (Art. 18 EKG und § 16 des Gesetzes über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen des Kantons Aargau vom 24. Oktober 2006 [IDAG; 150.700]). Alle anderen Kantone sehen ein solches Recht auf Widerspruch unabhängig davon vor, um welche Arten von Daten es sich handelt.[11] Im Jahr 2003 hat die ehemalige Eidgenössische Datenschutzkommission in Bezug auf den Kantons Freiburg erklärt hat, dass die Einschränkung des Widerspruchsrechts bei gewissen Datenkategorien **im Widerspruch zum Datenschutzrecht stehe** (Urteil der ehemaligen Datenschutzkommission vom 22. Mai 2003, in: VPB 68.69). Der Vorentwurf sieht folglich **die Einführung eines erweiterten Rechts auf Widerspruch** vor, das unabhängig von den fraglichen Datentypen gegeben ist.

3. Das Recht auf Widerspruch gilt **weder generell noch absolut**. Erstens darf es sich nur auf davor definierte Daten der betroffenen Person beziehen (Abs. 1 in fine). Zweitens kann die Sperrung von Daten unter den in Absatz 2 Bst. a-c genannten Bedingungen aufgehoben werden. Dies ist dann der Fall, wenn die Bekanntgabe ausdrücklich gesetzlich angeordnet ist (Bst. a), wenn ohne Bekanntgabe der Daten die Erfüllung der Aufgaben des öffentlichen Organs erheblich behindert ist (Bst. b) oder wenn sie dazu führen würde, dass eine Drittperson ihre legitimen Interessen nicht verteidigen kann (Bst. c). In den in den Bst. b und c vorgesehenen Fällen erfordert die Einschränkung des Widerspruchsrechts eine **Abwägung der beteiligten Interessen**. Im Rahmen des Möglichen wird die betroffene Person angehört (Abs. 3).

[11] WALDMANN / OESCHGER, in Belser / Epiney / Waldmann (Hrsg.), Datenschutzrecht – Grundlagen und öffentliches Recht, Bern 2011, § 13, Nr. 140 ff.

Art. 30, Abwehrklagen

1. In Absatz 1 werden die drei **traditionellen Verteidigungsmittel** präsentiert, die im Falle einer Verletzung oder des Risikos einer Verletzung der Rechte von Personen, die auf eine rechtswidrige Datenbearbeitung zurückzuführen ist, zur Anwendung gelangen. Gegenüber dem geltenden Gesetzestext wurde der einführende Satz geändert, um besser hervorzuheben, dass die in dieser Bestimmung vorgesehenen Rechte nicht nur von der betroffenen Person, sondern auch von jeder anderen Person oder Einheit, die ein schutzwürdiges Interesse hat, geltend gemacht werden können. Neben der betroffenen Person selbst, die immer ein schutzwürdiges Interesse hat, können die zur Geltendmachung der einen oder anderen Ansprüche nach Artikel 30 Abs. 1 berechtigten Personen **Verwandte der betroffenen Person** oder bestimmte **Vereine oder Verbände** sein, wenn diese ihre eigenen Interessen oder diejenigen ihrer Mitglieder vertreten («recours égoïste»; deutsch «egoistische Verbandsbeschwerde»). Man findet die gleiche Lösung im Bundesrecht sowohl im geltenden Gesetz (Art. 25 Abs. 1) wie auch im Revisionsentwurf (Art. 37 Abs. 1)[12].

2. Absatz 2 sieht verschiedene datenschutzrechtliche Behelfe und Instrumente vor, 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 nicht exakte Daten **gelöscht** oder **berichtigt** werden müssen; sie kann auch **die Hinzufügung eines Vermerks auf den strittigen Charakter** gewisser Daten verlangen, wenn weder ihre Richtigkeit noch ihre Unrichtigkeit erstellt werden kann. Weiter können die **Bekanntgabe an Dritte** oder die **Veröffentlichung** der Löschung, der Berichtigung der Personendaten oder die Hinzufügung der Erwähnung ihres strittigen Charakters verlangt werden. Neu gegenüber dem geltenden Recht ist die Einführung eines neuen Rechts auf **Beschränkung der Bearbeitung**. Weniger radikal als die Berichtigung oder Löschung von Daten, kann die Einschränkung der Bearbeitung dazu dienen, die Auswirkungen einer rechtswidrigen Verletzung **vorübergehend** zu begrenzen, indem sie die Möglichkeiten zur Bearbeitung bestimmter Daten einschränkt, wenn sie aufgrund eines übergeordneten privaten oder öffentlichen Interesses oder weil die Rechtswidrigkeit der Bearbeitung noch nicht nachgewiesen ist, nicht gelöscht oder geändert werden können. Konkret kann die oder der Verantwortliche für die Bearbeitung – oder muss – während der ganzen Dauer der Massnahme die betroffenen Daten **weiterhin intakt halten**, aber kann sie zu anderen Zwecken nicht mehr bearbeiten, bis der Grund für die Einschränkung der Bearbeitung geklärt ist.

Art. 31, Recht bei einem automatisierten Einzelentscheid

1. Es existieren verschiedene Bereiche in denen heute Entscheidungen von einem öffentlichen Organ auf Basis einer automatisierten Bearbeitung von Daten gefällt werden, **ohne dass ein Mensch zu intervenieren braucht**. Zu denken ist hier etwa an den Erlass einer

[12] Vgl. zu diesem Thema: BANGERT Jan, in Maurer-Lambrou / Blechta (Hrsg.), Basler Kommentar Datenschutzgesetz & Öffentllichkeitsgesetz, 3. Auflage, Basel 2014, *ad* Art. 25/25bis DSG, Nr. 29 ff.

Steuerveranlagung, an den Versand einer Busse wegen Übertretens der Höchstgeschwindigkeit, an die Zahlung von Versicherungsleistungen, an die Zulassung zu einem Wettbewerb usw. In diesen Bereichen ermöglicht der Rückgriff auf technologische Mittel die Kapazität und den Rhythmus der Dossierbearbeitung **spürbar zu erhöhen**, was zu erheblichen Einsparungen bei den Ressourcen führt. Gleichwohl sind die Algorithmen, die solchen Entscheiden zugrunde liegen, **nicht unfehlbar** und sie können sich täuschen. Und so ist es wesentlich, dieses Risiko durch **angemessene Verfahrensgarantien** zu kompensieren.

2. Gemäss Absatz 1 dieser Bestimmung muss eine individuelle Entscheidung, die alleine auf Basis einer automatisierten Bearbeitung gefällt wurde, obligatorisch und ausdrücklich **als solche kenntlich gemacht** werden. In Absatz 2 wird ergänzend erwähnt, dass die Verwaltung auf Antrag der betroffenen Person die **Logik und die Kriterien** der Bearbeitung mitteilen muss, die zur Entscheidung geführt haben. Diese Garantie ist erforderlich, um es der betroffenen Person zu ermöglichen, die Richtigkeit der Entscheidung **zu bewerten**, bevor **sie** gegebenenfalls **angefochten** wird. Absatz 3 führt die Möglichkeit einer **raschen und kostenlosen** aussergerichtlichen Überprüfung der Bearbeitungsoperationen ein, die mit der automatisierten Entscheidung verbunden sind, sofern Klarheit darüber herrscht, dass diese durch einen **offensichtlichen und nicht rechtlichen Mangel** beeinträchtigt wird, der voll der Maschine zurechenbar ist, die den Entscheid gefällt hat. Aus verfahrenstechnischer Sicht folgt der Antrag auf Überprüfung den gleichen Regeln wie im Falle einer **Einsprache** im Sinne von Artikel 103 VRG. Die Fälle, für welche das Gesetz ein Einspracheverfahren vorsieht, bleiben vorbehalten (z. B.: Art. 174 ff. DStG).

3. Die Notwendigkeit, im Zusammenhang mit dem Erlass von automatisierten Einzelentscheidungen spezifische Garantien einzuführen, ergibt sich aus den Artikeln 11 der Richtlinie (EU) 2016/680; 22 der Verordnung (EU) 2016/679 und 9 Ziffer 1 Bst. c der Konvention SEV 108+. Im Bundesrecht werden solche Garantien in Artikel 17a DSG seit mehreren Jahren vorgesehen und wurden in Artikel 19 E-DSG wiedereingeführt.

