Vortrag

Datum RR-Sitzung:	21. Juni 2023
Direktion:	Direktion für Inneres und Justiz
Geschäftsnummer:	2019.JGK.647
Klassifizierung:	Nicht klassifiziert

Datenschutzgesetz

Inhaltsverzeichnis

1. Zusammenfassung

Das Recht auf Datenschutz ist ein Grundrecht. Das kantonale Datenschutzgesetz erläutert die Grundrechtsgarantien aus Bundes- und Kantonsverfassung und setzt weitere internationale Verpflichtungen um. Primär handelt es sich um das in Artikel 13 Absatz 2 der Bundesverfassung vom 18. April 1999 (BV)[1] enthaltene Recht auf informationelle Selbstbestimmung, das vom bernischen Gesetzgeber in Artikel 18 der Verfassung des Kantons Bern vom 6. Juni 1993 (KV)[2] als Recht auf Datenschutz konkretisiert worden ist. Die verfassungsmässige Verankerung verdeutlicht die Wichtigkeit des Datenschutzes. Deren Ursprung ist auf die Angst vor der Kontrolle des Individuums durch den Staat («gläserner Mensch») zurückzuführen. Eine verfassungskonforme Umsetzung des Grundrechts auf Datenschutz bedeutet insbesondere sachgerecht und transparent mit Personendaten umzugehen, individuelle Kenntnis- und Einflussmöglichkeiten zu gewährleisten und adäquate Kontrollen zu schaffen.

Für Bundesbehörden und Private ist das Bundesgesetz vom 19. Juni 1992 über den Datenschutz (Datenschutzgesetz, DSG)[3] anwendbar; für kantonale und kommunale Behörden richtet sich die Bearbeitung von Personendaten nach deren Datenschutzgesetzen.

[1] SR 101
[2] BSG 101.1
[3] SR 235.1

Beim Datenschutzrecht handelt es sich um eine Querschnittsmaterie. Folglich regelt das kantonale Datenschutzgesetz vom 19. Februar 1986 (KDSG)[4] den Datenschutz im Allgemeinen (Bearbeitungsgrundsätze, Rechte der betroffenen Personen, Aufsicht usw.). Seine Grundsätze bedürfen der Umsetzung im Spezialgesetz (auch bereichsspezifisches Fachrecht oder materielles Datenschutzrecht genannt).

Bund und Kantone sind gestützt auf die Weiterentwicklung des Schengen-Besitzstands verpflichtet, ihre Gesetzgebung im Bereich des Datenschutzes EU-konform auszugestalten. Die Vorlage passt die kantonalen Grundlagen ans europäische Recht und die Bundesgesetzgebung an: Der generelle Geltungsausschluss des kantonalen Datenschutzgesetzes für hängige Verfahren der Rechtspflege ist aufzuheben. Lediglich die konkrete Bearbeitung von Personendaten und die Rechte der betroffenen Personen sind weiterhin vom Geltungsbereich ausgenommen. Infolgedessen ist in Gerichtsverfahren, Verfahren der Verwaltungsrechtspflege und in Verfahren nach einer besonderen Verfahrensordnung beispielsweise die Datensicherheit als Grundsatz des Datenschutzes zu gewährleisten. Ebenfalls unterstehen die administrativen Tätigkeiten der betroffenen Behörden der kantonalen Datenschutzgesetzgebung. Mit der Revision ergänzt wird der Katalog der besonders schützenswerten Personendaten um gewerkschaftliche, ethnische, genetische und biometrische Daten sowie um verwaltungsrechtliche Verfolgungen oder Sanktionen. Die Informations- und Meldepflichten der verantwortlichen Behörden werden erweitert und die Rechte der betroffenen Personen klarer definiert. Der Aufwand der verantwortlichen Behörden wird verringert, indem das Register der Datensammlungen beschränkt wird.

Ein wichtiger Punkt der Revision ist ausserdem die Stellung und Unabhängigkeit der Datenschutzaufsichtsstellen. Um den technischen Anforderungen gerecht zu werden und die Gemeinden zu entlasten, wird die bisher föderalistisch ausgestaltete Datenschutzaufsicht grösstenteils zentralisiert. In Übereinstimmung mit den erhöhten europäischen Standards werden den verbleibenden Datenschutzaufsichtsstellen Verfügungsbefugnisse eingeräumt. Ferner spricht das kantonale Datenschutzgesetz neu von Datenschutzbehörden statt von Aufsichtsstellen. Dies soll klarstellen, dass die Datenschutzbehörden vorwiegend beraten, anleiten und ausbilden und nicht kontrollieren und sanktionieren.

Die zahlreichen sowohl inhaltlichen als auch systematischen Änderungen bedingen eine Totalrevision des kantonalen Datenschutzgesetzes.

2. Ausgangslage

2.1 Auswirkungen der europäischen Rechtsentwicklungen auf die Schweiz

Am 27. April 2016 verabschiedeten das Europäische Parlament und der Rat der Europäischen Union eine Reform der Datenschutzgesetzgebung, die zwei Erlasse umfasst: Die Verordnung (EU) 2016/679 (nachfolgend: Datenschutz-Grundverordnung)[5] und die Richtlinie (EU) 2016/680[6]. Am 10. Oktober 2018 beschloss der Europarat ausserdem das Zusatzprotokoll[7] zum Übereinkommen vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (nachfolgend: SEV Nr. 108+), das die Bundesversammlung am 19. Juni 2020 genehmigte.[8] Das Zusatzprotokoll entspricht inhaltlich weitgehend der Richtlinie (EU) 2016/680 und der Datenschutz-Grundverordnung, ist jedoch weniger detailliert.

Die Richtlinie (EU) 2016/680 stellt für die Schweiz eine Weiterentwicklung des Schengen-Besitzstands dar. Deshalb ist sie verpflichtet, ihre innerstaatliche Rechtsordnung entsprechend anzupassen. Die Notifikation erfolgte am 1. August 2016; die zweijährige Frist für die Übernahme des Rechtsaktes dauerte bis

[4] BSG 152.04
[5] Vollständiger Name: Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).
[6] Vollständiger Name: Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr.
[7] BBl 2020 599
[8] BBl 2020 5725

zum 1. August 2018. Der Kanton Bern setzte die Anforderungen mit der Einführungsverordnung vom 4. Juli 2018 zur EU-Datenschutzrichtlinie (EV EDS)[9] um.

Ausserhalb der Schengen-Zusammenarbeit gilt die Schweiz als Drittstaat. Die Datenschutz-Grundverordnung gehört nicht zur Schengen-Acquis, weshalb sie grundsätzlich nicht zu übernehmen ist. Allerdings dürfen zwischen einem Drittstaat und den Mitgliedstaaten der Europäischen Union Personendaten nur ausgetauscht werden, wenn der Drittstaat ein angemessenes Schutzniveau gewährleistet. Ein angemessenes Schutzniveau wird mittels Angemessenheitsbeschluss von der Europäischen Union bestätigt. Künftig erfolgt die Überprüfung der schweizerischen Gesetzgebung anhand der in der Datenschutz-Grundverordnung enthaltenen Anforderungen. Die Schweiz kann die Anforderungen erfüllen, indem sie das SEV Nr. 108+ umsetzt, da bei dessen Erarbeitung auf ein angemessenes Schutzniveau geachtet wurde.

2.2 Umsetzung auf Bundesebene

Die beiden Räte verabschiedeten am 25. September 2020 die Totalrevision des Datenschutzgesetzes des Bundes. Mit der Revision erfolgte die Anpassung der schweizerischen Gesetzgebung an die Richtlinie (EU) 2016/680 und das SEV Nr. 108+. Das revidierte Bundesgesetz vom 25. September 2020 über den Datenschutz (Datenschutzgesetz, revDSG)[10] wird im September 2023 in Kraft treten. Mit Inkrafttreten wird das Schengen-Datenschutzgesetz[11] aufgehoben, welches bis dahin die Schengen-Acquis gewährleistet.

2.3 Umsetzung auf kantonaler Ebene

Mit der vorliegenden Revision passt der Kanton Bern seine Datenschutzgesetzgebung mit folgendem Ziel an die europäischen Vorgaben an: Erfüllen der Datenschutzanforderungen der Richtlinie (EU) 2016/680 und des SEV Nr. 108+, womit die Voraussetzungen für den Angemessenheitsbeschluss geschaffen werden. Den Handlungsbedarf auf kantonaler Ebene ermittelte die Arbeitsgruppe Datenschutz der Konferenz der Kantonsregierungen (KdK). Die vorliegende Revision orientiert sich – wie in den übrigen Kantonen – am von der Arbeitsgruppe verfassten Leitfaden (KdK-Leitfaden).

Da die Richtlinie (EU) 2016/680 bereits bis August 2018 ins Landesrecht umgesetzt sein musste, und dieses Ziel im ordentlichen Gesetzgebungsverfahren nicht zu erreichen war, wurden vorerst mit einer Dringlichkeitsverordnung die von der Richtlinie (EU) 2016/680 und dem SEV Nr. 108+ zwingend umzusetzenden Bestimmungen ins kantonale Recht übernommen. Die befristete und um drei Jahre zu verlängernde EV EDS wird mit der Revision ins reguläre Recht überführt und folglich aufgehoben.

Gleichzeitig werden im Rahmen der Revision verschiedene weitere Änderungsbedürfnisse umgesetzt:

- Umsetzung der Motion 224-2016 (Vogt) «Lockerungen im Datenschutz – für Regelungen mit Augenmass»,
- Anliegen der Geschäftsprüfungskommission des Grossen Rates (GPK) betreffend die Bestimmungen zu Aufsicht und Wahl der oder des Datenschutzbeauftragten und
- Zuständigkeitsfragen zwischen den kommunalen und kantonalen Datenschutzbehörden.

[9] BSG 152.043
[10] BBl 2020 7639
[11] Vollständiger Name: Bundesgesetz über den Datenschutz im Rahmen der Anwendung des Schengen-Besitzstands in Strafsachen» (Schengen-Datenschutzgesetz, SDSG).

3. Grundzüge der Neuregelung

3.1 Grundsatz

Mit der Anpassung an das europäische Recht erfährt der Datenschutz eine Aufwertung. Die wichtigsten Neuerungen sind:

- Die datenschutzrechtlichen Grundsätze finden auf die Gerichtsbehörden und die Staatsanwaltschaft Anwendung, mit Ausnahmen, soweit es das europäische Recht zulässt,
- Einführung des Profilings als neue Bearbeitungsart,
- Zusätzliches Instrument der Datenschutzfolgenabschätzung als Ergänzung zur Vorabkontrolle und
- Erhöhte Transparenz durch erweiterte Informationspflichten bei der Beschaffung von Personendaten und Meldepflichten bei Datenschutzverletzungen, mit Ausnahmen, soweit es das europäische Recht zulässt.

Zusätzlich zur Anpassung an das europäische Recht behandelt die Vorlage auch die Motion Vogt. Sie fordert eine Lockerung bzw. Vereinfachung der Datenschutzvorgaben für die kantonalen und kommunalen Behörden, insbesondere in rechtlicher und organisatorischer Hinsicht sowie die Vornahme bzw. Einleitung der nötigen Rechtsänderungen. Aufgrund der europäischen Vorgaben ist der Kanton Bern gezwungen, gewisse Instrumente in das kantonale Recht zu überführen, was im Widerspruch zur Motionsforderung eines gelockerten Datenschutzes steht. Um der Motionsforderung dennoch gerecht zu werden, setzt der Kanton Bern das europäische Recht mit Augenmass um und sieht dort Ausnahmen vor, wo es das europäische Recht zulässt. Dennoch ist es unvermeidbar, dass insbesondere hinsichtlich der Transparenz strengere Regeln gelten.

Die kantonale Aufsichtsstelle nennt sich neu kantonale Datenschutzbehörde. Sie übernimmt diverse aufsichtsrechtliche Aufgaben der Gemeinden, die somit in organisatorischer und fachlicher Hinsicht entlastet werden.

3.2 Geltungsbereich

Eine grundsätzliche Ausnahme für die Anwendung des Datenschutzes in hängigen Verfahren der Zivil-, Straf- und Verwaltungsrechtspflege wie nach bisherigem Recht ist wegen den europäischen Vorgaben nicht mehr zulässig. Das anwendbare Verfahrensrecht soll jedoch weiterhin die Bearbeitung von Personendaten und die Rechte der betroffenen Personen im konkreten Anwendungsfall regeln. Dennoch müssen die verantwortlichen Behörden in diesen Bereichen die Grundsätze des Datenschutzes einhalten. So sind sie beispielsweise verpflichtet, die Datensicherheit zu gewährleisten, unabhängig von einer Bearbeitung von Personendaten in einem konkreten Verfahren. Soweit das Datenschutzgesetz für diese Behörden gilt, unterstehen sie zudem der Aufsicht der kantonalen Datenschutzbehörde. Die kantonale Datenschutzbehörde kann jedoch gegenüber den Gerichten und der Staatsanwaltschaft keine Verwaltungsmassnahmen ergreifen, d.h. keine Verfügungen erlassen.

3.3 Aktualisierung des Katalogs der besonders schützenswerten Personendaten

Die Bearbeitung von bestimmten Daten führt von Gesetzes wegen zu einem schweren Eingriff in das Grundrecht auf Datenschutz. Diese Personendaten werden als besonders schützenswerte Personendaten bezeichnet. Die besonders schützenswerten Personendaten sollen nicht mehr in einem separaten Artikel normiert, sondern bei den Begriffsbestimmungen definiert werden. Die neue Systematik orientiert sich am Bundesrecht. In Übereinstimmung mit dem europäischen Recht und dem revidierten Datenschutzgesetz des Bundes soll ausserdem der Katalog ergänzt werden. Explizit aufgenommen werden gewerkschaftliche Daten, die bisher unter die weltanschaulichen oder politischen Ansichten subsumiert

worden sind. Weiter ergänzt wird der Katalog um die Ethnie, verwaltungsrechtliche Verfolgungen oder Sanktionen und genetische und biometrische Daten.

3.4 Transparenzbestimmungen

Die Richtlinie (EU) 2016/680 bzw. das Übereinkommen SEV Nr. 108+ auferlegt der verantwortlichen Behörde neue Pflichten, so

- die Pflicht zur Vornahme einer Datenschutzfolgenabschätzung,
- erweiterte Informationspflichten und
- in bestimmten Fällen die Pflicht, den betroffenen Personen Verletzungen der Datensicherheit mitzuteilen.

Diese Pflichten sind dem kantonalen Recht nicht völlig neu. Die Prüfung, ob eine Datenbearbeitung voraussichtlich ein hohes Risiko für eine Grundrechtsverletzung birgt (Datenschutzfolgenabschätzung), war zwar bis anhin im Datenschutzgesetz nicht verankert. Allerdings kennt das geltende Recht die Pflicht, gewisse Vorhaben mit besonderen Risiken der Datenschutzbehörde zur Stellungnahme zu unterbreiten (Vorabkontrolle; Art. 17a KDSG). Insofern ist die Datenschutzfolgenabschätzung in der Pflicht der Vorabkontrolle enthalten. Auf Stufe Kanton kennt das geltende Recht ausserdem die Informationssicherheit und Datenschutz (ISDS)-Analyse für den Einsatz von Informations- und Telekommunikationstechnologien (ICT) durch die Kantonsverwaltung, die in wesentlichen Teilen der Datenschutzfolgenabschätzung entspricht.

Ferner besteht bereits heute eine Informationspflicht im Zeitpunkt der Beschaffung der Personendaten, sofern die betroffene Person dies verlangt oder Personendaten systematisch, namentlich mittels Fragebogen, erhoben werden (Art. 9 Abs. 4 KDSG). Die europäischen Vorgaben erlauben Ausnahmen von der Informationspflicht, wovon im Kanton Bern mit Blick auf die Motion Vogt Gebrauch gemacht werden soll.

Neu zu regeln ist die Meldepflicht an die Datenschutzbehörde bei einer Verletzung der Datensicherheit, die voraussichtlich zu einem Risiko für die Grundrechte der betroffenen Personen führt. Das kantonale Datenschutzrecht stellt mehrere Instrumente zur Verfügung, die solche Verletzungen verhindern sollen (Datenschutzfolgeabschätzung, Vorabkontrolle, Massnahmen der Informationssicherheit etc.). Es ist deshalb davon auszugehen, dass sich solche Vorfälle nur selten ereignen. Kommt es zu einer Verletzung, kann aber im Einzelfall ein erheblicher Aufwand anfallen.

3.5 Register der Datensammlungen und Verzeichnis der Bearbeitungstätigkeiten

Das Register der Datensammlungen soll in abgespeckter Form weitergeführt werden. Neu müssen nur noch Datensammlungen erfasst werden, die besonders schützenswerte Personendaten enthalten, was gegenüber der geltenden Regelung eine Vereinfachung darstellt. Die Registerführung ist sehr aufwändig und stösst auf Kritik. Mit Blick auf die Motion Vogt ist die Registerführung deshalb zu beschränken. Aus datenschutzrechtlicher Sicht ist dies unerfreulich, da die Beschränkung der Registerführung auf Datensammlungen mit besonders schützenswerten Personendaten dem Anspruch an eine transparente Datenbearbeitung gegenübersteht. Nur wer weiss, welche Personendaten über sie oder ihn bearbeitet werden, kann die aus dem Grundrecht auf Datenschutz fliessenden Rechte geltend machen. Personen können zwar weiterhin bei der verantwortlichen Behörden Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden, eine zentrale Erfassung aller Datensammlungen fällt jedoch weg.

Zudem verlangt Artikel 24 der Richtlinie (EU) 2016/680, dass die im Justiz- und Polizeibereich tätigen Behörden ein Verzeichnis über ihre Bearbeitungstätigkeiten führen. Die Pflicht soll ins kantonale Datenschutzrecht aufgenommen werden. Der Inhalt des Verzeichnisses regelt der Regierungsrat auf Verordnungsstufe.

3.6 Aufsichtsbereich

Die kantonale Aufsichtsstelle nennt sich neu kantonale Datenschutzbehörde. Sie ist vorwiegend beratend, anleitend und ausbildend tätig und nicht kotrollierend und sanktionierend, was sich auch im Namen widerspiegeln soll. Ziel ist es, den Missbrauch von Personendaten zu verhindern und nicht diesen später zu sanktionieren.

Als Ausfluss der Gemeindeautonomie führt heute jede Gemeinde und gemeinderechtliche Körperschaft für ihren Bereich eine eigene Aufsichtsstelle, die die Aufgaben der Datenschutzbehörde wahrnimmt. Im Rahmen der Revision sollen die Gemeinden entlastet werden. Die Qualität und Verfügbarkeit der kommunalen Datenschutzbehörden ist sehr unterschiedlich. Oft übernimmt die Aufgabe das Rechnungsprüfungsorgan oder die Geschäftsprüfungskommission, die mangels Expertise bzw. Fallhäufigkeit nicht über das notwendige Fachwissen verfügt. Die Datenschutzfragen sind komplex und werden immer anspruchsvoller. Besonders der technische Wandel (z.B. die vermehrte Nutzung von Cloud-Services) erfordert ein grosses und aktuelles Expertenwissen auch im Bereich der Informationssicherheit. Entsprechend erhält die kantonale Datenschutzbehörde schon heute regelmässig Anfragen von Gemeindebehörden, welche sie zuständigkeitshalber an die kommunalen Datenschutzbehörden verweisen muss. Ausserdem ist es wenig effizient, wenn jede kommunale Datenschutzbehörde die gleichen Rechtsabklärungen trifft und die Einhaltung der datenschutzrechtlichen Bestimmungen prüft. Vielerorts ist weder den Angestellten der verantwortlichen Behörde noch den Bürgerinnen und Bürgern bekannt, dass eine kommunale Anlaufstelle für Datenschutzfragen besteht.

Zusammen mit der kantonalen Datenschutzbehörde, dem Amt für Gemeinden und Raumordnung, dem Verband Bernischer Gemeinden (VBG), der Geschäftsleitung der Regierungsstatthalterinnen und Regierungsstatthalter sowie unter Einbezug verschiedener Gemeinden unterschiedlicher Grössen wurde ein neues Modell entwickelt. Grundsätzlich verschieben sich die bisherigen Aufgaben der kommunalen Datenschutzbehörden zur kantonalen Stelle, davon ausgenommen sind die vier bevölkerungsstärksten Gemeinden (Biel/Bienne, Bern, Köniz und Thun). Der Fokus der kantonalen Datenschutzbehörde liegt dabei auf der Beratung, Anleitung und Ausbildung der Gemeindebehörden. Das Datenschutzniveau in den Gemeinden soll dadurch gestärkt und die Ressourcen effizienter eingesetzt werden. Die Zentralisierung soll mittels Lastenausgleich abgegolten werden, wobei dank Synergieeffekten insgesamt spürbare Einsparungen erwartet werden können.

3.7 Gesetzessystematik

Die umfassenden inhaltlichen Änderungen des Gesetzes bedürfen auch einer Änderung der Systematik, welche die Verschiebung diverser Kapitel und Artikel zur Folge hat.

Der besseren Übersicht halber sollen die Kapitel zur Bearbeitung von Personendaten und zur Datenschutzbehörde jeweils in Abschnitte unterteilt werden. Wie auf Stufe Bund wird ein separates Kapitel geschaffen für die Pflichten der verantwortlichen Behörden und von beauftragten Dritten, welches das bisherige Kapitel der Datensammlungen konsumiert. Ferner verschiebt sich das Kapitel Verfahren und Rechtsschutz – wie in der bernischen Gesetzgebung üblich – nach hinten und wird mit dem Kapitel über die Datenschutzbehörde getauscht. Im Vergleich ergibt sich folgende Gesetzessystematik:

KDSG	VE-revKDSG
1 Allgemeine Bestimmungen	1 Allgemeine Bestimmungen
2 Bearbeiten von Personendaten	2 Bearbeiten von Personendaten
	2.1 Grundsätze 2.2 Besondere Bearbeitungsformen 2.3 Bearbeiten für nicht personenbezogene Zwecke

3	Datensammlungen	3	Pflichten der verantwortlichen Behörde und von beauftragten Dritten 3.1 Pflichten vor Inbetriebnahme 3.2 Registereintragungs- und Verzeichnispflicht 3.3 Informationspflichten 3.4 Meldepflichten bei Verletzungen von Datensicherheit
4	Rechte der betroffenen Person	4	Rechte der betroffenen Person
6	Aufsicht	5	Datenschutzbehörden
			5.1 Kantonale Datenschutzbehörde 5.2 Gemeinderechtliche und landeskirchliche Datenschutzbehörden 5.3 Aufgaben der Datenschutzbehörden
5	Verfahren und Rechtsschutz	6	Verfahren und Rechtsschutz
		7	Ausführungsbestimmungen
7	Schlussbestimmungen	8	Übergangs- und Schlussbestimmungen

3.8 Revision weiterer Gesetze

3.8.1 Revision Facherlasse

Indirekte Änderungen in anderen Erlassen werden nur vorgenommen, soweit die Revision des kantonalen Datenschutzgesetzes zu Widersprüchen, Lücken oder Unklarheiten in Facherlassen führt. Eine indirekte Änderung ist ausserdem nur zulässig, wenn Erlasse der gleichen Erlassart betroffen sind. Demzufolge erfordert die Anpassung eines Dekrets oder einer Verordnung eine separate Vorlage[12].

Das kantonale Datenschutzgesetz ist ein sogenanntes Querschnittgesetz. Daraus folgt, dass die Grundsätze des Datenschutzes wie das Erfordernis einer gesetzlichen Grundlage, der Zweckbindungsgrundsatz, der Grundsatz von Treu und Glauben, die Verhältnismässigkeit, die Datenrichtigkeit oder Datensicherheit von sämtlichen Behörden zu beachten sind, für die das kantonale Datenschutzgesetz gilt. Es liefert jedoch nicht die gesetzliche Grundlage für eine konkrete Datenbearbeitung. Diese findet sich im Fachgesetz. Je nach Art der bearbeiteten Personendaten gelten hierfür unterschiedliche Anforderungen (vgl. Erläuterungen zu Art. 4 VE-revKDSG). In folgenden Gesetzen hat die Revision inhaltliche Änderungen zur Folge:

3.8.2 Gesetz vom 7. März 2022 über die digitale Verwaltung (DVG)[13]

Die als vorübergehend konzipierten datenschutzrechtlichen Bestimmungen im DVG werden in leicht geänderter Fassung ins kantonale Datenschutzgesetz überführt. Mehr dazu unter Ziff. 7.9.2.

3.8.3 Gesetz vom 12. September 1985 über Niederlassung und Aufenthalt der Schweizer (GNA)[14] und das Einführungsgesetz vom 9. Dezember 2019 zum Ausländer- und Integrations- sowie Asylgesetz (EG AIG und AsylG)[15]

Mit der Revision werden die Bestimmungen zur Bekanntgabe von Personendaten zusammengefasst und die Bekanntgabe durch die Einwohnergemeinde in das Spezialgesetz verschoben (vgl. Ziff. 7.9.3). Bei

[12] vgl. zum Ganzen Rechtsetzungstechnische Richtlinien, Modul 3, Ziff. 2.2.4.2.
[13] BSG 109.1
[14] BSG 122.11
[15] BSG 122.20

letzterer Bestimmung handelt es sich um materielles Datenschutzrecht, welches nicht im Datenschutzrecht als Querschnittsmaterie zu regeln ist und bisher einen Fremdkörper im Gesetz darstellt.

3.8.4 Gesetz vom 20. Juni 1985 über die Organisation des Regierungsrates und der Verwaltung (Organisationsgesetz, OrG)[16]

Die kantonale Datenschutzbehörde ist eine organisatorisch und institutionell unabhängige Aufsichtsstelle wie die Finanzkontrolle. In Angleichung an die Finanzkontrolle soll der Titel 2a mit «kantonale Datenschutzbehörde» ergänzt und ein zusätzlicher Artikel 40b analog zu demjenigen der Finanzkontrolle geschafften werden, der die kantonale Datenschutzbehörde als selbständige Organisationseinheit bezeichnet. Aus der Systematik ergibt sich ausserdem, dass die kantonale Datenschutzbehörde zur Verwaltung gehört. Mehr dazu unter Ziff. 7.9.4.

3.9 Verworfene Bestimmungen

3.9.1 Versuchsverordnung

Eine Versuchsverordnung bietet die Möglichkeit, neue Formen des Verwaltungshandelns zu erproben. Die experimentelle Gesetzgebung dient der Abschätzung der Auswirkungen möglicher neuer Regelungen und damit der Verbesserung der Entscheidungsgrundlagen des Gesetzgebers im ordentlichen Rechtsetzungsverfahren. Anlässlich der verwaltungsinternen Vorabkonsultation wurde die Prüfung beantragt, ob eine Rechtsgrundlage für den Erlass von Versuchsverordnungen im kantonalen Datenschutzgesetz zu erlassen ist. Die Grundlage in Artikel 44 OrG ist hierfür ausreichend. Gestützt auf die ausdrückliche Ermächtigung in Absatz 3 können Versuchsverordnungen auch Bestimmungen enthalten, die von kantonalen Gesetzen abweichen. Zwingende Bestimmungen des Bundesrechts, des kantonalen Verfassungsrechts und von interkantonalen Vereinbarungen sind jedoch stets zu beachten. Folglich kann in Versuchsverordnungen unter Umständen auch die Bearbeitung von besonders schützenswerten Personendaten geregelt werden, sofern die Delegationsgrundsätze nach Artikel 69 Absatz 4 der Verfassung vom 6. Juni 1993 des Kantons Bern (KV)[17] eingehalten sind. Insbesondere müsste die Aufgabe, die eine Bearbeitung von besonders schützenswerten Personendaten erforderlich macht, im Gesetz geregelt sein.

3.9.2 Datenschutzberaterin oder Datenschutzberater

Im Polizei- und Justizbereich sieht Artikel 32 der Richtlinie (EU) 2016/680 vor, dass die verantwortlichen Behörden sogenannte Datenschutzbeauftragte ernennen. Sie übernehmen die verwaltungsinterne Beratungsfunktion für den Datenschutz und sind nicht zu verwechseln mit den schweizerischen Datenschutzbeauftragten auf Bundes- und Kantonsebene, die eine unabhängige Aufsichtsfunktion ausüben. Die Aufgaben der oder des Datenschutzbeauftragten nach der Richtlinie (EU) 2016/680 entsprechen im Kanton Bern der internen Kontaktstelle für Datenschutz nach Artikel 15 der Datenschutzverordnung vom 22. Oktober 2008 (DSV)[18], die mindestens jede Direktion und die Staatskanzlei bezeichnen müssen. Sofern vorhanden, sind zudem die Amtsjuristinnen und Amtsjuristen je für ihren Zuständigkeitsbereich Kontaktstelle. Zu ihren Aufgaben gehört die Überwachung, Beratung und Zusammenarbeit mit der kantonalen Datenschutzbehörde. Die Kontaktstellen sind das Äquivalent zu den Datenschutzberaterinnen und Datenschutzberatern auf Bundesebene (Art. 10 Abs. 4 revDSG) und sollen mit der Revision der kantonalen Datenschutzverordnung künftig gleich bezeichnet werden. Gemäss Artikel 150 des Polizeigesetzes

[16] BSG 152.01
[17] BSG 101.1
[18] BSG 152.040.1

(PolG) vom 10. Februar 2019[19] erfüllt die oder der Datenschutzverantwortliche diese Aufgabe. Mit einer indirekten Änderung des Polizeigesetzes ist auch diese Bezeichnung anzugleichen. Im Bereich des Justizvollzuges übernimmt die zuständige Amtsjuristin oder der zuständige Amtsjurist diese Funktion. Auf Initiative der kantonalen Datenschutzbehörde soll sich der Kontakt zwischen den beratenden Stellen verstärken und das Datenschutzniveau dadurch künftig verbessern.

Die verwaltungsinterne Pflicht, eine Datenschutzberaterin oder einen Datenschutzberater zu bezeichnen, ist Ausfluss der Datenschutzverantwortung der zuständigen Behörde. Nach dem Grundsatz der Organisationsautonomie des Regierungsrates erfolgt die verwaltungsinterne Aufgabenzuweisung zur Bezeichnung der Datenschutzberaterinnen und Datenschutzberater durch Verordnung.

Die Gerichte und andere unabhängige Justizbehörden wie die Staatsanwaltschaft können jedoch im Rahmen der justiziellen Tätigkeit von dieser Pflicht befreit werden, weshalb auf die Aufnahme einer entsprechenden Bestimmung verzichtet wird. Ausserhalb der justiziellen Tätigkeit wird die Funktion von der Justizleitung als gemeinsames Selbstverwaltungsorgan des Obergerichts, des Verwaltungsgerichts und der Generalstaatsanwaltschaft wahrgenommen.

3.9.3 Haftungsbestimmung

Das kantonale Datenschutzgesetz regelt bisher in Übereinstimmung mit dem allgemeinen Verantwortlichkeits- bzw. Staatshaftungsrecht, dass bei widerrechtlicher Datenbearbeitung ein Anspruch auf Schadenersatz und Genugtuung besteht (Art. 25 KDSG). Es handelt sich dabei um eine spezialgesetzliche Norm, die grundsätzlich den allgemeinen Regeln vorgeht. Der Bestimmung ist jedoch letztlich kein vom allgemeinen Staatshaftungsrecht abweichender Gehalt inhärent.[20] Die Bestimmung ist daher nicht ins neue Recht zu überführen.

4. Erlassform

Beim Datenschutz handelt es sich um ein verfassungsmässiges Recht (Art. 18 KV). Die Grundzüge des Datenschutzes verlangen eine Grundlage in einem Gesetz. Dazu gehören die materiellen Grundregeln des Datenschutzes wie die Grundsätze des Bearbeitens von Personendaten oder die Rechte der betroffenen Person und die organisatorisch-institutionellen Regeln wie das Verfahren zur Durchsetzung der Rechte oder die Sicherstellung und Wirksamkeit der Datenschutzbehörden.

Das Datenschutzrecht liefert aber auf weiten Strecken keine gesetzliche Grundlage für eine Grundrechtseinschränkung durch das Bearbeiten von Personendaten; vielmehr handelt es sich um ein Querschnittsrecht. Deshalb regelt es lediglich die Grundzüge für die Bearbeitung von Personendaten und die Rechte der betroffenen Personen. Die Sachgesetze regeln in ihrem Sachbereich die sachspezifischen Aspekte wie etwa besondere Rechte für die Bekanntgabe von Personendaten oder besondere Geheimhaltungspflichten. Für Einzelheiten und Modalitäten genügt es, wenn das Gesetz den Rahmen vorgibt und der Regierungsrat Weiteres durch Verordnung regelt.

5. Rechtsvergleich

Der Kanton Bern hat als Vorreiter bereits am 4. Juli 2018 die EV EDS erlassen, um die Anforderungen der Richtlinie (EU) 2016/680 innert der kurzen Umsetzungsfrist provisorisch umzusetzen. In den Kantonen Aargau, Appenzell Innerhoden, Basel-Land, Freiburg, Luzern, St. Gallen, Schaffhausen, Schwyz,

[19] BSG 551.1
[20] BVR 2008 S. 49 E. 6.6.2; Schwegler, Ivo (2021): Informations- und Datenschutzrecht. In: Müller, Markus /Feller, Reto (Hrsg.), Kommentar zum bernischen Verwaltungsrecht. Bern: Stämpfli Verlag AG: S. 396.

Zug und Zürich sind die Anpassungen an die europäischen Grundlagen per Mitte 2022 ebenfalls vollzogen. Es folgt ein Überblick über die Rechtslage in den Kantonen Aargau, St. Gallen, Zürich und Luzern.

5.1 Kanton Aargau

Im Aargauer Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (SAR Nr. 150.700) beschränkt sich der Geltungsbereich neu in Angleichung an das übergeordneten Recht auf natürliche Personen. Neu explizit erwähnt ist das Recht auf Löschung der Daten und die Informationspflicht der öffentlichen Organe bei der Beschaffung von Personendaten. Ebenfalls aufgenommen hat der Kanton Aargau das Instrument der Datenschutzfolgenabschätzung und eine erweiterte Pflicht zur Vorabkonsultation bei der oder dem Beauftragten für Öffentlichkeit und Datenschutz, die Meldepflicht bei unbefugten Datenbearbeitungen und Datenverlusten, sofern diese zu einem Risiko für die Rechte der betroffenen Person führen. Die Stellung der oder des Beauftragten für Datenschutz wurde gestärkt, indem sie oder er gegenüber den Behörden nach Abschluss der Untersuchung eine Verfügung erlassen kann.

Aufgehoben wurde die Bestimmungen über Pilotprojekte und Evaluationen sowie das Register der Datensammlungen, ausgenommen die Register über die Datenbearbeitungstätigkeiten der Strafbehörden, die im Spezialerlass geregelt sind.

5.2 Kanton St. Gallen

Auch der Kanton St. Gallen nimmt in seinem geänderten Datenschutzgesetz (sGS Nr. 142.1) die juristischen Personen vom Geltungsbereich aus. Eingefügt hat er die Datenschutzfolgenabschätzung, die Vorabkonsultation und die Meldepflicht bei Verletzungen der Datensicherheit. Das Register für Datensammlungen bleibt bestehen. Zudem führen die Justizbehörden und die Polizei ein Verzeichnis der Bearbeitungstätigkeiten. Die Leiterin oder der Leiter der kantonalen Fachstelle für Datenschutz erhält die Befugnis, Verfügungen zu erlassen, wenn absehbar ist, dass die Behörde eine Empfehlung ablehnt oder ihr nicht Folge leistet. Zudem wird sie oder er neu auf eine Amtsdauer von vier Jahren gewählt und erhält die Befugnis, Mitarbeiterinnen und Mitarbeiter anzustellen.

5.3 Kanton Zürich

Das Gesetz über die Information und den Datenschutz (IDSG, LS Nr. 170.4) verzichtet darauf, den Geltungsbereich des Gesetzes auf natürliche Personen zu beschränken. Änderungen betreffen die Datenschutzfolgenabschätzung, die Vorabkontrolle sowie die Meldepflicht bei einer unbefugten Datenbearbeitung oder nach einem Datenverlust, wenn die Grundrechte der betroffenen Person gefährdet sind. Zudem werden die Informationspflichten der verantwortlichen öffentlichen Organe erweitert. In den Fachgesetzen wurden die Gerichts-, Straf- und Justizvollzugsorgane verpflichtet, eine für die Datenschutzberatung zuständige Person zu bezeichnen. Diese Person berät und unterstützt die entsprechende Behörde in Datenschutzbelangen, nimmt Datenschutzfolgenabschätzungen vor und ist Ansprechperson des oder der Beauftragten für den Datenschutz und arbeitet mit dieser oder diesem zusammen. Der oder die Beauftragte für den Datenschutz kann bei Verletzungen von Datenschutzbestimmungen eine Verfügung erlassen und beispielsweise die Einstellung der Datenbearbeitung verlangen.

5.4 Kanton Luzern

Das kantonale Gesetz über den Schutz von Personendaten (Kantonales Datenschutzgesetz, KDSG, SL Nr. 38) verzichtet auf den Schutz der juristischen Personen, führt jedoch in den Fachgesetzen diverse

Bestimmungen zu deren Schutz ein. Das Gesetz verstärkt die Informations- und Meldepflichten der öffentlichen Organe und die Rechte der betroffenen Personen auf Auskunft über die bearbeiteten Daten. Bei gewissen Datenbearbeitungen werden die dem Gesetz unterstellten öffentlichen Organe verpflichtet, Datenschutzfolgenabschätzungen zu erstellen. Des Weiteren haben die Gerichte, die Strafverfolgungs- und die Strafvollzugsbehörden innerhalb ihrer Organisationseinheiten einen Datenschutzberater oder eine Datenschutzberaterin zu bezeichnen. Ein wichtiger Punkt der Revision ist die Stellung und Unabhängigkeit der Datenschutzbehörden. In Übereinstimmung mit dem höheren europäischen Standard erhält der oder die Beauftragte für den Datenschutz Verfügungsbefugnisse. Im Gesetz sind die Wählbarkeitsvoraussetzungen normiert und eine Wahl der oder des Beauftragten für den Datenschutz durch den Kantonsrat auf Amtsdauer vorgesehen.

5.5 Fazit

Die Kantone passen ihre Datenschutzgesetze an die neuen Instrumente wie die Datenschutzfolgenabschätzung an und erweitern die Informationspflichten im Sinne der europäischen Datenschutzreformen. Die Regelungsdichte ist kantonal sehr unterschiedlich. So normiert der Kanton Zürich häufig nur die Grundsätze und andere Kantone wie der Kanton St. Gallen normieren sehr detailliert, was sich beispielsweise bei der Vorabkontrolle zeigt. Ob die kantonalen Datenschutzgesetze weiterhin juristische Personen schützen, wird sehr unterschiedlich gehandhabt. Sofern sie vom Schutzbereich ausgeschlossen werden, erlassen die Kantone analog zur Regelung des Bundes teilweise bereichsspezifische Schutzbestimmungen. Manche Kantone verringern teilweise den Administrativaufwand, indem sie namentlich die Pflicht zur Führung des Registers über die Datensammlungen abschaffen. Die Kompetenz der oder des Beauftragten für Datenschutz Verfügungen zu erlassen, findet sich bei allen konsultierten Kantonen. Eine grundsätzliche Aufteilung der Datenschutzgesetzgebung in Bestimmungen, die im Sinn der Richtlinie (EU) 2016/680 für die Strafbehörden und die Justizvollzugsbehörden gilt, und in Bestimmungen, die für die übrige Verwaltung gilt, findet sich in keinem der betrachteten Kantone.

6. Umsetzung, geplante Evaluation des Vollzugs

Erläuterungen, inwiefern der Ausführungserlass die Gesetzgebung konkretisiert, finden sich bei den jeweiligen Gesetzesbestimmungen. Die Evaluation erfolgt mittels Berichterstattung der Datenschutzbehörden an ihre Wahlorgane (Art. 48 VE-revKDSG).

7. Erläuterungen zu den Artikeln

7.1 Allgemeine Bestimmungen

Titel

Es besteht eine gewisse Verwechslungsgefahr zum neuen Bundesgesetz über den Datenschutz, was künftig den Kurztitel «Datenschutzgesetz» aufweist. Der Gesetzestitel des kantonalen Gesetzes lautet deshalb neu Kantonales Datenschutzgesetz (KDSG).

Artikel 1 – Zweck

Das kantonale Datenschutzgesetz konkretisiert die Grundrechtsgarantien aus Bundes- und Kantonsverfassung und setzt weitere internationale Verpflichtungen um. Primär handelt es sich um das in Artikel 13 Absatz 2 BV enthaltene Recht auf informationelle Selbstbestimmung, das vom bernischen Gesetzgeber in Artikel 18 KV als Recht auf Datenschutz konkretisiert worden ist. Die Kantonsverfassung richtet sich an die Behörden und statuiert die wichtigsten Rechte der betroffenen Person (das Einsichtsrecht, als

Teilgehalt des Rechts auf Auskunft, das Berichtigungsrecht bei falschen Personendaten sowie das Recht auf Vernichtung bei ungeeigneten oder unnötigen Personendaten). Das kantonale Datenschutzgesetz konkretisiert die Pflichten der Behörden, weshalb sich der Zweckartikel an sie wendet. Behörden dürfen Personendaten nur soweit bearbeiten, als dies mit der Kantonsverfassung und dem kantonalen Datenschutzgesetz vereinbar ist.