Art. 32, Vorbehalt der Prozessordnungen

Die Rechte der Personen bei der Bearbeitung von Personendaten, die im Rahmen von laufenden Zivil-, Straf- und Verwaltungsverfahren erfolgen, unterliegen dem **anwendbaren Verfahrensrecht**. Das Verfahrensrecht garantiert den Schutz der Persönlichkeit und der Grundrechte aller beteiligten Personen und bietet damit einen gleichwertigen Schutz wie der Datenschutz. Indem die Vorschrift das Verhältnis zwischen der Datenschutzgesetzgebung und dem Verfahrensrecht regelt, verhindert sie das Risiko von Normkonflikten oder Widersprüchen, die den guten Ablauf des Verfahrens stören könnten. Sie steht im Einklang mit der Rechtsprechung des Bundesgerichts in diesem Bereich (s. BGE 138 III 425, Erw. 4.3).

Art. 33, Daten einer verstorbenen Person

Diese Bestimmung führt für jede Person die Möglichkeit ein, über ihre Daten mit persönlichem Charakter für die Zeit **nach dem Tod** verfügen zu können. Sie kann zu diesem

Zweck einen Dritten ihres Vertrauens damit beauftragen oder sich direkt an die oder den Verantwortlichen für die Datenbearbeitung wenden, um zu beantragen, dass sie oder er zum gegebenen Zeitpunkt die erforderlichen Bearbeitungen ihrer Daten durchführen solle. Wie bei den anderen Rechten im Rahmen des Datenschutzes auch, ist auch das Recht, nach dem eigenen Tod über seine Daten verfügen zu können, **nicht absolut** zu verstehen. Es muss mit anderen öffentlichen und privaten Interessen abgewogen werden. Man findet eine ähnliche Regelung in Artikel 16 E-DSG.

Art. 34, Verfahren und Rechtsmittel

Kein Kommentar.

Art. 35, Schadenersatz und Genugtuung

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

2.4 Abschnitt 4, Durchführung des Datenschutzes

Art. 36 und 37, Verantwortlichkeit

1. Der Artikel 36 erfährt gegenüber der geltenden Version des Gesetzes **keinerlei Änderung**. Wie dies bereits heute der Fall ist, ist das Organ, das Personendaten bearbeitet, verantwortlich für den Schutz und die Sicherheit derselben. Diese Verantwortung kann intern geteilt werden, wenn eine Datenbearbeitung mehrere Akteure mitinvolviert (s. Art. 4 Bst. g und Art. 38 Abs. 1 Bst. h *in fine*). Die Frage der internen Aufgabenverteilung hat indes **keinerlei Einfluss auf die Situation der betroffenen Person**, die berechtigt ist, alle ihre Rechte und Ansprüche einer oder einem einzigen Verantwortlichen für die Datenbearbeitung gegenüber geltend zu machen.

2. In Artikel 37 werden die Fragen der Verantwortung geregelt, die sich stellen, wenn ein öffentliches Organ die Mitarbeit von Privatpersonen beim Bearbeiten von Personendaten in Anspruch nimmt (Auftragsdatenbearbeitung). Die Bearbeitungshandlungen, die einem Auftragsbearbeiter übergeben werden, können entweder direkt im Tätigkeitsperimeter des Verantwortlichen stattfinden, was bedeutet, dass der Auftragsbearbeiter das Informatikmaterial des Staates nutzt, oder vollständig in die Informatikinfrastrukturen und -systeme des Auftragsbearbeiters ausgelagert werden; in diesem Fall **gelangt ausserdem Artikel 20** über die Auslagerung von Daten zur Anwendung.

Absatz 1 – Die Bestimmung weist darauf hin, dass **der Schutz und die Sicherheit der Daten**, die für ein Organ des Staats von einem Auftragsbearbeiter bearbeitet werden, gewährleistet sein muss, wie wenn das Bearbeiten vom Organ selber ausgeführt würde (das Organ seinerseits bleibt allein verantwortlich für den Schutz der bearbeiteten Daten).

Absatz 2 – Gemäss dieser Bestimmung dürfen die Daten, bei denen eine gesetzliche oder vertragliche **Geheimhaltungspflicht** besteht, nur einer Auftragsbearbeiterin oder einem Auftragsbearbeiter übergeben werden, wenn die Vertraulichkeit nicht nur gegenüber Dritten, sondern **auch gegenüber der Auftragsbearbeiterin oder dem Auftragsbearbeiter** sichergestellt ist, wenn die bekanntgegebenen Daten kodiert wurden und der Auftragsbearbeiter nicht über den Schlüssel zur Dekodierung verfügt.

Absatz 3 – In der Bestimmung wird der Auftragsbearbeiterin oder dem Auftragsbearbeiter verboten, das Bearbeiten ohne vorherige Bewilligung des Verantwortlichen **einem Dritten zu übertragen**. Da der Auftragsbearbeiter grundsätzlich nicht direkt der kantonalen Gesetzgebung untersteht, muss diese Vorsichtsmassnahme **im Auftragsvertrag** stehen.

Art. 38–40, Bearbeitungsregister und Anmeldung der Bearbeitungsaktivitäten

1. Die Anmeldung der Bearbeitungsaktivitäten und das Bearbeitungsregister sind die **beiden Governance-Instrumente** im Bereich des Datenschutzes, mit denen die Transparenz und die Kontrolle bei der Datenbearbeitung des Staates, der Gemeinden und der anerkannten Kirchen sichergestellt werden.

2. Artikel 38 listet die Informationen auf, welche die oder der Verantwortliche für die Datenbearbeitung zum Zeitpunkt liefern muss, wenn sie oder er zur Bearbeitung übergeht. Artikel 39 legt eine gewisse Anzahl von Ausnahmen von der Meldepflicht fest. Jede dieser Bestimmungen ist weitgehend denjenigen des geltenden DSchG ähnlich.

3. Das Bearbeitungsregister wird von der **Kantonalen Aufsichtsbehörde für Datenschutz geführt** (Art. 40). Es ist öffentlich und kann kostenlos eingesehen werden. Gegenüber dem geltenden Gesetz fügt der Vorentwurf an, dass es online verfügbar sein muss, was bereits heute der Fall ist.[13] Die Gemeinden, die dies wünschen, können ihr eigenes Bearbeitungsregister führen; sie sind jedoch gehalten, ihre Bearbeitungen zusätzlich auch der kantonalen Aufsichtsbehörde zu melden. In jedem Fall müssen die Gemeinden mindestens eine aktuelle Liste über ihre Datenbearbeitungen führen, die sie der Öffentlichkeit zur Verfügung stellen (Abs. 2 und Abs. 3).

Art. 41, Organisatorische und technische Massnahmen

1. Die Verantwortlichen für die Datenbearbeitung müssen die erforderlichen und geeigneten organisatorischen und technischen Massnahmen ergreifen, um die Personendaten, die sie bearbeiten, gegen, vorsätzliches oder unabsichtliches, unsachgemässes Bearbeiten, das ihre Vertraulichkeit, Verfügbarkeit, Authentizität oder Integrität beeinträchtigen kann, zu schützen.

[13] 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.

2. In Übereinstimmung mit dem risikobasierten Ansatz legt das Gesetz keine spezifischen Massnahmen vor, die implementiert werden müssen, sondern übernimmt das Prinzip der Verantwortlichkeit, das man in den meisten modernen Gesetzen zum Datenschutz wiederfindet (Art. 4 Ziffer 4 der Richtlinie (EU) 2016/680; Art. 5 Ziffer 2 der Verordnung (EU) 2016/679 und Art. 10 Ziffer 1 der Konvention SEV 108+). Dieses neue Prinzip bedeutet für die Verantwortlichen für die Datenbearbeitung:
a) Sie müssen effektive, geeignete und an die Umstände angepasste Massnahmen **umsetzen**, mit dem Ziel, den Schutz und die Sicherheit der Personendaten, die sie bearbeiten, zu gewährleisten (Abs. 1).
b) Sie müssen in der Lage sein, den Aufsichtsbehörden und den betroffenen Personen das Vorhandensein und die Umsetzung der Massnahmen im Rahmen einer geeigneten Dokumentation **nachzuweisen** (Abs. 3).