Anders als die internationalen Vorgaben (und die meisten europäischen Staaten) schützen die schweizerischen Datenschutzgesetze bisher juristische und natürliche Personen. Das vom Bund verabschiedete Datenschutzgesetz verzichtet nun auf den Einbezug der juristischen Personen (Art. 1 und Art. 2 Abs. 1 revDSG), führt jedoch für die Bearbeitung von deren Personendaten eine Reihe von Bestimmungen im Regierungs- und Verwaltungsorganisationsgesetz vom 21. März 1997 (RVOG)[21] ein. Ausserdem regelt eine Übergangsbestimmung, dass während fünf Jahren mögliche Rechtslücken geschlossen werden können, indem in den Spezialerlassen Bestimmungen zur Bearbeitung von Personendaten juristischer Personen geschaffen werden.

Die Kantone sind nicht verpflichtet, den Geltungsbereich ihrer Datenschutzgesetze ebenfalls auf natürliche Personen zu beschränken. Würde der Geltungsbereich auf sie beschränkt werden, hätte dies zur Folge, dass sämtliche Gesetzesgrundlagen, welche die Bearbeitung von Personendaten regeln, auf juristische Personen nicht mehr anwendbar wären und allenfalls angepasst werden müssten. Zudem müsste der Schutzbedarf für die Daten juristischer Personen festgelegt werden. Es ist wenig sinnvoll, den Geltungsbereich des bernischen Datenschutzgesetzes auf natürliche Personen zu begrenzen, nur um zugleich in etlichen Spezialgesetzen gesonderte Bestimmungen zur Bearbeitung von Personendaten einzufügen. Nach Artikel 5 der Bundesverfassung ist die Grundlage staatlichen Handelns das Recht. Erliesse der Kanton Bern also keine spezialgesetzlichen Regelungen, die den Behörden das Bearbeiten juristischer Personendaten erlaubt, so würde es an der verlangten gesetzlichen Grundlage fehlen. Dasselbe und noch mehr ergibt sich aus Art. 18 KV: Neben der gesetzlichen Grundlage und dem Verhältnismässigkeitsprinzip statuiert die Kantonsverfassung zudem Rechte (Berichtigung unrichtiger Daten und Vernichtung ungeeigneter und unnötiger Daten), auf die sich auch juristische Personen berufen können. Ebenfalls in der Kantonsverfassung verankert, ist der Grundsatz der Datenrichtigkeit. Müssten all diese Grundsätze auch für juristische Personen festgehalten und konkretisiert werden, ergäbe sich eine parallele, unübersichtliche Gesetzgebung, welche nicht anwenderfreundlich ist. Auf eine Einschränkung des Geltungsbereichs ist deshalb zu verzichten. Ebenso verzichten beispielsweise die Kantone Zürich, Freiburg oder Schwyz darauf, den Geltungsbereich einzuschränken. Andere Kantone, die den Geltungsbereich auf natürliche Personen beschränken, führen gesonderte Bestimmungen in den Spezialgesetzen ein, so beispielsweise der Kanton Luzern.

Der Zweckartikel erfährt gegenüber dem bisherigen Recht bloss redaktionelle Änderungen.

Artikel 2 – Begriffe

Die Begriffe stimmen grösstenteils mit der bisherigen Gesetzgebung überein. Auf Ergänzungen und Abweichungen wird im Folgenden hingewiesen. Neue Begriffe sind das Profiling und die Verletzung der Datensicherheit. Ebenfalls eine Änderung erfährt der Behördenbegriff. Entgegen dem bisherigen Recht ist die Begriffsdefinition für die besonders schützenswerten Personendaten nicht mehr in einem separaten Artikel erfasst, sondern bei den Begriffen aufgeführt. Das entspricht der Systematik des Bundesdatenschutzgesetzes. Im Gegensatz zum bisherigen Recht und im Einklang mit den gesetzestechnischen Richtlinien sind die Begriffe in Buchstaben statt Absätze unterteilt.

Buchstabe a

Im Gegensatz zum Datenschutzgesetz des Bundes gelten auch Angaben zu bestimmten oder bestimmbaren juristischen Personen als Personendaten (vgl. Erläuterungen zu Art. 1 VE-revKDSG).

Buchstabe b

[21] SR 172.010

Das kantonale Datenschutzgesetz hält an der privilegierten Kategorie von Personendaten fest, bei deren Bearbeitung von einem schweren Eingriff in das Grundrecht auf Datenschutz auszugehen ist und deshalb erhöhte Anforderungen gelten (vgl. Art. 4 Abs. 2 VE-revKDSG). Es ist durchaus umstritten, ob der Gesetzgeber gewisse Personendaten als besonders schützenswert definieren soll. Massgeblich soll stattdessen das Gefährdungspotential für das Grundrecht auf Datenschutz sein. Die europäischen Vorgaben und der Bundesgesetzgeber behalten die Kategorien aber bei. Für die Gesetzesanwendung ist es durchaus sinnvoll, eine Kategorie von besonders schützenswerten Personendaten festzulegen, bei der kraft Gesetzes erhöhte Anforderungen gelten, ohne dass bei jeder Bearbeitung das Gefährdungspotential einzeln geprüft werden muss. Die Aufzählung ist aus Gründen der Rechtssicherheit abschliessend.

Ziffer 1

Bisher erwähnte das Gesetz die gewerkschaftliche Ansicht und Betätigung nicht explizit, weil sie zur politischen und weltanschaulichen Ansicht zählte. Im Einklang mit dem europäischen Recht und dem Bund wird die Gewerkschaftszugehörigkeit mit der Revision in die Aufzählung der besonders schützenswerten Personendaten aufgenommen. Damit wird auch ohne Auslegung ersichtlich, dass die Mitgliedschaft in einer Arbeitnehmerorganisation als besonders schützenswertes Personendatum gilt.

Ziffer 2

Der Begriff «Rassenzugehörigkeit» wird mit ethnischer Herkunft ersetzt. Damit gemeint ist die Zugehörigkeit zu einer Gruppe von Menschen, die sich aufgrund ihrer Kultur, Geschichte, Sprache, Sitten, Traditionen und Gebräuche als untereinander verbunden und dadurch als von der übrigen Bevölkerung differente Gemeinschaft erleben und/oder von der übrigen Bevölkerung als differente Gruppe wahrgenommen werden.

Im Gegensatz zum Bund und zum geltenden Recht verzichtet das kantonale Datenschutzgesetz auf den Begriff der «Rassenzugehörigkeit». Bereits heute ist fraglich, was darunter zu verstehen ist. Im Vordergrund steht wohl weniger der (wissenschaftlich nicht haltbare) Versuch, Menschen nach äusseren Merkmalen in «Rassen» einzuteilen, als vielmehr der Schutz vor dem Rassenvorwurf.[22] Im kantonalen Datenschutzgesetz kann auf den Begriff verzichtet werden, da es im Gegensatz zu anderen Rechtsgebieten nicht darum geht, rassendiskriminierendes Verhalten an bestimmte Rechtsfolgen zu knüpfen. Ausserdem benötigen Behörden solche Daten nicht, um ihre Aufgaben zu erfüllen. Besonders schützenswerte Personendaten sind vielmehr Daten über die ethnische Herkunft.

Ziffer 3

Im Einklang mit der bundesrechtlichen Gesetzgebung nennt das kantonale Datenschutzgesetz neu die Gesundheit und die Intimsphäre als besonders schützenswerte Personendaten statt den persönlichen Geheimbereich. Inhaltlich erfolgt keine Änderung.

Angaben über die Gesundheit sind alle Informationen, die Rückschlüsse auf den körperlichen oder geistigen Gesundheitszustand einer Person erlauben. Erfasst sind sämtliche Daten, die im weitesten Sinn einen medizinischen Befund darstellen. Dabei ist nicht nur die klassische medizinische Diagnose gemeint. So stellen beispielsweise bereits die auf einer Patientenrechnung enthaltenen Daten wie die medizinischen Anamnese, Befunde und Therapiedaten besonders schützenswerte Personendaten dar, da sie Rückschlüsse auf den Gesundheitszustand eines Patienten erlauben.[23]

Das Bundesgericht unterscheidet nach der «Drei-Säulen-Theorie»[24] zwischen der Intims- bzw. Geheimsphäre, der Privatsphäre sowie der Öffentlichkeitsphäre. Die Intimsphäre erfasst dabei alle auf die persönlichen Angelegenheiten der betroffenen Person bezogenen Informationen wie beispielsweise das Sexualleben, welches der Kenntnis Dritten grundsätzlich entzogen bleiben soll, ausser die betroffene Person informiert selbst darüber.

[22] vgl. Rudin, Beat (2014): Praxiskommentar zum IDG des Kanton Basel-Stadt. Zürich, Basel, Genf: Schulthess Juristische Medien AG: § 3 N 37 Fn. 71.
[23] Blechta, Gabor P. (2014): Zweck, Geltungsbereich und Begriffe. In: Maurar-Lambrou, Urs/ Blechta, Gabor P. (Hrsg.), Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz, Basel: Helbing Lichtenhahn Verlag: Art. 3 N. 33.
[24] BGE 97 II 100 f., E. 3; 118 IV 45; 119 II 222 ff., E. 2b.

Ziffer 4

Neu gelten genetische Daten als besonders schützenswerte Personendaten. Genetische Daten sind Informationen über das Erbgut einer Person, die durch eine genetische Untersuchung gewonnen werden; darin eingeschlossen ist auch das DNA-Profil (Art. 3 Bst. l des Bundesgesetzes vom 8. Oktober 2004 über genetische Untersuchungen beim Menschen [GUMG])[25].

Ziffer 5

Unter biometrischen Daten sind Personendaten zu verstehen, die durch ein spezifisches technisches Verfahren zu den physischen, physiologischen oder verhaltenstypischen Merkmalen eines Individuums gewonnen werden und die eine eindeutige Identifizierung der betreffenden Person ermöglichen oder bestätigen. Es handelt sich dabei beispielsweise um einen digitalen Fingerabdruck, Gesichtsbilder, Bilder der Iris, die Motorik, Gangart oder Aufnahmen der Stimme. Diese Daten müssen zwingend auf einem spezifischen technischen Verfahren beruhen, das die eindeutige Identifizierung oder Authentifizierung einer Person erlaubt. Dies ist beispielsweise grundsätzlich nicht der Fall bei gewöhnlichen Fotografien.[26]

Ziffer 6

Unverändert gelten als besonders schützenswerte Personendaten Massnahmen der sozialen Hilfe. Damit gemeint sind bedarfsabhängige Sozialleistungen, sowohl in finanzieller Hinsicht als auch die Inanspruchnahme von Betreuungs- und Beratungsinstitutionen. Der Begriff bezieht sich nicht nur auf Massnahmen der Sozialhilfe oder der sozialen Leistungsangebote. Er ist weit gefasst: Zu nennen sind etwa auch Ergänzungsleistungen, Krankenkassenprämienverbilligungen, Bevorschussung von Unterhaltsbeiträgen, Ausbildungsbeiträge oder Leistungen der Opferhilfe.[27]

Im Gegensatz zum Bund nennt das kantonalen Datenschutzgesetz ausdrücklich Massnahmen des Kindes- und Erwachsenenschutzes. Das geltende Recht nennt lediglich Massnahmen über die fürsorgerische Betreuung als besonders schützenswerte Personendaten, jedoch fielen bereits nach heutigem Verständnis grundsätzlich Massnahmen des Kindes- und Erwachsenenschutzes darunter[28]. Dazu zählen etwa Angaben über eine fürsorgerische Unterbringung. Mit der Revision soll die fürsorgerische Betreuung auch in den übrigen Gesetzen mit Massnahmen des Kindes- und Erwachsenenschutzes ersetzt werden (vgl. Ziff. 7.9.6).

Im Unterschied zu den Massnahmen der sozialen Hilfe werden Massnahmen des Kindes- und Erwachsenschutzes häufig gegen den Willen der betroffenen Personen angeordnet. Beiden Kategorien ist jedoch gemeinsam, dass die betroffenen Personen auf staatliche Unterstützung angewiesen sind. Ihnen ist es oft unangenehm solche Leistungen zu beziehen oder angeordnet zu bekommen, weshalb Angaben darüber als besonders schützenswert gelten.

Ziffer 7

Die Bestimmung wird an diejenige des Bundes angeglichen und um verwaltungsrechtliche Verfolgungen oder Sanktionen ergänzt. Damit gelten neben Personendaten über die Eröffnung, die Durchführung und den Abschluss von Verfolgungen und Sanktionen der Strafjustizbehörden auch Personendaten im Zusammenhang mit Disziplinarverfahren (z.B. Berufsausübungsverbote) sowie Daten im Hinblick auf Strafvollzugsmassnahmen als besonders schützenswerte Personendaten. Weiter fallen beispielsweise administrative Führerausweisentzüge, Tierhalteverbote, Beschlagnahmung von Tieren oder Dienstleistungssperren nach Entsendegesetz vom 8. Oktober 1999 (EntG)[29] darunter.

Buchstabe c

[25] SR 810.12
[26] BBl 17.059, S. 7020 Ziff. 9.1.3.1
[27] vgl. Rudin, Beat (2015). In: Baeriswyl, Bruno/Pärli, Kurt (Hrsg.), Datenschutzgesetz (DSG). Bern: Stämpfli Verlag AG: Art. 3 N. 27.
[28] vgl. für den Kanton Basel-Stadt zum Begriff Massnahmen der sozialen Hilfe: Rudin, Beat (2014), s.o., § 3 N. 38.
[29] SR 823.20

Der Begriff der Datensammlung ist aus dem bisherigen Recht zu übernehmen. Die verantwortlichen kantonalen Behörden melden ihre Datensammlungen der kantonalen Datenschutzbehörde, welche sie in einem Register veröffentlicht (Art. 21 VE-revKDSG).

Buchstabe d

Artikel 3 Ziffer 4 der Richtlinie (EU) 2016/680 regelt neu das «Profiling» als besondere, gefährliche Art des Bearbeitens von Personendaten. Mit der Aufnahme des Profilings als Bearbeitungsart ist klargestellt, dass es sich nicht um eine Personendatenart handelt. Die Begriffsdefinition findet sich in Buchstabe f.

Buchstabe e

Unverändert übernommen wird der Begriff des Bekanntgebens, der jedes Zugänglichmachen von Personendaten erfasst. Das Bekanntgeben von Personendaten ist eine Unterkategorie des Bearbeitens. Mit dem Bekanntgeben verlassen die Personendaten den Verantwortungsbereich der bisher verantwortlichen Behörde. Damit verbunden ist allenfalls auch eine Zweckänderung. Es spielt keine Rolle, wie – ob absichtlich oder durch Nachlässigkeit – eine andere Behörde oder Drittperson Zugang zu den Personendaten erhält.

Buchstabe f

Das Profiling ist eine bestimmte Datenbearbeitungsart, mithin ein dynamischer Prozess, der auf einen bestimmten Zweck ausgerichtet ist. Auf Bundesebene werden zwei Profilingvarianten unterschieden: Das Profiling und das Profiling mit hohem Risiko. Ersteres übernimmt die Definition der Richtlinie (EU) 2016/680 bzw. der Datenschutz-Grundverordnung und letzteres ist eine Schöpfung der Räte. In der politischen Debatte hat sich nämlich herauskristallisiert, dass nicht jedes Profiling heikel ist.

Wird ein Profiling durch Behörden betrieben, bestehen nach dem revDSG keine gesonderten Anforderungen für ein Profiling mit hohem Risiko. Massgebend für den Kanton ist alleine die Definition des «einfachen» Profilings, weshalb sich die Definition im kantonalen Datenschutzgesetz daran orientieren muss. Im Interesse einer einfachen Formulierung und Verständlichkeit weicht die Definition im kantonalen Datenschutzgesetz vom Begriff auf Bundesebene ab, enthält aber alle Elemente des einfachen Profilings. Demnach ist ein Profiling eine automatisierte Bearbeitung von Personendaten, um bestimmte persönliche Aspekte einer natürlichen Person zu bewerten, zu analysieren oder vorherzusagen.

Von einem Profiling ist beispielsweise auszugehen, wenn die Behörde ein Profil für den idealen Stellenbewerber definiert und dann vom Computer beurteilen lässt, wer diesem am besten entspricht.

Das Profiling muss je nach Gefährdungspotential denselben Anforderungen genügen wie das Bearbeiten von besonders schützenswerten Personendaten, d.h. es erfordert eine Grundlage im Gesetz (vgl. Erläuterungen zu Art. 4 Abs. 2 VE-revKDSG).

Die Aufzählung der bestimmten Aspekte der Persönlichkeit übernimmt die Aufzählung des Bundes in Artikel 5 Absatz 1 Buchstabe f revDSG. Das Wort «insbesondere» stellt klar, dass die Aufzählung nicht abschliessend ist.

Buchstabe g

Die EV EDS führte für verantwortliche kantonale Behörden der Strafprävention, Strafverfolgung und Strafvollstreckung eine Meldepflicht bei Datenschutzverletzungen ein, welche ins kantonale Datenschutzgesetz zu überführen ist (Art. 25–27 VE-revKDSG). Dementsprechend ist der Begriff der Verletzung des Datenschutzes in die Begriffsdefinitionen aufzunehmen, jedoch an den Wortlaut des Bundesgesetzes anzunähern (vgl. Art. 5 Bst. h revDSG). Im Gegensatz zur EV EDS lautet der Titel Verletzung der Datensicherheit und nicht des Datenschutzes, da die Bestimmung nur den Teilaspekt der Datensicherheit betrifft. Im Gegensatz zur Bundesdefinition wird «widerrechtlich» durch «unberechtigt» ersetzt, um die Definition an das zu erlassende kantonale Informations- und Cybergesetz anzugleichen. Der Begriff knüpft daran an, dass bei der Bearbeitung von Personendaten eine dem Risiko angemessene Datensicherheit mit geeigneten technischen und organisatorischen Massnahmen gewährleistet werden muss (Art. 10 VE-revKDSG).

Eine Verletzung der Datensicherheit liegt vor, wenn bearbeitete Personendaten unbeabsichtigt oder unberechtigt

- verlorengehen oder vernichtet werden (Verfügbarkeit von Personendaten),
- verändert werden (Verletzung der Integrität von Personendaten) oder
- offenbart oder Unbefugten zugänglich gemacht werden (Vertraulichkeit von Personendaten).

Die Datensicherheit ist grundsätzlich verletzt, wenn bei einer Datenbearbeitung in unvorhergesehener Weise die Verfügbarkeit, Integrität oder Vertraulichkeit von Personendaten beeinträchtigt wird, wenn beispielweise

- Datenträger (Laptop, Smartphone, Festplatte, USB-Stick usw.) verloren gehen oder gestohlen werden,
- unbefugte Dritte oder nicht berechtigte Mitarbeiter auf IT-Netzwerke zugreifen,
- wegen Stromausfällen, IT-Ausfällen oder Naturkatastrophen Personendaten gelöscht werden oder
- Personendaten an nicht Berechtigte bekanntgegeben werden, indem Personendaten an eine falsche E-Mailadresse gesendet werden.

Buchstabe h

Der Behördenbegriff soll gegenüber dem geltenden Recht (Art. 2 Abs. 6 KDSG) angepasst werden. Der bisherige Wortlaut ist missverständlich, teilweise zu eng oder auch zu weit. Die Neufassung soll verdeutlichen, dass der Behördenbegriff im Sinne des kantonalen Datenschutzgesetzes sehr weit zu verstehen ist. Er entspricht dem weiten, funktionalen Behördenbegriff der Kantonsverfassung.

Nach dem 5. Titel der Kantonsverfassung gehören zu den Organen bzw. zu den kantonalen Behörden der Grosse Rat, der Regierungsrat, die kantonale Verwaltung sowie die Gerichte und nach der Justizreform die Staatsanwaltschaft. Wegen den europäischen Vorgaben sind auch die Justizbehörden (Gerichtsbehörden und Staatsanwaltschaft) vom kantonalen Datenschutzrecht erfasst, wobei das anwendbare Verfahrensrecht spezialgesetzliche Regelungen enthält und die Justizbehörden teilweise von der Aufsicht ausgenommen sind (vgl. Art. 3 Abs. 3 und Art. 46 Abs. 4 VE-revKDSG).

Der Behördenbegriff bezieht sich folglich nicht nur auf oberste Exekutivorgane und auf die Verwaltung, sondern auch auf Parlamente, sowohl auf kantonaler (Grosser Rat) als auch auf kommunaler Ebene (Gemeindeparlamente). Dabei ist zu beachten, dass auch für sie oft spezialgesetzliche Datenschutzbestimmungen gelten, beispielsweise betreffend Informationsrechte, das Amtsgeheimnis oder die Auskunftspflicht (vgl. 4. Titel des Gesetzes über den Grossen Rat vom 4. Juni 2013, [Grossratsgesetzgebung, GRG])[30].

Die kantonale Verwaltung besteht aus der Zentralverwaltung und der Bezirksverwaltung bzw. dezentralen Verwaltung (Art. 92-94 KV und Art. 20 OrG). Zur Zentralverwaltung zählen ihre Direktionen, die Staatskanzlei, die Generalsekretariate, Ämter und ihnen gleichgestellte Organisationseinheiten, Abteilungen etc. Die Verwaltungseinheiten sind explizit zu erwähnen, da sie für die Umsetzung der datenschutzrechtlichen Anforderungen verantwortlich sind.

Als Gemeinden gelten öffentlich-rechtliche Körperschaften mit eigener Rechtspersönlichkeit. Dazu zählen nach Kantonsverfassung Einwohnergemeinden, Burgergemeinden, gemischte Gemeinden und Kirchgemeinden. Unterabteilungen und öffentlich-rechtliche Gemeindeverbände sind den Gemeinden gleichgestellt (Art. 107 Abs. 1 bis 3 KV). Kraft Gesetz sind weitere Körperschaften dem Gemeinderecht unterstellt. Es handelt sich dabei um die burgerlichen Kooperationen, die Gesamtkirchgemeinden der Landeskirchen, die Schwellenkooperationen und Regionalkonferenzen (Art. 2 Abs. 1 des Gemeindegesetzes vom 16. März 1998 [GG])[31]. Die Organe der Gemeinde sind in Artikel 10 GG aufgeführt. Für die Umsetzung der datenschutzrechtlichen Anforderung sind auch auf kommunaler Ebene die Verwaltungseinhei-

[30] BSG 151.21
[31] BVR 2013 S. 251 E. 4.3

ten verantwortlich, d.h. in der Regel die einzelnen Direktionen, Ämter oder Abteilungen, je nach Organisation der Gemeinden. Ausgenommen vom Geltungsbereich des kantonalen Datenschutzgesetzes sind selbstverständlich die Stimmberechtigten.

Die Mitarbeitenden werden bewusst nicht mehr erwähnt. Eine Verantwortung der einzelnen Mitarbeitenden widerspricht grundsätzlich den Verantwortlichkeitsregeln im Kanton. Verantwortlich für den Datenschutz sind die Behörden. In der Praxis kommt die Verantwortung den Leitungsorganen zu; sie tragen die Verantwortung in ihrem Zuständigkeitsbereich. Hierzu bekennen sie sich zum Datenschutz und zur Informationssicherheit, sie führen eine zweckmässige Organisation, erlassen die notwendigen Vorschriften, ordnen die erforderlichen technischen und organisatorischen Massnahmen an sowie wählen ihre Mitarbeitenden sorgfältig aus, instruieren und überwachen sie.

Zu den Verwaltungseinheiten des Kantons gehören auch die anderen Träger öffentlicher Aufgaben, beispielsweise die öffentlich-rechtlichen Anstalten wie die Universität Bern oder Körperschaften des Kantons. Private Träger öffentlicher Aufgaben sind jedoch nur erfasst, soweit sie ihnen übertragenen Aufgaben erfüllen. Demzufolge ist eine privatrechtliche Aktiengesellschaft der Gesundheitsversorgung (Spital) Behörde, soweit sie Personendaten in Erfüllung einer ihr übertragenen öffentlichen Aufgabe bearbeitet. Dasselbe gilt für die Gemeinden. Zu nennen sind hier etwa die Verkehrsbetriebe Biel oder Energie Wasser Bern.[32]

Weiter ist das Datenschutzgesetz wie bisher auf Datenbearbeitungen von Organen der Landeskirchen und ihrer regionalen Einheiten nach dem Gesetz vom 21. März 2018 über die bernischen Landeskirchen (Landeskirchengesetz, LKG)[33] anwendbar. Ebenfalls ausgenommen sind die Stimmberechtigten.

Artikel 3 – Geltungsbereich

Absatz 1

Wie bisher gilt das kantonale Datenschutzrecht für jedes Bearbeiten von Personendaten, und zwar unabhängig von den dabei angewendeten Mitteln und Verfahren. Diese Bestimmung erfährt keine Änderungen.

Absatz 2

Buchstabe a

Bereits heute gilt das kantonale Datenschutzrecht nicht für das privatwirtschaftliche Handeln der Behörde. Soweit Behörden privatrechtlich handeln, sollen die Regeln des kantonalen Datenschutzgesetzes weiterhin nicht gelten, weshalb die Regelung des bisherigen Rechts (Art. 4 Abs. 2 Bst. a KDSG) inhaltlich unverändert zu übernehmen ist. Allerdings müssen nach den neuen Vorgaben auch für sie – wie für Private, die dem Datenschutzgesetz des Bundes unterstehen – Datenschutzregeln gelten. Folglich ist das Datenschutzgesetz des Bundes für solche Datenbearbeitungen anwendbar, was indes nicht explizit im kantonalen Datenschutzgesetz aufzunehmen ist. Da solche Behörden aber nicht Private werden, sondern nur wie Private handeln, unterstehen sie auch für privates Handeln der kantonalen Aufsicht.

Anzumerken ist, dass das kantonale Datenschutzgesetz für Private nur anwendbar ist, soweit sie ihnen übertragene öffentliche Aufgaben erfüllen (Art. 2 Abs. 1 Bst. h Ziff. 2 VE-revKDSG). Die Bestimmung betrifft folglich öffentlich-rechtlich konstituierte Behörden (Art. 2 Abs. 1 Bst. h Ziff. 1 und 3 VE-revKDSG).

Buchstabe b

Wie bisher unterstehen persönliche Notizen, die ausschliesslich zum persönlichen Gebrauch verwendet werden, nicht den Bestimmungen dieses Gesetzes. Davon ausgenommen sind Notizen, die vorgesetzten, stellvertretenden oder nachfolgenden Personen dienen sollen.

Absatz 3

[32] Daum Michel (2020). In: Herzog, Ruth/Daum, Michel (Hrsg.), Kommentar zum Gesetz über die Verwaltungsrechtspflege des Kantons Bern. Bern: Stämpfli Verlag AG: Art. 2 N. 19.
[33] BSG 410.11

Dieser Absatz regelt das Verhältnis des Verfahrensrechts zum Datenschutzrecht. Nach dem geltenden Recht sind auf hängige Zivil-, Straf- und Verwaltungsrechtspflegeverfahren ausschliesslich die entsprechenden Verfahrensgesetze anwendbar (Art. 4 Abs. 2 Bst. c KDSG). Diese regeln insbesondere den Anspruch auf rechtliches Gehör, auf Akteneinsicht und die Begründungspflicht. Die generelle Ausnahme in dieser absoluten Form ist für hängige Gerichtsverfahren wegen den europäischen Vorgaben so nicht mehr erlaubt. Zulässig sind gemäss Artikel 14 Absatz 1 SEV Nr. 108+ lediglich Ausnahmen vom Grundsatz von Treu und Glauben, der Zweckbindung, Verhältnismässigkeit und der Richtigkeit der Daten sowie bei der Meldepflicht von Datensicherheitsverletzungen, bei der Informationspflicht und bei den Rechten der betroffen Person; bei ersteren handelt es sich indes um Grundsätze des rechtsstaatlichen Handelns nach der Verfassung, die das kantonale Recht beachten muss.

Beim kantonale Datenschutzgesetz handelt es sich um ein Querschnittsgesetz, welches durch Fachgesetze zu ergänzen ist oder deren Regeln als spezielleres Recht auch davon abweichen können. In diesem Sinne ergänzen die Verfahrensgesetze als bereichsspezifisches (oder materielles) Datenschutzrecht bereits heute das formelle Datenschutzrecht: Beispielsweise verlangt das Datenschutzrecht zur Bearbeitung von Personendaten eine gesetzliche Grundlage, die das Fachrecht, also das anwendbare Verfahrensrecht, liefert. Das Fachrecht kann datenschutzrechtliche Grundsätze auch einschränken, Ausnahmen vorsehen oder offene Regeln präzisieren.

Der neu gefasste Absatz soll eine klare Abgrenzung zwischen dem Datenschutzrecht und dem Verfahrensrecht als Fachrecht vornehmen und orientiert sich an der bundesrechtlichen Regelung. Demnach regelt das anwendbare Verfahrensrecht die Bearbeitung von Personendaten und die Rechte der betroffenen Personen in Gerichtsverfahren, Verfahren der Verwaltungsrechtpflege und in Verfahren nach besonderen Verfahrensordnungen. Mit Verfahren der Verwaltungsrechtspflege ist das das Gesetz vom 23. Mai 1989 über die Verwaltungsrechtspflege (VRPG)[34] gemeint. Zu den besonderen Verfahrensordnungen zählen beispielsweise das Gesetz vom 1. Februar 2012 über den Kindes- und Erwachsenenschutz (KESG)[35] oder das Grossratsgesetz. So regelt Art. 23 VRPG oder Art. 53 KESG die Akteneinsicht und das Grossratsgesetz kennt einen eigenen Titel zu den Informationsrechten, zum Amtsgeheimnis und der Auskunftspflicht. Die Verfahrensordnungen stellen im Rahmen ihrer Regelungen ebenfalls den Schutz der Grundrechte aller Beteiligten sicher und gewährleisten damit einen dem Datenschutzrecht äquivalenten Schutz. Käme in diesem Bereich das kantonale Datenschutzgesetz zur Anwendung, bestünde die Gefahr von Normkollisionen und Widersprüchen, die das austarierte System der jeweils anwendbaren Verfahrensordnung stören könnten.

Das Bearbeiten von Personendaten und die Rechte der betroffenen Person richten sich während der genannten Verfahren also ausschliesslich nach den anwendbaren Verfahrensordnungen, insbesondere nach der Schweizerischen Zivilprozessordnung vom 19. Dezember 2008 (Zivilprozessordnung, ZPO)[36], nach der Schweizerischen Strafprozessordnung vom 5. Oktober 2007 (Strafprozessordnung, StPO)[37] und nach dem VRPG. Das heisst, dass die Rechte der betroffenen Person (4. Titel VE-revKDSG) während dem Verfahren ruhen und für die Informationsansprüche beispielsweise Artikel 53 ZPO, Artikel 107 f. StPO und Artikel 23 VRPG gelten. Sowohl Datenbearbeitungen des Gerichts gegenüber den Verfahrensbeteiligten als auch Datenbearbeitungen, welche die Beteiligten gegenüber anderen Verfahrensbeteiligten durchführen, richten sich nach dem anwendbaren Verfahrensrecht. Dies gilt insbesondere für die Rechte der Parteien zur Kenntnisnahme der ins Verfahren einfliessenden Personendaten und zur allfälligen Berichtigung derselben sowie für die Datenbearbeitung im Rahmen der gerichtlichen Verfahren im Allgemeinen. Das bedeutet namentlich, dass die verschiedenen Rechtsbehelfe nach dem kantonalen Datenschutzgesetz weder gegenüber Datenbearbeitungen des Gerichts im Rahmen des Verfahrens noch gegenüber Datenbearbeitungen der anderen Verfahrensbeteiligten zum Tragen kommen. So können die Verfahrensbeteiligten beispielsweise kein Auskunftsrecht nach dem kantonalen Datenschutzgesetz geltend machen, um beim Gericht Akteneinsicht zu erhalten oder bei anderen Verfahrensbeteiligten

[34] 155.21
[35] BSG 213.316
[36] SR 272
[37] SR 312.0

Beweismittel zu beschaffen. Es ist mit anderen Worten nicht möglich, auf dem Wege des kantonalen Datenschutzgesetzes verfahrensrelevante Handlungen gegenüber dem Gericht oder unter den Verfahrensbeteiligten vorzunehmen, welche nach dem fraglichen Verfahrensrecht ausgeschlossen wären oder aber umgekehrt, unter bestimmten Voraussetzungen nach bestimmten Regeln und Grundsätzen zu erfolgen haben.

Auf den Begriff «hängiges» Verfahren ist wegen der Abgrenzungsschwierigkeiten zu verzichten, da lediglich im Zivilprozessrecht (Art. 62 ZPO) und in der Verwaltungsrechtspflege (Art. 16 VRPG) von Rechtshängigkeit die Rede ist. Massgebend ist, ob ein Verfahren von einer Verfahrensordnung geregelt ist. Für die Abgrenzung ist wesentlich, ob ein unmittelbarer Zusammenhang zu einem Verfahren besteht oder nicht. Ein solcher liegt vor, wenn die fragliche Bearbeitung von Personendaten konkrete Auswirkungen auf das Verfahren, dessen Ausgang oder die Verfahrensrechte der Parteien haben kann.[38] Ein besonderes Augenmerk ist auf das polizeiliche Ermittlungsverfahren zu richten: Die Strafprozessordnung regelt das sogenannte Vorverfahren, welches das polizeiliche Ermittlungsverfahren und die staatsanwaltschaftliche Untersuchung umfasst (Art. 299 Abs. 1 StPO). Von diesem Vorverfahren abzugrenzen ist die sogenannte Vorermittlungstätigkeit der Polizei, bei der erst ein vager Verdacht besteht. Diese fällt noch nicht unter die Strafprozessordnung.[39] Im Vorermittlungsverfahren ist folglich das kantonale Datenschutzgesetz massgebend, sofern das Polizeigesetz keine abweichende Regelung aufstellt (Art. 141 Abs. 1 PolG).

Mit dem Begriff «betroffene Personen» werden auch Personen erfasst, die nicht unter Artikel 104 StPO (Parteien) oder Artikel 105 StPO (andere Verfahrensbeteiligte) fallen und trotzdem über Informationsrechte verfügen (z.B. Drittpersonen bei einer geheimen Überwachungsmassnahme nach Art. 279 StPO).

Weiterhin findet nach Abschluss des Verfahrens das Datenschutzgesetz Anwendung (Art. 3 Abs. 1 Bst. b des Einführungsgesetzes zur Zivilprozessordnung, zur Strafprozessordnung und zur Jugendstrafprozessordnung vom 11. Juni 2009 [EG ZSJ][40]). Dies gilt auch für Verwaltungsrechtspflegeverfahren, auch wenn dies in Artikel 23 VRPG nicht explizit aufgeführt ist. Folglich darf die entscheidende Behörde einen Entscheid nur dann einer anderen Behörde mitteilen, wenn hierzu entweder im anwendbaren Verfahrensrecht (z.B. Art. 75 Abs. 1 StPO, Verordnung vom 10. November 2004 über die Mitteilung kantonaler Strafentscheide[41]) oder in einem anderen Facherlass eine genügende gesetzliche Grundlage besteht.

Im Umkehrschluss zu Absatz 3 ergibt sich, dass das kantonale Datenschutzrecht anwendbar ist auf Datenbearbeitungen durch die administrativen Dienste von Gerichten und Behörden, wie beispielsweise die Bearbeitung von Daten über das Personal. Ebenfalls müssen die Gerichte bei der Archivierung von Beweismitteln und Entscheiden die Datensicherheit gewährleisten.

Die Vorschrift von Artikel 3 Absatz 3 VE-revKDSG gilt nach Satz 2 nicht für Verwaltungsverfahren (Verfahren auf Erlass einer Verfügung). Folglich gelten für Verwaltungsverfahren die Bestimmungen des kantonalen Datenschutzgesetzes. Die Regelung aus dem bisherigen Recht ist unverändert beizubehalten.

Soweit die Gerichte und die Staatsanwaltschaft nicht vom Geltungsbereich des kantonalen Datenschutzrechts erfasst sind, unterliegen sie auch nicht der Aufsicht durch die kantonale Datenschutzbehörde. Sofern für sie das kantonale Datenschutzgesetz gilt, kann die kantonale Datenschutzbehörde gegenüber ihnen jedoch keine Verfügungen erlassen (vgl. Art. 46 Abs. 4 VE-revKDSG).

7.2 Bearbeiten von Personendaten

Artikel 4 – Rechtsgrundlage

Dieser Artikel legt fest, welche Rechtsgrundlage für die Bearbeitung welcher Art von Personendaten erforderlich ist. Daher lautet der Titel der Bestimmung neu «Rechtgrundlage».

[38] Vgl. BBl 17.059, S. 7013 Ziff. 9.1.2
[39] Vortrag des Regierungsrates zum Polizeigesetz (2017): S. 39 zu Art. 72.
[40] BSG 271.1
[41] SR 312.3

Jedes Bearbeiten von Personendaten durch Behörden stellt einen Eingriff in die Grundrechte der betroffenen Person dar. Als Ausfluss des verfassungsrechtlichen Legalitätsprinzips (Art. 5 Abs. 1 und Art. 36 Abs. 1 BV, Art. 28 KV) verlangt auch das Bearbeiten von Personendaten eine gesetzliche Grundlage. Dazu gehören im Kanton Bern Gesetze, Dekrete und Verordnungen. Die Rechtsgrundlagen der Gemeinden heissen i.d.R. Reglemente und Verordnungen. Schwerwiegende Einschränkungen eines Grundrechts müssen im Gesetz selbst vorgesehen werden. Gesetze (auf Gemeindeebene i.d.R. Reglemente) sind generell-abstrakte Normen, die im besonderen Verfahren der Gesetzgebung erlassen werden, wohingegen es sich bei Dekreten und Verordnungen um Erlasse einer niedrigeren Stufe handelt. Im kantonalen Datenschutzgesetz sind die Begriffe bisher uneinheitlich bzw. sogar falsch verwendet worden. Nun umfasst «Gesetz» sämtliche generell-abstrakte Normen, die im besonderen Gesetzgebungsverfahren erlassen werden. Auf Kantonsebene sind dies generell-abstrakte Normen, die vom Parlament erlassen werden und dem fakultativen Referendum unterstehen (Art. 69 Abs. 4 i.V.m. Art. 62 Abs. 1 Bst. a KV). Gemeinden können diese Kompetenz auch abschliessend dem Parlament übertragen.[42] Zu beachten ist, dass das Bearbeiten von besonders schützenswerten Personendaten und teilweise auch das Betreiben eines Profilings eine Grundlage in einem Gesetz bzw. einem Reglement erfordert (vgl. Abs. 2 und 3).

Die gesetzliche Grundlage kann unmittelbar oder mittelbar ausgestaltet sein: Die unmittelbare gesetzliche Grundlage regelt die Datenbearbeitung explizit, d.h. sie verpflichtet oder ermächtigt die verantwortliche Behörde, bestimmte Personendaten zu bearbeiten.[43] So regelt beispielsweise Artikel 39 Absatz 3 des Gesetzes vom 3. Dezember 2020 über die Leistungen für Kinder mit besonderem Förder- und Schutzbedarf (KFSG)[44], dass die zuständige Stelle der Direktion für Inneres und Justiz bei den Steuerbehörden die Informationen zu den Steuerdaten einholen kann.

Die mittelbare gesetzliche Grundlage weist der verantwortlichen Behörde eine Aufgabe zu, welche sie nur durch das Bearbeiten von Personendaten erfüllen kann.[45] Nach Artikel 144 Absatz 1 des Polizeigesetzes kann die Kantonspolizei beispielsweise im Einzelfall Personendaten an Behörden bekannt geben, soweit dies zur Erfüllung von Aufgaben im Sinne des Polizeigesetzes durch sie oder durch die empfangende Behörde erforderlich ist.

Zwischen einer unmittelbaren und einer mittelbaren gesetzlichen Grundlage kann nicht immer klar unterschieden werden. Je offener die gesetzliche Grundlage die Bearbeitung umschreibt, desto grösser ist der Beurteilungsspielraum der verantwortlichen Behörde. Folglich muss sie bei der Rechtsanwendung die Verhältnismässigkeit umso mehr im Blick behalten.

Absatz 1

Absatz 1 legt die Voraussetzungen für die Bearbeitung von Personendaten und das Betreiben eines Profilings fest. Im Unterschied zum geltenden Recht und zugunsten der Lesefreundlichkeit sind die unmittelbare und mittelbare gesetzliche Grundlage in zwei separaten Buchstaben unterteilt.

Personendaten dürfen nach Buchstabe a nur bearbeitet bzw. ein Profiling nur betrieben werden, wenn dazu eine gesetzliche Grundlage ermächtigt (unmittelbare gesetzliche Grundlage). Eine «ausdrückliche» Ermächtigung, wie sie das geltende Recht verlangt, ist nicht erforderlich. Aus den gesetzlichen Grundlagen muss aber mindestens hervorgehen, welche Behörde, zu welchem Zweck, welche Personendatenkategorien bearbeitet. Hingegen ist es nicht erforderlich, dass die gesetzliche Grundlage sämtliche Datenbearbeitungen aufführt.