3. Welche technischen und organisatorischen Massnahmen konkret von jedem Verantwortlichen für die Datenbearbeitung umgesetzt werden müssen, hängt von verschiedenen Kriterien ab: Anzahl und Typ der bearbeiteten Daten; Häufigkeit und Ausmass der Bearbeitungen; Risiken, die damit verbunden sind; aber auch der Umfang der Infrastruktur, die Ressourcen, über die sie verfügen, und die Technologie, die sie nutzen. Neben der Implementierung technischer Lösungen kann es sich um Massnahmen zur Sensibilisierung und zur Ausbildung sowie zum lokalen Schutz oder um Mechanismen handeln, um die Folgen eines Verlusts oder eines Diebstahls von mobilem Material zu beschränken. **Der Umfang der Dokumentationspflicht** hängt von den Umständen jedes Einzelfalls ab. Es kann im Detail die folgenden Formen annehmen: einfache regelmässig aktualisierte Liste der technischen und organisatorischen Massnahmen, die umgesetzt wurden, Charta, Politik, Nutzungsreglement *ad hoc* usw.

Art. 42, Datenschutz durch technische und datenschutzfreundliche Voreinstellungen

1. Die Prinzipien des Datenschutzes ab Planung und mit Voreinstellungen verankern einen **proaktiven Ansatz zum Schutz der** Privatsphäre entlang des Bearbeitungsprozesses von Daten. Sie sind vorgesehen in der Richtlinie (EU) 2016/680 (Art. 20 Ziffer 1), in der Verordnung (EU) 2016/679 (Art. 25) und in der Konvention SEV 108+ (Art. 10 Ziffern 2 und 3). Der Bundesrat hat sie in Artikel 6 des Totalrevisionsprojekts ebenfalls integriert (E-DSG).

2. Gemäss dem Prinzip des Datenschutzes durch Technik («***privacy by design***») müssen die Verantwortlichen für die Datenbearbeitung Massnahmen zum Schutz der Privatsphäre in **allen Phasen**, von der Planung bis zur Nutzung der Systeme und Anwendungen, in denen Personendaten bearbeitet werden, integrieren, einschliesslich insbesondere der Entwicklung, des Designs, der Planung, der Umsetzung, der Nutzung, der Kontrolle und des Unterhalts (Abs. 1). Die in diesem Bereich umzusetzenden Massnahmen können sich ebenso auf das Engineering der Systeme wie auf die Implementierung von technischen und organisatorischen Massnahmen beziehen (z. B. die Tatsache, im Vorfeld die zu sammelnden Daten für jeden Bearbeitungstyp zu definieren, die Festlegung von regelmässigen Fristen, um

Personendaten zu löschen oder zu anonymisieren, oder die Ausarbeitung eines Verfahrens, das im Fall einer Verletzung des Datenschutzes zur Anwendung gelangt).

3. Gemäss dem Prinzip des Datenschutzes durch datenschutzfreundliche Voreinstellungen («***privacy by default***»), müssen die Informationssysteme und Anwendungen standardmässig so parametrisiert sein, wie es dem Schutz der Privatsphäre **am dienlichsten** ist (strikt auf das Nötigste limitierte Sammlung von Daten, um die anvisierten Aufgaben erfüllen zu können, gezielte Datenbekanntgabe statt allgemeiner Zugang zu allen Daten ...).

Art. 43 und 44, Datenschutz-Folgenabschätzung – Grundsätze

1. Die mit dem Datenschutz verbundene Folgenabschätzung ist ein wichtiges Instrument für die Übertragung der Verantwortlichkeit an die Organe: Sie unterstützt sie nicht nur dabei, Datenbearbeitungen, die die Privatsphäre respektieren, zu erstellen, sondern auch dabei, aufzuzeigen, dass sie datenschutzkonform handeln. Die Folgenabschätzung muss von der oder vom Verantwortlichen für die Datenbearbeitung **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 europäische Recht (Art. 27 Ziffer 1 Richtlinie (EU) 2016/680 und Art. 35 Ziffer 1 Verordnung (EU) 2016/679, Konvention SEV 108+ (Art. 10 Ziffer 2)) und im Entwurf zur Totalrevision des DSG (Art. 20) ist die Folgenabschätzung für *die* Bearbeitung von Daten obligatorisch, die voraussichtlich zu einem **erhöhten Risiko** für die Rechte und Freiheiten der betroffenen Personen führen (Art. 43 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 43 Abs. 3 beschrieben. Deren Realisierung soll **ohne übertriebene Formalismen** und unter Beachtung der Verhältnismässigkeit durchgeführt werden.

3. Geht aus der Folgenabschätzung hervor, dass die geplante Datenbearbeitung ein **konkretes Risiko** für die Rechte der betroffenen Personen birgt, das spezielle Schutzmassnahmen erfordert, hat die oder der Verantwortliche für die Datenbearbeitung die Behörde für Öffentlichkeit und Datenschutz zu kontaktieren, bevor mit der Bearbeitung begonnen werden darf (Art. 44 Abs. 1). Letztere kann der oder dem Verantwortlichen für die Datenbearbeitung ihre eventuellen Einwände und Empfehlungen zur geplanten Datenbearbeitung mitteilen (Abs. 2). Die oder der Verantwortliche für die Datenbearbeitung ist **frei**, die Empfehlungen der Aufsichtsbehörde praktisch umzusetzen oder nicht, sie oder er muss sie aber in jedem Fall spätestens zum Zeitpunkt der Aufnahme der Bearbeitung über die getroffenen Massnahmen informieren (Abs. 3).

Art. 45 und 46, Verletzungen der Datensicherheit

1. Die zu ergreifenden Massnahmen bei einem Zwischenfall, mit dem eine Verletzung von Vertraulichkeit, Verfügbarkeit und Integrität der Daten einhergeht, **decken drei Bereiche ab**:
a) Feststellung der Verletzung und deren Korrektur (Art. 45 Abs. 1);
b) Aufzeichnung der Verletzung in einem schriftlichen Dokument (Art. 45 Abs. 1 *in fine*) und
c) wenn nötig Meldung der Verletzung an die Datenschutzbeauftragte oder den Datenschutzbeauftragten oder an die betroffene Person (Art. 45 Abs. 2 und 3 und Art. 46).

2. Das Gesetz verlangt nicht, dass jeder Zwischenfall im Bereich des Datenschutzes systematisch der oder dem Datenschutzbeauftragten gemeldet werden muss. Dies gilt nur für die **Zwischenfälle, mit denen ein Risiko** für die betroffene Person **verbunden ist**. Dies setzt jedoch nicht voraus, dass das Informationssystem des Organs Gegenstand eines Cyberangriffs war; der einfache Verlust eines USB-Sticks, der sensible Personendaten enthält, kann den Verantwortlichen für die Datenbearbeitung gegebenenfalls bereits zwingen, Meldung zu erstatten, wenn die betroffenen Personen leicht identifizierbar sind. Auch wenn es im Gesetz nicht ausdrücklich erwähnt wird, sollte die Frist für die Meldung 72 Stunden nicht überschreiten (Vergleich: Art. 30 Ziffer 1 Richtlinie (EU) 2016/680; Art. 33 Ziffer 1 Verordnung (EU) 2016/679).

3. Ist die fragliche Verletzung geeignet, einer oder mehreren Personen Schaden zuzufügen, so ist dies der betroffenen Person im Prinzip **persönlich mitzuteilen** (Art. 46 Abs. 1). Im Falle von Untätigkeit der oder des Verantwortlichen für die Datenbearbeitung kann die Bekanntmachung von der oder vom Beauftragten für den Datenschutz verordnet werden (Abs. 4). Für Verletzungsfälle, die eine grosse Anzahl Personen betreffen, ist es möglich, in Form einer **öffentlichen Mitteilung** zu informieren, sei das über die Zeitungen, das Fernsehen oder das Internet (Abs. 3). In einem solchen Fall ist dafür zu sorgen, dass die betroffenen Personen die Möglichkeit haben, präzisere und persönlichere Informationen zu erhalten, und zwar über die Bereitstellung einer geeigneten Kontaktmöglichkeit. Ausnahmsweise kann die Meldepflicht in gewissen spezifischen Situationen eingeschränkt, aufgeschoben oder darauf verzichtet werden (Abs. 2). In einem solchen Fall muss dennoch eine Meldung zuhanden der oder des Datenschutzbeauftragten gemacht werden; ihr oder ihm kann in einem solchen Fall das Amtsgeheimnis nicht entgegengehalten werden (s. Art. 56 Abs. 3).