Die mittelbare gesetzliche Grundlage in Buchstabe b entspricht inhaltlich dem bisherigen Recht. Die Bestimmung legt fest, dass eine Behörde auch Personendaten bearbeiten oder ein Profiling betreiben darf, wenn es für die Erfüllung einer gesetzlichen Aufgabe erforderlich ist (mittelbare gesetzliche Grundlage). Das geltende Recht verlangt lediglich, dass die Bearbeitung der Personendaten der Aufgabenerfüllung

[42] Wichtermann, Jürg (1999). In: Kommentar zum Gemeindegesetz des Kantons Bern. Bern: Stämpfli Verlag AG: Vorbem. zu Art. 50-60 N. 12.
[43] Rudin, Beat (2014), s.o.: § 9 N. 16.
[44] BSG 213.319
[45] Rudin, Beat (2014), s.o.: § 9 N. 17.

«dient». Der Wortlaut suggeriert, dass es genügt, wenn die Bearbeitung der Personendaten für die Aufgabenerfüllung nützlich ist, was nicht zutrifft. Dem Verhältnismässigkeitsgrundsatz entsprechend muss die Datenbearbeitung erforderlich sein, um die gesetzliche Aufgabe zu erfüllen, was nun auch aus dem Gesetzestext hervorgeht.

Absatz 2

Weiterhin gelten zusätzliche Anforderungen, wenn eine Behörde besonders schützenswerte Personendaten bearbeitet, da es sich bei solchen Bearbeitungen nach dem gesetzgeberischen Willen um einen schweren Grundrechtseingriff handelt. Die gleichen Anforderungen gelten auch für bestimmte Profilings. Da es auch Profilings gibt, die weniger schwer in die Grundrechte der betroffenen Personen eingreifen (vgl. Erläuterungen zu Art. 2 Bst. f VE-revKDSG), bedarf es die zusätzlichen Anforderungen nach Absatz 2 nur, wenn dessen Bearbeitungszweck besondere Risiken für die Grundrechte der betroffenen Personen birgt. Falls die Vornahme eines Profilings keine besonderen Risiken birgt, reicht eine unmittelbare oder mittelbare Rechtsgrundlage nach Absatz 1 aus. Ob die verantwortliche Behörde ein Profiling mit einem besonderen Risiko betreibt und folglich von einem schweren Eingriff in das Grundrecht auf Datenschutz auszugehen ist, muss im Einzelfall beurteilt werden.

Zusätzlich zu den Anforderungen nach Absatz 1 darf eine Behörde besonders schützenswerte Personendaten nur bearbeiten oder ein Profiling, dessen Bearbeitungszweck besondere Risiken für die Grundrechte der betroffenen Personen birgt, nur betreiben, wenn dazu eine «hinreichend bestimmte» Grundlage im Gesetz ermächtigt. Die Regelung auf Gesetzesstufe darf sich auf die Grundsätze beschränken, d.h. daraus muss sich «hinreichend bestimmt» ergeben, welche Behörde zu welchem Zweck welche besonderen Datenkategorien bearbeitet bzw. ein Profiling betreibt. Die Gesetzesbestimmung muss aber nicht jeden Datenbearbeitungszweck oder sämtliche Datenbearbeitungen einzeln aufführen. Das würde zu einer enormen Regelungsdichte führen. So können auch andere Grundrechte beschränkt werden, ohne dass eine detaillierte Regelung bereits auf Gesetzesstufe notwendig wäre (vgl. Art. 28 Abs. 1 KV). Die Kategorien der bearbeiteten Personendaten ergeben sich in der Regel bereits aus dem Zweck der Datenbearbeitung, ohne dass dazu eine separate Regelung erforderlich ist. Andernfalls sind die Kategorien auf Verordnungsstufe aufzuführen, wozu es eine Delegationsnorm auf Gesetzesstufe benötigt. Andere Einzelheiten der Datenbearbeitung können auf Verordnungsstufe präzisiert werden.

Beizubehalten ist auch der Fall, bei dem sich die Bearbeitung aus einer mittelbaren Grundlage im Gesetz ergibt (Bst. b). Das heisst, eine Behörde kann eine ihr im Gesetz zugewiesene Aufgabe nur erfüllen, wenn sie besonders schützenswerte Personendaten bearbeitet oder ein risikobehaftetes Profiling betreibt. Die Bearbeitung muss für die Aufgabenerfüllung «zwingend» erforderlich sein. Die betroffenen Personen müssen gestützt auf die Aufgabennormen und Zuständigkeitsvorschriften auf Gesetzesstufe abschätzen können, welche besonders schützenswerten Personendaten zu welchem Zweck über sie bearbeitet oder zu welchem Zweck Profilings betrieben werden. Folglich muss die Aufgabennorm «hinreichend bestimmt» ausgestaltet sein. Müssen die betroffenen Personen nicht mit solchen Bearbeitungen rechnen, dann ist eine hinreichend bestimmte Grundlage im Gesetz zu schaffen (Bst. a). Zu beachten sind insbesondere Fälle, bei denen ein bestimmter Aufgabenbereich verlassen wird, womit eine Zweckänderung einhergeht. Beispielsweise, wenn eine Behörde einer anderen Behörde mit einem anderen Aufgabengebiet besonders schützenswerte Personendaten systematisch bekanntgibt (so genannte Abrufverfahren). Dies entspricht dem geltenden Recht, wobei die Anforderungen neu auch für das Betreiben von risikobehafteten Profilings gelten.

Ebenfalls beizubehalten ist, dass eine Grundlage auf niedrigerer Stufe (Dekret oder Verordnung) genügt, wenn die betroffene Person in die Datenbearbeitung eingewilligt hat (Bst. c). In Angleichung an das Bundesrecht genügt nicht mehr nur die ausdrückliche Zustimmung der betroffenen Person für den Verzicht auf eine gesetzliche Grundlage, sondern auch wenn die betroffene Person die Daten allgemein zugänglich gemacht und die Bearbeitung nicht ausdrücklich untersagt hat. Im Gegensatz zum Bund entbehrt eine Einwilligung nicht von jeglicher gesetzlichen Grundlage, sondern lediglich von einer Grundlage auf Gesetzesstufe, was aus dem Einleitungssatz mit der Formulierung «zusätzlich» hervorgeht.

Nicht ins kantonale Recht zu übernehmen ist das Erfordernis einer Grundlage im Gesetz für Personendatenbearbeitungen, die zu einem schweren Eingriff in die Grundrechte führen können (Art. 34 Abs. 2 Bst. c revDSG). Diese Anforderung ergibt sich aus der eidgenössischen und kantonalen Verfassung (Art. 36 Abs. 1 BV und Art. 28 Abs. 1 KV).

Absatz 3

Das Amtsgeheimnis und besondere Geheimhaltungspflichten nach der Spezialgesetzgebung (z.B. Sozialhilfegeheimnis) inkl. Berufsgeheimnisse (z.B. Arztgeheimnis) bleiben vorbehalten. Rechtlich gesehen besteht eine Kollision: Das kantonale Datenschutzgesetz sieht die Bearbeitung von Personendaten vor, während das Fachgesetz die Geheimhaltung vorschreibt. Diese Kollision ist nach den allgemeinen Kollisionsregeln zu lösen, weshalb in der Regel die Bearbeitung nach dem kantonalen Datenschutzgesetz als lex generalis gegenüber der Geheimhaltungsvorschrift im Sachgesetz als lex specialis zurückzutreten hat. Der Vorbehalt im kantonalen Datenschutzgesetz ist daher lediglich deklaratorisch. Er findet sich jedoch auch im geltenden Recht (Art. 5 Abs. 5 KDSG) und wird zur Klarheit beibehalten.

Artikel 5 – Bearbeiten bei besonderer Gefahrenlage

Absatz 1

In Abweichung von Artikel 4 ist eine Bearbeitung von Personendaten, einschliesslich besonders schützenswerten Personendaten, auch zulässig, wenn die Bearbeitung wegen einer besonderen Gefahrenlage erforderlich ist. Dies entspricht Artikel 10 Buchstabe b der Richtlinie (EU) 2016/680 und Artikel 6 Absatz 1 Buchstabe d der Datenschutz-Grundverordnung. Demnach ist die Bearbeitung ebenfalls zulässig, wenn sie notwendig ist, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen, wenn es nicht möglich ist, die Einwilligung der betroffenen Person innert angemessener Frist einzuholen. Mit Artikel 5 wird eine Grundlage im Gesetz geschaffen, die bei einer solchen Gefahrenlage herangezogen werden kann. In Abstimmung mit Art. 12 Abs. 1 der Kantonsverfassung wird neben der körperlichen auch die geistige Unversehrtheit erwähnt.

Selbst besondere gesetzliche Geheimhaltungspflichten stehen einer solchen Bearbeitung nicht entgegen. Die betroffenen Interessen rechtfertigen eine Verletzung der Geheimhaltungspflicht.

Verzichtet wird auf die Aufnahme der Einzelfallbewilligung durch den Regierungsrat (vgl. Art. 34 Abs. 4 Bst. a revDSG). Die Einzelfallbewilligung einer Personendatenbearbeitung ohne gesetzliche Grundlage mittels Ermessensentscheid der Exekutivbehörde ist kaum mit dem Legalitätsprinzip vereinbar.

Artikel 6 und 7 – Zweckbindung und Verhältnismässigkeit

Diese Artikel verankern die weiteren Grundsätze des rechtsstaatlichen Handelns und entsprechen dem bisherigen Recht (Art. 5 Abs. 3 bis Abs. 5 KDSG).

Der Titel der Bestimmung lautet Zweckbindung. Daraus ergibt sich, dass es sich um einen Teilgehalt der Verhältnismässigkeit handelt. Wie bisher, muss der Zweck der Datenbearbeitung bestimmt sein (Artikel 6 Abs. 1 VE-revKDSG). Dieser ergibt sich aus den für die Aufgabenerfüllung anwendbaren Rechtgrundlagen. Vereinbar mit dem ursprünglichen Zweck ist auch die Aufbewahrung von Personendaten in der semi-aktiven Phase, während derer die Personendaten nicht mehr ständig zur Aufgabenerfüllung benötigt werden, oder die Archivierung in der inaktiven Phase (vgl. Erläuterungen zu Art. 16). Der in Artikel 6 Absatz 2 statuierte Grundsatz von Treu und Glauben gebietet ein loyales und vertrauenswürdiges Verhalten zwischen den verantwortlichen Behörden und den Privaten. Folglich dürfen verantwortliche Behörden Personendaten nur bekanntgegeben, wenn die betroffene Person damit rechnen muss, vorbehalten die abweichenden Bestimmungen im kantonalen Datenschutzgesetz. Im Unterschied zum bisherigen Recht ist Absatz 2 positiv formuliert.

Nach Artikel 7 muss die Bearbeitung von Personendaten verhältnismässig sein (bisher Art. 5 Abs. 3 KDSG). Das bedeutet, dass die Bearbeitung der Personendaten zur Zweckerreichung geeignet und erforderlich sein muss und der betroffenen Person zugemutet werden kann. Hierfür muss der Zweck der Datenbearbeitung bestimmt sein (Artikel 6 VE-revKDSG).

Artikel 8 – Richtigkeit

Die Bestimmung entspricht dem bisherigen Recht (Art. 7 KDSG). Natürliche Personen und Behörden haben gleichermassen ein Interesse daran, dass die bearbeiteten Personendaten richtig und vollständig sind. Die Qualität der Daten ist aber immer relativ. Daher kennt das kantonale Datenschutzgesetz wie bisher ein Berichtigungsverfahren (Art. 31 VE-revKDSG). Die vorliegende, allgemeine Vorschrift verpflichtet die bearbeitende Behörde, im Rahmen des Zumutbaren zu prüfen, ob die Daten richtig und vollständig sind. Je älter die Datenbestände sind, desto weniger streng kann das Prinzip gehandhabt werden.

Artikel 9 – Datenschutz durch Technik und datenschutzrechtliche Voreinstellungen

Dieser Artikel führt die Pflicht zur Einhaltung der Datenschutzbestimmungen durch Technik sowie durch datenschutzfreundliche Voreinstellungen ein. Die Norm setzt die Anforderungen von Artikel 10 Ziffer 3 SEV Nr. 108+ sowie Artikel 20 der Richtlinie (EU) 2016/680 um und entspricht Artikel 7 revDSG.

Absatz 1

Absatz 1 setzt die Pflicht zum Privacy by Design (Datenschutz durch Technik) um. Dementsprechend sollen technische und organisatorische Vorkehrungen den Verstoss gegen Datenschutzbestimmungen verunmöglichen oder zumindest die Gefahr erheblich verringern. Dieser Grundsatz ist bereits ab der Planung umzusetzen.

Mit den Datenschutzbestimmungen sind alle Vorschriften gemeint, die den Schutz personenbezogener Daten im Rahmen einer konkreten Datenbearbeitung sicherstellen, insbesondere die Bearbeitungsgrundsätze, Vorgaben an die Auftragsbearbeitung, Regeln zur Bekanntgabe von Personendaten ins Ausland, das Auskunftsrecht etc. Nicht erfasst sind die Pflicht zur Meldung der Datensammlungen an die Datenschutzbehörde oder die Pflicht zur Datenschutzfolgenabschätzung und der Vorabkontrolle.

Die zu treffenden technischen und organisatorischen Massnahmen werden selbst bestimmt. In einem ersten Schritt sind alle wesentlichen datenschutzrechtlichen Einflussfaktoren bezüglich der Datenbearbeitung zu definieren und in einem zweiten Schritt ist sicherzustellen, dass die Datenbearbeitung wie vorgesehen stattfindet und alle Datenschutzvorschriften eingehalten werden. Die Mittel dazu sind insbesondere interne Weisungen, Verschlüsselungen, Automatisierung von Löschungen, Zuständigkeitsregeln, Regelungen zur Aufbewahrungsdauer usw. In einem dritten Schritt sind die definierten Massnahmen umzusetzen.[46]

Absatz 2

Absatz 2 präzisiert die Anforderungen an die Vorkehren nach Absatz 1. Diese müssen insbesondere nach dem Stand der Technik, der Art und dem Umfang der Datenbearbeitung sowie der Eintrittswahrscheinlichkeit und Schwere der Risiken, welche die fragliche Bearbeitung für die Grundrechte der betroffenen Person mit sich bringt, angemessen sein.

Die Norm bringt den risikobasierten Ansatz zum Ausdruck. Das Risiko, das mit einer Bearbeitung einhergeht, muss zu den technischen Möglichkeiten in Beziehung gesetzt werden, um dieses zu verringern. Je höher das Risiko, je grösser die Eintrittswahrscheinlichkeit und je umfangreicher die Datenbearbeitung ist, umso höher sind die Anforderungen an die technischen Vorkehren, damit sie im Sinne der vorliegenden Bestimmung als angemessen gelten können.[47]

Absatz 3

Dieser Absatz führt die Verpflichtung ein, mittels geeigneter Voreinstellung sicherzustellen, dass die Bearbeitung der Personendaten auf das für den Verwendungszweck nötige Mindestmass beschränkt ist, soweit die betroffene Person nicht etwas anderes bestimmt. Damit wird der Grundsatz Privacy by Default umgesetzt. Dieser Bearbeitungsgrundsatz spielt bei der Datenbearbeitung durch Behörden eine unterge-

[46] vgl. Rosenthal David (2020): Das neue Datenschutzgesetz. In: Jusletter vom 16. November 2020, Rz. 44.
[47] BBl 17.059, S. 7029 f. Ziff. 9.1.3.1

ordnete Rolle, da die Datenbearbeitung selten auf der Einwilligung der betroffenen Person beruht. Dennoch soll hier der Grundsatz festgehalten werden, dass bei Standardeinstellungen die am wenigsten weitgehende Einstellung vorgesehen werden soll, wenn die verantwortliche Behörde bei einem Service, einer Software oder einem Gerät mehre Möglichkeiten vorsieht, wie Personendaten bearbeitet werden können und die Benutzerin oder der Benutzer die Einstellungen selbst anpassen kann.

Auf das für den Verwendungszweck nötige Mindestmass ist die Personendatenbearbeitung dann beschränkt, wenn der Eingriff in das Grundrecht auf Datenschutz für die betroffenen Personen am geringsten ist, und nicht etwa, wenn volumenmässig am wenigsten Daten bearbeitet werden.

Anzumerken ist, dass mit der datenschutzfreundlichen Voreinstellung kein Koppelungsverbot einhergeht. Die verantwortliche Behörde kann also bestimmen, dass eine bestimmte Datenbearbeitung nur gewählt werden kann, wenn zugleich auch andere Datenbearbeitungen zugelassen werden. Eingeschränkt wird dies höchstens durch den Grundsatz der Verhältnismässigkeit oder der Freiwilligkeit der Einwilligung.[48]

Artikel 10 – Datensicherheit

Im Artikeltitel ersetzt der Begriff «Datensicherheit» den überholten Begriff der «Datensicherung».

Absatz 1

Der Wortlaut von Absatz 1 wird an das revDSG angeglichen. Im Unterschied zum vorangehenden Artikel (Datenschutz durch Technik und datenschutzrechtliche Voreinstellungen) regelt dieser Artikel die Datensicherheit im engeren Sinn. Mit den technischen und organisatorischen Massnahmen sorgt die verantwortliche Behörde für den Schutz der Personendaten bezüglich ihrer Vertraulichkeit, Verfügbarkeit und Integrität. Vorkehrungen zur Verhinderung anderer Datenschutzverletzungen fallen dagegen unter den vorangehenden Artikel.

Typische Massnahmen zur Erreichung angemessener Datensicherheit sind Zugriffsbeschränkungen oder Zugangsbeschränkungen, aber auch Weisungen, Schulungen oder die sorgfältige Auswahl der beauftragten Dritten. Die Massnahmen müssen keinen absoluten Schutz bieten, sondern bei objektiver Betrachtung in einem vernünftigen Verhältnis zum Risiko einer Verletzung der Datensicherheit stehen. Es ist Aufgabe der verantwortlichen Behörde, die notwendigen Massnahmen zu bestimmen. Auf Verordnungsstufe werden Leitlinien für die Bestimmung der zu ergreifenden Massnahmen erlassen (vgl. Absatz 2), welche die Vielfalt der Personendatenbearbeitungen berücksichtigen und die notwendige Flexibilität gewährleisten.

Absatz 2

Der Kanton Bern erlässt ein neues Informations- und Cybersicherheitsgesetz (ICSG)[49] mit entsprechender Verordnung, welches die Informationssicherheit datenschutzübergreifend regelt. Deshalb wird hier auf die entsprechende Gesetzgebung verwiesen. Die Grundsätze des ICSG (2. Abschnitt des Gesetzes) gelten für den Datenschutz sinngemäss. Die verantwortlichen Behörden ergreifen entsprechend dem festgelegten Schutzbedarf Massnahmen bezüglich der Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit von Personendaten. Sie stellen sicher, dass auch beauftragte Dritte diese Anforderungen und Massnahmen beachten. Die Schutzstufen und Massnahmen werden über die jeweiligen Ausführungsbestimmungen synchronisiert.

Artikel – 11 Verantwortung

Nach dem übergeordneten Recht muss die Verantwortlichkeit für die Datenbearbeitung klar zugeordnet werden. Das gilt insbesondere bei gemeinsamen Datenbearbeitungen, wo die Verantwortlichkeiten transparent zu regeln sind. Die heutige Bestimmung zur Verantwortlichkeit genügt diesen Anforderungen nicht (Art. 8 KDSG). Der Grosse Rat verabschiedete am 7. März 2022 das DVG, welches eine den übergeordneten Vorgaben des europäischen Rechts adäquate Bestimmung zur Verantwortlichkeit enthält. Diese

[48] vgl. Rosenthal, David (2020), s.o.: Rz. 50.
[49] BSG [noch zu bestimmen]

Regelung ist ins kantonale Datenschutzgesetz zu überführen und gleichzeitig ist die provisorische Regelung im DVG aufzuheben (vgl. Ziff. 7.9.2).

Absatz 1

Entgegen der im März 2022 verabschiedeten Regelung soll jedoch nicht massgebend sein, dass die Behörde über den Zweck und die Mittel der Datenbearbeitung entscheidet. Vielmehr muss im Grundsatz gelten, dass wer Personendaten zur Erfüllung seiner gesetzlichen Aufgaben bearbeitet oder bearbeiten lässt, auch datenschutzrechtlich verantwortlich ist. Es trifft zwar zu, dass die Formulierung «wer über den Zweck und die Mittel der Datenbearbeitung entscheidet» sowohl in den europäischen Vorbildern als auch im Bundesdatenschutzgesetz verwendet wird und vorübergehend Eingang in die kantonale Gesetzgebung gefunden hat. Es ist aber zu beachten, dass die Formulierung sowohl auf europäischer als auch auf Bundesebene immer auch für Private gilt und deshalb generisch gefasst sein muss. Im ausschliesslich für behördliche Datenbearbeitungen geltenden kantonalen Datenschutzgesetz kann und muss die Verantwortung nach wie vor daran anknüpfen, wer Träger der öffentlichen Aufgabe ist und deshalb deren Erfüllung und die Verfassungsmässigkeit der dazu erforderlichen Datenbearbeitungen verantwortet. Mit der aus dem heutigen Recht übernommenen Formulierung wird dies – auch mit Blick auf die Unterscheidung, ob eine öffentliche Aufgabe übertragen wird (so, dass der Empfänger selbst zur verantwortlichen Behörde wird) oder ob eine Hilfsperson als beauftragte Dritte beigezogen wird (so, dass die Verantwortung bei der ursprünglichen Behörde verbleibt) – unmissverständlich festgehalten. Die Regelung erwähnt neben der Verantwortung für den Datenschutz auch die Datensicherheit. Letztere ist zwar in den Datenschutzbestimmungen enthalten, die Nennung soll jedoch ihre Wichtigkeit verdeutlichen.

Nicht als verantwortliche Behörde, sondern als beauftragter Dritter gilt, wer Datenbearbeitungen lediglich auf Weisung ausführt, selbst wenn dabei eine gewisse Entscheidungsfreiheit bleibt, wie beispielsweise über eingesetzte Abläufe, Auswahl der Programme oder Datensicherheitsmassnahmen.

Fragen der Verantwortlichkeit stellen sich beispielsweise, wenn die Konzernapplikation PERSISKA des Personalamts von vielen anderen Ämtern zur Personalverwaltung genutzt wird und die Daten über Netzwerke und Server laufen, die das Kantonale Amt für Informatik und Organisation (KAIO) als Teil der ICT-Grundversorgung zur Verfügung stellt (und damit Dritte beauftragt). In solchen Fällen ist die Verantwortlichkeit zu regeln (Abs. 2).

Absatz 2

Sind mehrere Behörden an einer Datenbearbeitung beteiligt, müssen sie einander ihre jeweilige Verantwortung transparent zuweisen. Das verhindert Verantwortungslücken.

Im oben erwähnten Beispiel wäre primär das Personalamt als Fachamt für den Datenschutz verantwortlich, aber auch die Behörden, die PERSISKA zur Verwaltung ihres Personals nutzen, müssen insoweit Mitverantwortung übernehmen, wie sie Daten ihrer Angestellten verwalten und dazu ihren Personalverantwortlichen Zugriffsberechtigungen erteilen. Das Personalamt muss daher mittels Nutzungsbestimmungen regeln, welche Datenschutzverantwortung die Nutzerämter tragen (regelmässige Überprüfung der Berechtigungen etc.). Das KAIO wirkt an der Datenbearbeitung ebenfalls mit, indem es mit der ICT-Grundversorgung technische Mittel dafür zur Verfügung stellt. Es regelt in seinen technischen Weisungen, welches Datenschutz- und Datensicherheitsniveau mit diesen Mitteln sichergestellt ist, so dass die nutzenden Behörden wissen, welche allfälligen Zusatzmassnahmen sie ergreifen müssen, um das von ihnen angestrebte Schutzniveau zu erreichen.

Absatz 3

Die Vereinbarung zwischen den Verantwortlichen soll der Transparenz willen veröffentlicht werden. So kann sich die betroffene Person leicht darüber informieren, an welche Behörde sie sich wenden kann, wenn sie ihre Rechte geltend machen will. Kennt die betroffene Person eine Behörde, die an der Datenbearbeitung beteiligt ist, kann sie auch bei dieser anfragen, wie die Verantwortlichkeiten aufgeteilt sind.

Entsprechend der bundesrechtlichen Regelung (Art. 33 revDSG) verzichtet das kantonale Datenschutzgesetz auf eine explizite Nachweispflicht über die Einhaltung der Datenschutzbestimmungen, wie sie Artikel 12 SEV Nr. 108+ und Artikel 4 Absatz 4 der Richtlinie (EU) 2016/680 verlangen. Nichtsdestotrotz kann die Datenschutzbehörde entsprechende Nachweise zur Einhaltung der Datenschutzbestimmungen einholen (vgl. Art. 44 Abs. 2 Bst. a VE-revKDSG).

Artikel 12 – Bearbeiten im Auftrag

Artikel 22 und Artikel 23 der EU-Richtlinie enthalten detaillierte Vorschriften, unter welchen Voraussetzungen eine Bearbeitung durch Dritte zulässig ist. Die Richtlinie stellt insbesondere Anforderungen an die Auftragsnehmerin bzw. den Auftragsnehmer, enthält Formvorschriften und inhaltliche Anforderungen an die Auftragserteilung sowie Voraussetzungen für das Unterauftragsverhältnis. Der Bund hat den Begriff der Auftragsbearbeiterin bzw. des Auftragsbearbeiters ins revDSG übernommen und die europäischen Anforderungen inhaltlich in Artikel 9 revDSG umgesetzt. Neu regelt das revDSG insbesondere die Unterauftragsbearbeitung (Art. 9 Abs. 3 revDSG). Der Kanton Bern kennt mit Artikel 28 DVG ebenfalls eine Bestimmung zur Datenbearbeitung durch Dritte, die sich – mit einer Ausnahme – am revDSG orientiert. Die einzige Abweichung zum neuen DSG korrigiert ein vermutliches Versehen des DSG-Gesetzgebers: Das revDSG hält in Absatz 2 abweichend von der Botschaft fest, dass der Auftragsbearbeiter nur «in der Lage» sein muss, die Datensicherheit zu gewährleisten. Dies wäre nicht sachgerecht: massgeblich ist die tatsächliche Sicherheit, nicht die potenzielle. Das DVG sieht deshalb vor, dass die verantwortliche Behörde sich vergewissern muss, dass die oder der Dritte die Datensicherheit gewährleistet. Diese Regelung ist in das kantonale Datenschutzgesetz zu übernehmen und gleichzeitig die provisorische Regelung im DVG aufzuheben (vgl. Ziff. 7.9.2).

Der Kanton Bern lässt im ICT-Bereich regelmässig Datenbearbeitungen durch Dritte durchführen. Dazu gehört namentlich der Betrieb staatlicher Applikationen in einem Rechenzentrum, z.B. der kantonseigenen Bedag Informatik AG. Die ICT-Strategie sieht die Auslagerung solcher Betriebsaufgaben als Grundsatz vor.

Die beauftragten Dritten führen eine Datenbearbeitung auf Weisung hin aus. Die Datenbearbeitung innerhalb einer Verwaltungseinheit stellt dagegen keine Auftragsbearbeitung dar. Werden Daten in einer sogenannten Cloud aufbewahrt, handelt es sich dabei grundsätzlich um einen Anwendungsfall der Auftragsbearbeitung, welche die entsprechenden Voraussetzungen erfüllen muss. Falls hierfür Daten ins Ausland bekanntgegeben werden, müssen zudem die Voraussetzungen von Artikel 15 VE-revKDSG erfüllt sein.

Absatz 1

Absatz 1 begründet eine Sorgfaltspflicht für die verantwortliche Behörde: Bei der Auftragsbearbeitung muss sie die Rechte der betroffenen Person wahren. Sie muss aktiv sicherstellen, dass die beauftragten Dritten das Gesetz im selben Umfang einhalten wie sie selbst (Bst. a). Das betrifft insbesondere die Einhaltung der allgemeinen Grundsätze, die Regeln zur Datensicherheit sowie diejenigen zur Bekanntgabe ins Ausland. Die verantwortliche Behörde muss Verstösse gegen die Datenschutzgesetzgebung verhindern. Infolgedessen ist sie verpflichtet, die beauftragten Dritten sorgfältig auszuwählen, sie angemessen zu instruieren und – soweit als möglich – zu überwachen. Nicht mehr erwähnt ist, dass eine Beauftragung von Personendatenbearbeitungen mittels Gesetz oder Vertrag erfolgt. Die Übertragung von Datenbearbeitungen durch die Gesetzgebung führt regelmässig zu einer eigentlichen Übertragung der Aufgabenerfüllung, so dass die Person, welche die Aufgabe nun erfüllt, selbst zur Behörde wird (Behörde im Sinne des kantonalen Datenschutzgesetzes).

Einer Auftragsdatenbearbeitung können sowohl Gesetzesbestimmungen als auch vertragliche Pflichten entgegenstehen, so beispielsweise die explizite Vorgabe zur Datenhaltung in der Schweiz. Die Geheimhaltungspflichten sind als Sonderregelung in Absatz 2 adressiert.

Absatz 2

Die Geheimhaltungspflichten sind spezifisch zu adressieren. Das «notwendige Minimum» hängt vom konkreten Service ab: Bei einer reinen Storage-Lösung ist in aller Regel kein Zugang notwendig; bei Software-as-a-Service (SaaS-)Diensten müssen die Daten während der Bearbeitung unverschlüsselt sein. Hier müssen die technischen oder organisatorischen Massnahmen rundherum den Zugriff minimieren. Die Massnahmen sind kumulativ oder alternativ zu ergreifen.

Absatz 3

Die Richtlinie (EU) 2016/680 verlangt, dass die beauftragten Dritten mit geeigneten technischen und organisatorischen Massnahmen hinreichende Garantien für eine gesetzeskonforme Datenbearbeitung bieten müssen. Deshalb werden die Anforderungen an die Datensicherheit explizit erwähnt.

Absatz 4

Dieser Absatz sieht vor, dass die beauftragten Dritten die Bearbeitung nur mit vorgängiger Genehmigung der verantwortlichen Behörde an Dritte übertragen dürfen. Die Genehmigung hat schriftlich zu erfolgen, wobei in elektronischer Form genügt. Die Formvorschriften sind auf Verordnungsstufe zu konkretisieren.

Artikel 13 – Beschaffen

Im Anschluss an die allgemeinen Bearbeitungsgrundsätze enthalten die folgenden Bestimmungen weitergehende Regeln für besondere Bearbeitungsformen wie das Beschaffen oder die Bekanntgabe von Personendaten.

Die Grundsätze für die Beschaffung von Personendaten sind aus dem bisherigen Recht (Art. 9 Abs. 1 bis 3 KDSG) zu übernehmen. Demnach sollen Personendaten grundsätzlich nicht bei privaten Personen erhoben werden. Das Wort «grundsätzlich» bedeutet, dass auch Ausnahmen möglich sind. Eine Ausnahme ist insbesondere anzunehmen, wenn sonst der Zweck der Datenbeschaffung nicht erreicht werden könnte. Vom Bürger wird es mitunter als lästig empfunden, wenn er immer wieder das Gleiche gefragt wird, weshalb Personendaten auch verwaltungsintern beschafft werden können, sofern dieses Gesetz nicht entgegensteht. Die private Person kann davon ausgehen, dass Personendaten nur beschafft werden, wenn sie zur Auskunft verpflichtet ist. Ist das nicht der Fall, muss die verantwortliche Behörde auf die Freiwilligkeit der Auskunft hinweisen.

Die Informationspflichten (Art. 9 Abs. 4 KDSG) sind neu unter dem 3. Titel «Pflichten der verantwortlichen Behörde und von beauftragten Dritten» geregelt.

Artikel 14 – Bekanntgabe

Bisher regelt das kantonale Datenschutzgesetz die Bekanntgabe an Behörden (Art. 10 KDSG) und an Private (Art. 11 KDSG) separat, obwohl sich die Bestimmungen mehrheitlich überschneiden. Im Unterschied zum Kanton Bern kennen die meisten anderen Kantone keine separaten Bestimmungen. Mit der Revision werden die Bestimmungen zusammengefasst und die Bekanntgabe durch die Einwohnergemeinde in die Spezialgesetze verschoben (vgl. Ziff. 7.5.3). Bei letzterer Bestimmung handelt es sich um materielles Datenschutzrecht, welches nicht im Datenschutzrecht als Querschnittsmaterie zu regeln ist. Sie ist bisher ein Fremdkörper im Gesetz.

Die Bekanntgabe von Personendaten ist eine Unterkategorie des Bearbeitens von Personendaten. Deshalb unterscheiden sich die Anforderungen an die Datenbekanntgabe im Grundsatz auch nicht von den Voraussetzungen, unter welchen Personendaten bearbeitet werden dürfen. Hinzu kommt jedoch, dass die Bekanntgabe an eine andere Behörde zusätzlich erfolgen darf, wenn diese zur Bearbeitung der betreffenden Personendaten berechtigt ist und keine besonderen Geheimhaltungspflichten entgegenstehen (Abs. 2).

Absatz 1

Wie nach geltendem Recht benötigt die Bekanntgabe an eine andere Behörde oder an eine Privatperson eine unmittelbare oder eine mittelbare gesetzliche Grundlage, wobei generell-abstrakte Normen aller

Rechtsetzungsstufen in Betracht fallen, wie auch z. B. Mitteilungspflichten in einer Vollziehungsverordnung. «Dazu» drückt aus, dass sich die Rechtsgrundlage auf die Bekanntgabe beziehen muss. Bei besonders schützenswerten Personendaten sind die erhöhten Anforderungen an die gesetzliche Grundlage zu beachten, d.h. es braucht zusätzlich eine Grundlage im Gesetz oder die betroffene Person hat im Einzelfall ausdrücklich eingewilligt oder ihre Personendaten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt (vgl. Erläuterungen zu Art. 4 Abs. 2 VE-revKDSG).

Wie bereits ausgeführt, kann die verantwortliche Behörde Personendaten auch gestützt auf eine Einwilligung nicht ohne jegliche gesetzliche Grundlage bearbeiten (vgl. Erläuterungen zu Art. 4 VE-revKDSG). Hingegen ist es möglich, dass die verantwortliche Behörde Personendaten bekanntgibt, die sie rechtmässig erhoben hat, wenn die betroffene Person im Einzelfall ausdrücklich zugestimmt hat oder ihre Personendaten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat (Bst. c). Gibt die Behörde die rechtmässig erhobenen Personendaten bekannt, verstösst sie aber gegen den Grundsatz der Zweckbindung, da die Personendaten zu einem anderen Zweck bearbeitet werden, als denjenigen für den sie beschafft worden sind. Deshalb sieht Artikel 6 Absatz 2 VE-revKDSG einen entsprechenden Vorbehalt für die Bekanntgabe vor.

Die verantwortliche Behörde kann Personendaten ausserdem bei einer besonderen Gefahrenlage bekanntgeben (Bst. c). Auch hier werden die Personendaten nicht mehr zum ursprünglichen Zweck bearbeitet.

Absatz 2

Wie nach bisherigem Recht kann auch nur die verlangende Behörde zur Datenbearbeitung befugt sein, sofern keine besonderen Geheimhaltungspflichten entgegenstehen (Bst. b). Die bekanntgebende Behörde soll nicht nach den gesetzlichen Grundlagen suchen müssen, welche die empfangende Behörde zur Bearbeitung der Personendaten ermächtigt. Deshalb soll die verlangende Behörde die gesetzlichen Grundlagen darlegen und begründen, inwiefern sie dadurch zur Bearbeitung der fraglichen Personendaten ermächtigt ist. Bei besonders schützenswerten Personendaten sind jeweils die erhöhten Anforderungen an die gesetzliche Grundlage zu beachten, d.h. es braucht eine Grundlage im Gesetz.

Absatz 3

Der Bekanntgabe können besondere gesetzliche Geheimhaltungspflichten entgegenstehen. Es muss sich um eine gesetzlich verankerte Geheimhaltungspflicht handeln, beispielsweise ein gesetzlich verankertes Berufs- oder besonderes Amtsgeheimnis (Arzt- oder Steuergeheimnis).

Die Bestimmung erfährt zudem gegenüber dem geltenden Recht (Art. 14 KDSG) eine redaktionelle Anpassung: «Überwiegende öffentliche Interessen oder besondere schützenswerte private Interessen» wird in Übereinstimmung mit den restlichen Bestimmungen ersetzt durch «überwiegende öffentliche oder private Interessen», da es sich um einen klassischen Anwendungsfall der Interessensabwägung handelt. Folglich wird eine Bekanntgabe von Personendaten immer verweigert, eingeschränkt oder aufgeschoben werden, wenn überwiegende öffentliche oder private Interessen entgegenstehen.

Artikel 15 – Bekanntgabe ins Ausland (Varianten-Entscheid)

Betreffend die Bekanntgabe von Personendaten ins Ausland schickt der Regierungsrat zwei Varianten in die Vernehmlassung. Grundsätzlich dürfen die verantwortlichen Behörden Personendaten ins Ausland bekanntgeben, wenn sie ein angemessenes Datenschutzniveau gewährleisten (Abs. 1 und 2), ausser sie können sich auf einen Ausnahmetatbestand (Abs. 3) berufen. Die Varianten unterscheiden sich bezüglich der Ausnahmetatbestände. Sie ergeben sich mit Blick auf das Urteil «Schrems II» vom 16. Juli 2020 des Europäischen Gerichtshof (EuGH), wonach die USA keinen dem europäischen Datenschutzrecht gleichwertigen Schutz gewährleistet. Dadurch ergeben sich auch in der Schweiz Unsicherheiten bezüglich der Nutzung von US-Cloud-Lösungen wie Microsoft 365.

Die Variante 1 umfasst Artikel 15 Abs. 1 bis 3 Buchstabe a bis c. Sie sieht nur restriktive Ausnahmetatbestände vor und gewichtet das Grundrecht auf Datenschutz der betroffenen Personen höher als die öffentlichen Interessen der verantwortlichen Behörden, die sich aus der Nutzung von US-Cloud-Lösungen ergeben.

Die Variante 2 sieht zusätzlich zu Artikel 15 Absatz 1 bis 3 Buchstabe a bis c einen weiteren Ausnahmetatbestand in Buchstabe d vor, der die Nutzung von US-Cloud-Lösungen erleichtern soll. Sie gewichtet die öffentlichen Interessen der verantwortlichen Behörden an der Nutzung der US-Cloud-Lösungen höher als die in dieser Variante als unwahrscheinlich betrachteten Eingriffe in die Grundrechte der betroffenen Personen.

Zu Variante 1 und 2:

Absatz 1

Die verfassungsmässigen Garantien bei der Einschränkung von Grundrechten sind auch bei einer Bekanntgabe von Personendaten ins Ausland zu gewährleisten. Als Grundregel gilt deshalb, dass die Übermittlung von Personendaten an Drittstaaten zulässig ist, wenn diese über ein angemessenes Schutzniveau verfügen (Art. 16 Abs. 1 und 2 revDSG, Art. 17 SEV108+ und Art. 36 Abs. 1 Richtlinie (EU) 2016/680). Es stellt sich also die Frage, ob das Drittland einen Datenschutz gewährleistet, der mit den schweizerischen und kantonalen Verfassungsgrundsätzen vereinbar ist. Als solche zu nennen sind:

- Legalitätsprinzip (Art. 5 und 164 BV, Art. 18 Abs. 2, 66 Abs. 2 und 69 Abs. 4 KV): Jede Bearbeitung von Personendaten bedarf einer hinreichend bestimmten und klaren Rechtgrundlage.
- Verhältnismässigkeit (Art. 36 Abs. 3 BV, Art. 28 Abs. 3 KV): Die Eingriffe in das Grundrecht auf Datenschutz müssen geeignet und erforderlich sein, um die gesetzlichen Zwecke zu erfüllen. Die Eingriffe müssen für die betroffenen Personen zumutbar sein.
- Wirksames Rechtsmittel (Art. 13 Abs. 2 BV, Art. 18 Abs. 1 und 3 KV): Die betroffenen Personen müssen einen wirksamen, gesetzlich verankerten Rechtsbehelf für die Durchsetzung ihrer Rechte (z.B. Auskunftsrecht, Berichtigungs- und Löschungsrecht) haben.
- Rechtsweggarantie (Art. 29 ff. BV, Art. 18 Abs. 1 und 3 KV): Eingriffe in das Grundrecht auf Datenschutz müssen von einem Gericht oder anderen unabhängigen Stellen überprüfbar sein.

Im Gegensatz zum bisherigen Artikel 14a KDSG wird die Bestimmung positiv formuliert und ans Bundesrecht angepasst.

Absatz 2

Damit nicht bei jeder Auslandbekanntgabe das Datenschutzniveau erneut geprüft werden muss, sieht das kantonale Datenschutzgesetz (wie auch der Bund) vor, dass unter gewissen Voraussetzungen ein angemessenes Schutzniveau gewährleistet werden kann.

Ein angemessenes Schutzniveau kann gewährleistet werden durch einen völkerrechtlichen Vertrag (Bst. a), einen Feststellungsbeschluss des Bundesrats (Bst. b) oder andere hinreichende Garantien (Bst. c). So sieht es auch Artikel 16 Absatz 1 und 2 revDSG vor.

Buchstabe a

«Völkerrechtlicher Vertrag» meint nicht nur ein internationales Datenschutzübereinkommen wie das Übereinkommen SEV Nr. 108+, dem der Empfängerstaat angehört und dessen Anforderungen von der Vertragspartei im innerstaatlichen Recht umgesetzt worden sind, sondern auch jedes andere internationale Abkommen, das materiell den Anforderungen des Übereinkommens SEV Nr. 108+ entspricht. Wenn die Daten in ein Land der Europäischen Union übermittelt werden, kann von einem angemessenen Datenschutzniveau ausgegangen werden, sofern eine weitere Übermittlung in ein Drittland ausgeschlossen ist.