4. Gemäss Artikel 45 Abs. 3 muss jede Verletzung des Datenschutzes, die bei einem privaten Beauftragen der öffentlichen Verwaltung auftritt, unabhängig davon, wie schwerwiegend sie ist, der oder dem Verantwortlichen für die Datenbearbeitung gemeldet werden (Ausnahmen davon sind etwa Bagatellfälle, die kein Risiko für die betroffenen Personen darstellen). Wenn die oder der Verantwortliche für die Datenbearbeitung über eine solche Verletzung benachrichtigt wird, entscheidet sie oder er gemäss den oben genannten Regeln, ob die Verletzung der oder dem Datenschutzbeauftragten gemeldet werden soll.

Art. 47, Ansprechperson für Datenschutz

1. Der Vorentwurf führt für die öffentlichen Organe, die Personendaten bearbeiten, die Verpflichtung ein, eine Ansprechperson für Datenschutz zu bezeichnen, die damit beauftragt ist, die oder den Verantwortlichen für die Datenbearbeitung bei ihrer oder seiner Tätigkeit unter juristischen Gesichtspunkten **zu beraten und zu begleiten**. Eine ähnliche Verpflichtung figuriert in den Artikeln 32 ff. der Richtlinie (EU) 2016/680 und in den Artikeln 37 ff. der Verordnung (EU) 2016/679, welche die Bezeichnung eines oder einer «Datenschutz-delegierten» fordern. Im Bundesrecht wird bei der Totalrevision des E-DSG in Artikel 9 Abs. 3 vorgesehen, dass die eidgenössischen Organe einen «Datenschutzberater» ernennen müssen.

2. Aus Gründen der Verhältnismässigkeit und des Pragmatismus ist nicht vorgesehen, die Verpflichtung dahingehend auszuweiten, dass jedes Organ, das etwa nur **punktuell** Daten bearbeitet, eine Ansprechperson für Datenschutz bezeichnen muss; dies betrifft nur die Organe, die im Rahmen ihrer ordentlichen Tätigkeit **regelmässig und systematisch** Personendaten bearbeiten (Abs. 1). Ausserdem ist es nicht nötig, dass jede Verwaltungseinheit über ihre eigene Ansprechperson für Datenschutz verfügen muss; ein und die gleiche Person kann diese Rolle im Auftrag mehrerer Verwaltungseinheiten im Rahmen einer gleichen Struktur ausüben.

3. Die Ansprechperson für Datenschutz nimmt vor allem eine beratende Rolle ein; sie ist **nicht verantwortlich** für die Konformität der Bearbeitung (Abs. 3 *in fine*). Die Ansprechperson für Datenschutz hat indes die Aufgabe, dafür zu sorgen, dass die Verpflichtungen, die sich aus der **Umsetzung des Gesetzes** ergeben, korrekt erfüllt werden. Dies gilt insbesondere für die Verpflichtung, Bearbeitungen beim Bearbeitungsregister zu melden (Art. 38), für die Verpflichtung, die technischen und organisatorischen Massnahmen zu dokumentieren, die ergriffen werden (Art. 41 Abs. 3), für die Verpflichtung, vor gewissen Datenverarbeitungsarten eine Folgenabschätzung durchzuführen, und, falls dies nötig erscheint, die Aufsichtsbehörde zu kontaktieren (Art. 43 und Art. 44) und schliesslich Verstösse gegen die Datensicherheit der Aufsichtsbehörde sowie den betroffenen Personen zu melden (Art. 45 und 46). Die Ansprechperson für Datenschutz sorgt auch dafür, dass Personen, die ihre Rechte im Bereich des Datenschutzes ausüben, angemessene Antworten auf ihre Anfragen seitens der Verantwortlichen für die Bearbeitung erhalten. Schliesslich ist die Ansprechperson für Datenschutz **der privilegierte Gesprächspartner** der Aufsichtsbehörde für den Datenschutz und stellt so den Übergang zur oder zum Verantwortlichen für die Datenbearbeitung her.

4. Die Bestimmung legt **zwei Bedingungen** fest, damit die Ansprechperson für Datenschutz ihre Funktion korrekt erfüllen kann:

a) Einerseits muss sie in der Lage sein, die **wichtigsten Herausforderungen** im Zusammenhang mit dem Datenschutz und dessen Umsetzung zu verstehen (Abs. 3).
b) Andererseits ist es wichtig, dass sie **in genügendem Masse** zu den Tätigkeiten der Daten-

bearbeitung **beigezogen** wird, die in ihrer Struktur durchgeführt werden; die Verantwortlichen der Datenbearbeitung müssen ihr von Amtes wegen alle erforderlichen Informationen zu ihren Tätigkeiten mitteilen und auf Fragen antworten, die an sie gerichtet werden (Abs. 4).

2.5 Abschnitt 5, Aufsicht

2.5.1 Abschnitt 5.1: Aufsichtsbehörden für Datenschutz

Art. 48, Aufsichtsbehörde

1. Die Bezeichnung einer Aufsichtsbehörde ist eine zwingende Bedingung zur Realisierung eines Systems der Kontrolle des Datenschutzes in einer demokratischen Gesellschaft. Auf **kantonaler Ebene** ist diese Funktion gemäss Absatz 1 der Behörde für Öffentlichkeit und Datenschutz (nachfolgend: die kantonale Behörde) übertragen.

2. Gemäss geltendem Gesetz haben die **Gemeinden**, sofern sie dies wünschen, die Möglichkeit, ihre eigene Aufsichtsbehörde in diesem Bereich zu bezeichnen. Diese Möglichkeit wurde im Vorentwurf wiederaufgenommen (Abs. 2). Es ist jedoch zu beachten, dass diese Lösung bis heute **von keiner Gemeinde** gewählt wurde. Unter diesen Umständen darf die Frage gestellt werden, ob die Aufrechterhaltung dieser Bestimmung gerechtfertigt ist, umso mehr, als die in diesem Bereich zu vollziehenden Aufgaben immer komplexer werden und folglich auch die entsprechenden Ressourcen erfordern. Wenn die Hinweise aus der Vernehmlassung in die Richtung einer **Aufhebung** dieser Bestimmung gehen, wird es grundsätzlich auch nötig sein, sein Gegenstück in Artikel 39 Abs. 4 InfoG aufzuheben.

3. Gegenüber der jetzigen Situation sieht der Vorentwurf vor, dass die **anerkannten Kirchen**, die ihre eigenen Regelungen in Sachen Datenschutz erlassen haben, gehalten sind, ihre eigene Aufsichtsbehörde zu einzurichten (Abs. 3). Diese Änderung geht in Richtung einer besseren Berücksichtigung von Artikel 6 KSG, der **die Autonomie der Kirchen** gegenüber Kanton und Gemeinden anerkennt. Sie trägt auch den Unterschieden zwischen dem Staat und einer Kirche bei der Bearbeitung von Personendaten Rechnung.

4. Die kommunalen und kirchlichen Aufsichtsbehörden müssen, namentlich beim Budget und der Unabhängigkeit, über **analoge Kompetenzen** und die **gleichen Garantien,** wie sie im geltenden Gesetz beschrieben sind, verfügen. Bei einem schwerwiegenden Verstoss gegen diese Anforderungen kann die kantonale Behörde die kommunale oder kirchliche Aufsichtsbehörde ersetzen. Auch aus dieser Sichtweise versteht sich, dass, gemäss Artikel 51 Abs. 1 Bst. f, die kantonale Aufsichtsbehörde durch die kantonale Öffentlichkeits- und Datenschutzkommission weiterhin **die Oberaufsicht** über diese Behörden wahrnimmt.