Buchstabe b

Ein angemessener Schutz ist zudem gewährleistet, wenn ein Staat auf der Positivliste des Bundesrates zu finden ist (Bst. b). Gemäss Artikel 16 Absatz 1 revDSG stellt der Bundesrat in einer Positivliste fest,

welche Staaten ein angemessenes Datenschutzniveau haben. Die Liste ist als Anhang im Verordnungsrecht aufgeführt. 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.[50] Hier handelt es sich um eine klare Erleichterung für die verantwortlichen Behörden. Liegt nämlich ein entsprechender Angemessenheitsbeschluss des Bundesrates vor, so ist es nicht mehr an der verantwortlichen Behörde zu prüfen, ob ein Drittstaat ein angemessenes Datenschutzniveau bietet. Es handelt sich um eine Vereinfachung und trägt damit der Motion Vogt Rechnung.

Der EuGH hat in seinem Urteil «Schrems II» vom 16. Juli 2020 festgestellt, dass die USA keinen dem europäischen Datenschutzrecht gleichwertigen Schutz gewährleisten. Der Gerichtshof führte u.a. aus, dass gestützt auf die innerstaatlichen Vorschriften der USA (Section 702 Foreign Intelligence Surveillance Act, FISA; Executive Order 12333) ihre Behörden auf dorthin übermittelte personenbezogene Daten zugreifen können. Dadurch werde unverhältnismässig in die Grundrechte der betroffenen Personen eingegriffen, da weder der Zugriff auf die Personendaten beschränkt sei noch ein wirksamer Rechtsschutz bestehe. Der Bundesrat ist dieser Einschätzung insofern gefolgt, als dass sich die USA nicht auf der Positivliste des Bundesrates befindet (Anhang 1 zur Datenschutzverordnung, die am 23. September 2023 in Kraft tritt).

Die verantwortlichen Behörden müssen daher bei der Bekanntgabe von Personendaten in die USA – namentlich bei der Nutzung der Services von US-Cloud-Anbietern – mit anderen Garantien (wie z.B. den Standardvertragsklauseln) und zwingenden zusätzlichen Massnahmen (wie z.B. der Verschlüsselung der Personendaten, Bst. c) ein angemessenes Schutzniveau gewährleisten oder sich auf einen Ausnahmetatbestand nach Absatz 3 stützen können.

Nach Variante 1 ist es zulässig, wenn Datenbearbeitungen in der Schweiz oder der Europäischen Union durch Cloud-Anbieter erfolgen, welche zwar wirtschaftlich aus dem Ausland kontrolliert werden, wenn zusätzliche Massnahmen ergriffen werden (vertragliche Regelungen, Verschlüsselung etc.) und die Daten «physisch» in der Schweiz oder der Europäischen Union bleiben.

Da die Nutzung von US-Cloud-Lösungen für die verantwortlichen Behörden bei restriktiven Anforderungen erheblich erschwert wird, unterbreitet der Regierungsrat mit der Vernehmlassungsvorlage einen zusätzlichen Ausnahmetatbestand als Variante 2 (siehe Abs. 3 Bst. d).

Buchstabe c

Ein angemessenes Schutzniveau kann auch mittels hinreichender Garantien erreicht werden (Bst. c). Wie im bisherigen Recht und im Gegensatz zum Bund (Art. 16 Abs. 2 Bst. b bis e revDSG) verzichtet das kantonale Datenschutzgesetz darauf, die einzelnen Garantien aufzuführen. Solche Garantien sind beispielsweise die vom Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten genehmigten Standardvertragsklauseln. Die hinreichenden Garantien sind in den Ausführungsbestimmungen zu konkretisieren.

Artikel 17 SEV 108+ sieht für die Anpassung von 14 Absatz 5 SEV108 eine Informationspflicht an die Datenschutzbehörde vor, sofern Daten gestützt auf Garantien ins Ausland bekanntgegeben werden. Eine entsprechende Informationspflicht sieht auch das geltende Recht vor (Art. 14a Abs. 3 KDSG). Der Bund hat jedoch auf diese Informationspflicht verzichtet bzw. das Parlament hat sie in der Beratung gestrichen. Geblieben ist lediglich die Information auf Anfrage, sofern die Bekanntgabe in unmittelbarem Zusammenhang mit einem Vertragsabschluss zugunsten der betroffenen Person steht, oder sofern sie aufgrund überwiegender öffentlicher Interessen, im Zusammenhang mit Rechtsansprüchen notwendig ist oder sofern sie zum Schutz der betroffenen Person erfolgt. Da die Datenschutzbehörde sowieso gestützt auf Artikel 44 Absatz 2 Bst. a VE-revKDSG Auskünfte einholen kann, muss dies hier nicht explizit geregelt werden. In Angleichung an das Bundesrecht wird auf die Informationspflicht verzichtet. Es handelt

[50] BBl 2017 6941, S. 7039

sich dabei um eine Erleichterung für die verantwortliche Behörde, weshalb die Nichtübernahme auch der Umsetzung der Motion Vogt dient.

Absatz 3

Personendaten dürfen auch ins Ausland bekanntgegeben werden, wenn zwar kein angemessenes Schutzniveau vorliegt, aber eine Voraussetzung nach Absatz 3 gegeben ist. Gegenüber dem heutigen Recht wird die Bestimmung stark gestrafft, da die Regelungen auf private Personen zugeschnitten waren und Anwendungsfälle für verantwortliche Behörden fehlten.

Buchstabe a

Buchstabe a entspricht dem bisherigen 1. Satz des Buchstaben d. Das Vorliegen eines überwiegenden öffentlichen Interesses muss unter den konkreten Umständen nachgewiesen werden. Ein rein hypothetisches Interesse genügt nicht. Unter der «Wahrung eines überwiegenden öffentlichen Interesses» ist beispielsweise die innere Sicherheit der Schweiz oder eines Drittstaates zu verstehen. Aufgrund dieser Bestimmung dürfen Personendaten auch aus humanitären Gründen ins Ausland bekannt gegeben werden, beispielsweise wenn die verantwortliche Behörde sie bekannt gibt, um bei der Suche nach Personen zu helfen, die in einem Konfliktgebiet vermisst werden oder in einer Region, in der eine Naturkatastrophe stattgefunden hat.

Buchstabe b

Beibehalten wird die Möglichkeit der Auslandsbekanntgabe im Falle der ausdrücklichen Einwilligung. Diese hat sowohl im Einzelfall zu erfolgen und muss ausdrücklich sein. Die ausdrückliche Zustimmung ergibt sich aus Artikel 17 SEV108+. Ausdrücklich bedeutet, dass aus der Einwilligung der Wille der betroffenen Person klar hervorgehen muss. Dies ist insbesondere möglich durch das Ankreuzen eines Kästchens, die aktive Auswahl bestimmter technischer Parameter oder anderweitige Erklärungen. Dasselbe gilt für die nonverbale Äusserung mittels eines im konkreten Kontext klaren Zeichens oder einer entsprechenden Bewegung. Wo eine ausdrückliche Einwilligung erforderlich ist, kann diese nicht stillschweigend gegeben werden. Die betroffene Person muss insbesondere den Namen des Drittstaats kennen und über die Risiken der Bekanntgabe im Zusammenhang mit dem Datenschutzniveau im ausländischen Staat informiert werden. Weiter zu übernehmen ist Artikel 17 Absatz 1 Buchstabe e revDSG. Dieser erlaubt die Bekanntgabe auch, wenn die betroffene Person die Daten der Allgemeinheit zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat. Unter den gleichen Voraussetzungen ist auch die Bekanntgabe im Inland zulässig (Art. 14 Abs. 1 Bst. b VE-revKDSG).

Buchstabe c

Buchstabe c ermöglicht die Bekanntgabe ins Ausland, um das Leben oder die körperliche oder geistige Unversehrtheit der betroffenen Person oder eines Dritten zu schützen. Dies entspricht dem bisherigen Artikel 14a Absatz 2 Buchstabe e KDSG, abgesehen vom Zusatz «und es ist nicht möglich, innerhalb einer angemessenen Frist die Einwilligung der betroffenen Person einzuholen». Die Anpassung erfolgt gestützt auf das revDSG. Eine Einwilligung ist beispielsweise nicht möglich, wenn die betroffene Person körperlich dazu nicht in der Lage ist oder sie mit Hilfe der üblichen Kommunikationsmittel nicht erreichbar ist.

Zusatz zu Variante 2:

Buchstabe d

Praktisch jede Behörde verfügt über ein Twitter-, YouTube- oder Instagram-Konto und Software-Lösungen wie Zoom oder Teams werden seit der Corona-Pandemie im Bildungssektor regelmässig genutzt. Die Rechtsprechung des EuGH zum Datenschutzniveau der USA und die dieser folgenden Beurteilung durch den Bundesrat erschweren für die verantwortlichen Behörden die Nutzung solcher Services von US-Anbietern, da es massgebend ist, ob die Personendaten in der Schweiz, der Europäischen Union oder in den USA bearbeitet werden. Der Regierungsrat des Kantons Bern unterbreitet deshalb in der Ver-

nehmlassung einen weiteren Ausnahmetatbestand als Variante, bei dem kein angemessenes Datenschutzniveau für die Auslandbekanntgabe verlangt wird. Damit soll der Realität entsprochen und die Nutzung von US-Cloud-Lösungen erleichtert werden.

Diese abweichende Regelung gegenüber dem Bund und soweit bekannt auch gegenüber den übrigen Kantonen - beinhaltet einen Standortvorteil für den Kanton Bern. Die Nutzung von US-Cloud-Lösungen soll demnach zulässig sein, wenn die Voraussetzungen der Bearbeitung im Auftrag erfüllt sind. Das würde bedeuten, dass die verantwortlichen Behörden lediglich die Datensicherheit gewährleisten müssten (Art. 12 Abs. 3 VE-KDSG). Diese orientiert sich an dem Risiko einer Grundrechtsverletzung (Art. 10 Abs. 1 VE-KDSG). In dieser Variante wird davon ausgegangen, dass die Datenschutzrisiken, die sich für die betroffenen Personen aus der Nutzung von US-Cloud-Lösungen ergeben können, theoretischer Natur sind und in der Praxis kaum relevant sind. Dem gegenüber stehen die grossen praktischen öffentlichen Interessen an der Nutzung der weltweit besten Cloud-Lösungen: Mit ihnen können die Behörden ihre Digitalisierungsziele viel rascher, kostengünstiger und kundenfreundlicher erreichen als mit konventioneller, nicht cloudbasierter Software. Tiefer gewichtet werden die gegebenenfalls erleichterten Zugriffe ausländischer Strafbehörden oder Nachrichtendienste auf Daten oder die eingeschränkten Möglichkeiten, sich gerichtlich gegen Datenschutzverletzungen im Ausland zu wehren.

Die Nutzung von US-Cloud-Software ist im privaten und im privatwirtschaftlichen Umfeld die Norm. Fast alle Menschen haben ein Apple-, Microsoft- oder Google-Konto sowie entsprechende Geräte, und die meisten Unternehmen könnten ohne US-Cloud-Software nicht mehr funktionieren. In diesem Umstand liegt ein gesamtgesellschaftlicher Risikoentscheid, der in dieser Variante vom Gesetzgeber berücksichtigt wird: Wenn fast alle Menschen und Unternehmen die zur Diskussion stehenden Risiken für sich selbst als verhältnismässig und tragbar erachten, dann darf und soll dies auch der Kanton für seine Bevölkerung tun. Im Gegensatz zu Privaten sind Behörden zwar zusätzlich an verfassungsmässige Grundsätze wie das Legalitätsprinzip gebunden, weshalb die Situationen nur bedingt vergleichbar sind. Dennoch sollte auch der Kanton die private Risikoabwägung berücksichtigen können, weshalb die vorliegende Variante in die Vernehmlassung geschickt wird.

Artikel 16 – Vernichtung und Archivierung

Dieser Artikel regelt die Berührungs- und Schnittpunkte zwischen der Datenschutz- und Archivgesetzgebung. Das Bearbeiten von Personendaten erfolgt zur Aufgabenerfüllung, wobei der Verhältnismässigkeitsgrundsatz gebietet, dass das Bearbeiten von Personendaten zeitlich befristet wird.

Geschäfte durchlaufen nach heutigem Verständnis der Archivwissenschaften grundsätzlich drei Lebenszyklen, bestehend aus einer aktiven, einer semiaktiven und einer inaktiven Phase. Die Geschäfte durchlaufen die Phasen jedoch nicht strikt nacheinander, sondern teilweise parallel. Die einzelnen Phasen sehen wie folgt aus:

- Aktive Phase: Sie beginnt mit der Eröffnung eines Geschäfts und endet mit dessen Abschluss. Während dieser Phase bearbeitet die verantwortliche Behörde die Personendaten zu einem bestimmten Zweck. Dieser Zweck verknüpft die Datenbearbeitung mit der gesetzlichen Aufgabe, zu deren Erfüllung die Datenbearbeitung erfolgt und sich dadurch rechtfertigt.
- Semiaktive Phase: Sie beginnt nach dem Abschluss eines Geschäfts und endet nach Ablauf der Aufbewahrungsfrist des Dossiers. Das Geschäft und die im Dossier abgelegten Dokumente erfahren in dieser Phase keine Änderungen mehr. Die Rechtfertigung für die Datenbearbeitung ergibt sich immer noch aus der ursprünglichen Aufgabenerfüllung, wobei sich der Zweck geändert hat. Die Datenbearbeitung beschränkt sich auf den Zweck, für den die Personendaten aufbewahrt werden.
- Inaktive Phase: Nicht mehr benötigte, archivwürdige Daten, werden dem Archiv übergeben. Durch die Archivierung erfahren die Daten eine Zweckänderung. Archivierte Daten dienen der Erfüllung der Wirkungsziele gemäss Artikel 2 des Gesetzes vom 31. März 2009 über die Archivierung (ArchG)[51] und

[51] BSG 108.1

werden zu diesem Zweck weiterhin benötigt. Der Zugriff auf die Daten ist nur noch zu den in der Archivgesetzgebung vorgesehenen Zwecken zulässig.

Absatz 1

Absatz 1 legt den Grundsatz fest, dass Personendaten zu vernichten sind, die nicht mehr benötigt werden. Benötigt werden Daten, welche für einen gesetzlich erlaubten Zweck notwendig sind. Das kann sein für die Bearbeitung während der gesetzlichen Aufgabenerfüllung als primären Zweck (aktive Phase, Abs. 1), für die Aufbewahrung (semi-aktive Phase, Abs. 2 und 3) oder für die dauernde Aufbewahrung im Sinne der Archivgesetzgebung als sekundären Zweck (inaktive Phase, Abs. 4).

Absatz 2

In Absatz 2 verpflichtet der Gesetzgeber die verantwortlichen Behörden mittels einer Aufbewahrungsfrist festzulegen, ob und wie lange Personendaten aufzubewahren sind, wenn sie nicht mehr ständig für die Aufgabenerfüllung benötigt werden. In die semiaktive Phase (Aufbewahrungsphase) werden die Personendaten nur überführt, wenn sie weiterhin benötigt werden. Entweder, weil die verantwortliche Behörde eine Aufbewahrungsfrist festgelegt hat, oder weil die besondere Gesetzgebung eine solche vorsieht. Der Vorbehalt in Absatz 2 bezieht sich auf die behördlich festgelegte Aufbewahrungsfrist. Eine besondere Aufbewahrungsfrist findet sich beispielsweise in Artikel 26 Absatz 2 Gesundheitsgesetz vom 2. Dezember 1984 (GesG)[52], wonach Behandlungsdokumentationen mindestens während zwanzig Jahren aufzubewahren sind.

Die Aufbewahrungsfristen schaffen vom Einzelfall unabhängig die Vermutung, dass die Personendaten weiterhin für einen gesetzlich erlaubten Zweck benötigt werden, sei es zu Sicherungs- und Beweiszwecken oder für die Nachvollziehbarkeit der Aufgabenerfüllung. Der Aufbewahrungszweck stützt sich weiterhin auf den primären Zweck der Aufgabenerfüllung. Aufbewahrungsfristen werden in vielen Fällen normativ durch die besondere Gesetzgebung festgelegt, weshalb das geltende Recht in Absatz 4 die besonderen Aufbewahrungsvorschriften vorbehält. Aus Gründen der Übersichtlichkeit und zur Verbesserung der systematischen Ordnung wird dieser Vorbehalt von Absatz 4 in Absatz 2 verschoben.

Absatz 3

In Absatz 3 werden die Voraussetzungen aufgeführt, welche die Aufbewahrung über den Zeitpunkt rechtfertigt, den die verantwortliche Behörde nach Absatz 2 festgelegt hat oder den die Aufbewahrungsfrist der besonderen Gesetzgebung verlangt (vgl. Abs. 2). Die Behörde kann also im Einzelfall darlegen, dass sie die Personendaten weiterhin benötigt und sie deshalb über die festgelegten Fristen hinaus aufbewahrt werden müssen.

Absatz 4

Gleichzeitig wird in Absatz 4 der Vorbehalt zugunsten der Archivgesetzgebung neu formuliert und ergänzt. Die Archivierung stellt einen vom Gesetz erlaubten Zweck dar, demzufolge die zur Archivierung bestimmten Daten nicht vernichtet werden dürfen (vgl. Abs. 1). Auf die Archivgesetzgebung wird sodann nicht mehr im Sinn eines Vorbehalts verwiesen, da dieser Absatz vielmehr ein Bindeglied zwischen der Datenschutzgesetzgebung und der Archivgesetzgebung darstellt. Damit soll verdeutlicht werden, dass die Archivierung keine Ausnahme des Grundsatzes der Vernichtung von nicht mehr benötigten Daten (Abs. 1) darstellt, sondern ein weiterer gesetzlich erlaubter Bearbeitungszweck ist.

Artikel 17 – Bearbeiten für nicht personenbezogene Zwecke

Die Bearbeitung von Personendaten für Zwecke der Statistik, Planung oder wissenschaftlichen Forschung geniesst datenschutzrechtlich weitgehende Privilegien, weil hier die betroffene Person nicht als individuelle Persönlichkeit, sondern lediglich anonym, als statistische Einheit interessiert. Ausgangspunkt sind Personendaten, deren Personenbezug im Verlauf der Bearbeitung wegfällt, weshalb die Grundrechte nicht mehr betroffen sind.

[52] BSG 811.01

Im Unterschied zum bisherigen Recht wird der Titel der Bestimmung neutraler formuliert und lautet neu «Bearbeiten für nicht personenbezogene Zwecke».

Absatz 1

In Absatz 1 werden beispielhaft die nicht personenbezogenen Zwecke wie Forschung, Praxisbildung, Statistik oder Planung aufgezählt. Die Voraussetzungen der Bearbeitung entsprechen dem bisherigen Recht, erfahren jedoch redaktionelle Anpassungen.

Personendaten müssen, sobald es der Bearbeitungszweck erlaubt, anonymisiert oder pseudonymisiert werden (Bst. a). Der bisherige Wortlaut, wonach die Personendaten nur «ohne direkte Personenkennzeichnung» verwendet werden dürfen, wird durch «pseudonymisiert» ersetzt und nimmt damit den bekannten Begriff der Datenschutz-Grundverordnung und der Richtlinie (EU) 2016/680 auf und entspricht dazu dem Vorschlag des KdK-Leitfadens. Personendaten gelten demzufolge als pseudonymisiert, wenn sie ohne zusätzliche Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. Die zusätzlichen Informationen müssen gesondert aufbewahrt werden und technischen und organisatorischen Massnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer natürlichen Person zugeordnet werden können.

Im Vergleich zur bisherigen Bestimmung soll mit dem Zusatz «im Fall» verdeutlicht werden, dass die verantwortliche Behörde, die Ergebnisse nicht bekanntgeben muss, sondern nur sicherstellen muss, dass die betroffenen Personen im Zeitpunkt der Bekanntgabe nicht bestimmbar sind.

Absatz 2

Die verantwortliche Behörde kann Personendaten zur Bearbeitung von nicht personenbezogenen Zwecken unter bestimmten Voraussetzungen auch Dritten bekanntgeben. Die zusätzlichen Anforderungen nach Absatz 2 sind mit einem Vertrag oder – wo angezeigt – mittels Verfügung sicherzustellen.[53]

In diesem Fall hat sie die Verpflichtung, die Daten zu anonymisieren bzw. zu pseudonymisieren sowie die Anforderungen an die Publikation der Ergebnisse dem Dritten aufzuerlegen (Bst. a).