Art. 48–53, Organisation der kantonalen Aufsichtsbehörde

1. Der Vorentwurf behält die jetzige Struktur der Kantonalen Aufsichtsbehörde für Datenschutz bei. Diese setzt sich einerseits aus einer **kantonalen Kommission** und andererseits **einer oder einem Datenschutzbeauftragten** zusammen (s. Art. 29a Abs. 1 DSchG). Mit diesem System konnte bis jetzt die Unabhängigkeit gegenüber der Verwaltung und die Legitimität, die durch eine vom Grossen Rat gewählten Kommission gegeben ist, einerseits mit der Professionalität und andererseits mit der täglichen Verfügbarkeit einer oder eines Datenschutzbeauftragten wirksam vereinbart werden. Das ist der Grund für die Beibehaltung.

2. Die Zusammensetzung und Organisation der kantonalen Öffentlichkeits- und Datenschutzkommission wird in Artikel 50 geregelt. Sie ist ein **multidisziplinäres Organ**, das mehrere Berufsbilder und so viele Fähigkeiten, wie sie für ein möglichst breites Verständnis der mit dem Bereich des Datenschutzes zusammenhängenden Herausforderungen erforderlich sind, vereint. Die Mitglieder der Kommission **werden** auf Vorschlag des Staatsrates vom Grossen Rat **gewählt**. Diese Lösung, die seit dem Inkrafttreten des geltenden Gesetzes besteht, garantiert einerseits die Unabhängigkeit der Aufsichtsbehörde gegenüber der kantonalen Exekutive und der Verwaltung, die von ihr abhängt, und fördert die Wahl der Mitglieder vor allem aufgrund der erforderlichen Kompetenzen. Gegenüber der jetzigen Situation wird die Zusammensetzung der Kommission **leicht geändert,** um darin auch eine juristische Vertretung zu haben (Abs. 2). Diese Anfügung entspricht der aktuellen Praxis: Seit der Einrichtung war in der kantonalen Öffentlichkeits- und Datenschutzkommission immer eine Juristin oder ein Jurist vertreten.

3. Die Befugnisse der Kommission werden in Artikel 51 geregelt. Dazu gehören insbesondere Funktionen der Aufsichtsbehörde, die eine **grössere Legitimation** erfordern: Sie nimmt Stellung zu Entwürfen von Erlassen, die den Datenschutz berühren (Bst. d), ordnet die nötigen Massnahmen gegenüber den Verantwortlichen für die Datenbearbeitung an, welche die gesetzlichen Vorschriften nicht einhalten (Bst. e), und übt die Oberaufsicht über die anderen Kantonsbehörden beim Datenschutz aus (Bst. f).

4. Die oder der Kantonale Datenschutzbeauftragte gemäss Artikel 52 des Vorentwurfs ist eine **Spezialistin oder ein Spezialist** des Datenschutzrechts. Sie oder er wird auf Stellungnahme der Kommission hin vom Staatsrat ernannt. Auch hier handelt es sich um ein System, mit dem Legitimität, Unabhängigkeit und erforderliches Kompetenzniveau möglichst gut vereinbart werden können. Im Verhältnis zu anderen kantonalen Verwaltungsmitarbeiterinnen und -mitarbeitern verfügt die oder der Datenschutzbeauftragte über einen **speziellen Status**, der von den normalen Regelungen der Gesetzgebung über das Staatspersonal abweicht. Wie die oder der Eidgenössische Datenschutzbeauftragte (s. Art. 39 Abs. 5 des Entwurfs der Totalrevision des DSG) kann sie oder er nicht von der kantonalen Exekutive und auch von keinem anderen Organ der Kantonsverwaltung beurteilt werden. Diese Aufgabe wurde der hierfür zuständigen Kommission übertragen (Abs. 2),

welche die Tätigkeit der oder des Datenschutzbeauftragten leitet. Weiter sind die Möglichkeiten, das Dienstverhältnis der oder des Beauftragten zu kündigen, sehr eingeschränkt (Abs. 3). In seiner letzten Empfehlung anlässlich der Evaluation der Anwendung des Schengen-Abkommens in der Schweiz von 2018 hat der Europarat den Kanton Luzern ersucht, in seinem Gesetz die Möglichkeit zu löschen, die oder den Beauftragten wegen «berechtigter Gründe» und nicht nur wegen schwerer Fehler absetzen zu können.[14] Diese spezifische Besonderheit ist nötig, um die **Unabhängigkeit** der oder des Datenschutzbeauftragten in der Ausübung ihrer oder seiner Funktion **garantieren zu können** (s. Kommentar zum Art. 54).

5. Die oder der Datenschutzbeauftragte übt im Wesentlichen die **laufende Aufsichts- und Beratungsätigkeit** in Datenschutzfragen in der Kantonsverwaltung sowie gegenüber Gemeinden und Dritten aus. Die Liste ihrer oder seiner Befugnisse befindet sich in Artikel 53 des Vorentwurfs. Wie bisher ist die oder der Beauftragte der Kommission unterstellt, die deren oder dessen **Tätigkeit lenkt** und dabei ihr oder ihm gewisse spezielle Arbeiten übertragen kann (Art. 51 Abs. 1 Bst. a).

Art. 54, Unabhängigkeit und Geheimhaltungspflicht

1. Die Unabhängigkeitsgarantie der Aufsichtsbehörde für den Datenschutz ist eine **grundlegende Anforderung** in diesem Bereich, die bereits im geltenden Gesetzestext figuriert (Art. 29 Abs. 3 DSchG) und die man allgemein in der schweizerischen und europäischen Regulierung im Bereich des Datenschutzes vorfindet (s. Art. 42 der Richtlinie (EU) 2016/680; Art. 52 der Verordnung (EU) 216/679; Art. 15 Ziffer 5 der Konvention SEV 108 (modernisiert); Art. 26 Abs. 3 DSG und Art. 39 Abs. 3 p-DSG). Sie setzt **angemessene organisatorische Garantien** für die Stellung der Aufsichtsbehörde innerhalb der Verwaltung, die Ressourcen, über die sie verfügt, und die Bezeichnung und den juristischen Status der oder des Datenschutzbeauftragten voraus.

2. Das Kriterium der Unabhängigkeit vereint **mehrere Elemente**, die bei dieser Bestimmung allgemein oder gezielt berücksichtigt wurden:

a) *Funktionale Unabhängigkeit*: Die Aufsichtsbehörde muss über die erforderlichen Kompetenzen verfügen, die zur Erledigung der ihr vom Gesetz übertragenen Aufgaben erforderlich sind, und darf in der Ausübung ihrer Funktion nicht behindert werden;
b) *Institutionelle Unabhängigkeit*: Die Aufsichtsbehörde darf von der kantonalen Exekutive oder einem anderen Organ des Staates keine Weisungen dazu empfangen, wie sie das Amt auszuüben hat;
c) *Materielle Unabhängigkeit*: Die Aufsichtsbehörde muss über die erforderlichen

[14] EUROPÄISCHER RAT, *Durchführungsbeschluss des Rates zur Festlegung einer Empfehlung zur Beseitigung der 2018 bei der Evaluierung der Anwendung des Schengen-Besitzstands im Bereich des Dtenschutzes durch die Schweiz festgestellten Mängel*, 8. März 2019, Empfehlung Nr.2.

personellen und finanziellen Ressourcen verfügen können, die für die Erfüllung der ihr vom Gesetz aufgetragenen Aufgaben erforderlich sind;

d) *Personelle Unabhängigkeit*: Die Mitglieder der Aufsichtsbehörde dürfen keine Interessenbindungen haben, die ihre Entscheidungen in Bezug auf Aufgaben des Datenschutzes, die sie wahrnehmen, beeinflussen können.

3. Im Weiteren ruft die Bestimmung in Erinnerung und präzisiert, dass jede Person, die für die Aufsichtsbehörde im Bereich Datenschutz arbeitet, dem Amtsgeheimnis und der Geheimhaltungspflicht unterstellt ist (Abs. 4). Daraus folgt, dass die Behörde bei den an sie gerichteten Anfragen und beim Austausch mit ihr **Anonymität garantiert,** es sei denn, die betroffene Person gebe ausdrücklich ihre Einwilligung dazu, dass sie offengelegt werden, namentlich gegenüber dem Organ, das mutmasslich Vorschriften über den Datenschutz verletzt haben soll.

Art. 55, Selbstkontrolle der Aufsichtsbehörde

Diese Bestimmung verpflichtet die Aufsichtsbehörde, 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, Eingriffsmittel

1. Der Vorentwurf sieht vor, dass die **Interventionsmöglichkeiten** der Aufsichtsbehörde gemäss den neuen Standards der Gesetze im Bereich des Datenschutzes (s. Art. 47 Ziffer 2 der Richtlinie (EU) 2016/680 und Art. 58 Ziffer 2 der Verordnung (EU) 2016/679; Art. 15 Ziffer 2 Bst. a bis d Konvention SEV 108+ und Art. 44 und 45 E-DSG) zu **verstärken**.

2. Zusätzlich zu den Untersuchungsbefugnissen und zur Prozessfähigkeit oder zur Befugnis, die Justizbehörde auf Verstösse gegen die Bestimmungen des Datenschutzes hinzuweisen, muss die Aufsichtsbehörde künftig über die Kompetenz verfügen können, **verbindliche Entscheide** für die Verantwortlichen der Datenbearbeitung zu **fällen**. Die Verleihung der Entscheidungskompetenz an die Aufsichtsbehörde ist ein wesentliches Element im Sinne von Artikel 45 der Verordnung (EU) 2016/679 im Hinblick auf die Aufrechterhaltung des **Angemessenheitsbeschlusses** der Europäischen Kommission zugunsten der Schweiz. Sie ist Teil der **Empfehlungen** derselben Behörde anlässlich der Evaluation der Schweiz im Jahr 2018 bei der Beurteilung der Anwendung des Schengen-Abkommens durch die Schweiz.[15]

[15] EUROPÄISCHER RAT, *Durchführungsbeschluss des Rates zur Festlegung einer Empfehlung zur Beseitigung der 2018 bei der Evaluierung der Anwendung des Schengen-Besitzstands im Bereich des Dtenschutzes durch die Schweiz festgestellten Mängel*, 8. März 2019, Empfehlungen Nr.3 und 4.

3. Die Eingriffsmittel der Aufsichtsbehörde können in **zwei Kategorien** aufgeteilt werden: diejenigen, die direkt der oder dem Datenschutzbeauftragten zur Verfügung stehen und diejenigen, für welche die kantonale Öffentlichkeits- und Datenschutzkommission zuständig ist:

a) *Die oder der Datenschutzbeauftragte* ist die zuständige Stelle, um eine **Untersuchung** bei einer oder einem Verantwortlichen für die Datenbearbeitung oder gegenüber einer externen Auftragnehmerin oder einem externen Auftragnehmer **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 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 Dokumenten verlangen, Audits oder Inspektionen vor Ort durchführen. Das Amtsgeheimnis kann ihr oder ihm nicht entgegengehalten werden (Abs. 3). Falls die oder der Datenschutzbeauftragte einen Verstoss gegen die Datenschutzvorschriften feststellt, kann sie oder er **eine Aufforderung** gegenüber der oder dem Verantwortlichen für die Datenbearbeitung oder des von ihr oder ihm beauftragten Unternehmens aussprechen, wonach Bearbeitungen wieder gemäss den gesetzlichen Anforderungen zu erfolgen haben (Art. 57 Abs. 1). Falls die oder der Verantwortliche für die Datenbearbeitung einer Aufforderung der oder des Datenschutzbeauftragten nicht nachkommt, kann Letztere oder Letzterer den Fall der Kommission übertragen (Abs. 2).

b) Als Kollegialorgan, das vom Grossen Rat gewählt wird, *ist die kantonale Öffentlichkeits- und Datenschutzkommission* das zuständige Organ, um gegenüber den Verantwortlichen für die Datenbearbeitung verbindliche Entscheidungen zu fällen (Art. 58). Sie kann von Amtes wegen handeln oder kann von der oder vom Datenschutzbeauftragten zum Handeln aufgefordert werden. 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 den von ihr gefällten Entscheiden beachtet die Kommission das **Prinzip der Verhältnismässigkeit**. Anstatt beispielsweise die Einstellung der Bearbeitung anzuordnen, kann die Kommission eine Änderung anordnen und die Massnahme auf den Teil der Bearbeitung beschränken, der Probleme bereitet. Falls eine Verantwortliche oder ein Verantwortlicher für die Datenbearbeitung es versäumt hat, eine Datenschutz-Folgenabschätzung durchzuführen, obwohl die Bedingungen für eine solche Analyse gegeben sind, kann die Kommission den Unterbruch der Datenbearbeitung anordnen, bis die Folgenabschätzung durchgeführt ist. In **wirklich gravierenden** Fällen, in denen die Rechte der Personen aufgrund einer Bearbeitung, welche die rechtlichen Anforderungen auf jeden Fall nicht erfüllt, augenscheinlich und ernsthaft in Gefahr sind, kann die Kommission **einstweilige Massnahmen** aussprechen und die Aussetzung der Bearbeitung anordnen, bis ein gerichtlicher Entscheid in der Angelegenheit vorliegt (Abs. 4).

4. Wie es in Artikel 59 Abs. 1 im Vorentwurf vorgesehen ist, beachten sowohl die oder der Datenschutzbeauftragte als auch die kantonale Öffentlichkeits- und Datenschutzkommission in ihren Eingriffen die Bestimmungen des VRG. Insbesondere müssen die ausgesprochenen Massnahmen **hinreichend präzise sein**, damit die oder der Verantwortliche für die Datenbearbeitung nachvollziehen kann, welche Bearbeitungen fraglich sind und welche Gründe die Massnahme ausgelöst haben. Da die kantonale Öffentlichkeits- und Datenschutzkommission nicht dauerhaft tagt und über kein eigenes Personal verfügt, ist vorgesehen, dass die oder der Beauftragte für den Datenschutz die Geschäfte, die in der Kompetenz der Kommission liegen, **instruiert**. Sie oder er handelt dabei als Gerichtsschreiberin-Berichterstatterin bzw. als Gerichtsschreiber-Berichterstatter und verfügt nur über eine konsultative Stimme (Art. 58 Abs. 5).

Art. 60 und 61, Koordination beim Datenschutz zwischen den Behörden

1. Zusätzlich zu den direkten Handlungsmöglichkeiten, über welche die Aufsichtsbehörde für Datenschutz verfügt, setzt der Vorentwurf auch einen Akzent im Bereich **der Koordination und der Kooperation** mit anderen kantonalen Aufsichtsbehörden in ihrem Kompetenzbereich und anderen Aufsichtsbehörden im Datenschutzbereich in der Schweiz und im Ausland.

2. Wenn irgendeine kantonale Verwaltungsbehörde in Ausübung ihrer Funktion feststellt, dass ein öffentliches Organ ausserhalb der kantonalen Verwaltung, das aber ihrer Aufsicht unterstellt ist, die Bestimmungen des Gesetzes über den Datenschutz nicht einhält, und dass diese Situation gegebenenfalls zu einer Entscheidung von ihr führt, ist sie gehalten, die Aufsichtsbehörde für Datenschutz einzuladen, **Stellung zu nehmen** (Art. 60). Das kann z. B. dann der Fall sein, wenn die kantonale Aufsicht über die Notarinnen und Notare (die Notariatskommission) bei einer Person, die ihrer Aufsicht unterstellt ist, einen Mangel beim Datenschutz feststellt. Wenn die Aufsichtsbehörde für Datenschutz, nachdem sie darüber informiert wurde, entscheidet, eine Untersuchung zu eröffnen, müssen die beiden Behörden **sich untereinander koordinieren**.

3. Gemäss Artikel 61 des Vorentwurfs müssen die Aufsichtsbehörden für Datenschutz der Schweiz und des Auslandes bei der Erfüllung ihrer Aufgaben soweit nötig miteinander **kooperieren**, namentlich indem Informationen ausgetauscht werden, die im Zusammenhang mit der Datenbearbeitung im Gebiet, für das sie zuständig sind, stehen. Die Zusammenarbeit sollte auch die Koordination ihrer Untersuchungen oder ihrer Eingriffe und die Durchführung gemeinsamer Aktionen umfassen. Der Vorentwurf sieht vor, dass der Typ und die Breite der Kooperation Gegenstand einer **schriftlichen Vereinbarung**, **die deren Umfang absteckt,** sein müssen. Beispielhaft für eine Zusammenarbeit sieht der Absatz 3 explizit vor, dass die kantonale Aufsichtsbehörde auch bei privaten Unternehmen eingreifen kann, die sich auf Kantonsgebiet befinden, sofern die oder der Eidgenössische Beauftragte für den Datenschutz ihr ein einen entsprechenden Auftrag erteilt.

Art. 62, Ausnahme zugunsten der Justiz

Im Vorentwurf wird die Ausnahme gestrichen, gemäss welcher das Gesetz über den Datenschutz in der Regel nicht für Gerichtsverfahren gilt (s. Art. 2 Abs. 2 Bst. b des geltenden Gesetzes). Die neue Bestimmung lautet, dass **die kantonale Aufsichtsbehörde für Datenschutz** bei Datenbearbeitungen, die von der richterlichen Gewalt in Ausübung ihrer richterlichen Funktionen durchgeführt werden, nicht zuständig ist. Diese Ausnahmeregelung, deren Geltungsbereich strikt auf gerichtliche Tätigkeiten beschränkt ist, hat das Ziel, die Gewaltentrennung und die Unabhängigkeit der Gerichtsbarkeit sicherzustellen. Sie ist ausdrücklich vorgesehen in Artikel 45 Ziffer 2 der Richtlinie (EU) 2016/680; Artikel 55 Ziffer 3 Verordnung (EU) 2016/679 und Artikel 15 Ziffer 10 Konvention SEV 108+.

2.5.3 Abschnitt 5.3, Weitere Aufgaben der Aufsichtsbehörde

Art. 63 Register der Bearbeitungstätigkeiten

Gemäss dieser Bestimmung ist die Behörde für Öffentlichkeit und Datenschutz für die korrekte und aktuelle Führung des Registers der Bearbeitungstätigkeiten, das in den Artikeln 38–40 des Vorentwurfs vorgesehen ist, verantwortlich. Die Gemeinden können ihr eigenes Register führen. Sie bleiben in diesem Fall aber gehalten, ihre Bearbeitungen zusätzlich der kantonalen Aufsichtsbehörde zu melden.

Art. 64 Tätigkeitsbericht und Information der Öffentlichkeit

1. Die Verpflichtung der Aufsichtsbehörden für Datenschutz, einen Tätigkeitsbericht zu erstellen, ist in Artikel 49 der Richtlinie (EU) 2016/680 und Artikel 59 der Verordnung (EU) 2016/679 ebenso wie in Artikel 15 Ziffer 7 der Konvention SEV 108+ vorgesehen. Sie existiert im geltenden Gesetz bereits unter Artikel 30a Abs. 2. Auf Bundesebene wird die Verpflichtung in Artikel 30 Abs. 1 DSG erwähnt und wurde im Artikel 51 Abs. 1 E-DSG wiederaufgenommen.

2. Die Möglichkeit der Aufsichtsbehörde, **die Öffentlichkeit** über ihre Feststellungen **zu informieren**, wenn das allgemeine Interesse dieses rechtfertigt, ist eine Folge ihrer **Unabhängigkeit**. Aufgrund eines Rechtsgutachtens des Instituts für Föderalismus, das genau dieser Frage im Kanton Freiburg nachging, kann die Aufsichtsbehörde Stellungnahmen abgeben und die öffentliche Meinung auf Verstösse gegen Prinzipien des Datenschutzes aufmerksam machen, die aus ihrer Sicht von den kantonalen Behörden begangen wurden, **ohne dass sie davor ein entsprechendes Einverständnis** einer übergeordneten Behörde **einholen muss**.[16]

[16] WALDMANN Bernhard / SPIELMANN Andre, L'indépendance de l'autorité cantonale de surveillance en matière de protection des données – Avis de droit réalisé sur mandat de la Direction de la Sécurité et de la Justice du canton de Fribourg, Februar 2010, Nr. 133.

2.6 Abschnitt 6, Übergangsbestimmungen

Art. 65, Übergangsrecht

1. Der Übergang zum neuen Recht, namentlich die Verschärfung der Anforderungen an die Sicherheit bei den Verantwortlichen für die Datenbearbeitung, kann **nicht 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 die alten Anforderungen noch galten. Aus diesem Grund sieht der Vorentwurf gewisse Ausnahmebewilligungen und Fristen vor, damit die Verantwortlichen für die Datenbearbeitung ihre Arbeit an die neuen Bestimmungen anpassen können.

2. Zunächst und gemäss Absatz 3 **bleiben** die Bearbeitungen, die unter dem alten Recht begannen, und die zum Zeitpunkt des Inkrafttretens des neuen Gesetzes beendet werden, **den Anforderungen des DSchG von 1994 unterworfen**. Andererseits und soweit dies technisch möglich ist, sind die betroffenen Personen ab dem Inkrafttreten des Gesetzes berechtigt, **sich auf Abschnitt 3 des Gesetzes** (erweitertes Zugangsrecht, Widerspruchsrecht, Recht auf Verfügung über ihre Daten nach dem Tod usw.) **zu berufen**. Die gleiche Regel gilt auch für laufende und künftige Bearbeitungen von Daten.

3. Gemäss Absatz 2 wird das Prinzip des Datenschutzes durch Technik und die damit zusammenhängende Verpflichtung zu einer Datenschutz-Folgenabschätzung nicht **auf Bearbeitungen angewendet, die unter altem Recht begonnen wurden** und die nach dem Inkrafttreten des neuen Rechts fortgesetzt werden, sofern der Zweck der Bearbeitung unverändert bleibt und keine neuen Daten erhoben werden. Diese Regelung ist gerechtfertigt, weil die Pflichten der Verantwortlichen für die Datenbearbeitung gemäss den Artikeln 42–44 sich vor allem auf die Vorphase der Datenbearbeitung beziehen. Die Verantwortlichen der Datenbearbeitung **sollen nicht dazu gezwungen werden, diese rückwirkend zu erfüllen**.

4. Was die übrigen Verpflichtungen betrifft, verfügen die Verantwortlichen der Datenbearbeitung **über eine Frist von zwei Jahren,** um ihre Tätigkeit an das neue Gesetz anzupassen. Die Meldungen von Verletzungen des Datenschutzes müssen der Aufsichtsbehörde oder den betroffenen Personen bereits ab Inkrafttreten des neuen Gesetzes gemacht werden (Abs. 1).

5. Um gemäss **der Richtlinie (EU) 2016/680**, die für die Schweiz ab dem 1. August 2018 verbindlich ist (s. BBI 2017 6941, S. 7170 f.), zu handeln, sollten die Verantwortlichen für die Datenbearbeitung alles daransetzen, um sicherzustellen, dass sie **mit dem Inkrafttreten des neuen Gesetzes** der Pflicht, die betroffenen Person über die Erhebung ihrer Daten zu informieren, und den Verpflichtungen im Zusammenhang mit der Umsetzung des Gesetzes gemäss Abschnitt 4 des Vorentwurfs nachkommen (Abs. 4).

2.7 Anpassung der Spezialgesetzgebung

2.7.1 Anpassung des StatG

Die Änderungen an den Artikeln 5 Abs. 1 und 16 Abs. 2 und 3 haben alleine zum Ziel, auf die neue Version des Gesetzes über den Datenschutz, das vom Grossen Rat verabschiedet wird, zu verweisen.

2.7.2 Anpassung des JG

Die Änderung von Artikel 140 Abs. 1 Bst. c hat keine direkte Verbindung mit der Revision der Gesetzgebung über den Datenschutz. Es handelt sich vielmehr um eine kosmetische Änderung des Gesetzes, die im Prinzip zum Zeitpunkt des Erlasses des ArchG hätte eingeführt werden müssen.

2.7.3 Anpassung des VidG

Die Überwachung mit Videokameras in weiten Teilen des öffentlichen Grunds stellt eine gravierende Beeinträchtigung der 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 43 und 44 des Vorentwurfs (Art. 4 Abs. 3) erforderlich ist.

2.7.4 Anpassung des E-GovSchG

Artikel 21 des E-GovSchG über Pilotprojekte wird aufgehoben, da die Bestimmung in Artikel 21 des Vorentwurfs zur Revision des DSchG eingefügt wurde. Da die beiden Bestimmungen einen sehr ähnlichen Inhalt haben, werden die Pilotversuche, die unter der Bestimmung von Artikel 21 E-GovSchG bewilligt wurden und beim Inkrafttreten dieser Bestimmung fortgeführt werden, **von dieser Änderung nicht tangiert**.

2.7.5 Anpassung des InfoG

In der Praxis arbeiten die oder der Datenschutzbeauftragte und die oder der Beauftragte für Öffentlichkeit und Transparenz dann regelmässig zusammen, wenn es um eine Anfrage für den Zugang zu einem offiziellen Dokument geht, das auch Personendaten enthält. Mit dem neuen Artikel 41 Abs. 2 Bst. c^{bis} wird diese Praxis auf Gesetzesebene verankert.

2.7.6 Anpassung des SchG

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

2.7.7 Anpassung des PolG

1. Die Änderungen, die im PolG erfolgen, dienen im Wesentlichen dazu, **die freiburgische Polizeigesetzgebung an** die Anforderungen der Richtlinie (EU) 2016/680, die für die Schweiz seit dem 25. August 2018 verbindlich ist, **anzupassen**.

2. In Artikel 38c Abs. 1 werden die Voraussetzungen geschaffen, unter denen es möglich wird, das **Profiling** zur Vorbeugung und zur Entdeckung von strafbaren Handlungen einzusetzen. Absatz 2 wird aufgehoben, weil die Bestimmungen, die vorbehalten werden, bereits unter den Geltungsbereich von Absatz 1 Bst. a fallen.

3. Die Aktivitäten in Zusammenhang mit der Prävention und der Entdeckung und der Verfolgung von strafbaren Handlungen setzen notwendigerweise die Bearbeitung von Personendaten **verschiedenener Personenkategorien** voraus. In Artikel 38e Abs. 2 wird verlangt, dass soweit möglich **klar** zwischen Personendaten der verschiedenen Kategorien betroffener Personen **unterschieden wird**: Verdächtige, Personen, die einer strafbare Handlung schuldig gesprochen wurden, Opfer und andere Parteien, so etwa Zeugen und Personen mit nützlichen Informationen oder Kontakten. Ausserdem wird in Absatz 3 gefordert, dass im Moment der Abfassung und Redigierung polizeilicher Protokolle besonders aufgepasst und dabei soweit möglich zwischen **Personendaten, die auf Tatsachen beruhen, und solchen, die auf persönlichen Bewertungen beruhen**, unterschieden wird. Diese beiden Pflichten sind ausdrücklich in den Artikeln 6 und 7 der Richtlinie (EU) 2016/680 vorgesehen.

4. Derzeit bestehen auf europäischer, schweizerischer und interkantonaler Ebene verschiedene Datenbanken, die für die polizeiliche Arbeit erforderlich sind. Artikel 38h bietet die erforderliche gesetzliche Grundlage, damit die freiburgische Polizei über ein **Abrufverfahren** Zugang zu diesen Datenbanken hat.

2.7.8 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.

<u>Anhang</u> *Liste der wichtigsten Abkürzungen*

Gesetzgebungsakte:

Ehemalige Konvention SEV 108	Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 (SR 0.235.1).	2. Änderung des DSG vom 19. März 2010	Bundesgesetz 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).

Ehemalige Richtlinie (EU) 95/46/EG	RICHTLINIE 95/46/EG DES EUROPAISCHEN PARLAMENTS UND DES RATES vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr	SDSG	Bundesgesetz über den Datenschutz im Rahmen der Anwendung des Schengen-Besitzstands in Strafsachen vom 28. September 2018 (Schengen-Datenschutzgesetz, SR 235.3)
Konvention SEV 108 +	Modernisiertes Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 17. und 18. Mai 2018	E-DSG	Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (BBI 2017 7192)
Zusatzprotokoll zum Übereinkommen SEV 108	Zusatzprotokoll zum Übereinkommen SEV 108 vom 8. November 2001 (SR 0.235.11).	DSchG	Gesetz über den Datenschutz des Kantons Freiburg vom 25. November 1994 (DSchG, SGF 17.1)
VRG	Gesetz über die Verwaltungsrechtspflege des Kantons Freiburg vom 23. Mai 1991 (VRG ; SGF 150.1).	Änderung des DSchG vom 8. Mai 2008	Gesetz zur Änderung des Gesetzes über den Datenschutz (Anpassung an das internationale Recht, insbesondere an die Abkommen von Schengen und Dublin) (ASF 2008_053)
Rahmenbeschluss 2008/977/JI	Rahmenbeschluss 2008/977/JI über den Schutz von Personendaten im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen vom 27. November 2008 (Amtsblatt der Europäischen Union L 350/60).	PolG	Gesetz über die Kantonspolizei vom 15. November 1990 (PolG ; SGF 551.1)
Richtlinie (EU) 2016/680	RICHTLINIE (EU) 2016/680 vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung	HGG	Gesetz über die Haftung der Gemeinwesen und ihrer Amtsträger vom 16. September 1986 (HGG; SGF 16.1)
ArchG	Gesetz über die Archivierung und das Staatsarchiv vom 10. September 2015 (ArchG; SGF 17.6).	SchG	Gesetz über die obligatorische Schule vom 9. September 2014 (SchG; SGF 411.0.1)

EKG	Kantonales Gesetz über die Einwohnerkontrolle vom 23. Mai 1986 (EKG; SGF 114.21.1).	GesG	Kantonales Gesundheits-gesetz vom 16. November 1999 (GesG; SGF 821.0.1).
InfoG	Gesetz über die Information und den Zugang zu Dokumenten vom 9. September 2009 (InfoG; RSF 17.5)	LSF	Bundesstatistikgesetz vom 9. Oktober 1992 (BStatG; SR 431.01)
KSG	Freiburger Gesetz über die Beziehungen zwischen den Kirchen und dem Staat vom 26. September 1990 (KSG ;SGF 190.1)		
E-GovSchG	Gesetz über den E-Government-Schalter des Staates vom 2. November 2016 (E-GovSchG; SGF 17.4)	RAG	Bundesgesetz über die Zulassung und Beaufsichtigung der Revisorinnen und Revisoren vom 16. Dezember 2005 (RAG; SR 221.302)
DStG	Gesetz über die direkten Kantons-steuern vom 6. Juni 2000 (DStG; SGF 631.1)	StatG	Gesetz über die kantonale Statistik vom 7. Februar 2006 (StatG; SGF 110.1)
JG	Kantonales Justizgesetz vom 31. Mai 2010 (JG; SGF 130.1)	BGSA	Bundesgesetz vom 17. Juni 2005 über Massnahmen zur Bekämpfung der Schwarzarbeit (Bundesgesetz gegen die Schwarzarbeit, BGSA; SR 822.41).
RVOG	Regierungs- und Verwaltungsorganisationsgesetz des Bundes vom 21. März 1997 (RVOG; SR 172.010)	BGÖ	Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung vom 17. Dezember 2004 (BGÖ; SR 152.3)
DSG	Bundesgesetz über den Datenschutz vom 19. Juni 1992 (DSG; SR 235.1).	VidG	Kantonales Gesetz über die Videoüberwachung vom 7. Dezember 2010 (VidG; SGF 17.3).
1. Änderung des DSG vom 24. März 2006	Änderung des Bundesgesetzes über den Datenschutz vom 24. März 2006 (AS 2007 4983)	DSR	Reglement über die Sicherheit der Personendaten vom 29. Juni 1999 (DSR ; SGF 17.15)

Andere Abkürzungen:

Art.: Artikel

Abs.: Absatz

ASF:	Amtliche Sammlung des Kantons Freiburg
AS:	Amtliche Sammlung des Bundesrechts
Aufl.:	Auflage
Bako:	Basler Kommentar
BBI:	Bundesblatt
BGE:	Bundesgerichtsentscheid
BSG:	Bernische Systematische Gesetzessammlung
EU:	Europäische Union
f.:	folgend
s.:	siehe
SEV:	Sammlung Europäischer Verträge
TGR:	Amtliches Tagblatt der Sitzungen des Grossen Rates