Im Unterschied zum bisherigen Recht ist die Weitergabe an Dritte mit Zustimmung der verantwortlichen Behörde möglich (Bst. b), welche die Zustimmung nur insoweit erteilen darf, als sichergestellt ist, dass auch die Dritten die Daten nur gemäss den Voraussetzungen von Art. 17 Abs. 2 bearbeiten.

Hingegen haben die Empfängerin oder der Empfänger wie nach bisherigem Recht für die Datensicherheit zu sorgen (Bst. c). Der veraltete Begriff der Datensicherung wird hier entsprechend dem Artikel 10 VE-revKDSG durch «Datensicherheit» ersetzt.

7.3 Pflichten der verantwortlichen Behörde und von beauftragten Dritten

Artikel 18 – Risikoanalyse bei geplanten, wiederkehrende Bearbeitungen

Absatz 1

Das europäische Recht verlangt in Artikel 12 SEV 108+ zur Änderung des Artikels 10 Ziffer 2 SEV Nr. 108 und in Artikel 27 Richtlinie (EU) 2016/680 eine Datenschutzfolgenabschätzung von der verantwortlichen Behörde und bei der Bearbeitung im Auftrag von den beauftragten Dritten. Im Kern handelt es sich um die datenschutzrechtliche Selbstbeurteilung von geplanten, systematischen Bearbeitungen von Personendaten durch die verantwortliche Behörde, die aus Sicht des Datenschutzes etwas heikler erscheinen. Die Beurteilung erfolgt nicht für jede einzelne Personendatenbearbeitung, weshalb das kantonale Datenschutzgesetz in Abweichung vom Bund nicht von «Bearbeitung» und «Bearbeitungsvorgängen» spricht, sondern von «geplanten, systematischen Bearbeitungen». Der Zusatz «geplant» verdeutlicht, dass die Risikoanalyse vor der Inbetriebnahme erfolgt.

[53] vgl. Art. 32 GERES-Verordnung (gegenüber Behörden mit eigener Rechtspersönlichkeit).

Auf Bundesebene findet sich eine entsprechende Bestimmung in Artikel 22 revDSG. Eine Risikoabschätzung, ob voraussichtlich ein hohes Risiko für die Grundrechte der betroffenen Personen besteht, muss in jedem Fall durchgeführt werden, was einen gewissen Aufwand bedeutet. An die Risikobeurteilung werden jedoch keine hohen Anforderungen gestellt. Eine Aktennotiz im Projekt reicht, sofern für Personendatenbearbeitungen in diesem Projekt keine besonderen Risiken bestehen und folglich keine besonderen Massnahmen getroffen werden müssen. Im bisherigen Recht ist eine solche Risikoanalyse nicht explizit verankert. Gedanklich war sie aber bereits im Rahmen der Vorabkontrolle vorzunehmen.

Beim Einsatz von ICT durch die Kantonsverwaltung musste bisher in der Phase «Voranalyse» mit einer Informations- und Datenschutzsicherheitsanalyse (ISDS-Analyse) geprüft werden, ob erhöhte ISDS-Anforderungen bestehen (Art. 5 Abs. 1 bis 4 der Direktionsverordnung vom 3. Januar 2011 über die Informationssicherheit und Datenschutz, ISDS DV)[54]. Sofern sich bei der ISDS-Analyse erhöhte Anforderungen ergeben, ist in der Phase «Konzept» ein ISDS-Konzept zu erstellen, welches die zusätzlichen organisatorischen und technischen Massnahmen festhält, die umzusetzen sind (Art. 5 Abs. 5 ISDS DV). Insofern wird auf Gesetzesstufe nun festgehalten, was für Informatikprojekte der Kantonsverwaltung ohnehin galt. Die Bestimmung verlangt deshalb weder grundsätzlich Neues noch werden übermässige Anforderungen gestellt. Vielmehr ist davon auszugehen, dass sämtliche Behörden diese Anforderungen ohne erheblichen Mehraufwand erfüllen können.

Absatz 2

Absatz 2 definiert, wann ein hohes Risiko besteht und folglich eine Datenschutzfolgenabschätzung durchzuführen ist. Die Aufzählung ist im Gegensatz zum Bund abschliessend.

Nach europäischem Recht ergibt sich ein erhöhtes Risiko insbesondere bei der Verwendung neuer Technologien, aufgrund der Art, des Umfangs der Umstände und dem Zweck der Personendatenbearbeitung. So auch Artikel 22 Absatz 2 revDSG.

Das bundesrechtliche Datenschutzgesetz präzisiert weiter, dass namentlich bei der umfangreichen Bearbeitung von besonders schützenswerten Personendaten und bei systematisch umfangreicher Überwachung im öffentlichen Bereich ein erhöhtes Risiko besteht (Art. 22 Abs. 2 Bst. a und b revDSG). Diese Elemente sind ins kantonale Recht zu übernehmen (Bst. a und b).

Ein erhöhtes Risiko besteht ebenfalls, wenn besondere gesetzliche Geheimhaltungspflichten betroffen sind (Bst. c). Diese Voraussetzung ist aus dem bisherigen Recht zur Vorabkontrolle zu übernehmen und wird gegenüber dem Bundesrecht ergänzt. Damit sind – wie unter dem bisherigen Recht – besondere gesetzliche Geheimhaltungspflichten gemeint, beispielsweise solche nach der Sozialversicherungsgesetzgebung. Nicht darunter fallen freiwillig vereinbarte vertragliche Pflichten, was mit dem Zusatz «gesetzlich» klargestellt ist.

Die in Buchstabe d erwähnten technischen Mittel sind auf Verordnungsstufe näher zu definieren. Darunter fallen beispielsweise auf Datenträgern gespeicherte Personendaten, die eine betroffene Person auf sich trägt.

Gegenüber dem bisherigen Recht (der Vorabkontrolle) fehlt für die Risikoabschätzung der Tatbestand zur zweifelhaften Rechtsgrundlage (Art. 17a Abs. 1 Bst. a KDSG). Da die verantwortlichen Behörden Personendaten nur bearbeiten dürfen, wenn eine genügende Rechtsgrundlage besteht, ist unklar, was Sinn und Zweck der Bestimmung ist. Diesbezüglich fehlen auch Ausführungen im Vortrag zur Einführung der Bestimmung. Der Tatbestand ist deshalb mangels Anwendungsfälle nicht ins neue Recht zu überführen und setzt insofern die Motion Vogt um.

Absatz 3

Stellt die verantwortliche Behörde mittels Selbstkontrolle fest, dass bei einem Vorhaben ein hohes Risiko besteht, so nimmt sie formell eine Datenschutzfolgenabschätzung vor. Auf Stufe Kanton bisher bekannt als ISDS-Konzept.

[54] BSG 152.040.2

Artikel 19 – Datenschutzfolgenabschätzung

Entsprechend den europäischen Vorgaben und der Regulierung des Bundes muss die Datenschutzfolgenabschätzung mindestens eine Beschreibung der geplanten Bearbeitung (Bst. a), eine Bewertung der Risiken für die Grundrechte auf Datenschutz der betroffenen Personen (Bst. b) sowie die Massnahmen zu deren Schutz (Bst. c) enthalten.

Mit den aufgezeigten, getroffenen oder noch zu treffenden Massnahmen sollen die negativen Auswirkungen einer Personendatenbearbeitung verhindert oder zumindest eingeschränkt werden. Darunter fallen beispielsweise die Beschränkung des Zugangs zu den Daten oder die Gewährleistung der Datensicherheit.

Artikel 20 – Vorabkontrolle

Absatz 1

Ergibt die Risikoanalyse, dass die geplante Datenbearbeitung ein hohes Risiko für die Grundrechte der betroffenen Personen birgt, so unterbreitet die verantwortliche Behörde die Datenbearbeitung vor deren Beginn der Datenschutzbehörde zur Stellungnahme. Die Bestimmung orientiert sich an der Vorabkontrolle wie sie im Entwurf zum revDSG aufgeführt war. Denn aus Sicht des Kantons ist jede Bearbeitung von Personendaten der Datenschutzbehörde zur Vorabkontrolle zu unterbreiten, wenn gemäss der Risikoanalyse ein erhöhtes Risiko für die Grundrechte der betroffenen Personen besteht und nicht nur, wenn trotz den von der verantwortlichen Behörde ergriffenen Massnahmen ein erhöhtes Risiko besteht. In diesem Punkt weicht das kantonale Datenschutzgesetz von der Regelung in Artikel 23 revDSG ab.

Die Risikoeinschätzung zur Datenschutzfolgenabschätzung orientiert sich am bisherigen Recht, wann eine Vorabkontrolle durchgeführt werden muss. Insofern sollten sich die Tatbestände, wann eine Vorabkontrolle durchzuführen ist, mit dem revidierten Recht nicht ändern. Im kantonalen Recht soll ausserdem das quantitative Element («Umfang», «umfangreich» gemäss Art. 22 Abs. 2 revDSG) hervorgehoben werden. Demnach soll eine Vorabkontrolle nur durchgeführt werden müssen, wenn eine grössere Anzahl von Personendaten bearbeitet werden. Keine Vorabkontrollpflicht besteht jedenfalls nach der bisherigen Praxis, wenn i.d.R. Personendaten von weniger als 1000 Personen bearbeitet werden. Das Ausführungsrecht wird dies konkretisierend festhalten.

Die Vorabkontrolle erlaubt es der Datenschutzbehörde präventiv und beratend tätig zu sein. Dies ist nicht zuletzt auch für die verantwortliche Behörde effizienter, da mögliche datenschutzrechtliche Problemfelder bereits in einem frühen Stadium der Datenbearbeitung erkannt werden und behoben werden können.

Absatz 2

Wie nach bisherigem Recht, unterliegen auch wesentliche Änderungen der Vorabkontrolle. Ab wann, eine Änderung wesentlich ist, definiert das Verordnungsrecht.

Absatz 3

Artikel 23 Absatz 2 revDSG enthält eine zweimonatige Frist, innert welcher die Datenschutzbehörde Einwände gegen die geplante Bearbeitung mitteilen kann. Aus Sicht des Kantons Bern ist eine Frist nur beschränkt tauglich, da kleine Vorabkonsultationen viel rascher erledigt werden können und bei grösseren Projekten in der Regel in verschiedenen Projektphasen Vorabkontrollen stattfinden. Im Gesetz wird deshalb – wie vom KdK-Leitfaden vorgeschlagen – keine fixe Frist festgelegt. Da sich eine Vorabkonsultation aber nicht auf unbestimmte Zeit hinziehen sollte, ist die Datenschutzbehörde verpflichtet, diese innert «angemessener Frist» durchzuführen.

Artikel 21 – Datensammlungen

Artikel 24 der Richtlinie (EU) 2016/680 verpflichtet die verantwortliche Behörde und von ihr beauftragte Dritte, ein Verzeichnis über die Datenbearbeitungstätigkeiten zu führen. Die Richtlinie gilt jedoch nur im Anwendungsbereich der Strafprävention, Strafverfolgung und Strafvollstreckung. Dementsprechend

könnte eine solche Pflicht auch nur bereichsspezifisch umgesetzt werden. Der Bund behält das Verzeichnis der Datensammlungen (neu: Bearbeitungstätigkeiten) bei und verpflichtet sämtliche verantwortlichen Behörden ihr Verzeichnis der Datenschutzbehörde zu melden, die ein Register über alle Verzeichnisse führt (Art. 12 und 56 revDSG).

Das Register der Datensammlungen will Transparenz schaffen: Einerseits soll die betroffene Person sich über vorhandene Datensammlungen informieren können, um ihre Rechte geltend zu machen, andererseits soll es die Arbeit der Datenschutzbehörde erleichtern. Deshalb soll das bisherige Register der Datensammlungen in abgeänderter Form auch im kantonalen Recht beibehalten werden. Mit Blick auf den bisherigen Aufwand soll das Register zukünftig aber auf Datensammlungen beschränkt werden, die besonders schützenswerte Personendaten enthalten. Dies gilt jedoch nicht im Anwendungsbereich der Richtlinie (EU) 2016/680, da hier eine Verzeichnispflicht besteht (vgl. Erläuterungen zur Verzeichnispflicht nach Art. 22 VE-revKDSG). Dazu kommt, dass die Informationspflicht nach Artikel 23 VE-revKDSG mit Verweis auf die veröffentlichten Datensammlungen erfüllt werden kann.

Absatz 1

Die kantonale Datenschutzbehörde führt und veröffentlicht ein Register der kantonalen Datensammlungen (Art. 42 Abs. 2 VE-revKDSG), die besonders schützenswerte Personendaten enthalten. Damit sie das Register führen kann, müssen die kantonalen Behörden ihre Datensammlungen melden. Die Pflicht wird in Absatz 1 statuiert. Mit der Meldepflicht einher geht auch die Pflicht, Mutationen zu melden. Zukünftig sollen nur noch Datensammlungen erhoben werden, die besonders schützenswerte Personendaten enthalten. In der Regel sind insbesondere solche Datensammlungen für die betroffenen Personen von Interesse.

Die kantonale Datenschutzbehörde wird eine Eingabemaske gestalten, in welche die kantonalen Behörden ihre Datensammlungen eingeben können. Nachdem die kantonale Datenschutzbehörde die Angaben geprüft hat, wird sie diesen Teil des Registers veröffentlichen. Das Register soll einer betroffenen Person ermöglichen, sich darüber zu informieren, wo über sie allenfalls besonders schützenswerte Personendaten bearbeitet werden. Die Informationsmöglichkeit stellt den Ausgangspunkt dar, dass eine betroffene Person ihre Rechte geltend machen kann, die ihr nach der Datenschutzgesetzgebung zustehen.

Absatz 2

Die gemeinderechtlichen und landeskirchlichen Behörden müssen ihre Register selber führen, jedoch legt die kantonale Datenschutzbehörde Standards fest, wie sie diese Pflicht zu erfüllen haben.

Absatz 3

Den Registerinhalt sowie die Ausnahmen von der Meldepflicht und Pflicht zur Eintragung ins Register regelt der Regierungsrat durch Verordnung. Der Inhalt des Registers soll den heutigen Anforderungen entsprechen. Zu nennen sind etwa die Rechtsgrundlage, die verantwortliche Behörde, der Zweck, Art und Umfang der bearbeiteten Personendaten sowie die Kategorien von Empfängern und die Aufbewahrungsdauer. Der Zweck des Bearbeitens kann beispielsweise lauten «Prüfen des Anspruchs auf Prämienverbilligung» oder «Durchführen eines Profilings». Die Kategorien bearbeiteter Personendaten bezeichnet die Art der bearbeiteten Daten, z. B. besonders schützenswerte Personendaten. Aufgeführt werden müssen ebenfalls die Kategorien von Empfängern, denen gegebenenfalls die Personendaten bekanntgegeben werden. Auch hier sind wiederum typisierte Gruppen mit gemeinsamen Merkmalen gemeint, wie z. B. «Aufsichtsbehörden».

Dem bisherigen Recht entsprechend, sollen kurzfristig geführte und bereits anderweitig veröffentlichte Datensammlungen von der Registerführungspflicht ausgenommen werden. Erstere liegen vor, wenn sie auf höchstens 2 Jahre angelegt sind. Letztere sind Datensammlungen, die beispielsweise im Staats- oder Gemeindearchiv archiviert worden sind oder in Form von Jahresbüchern der Öffentlichkeit zugänglich gemacht werden.

Artikel 22 – Verzeichnispflicht für Strafbehörden

Artikel 24 der Richtlinie (EU) 2016/680 verlangt, dass Behörden, die im Bereich der Strafverfolgung und Strafvollstreckung tätig sind, sowie deren beauftragte Dritte ein Verzeichnis über alle Kategorien ihrer Datenbearbeitungstätigkeiten führen. Die Strafverfolgungsbehörden und die Gerichte mit Befugnissen in Strafverfahren sind in Artikel 22 und Artikel 23 EG ZSJ aufgeführt. Als Strafverfolgungsbehörden gelten die Kantonspolizei und die anderen Polizeiorgane des Kantons und der Gemeinden, soweit sie im Bereich der Strafverfolgung tätig sind, und andere Personen, denen in der besonderen Gesetzgebung hinsichtlich bestimmter Amtsverrichtungen polizeiliche Aufgaben übertragen sind, sowie die Staatsanwaltschaft. Gerichtsbehörden mit gerichtlichen Befugnissen in Strafverfahren sind das Obergericht, das kantonale Zwangsmassnahmengericht, das Wirtschaftsstrafgericht, das Jugendgericht, die Regionalgerichte und die regionalen Zwangsmassnahmengerichte. Das Verzeichnis knüpft an die Datenbearbeitungstätigkeiten an und umfasst Angaben zum Bearbeitungszweck, zu den Kategorien von Empfängern der Personendaten und den Kategorien der betroffenen Personen. Eine Kategorie einer Bearbeitungstätigkeit könnte beispielswiese «Videoüberwachung mit Aufzeichnung» sein. Die Inhalte und Ausnahmen des Verzeichnisses regelt der Regierungsrat in der Verordnung. Die Bestimmung ist mit Augenmass umzusetzen. Der Aufwand sollte sich dabei in Grenzen halten, da die Daten mit dem heutigen Register für Datensammlungen bereits erfasst sein sollten.

Die Erstellung eines solchen Verzeichnisses kann als Massnahme der Selbstregulierung im Datenschutz angesehen werden. Es dient den verantwortlichen Behörden, sich selbst einen Gesamtüberblick über die von ihr bearbeiteten Personendaten zu verschaffen. Es soll jedoch auch der Datenschutzbehörde als Kontrollinstrument dienen.

Artikel 23 – Informationspflicht bei der Beschaffung von Personendaten

Die Regelung von Artikel 4 EV EDS (Grundsätze der Informationspflicht bei der Beschaffung von Personendaten) ist ins kantonale Datenschutzgesetz zu überführen.

Absatz 1 und 2

Die verantwortliche Behörde ist bei der Beschaffung von Personendaten verpflichtet, den betroffenen Personen gewisse Informationen zu erteilen, die mit der Datenbearbeitung zusammenhängen. Bisher sah das KDSG in Artikel 9 Absatz 4 lediglich eine Informationspflicht für den Fall der Datenbearbeitung im Rahmen von systematischen Befragungen vor. Anzugeben waren der Zweck der Bearbeitung und die gesetzliche Grundlage. Artikel 13 Richtlinie (EU) 2016/680 enthält in Absatz 1 und 2 eine detaillierte Aufzählung der zu erteilenden Informationen sowie in Absatz 3 und 4 Ausnahmen, wann auf die Informationen verzichtet werden kann. Die Beschränkung auf systematische Befragungen in Artikel 9 Absatz 4 KDSG ist unter diesen Umständen zu eng und der Katalog der mitzuteilenden Informationen unvollständig. Im kantonalen Datenschutzrecht ist deshalb in Anlehnung an das europäische Recht und den Leitfaden KdK Folgendes zu regeln:

- Die Feststellung, dass die Informationspflicht für sämtliche Arten von Personendatenbearbeitungen gilt,
- eine Erweiterung der Liste der zu erteilenden Informationen,
- die Art und Weise, wie die Informationspflicht erfüllt werden kann und
- die Ausnahmen von der Informationspflicht.

Zu beachten ist, dass die Behörde die Informationen neu stets unaufgefordert zur Verfügung stellen muss und nicht wie nach bisherigem Recht nur auf Verlangen der betroffenen Person. Die betroffene Person soll also die Informationen erhalten, ohne dass sie zuerst danach fragen muss. Ziel ist es, dass die betroffene Person sämtliche Informationen erhält, die sie braucht, um ihre Rechte geltend zu machen. Absatz 2 enthält die Mindestinformationen, was durch den Zusatz «mindestens» ausgedrückt wird. Nur ausnahmsweise werden darüber hinausgehende Angaben notwendig, beispielsweise bei einem erhöhten Risiko für eine missbräuchliche Datenbearbeitung.

Die Informationspflicht gilt nur insoweit, als die verantwortliche Behörde Personendaten «beschafft». Gelangt sie ungewollt oder durch Zufall an Personendaten, muss sie nicht informieren. Für spätere Änderung wie beispielsweise andere Speicherorte besteht keine Informationspflicht, ausser die Personendaten werden einem zusätzlichen Zweck zugeführt; erst dann handelt es sich um eine erneute Datenbeschaffung.

Absatz 3

Absatz 3 regelt, auf welche Weise die Informationspflicht erfüllt werden kann. Vorgesehen sind drei Möglichkeiten:

- durch Information im Register der Datensammlungen,
- auf der Internetseite der verantwortlichen Behörde oder
- durch direkte Mitteilung an die betroffene Person.

Welches Mittel der Information zu wählen ist, bemisst sich nach der Art der Datenbeschaffung. Werden Daten bei der betroffenen Person selbst beschafft, kann das Register der Datensammlungen oder eine Internetseite genügen. In jedem Fall muss die verantwortliche Behörde aber sicherstellen, dass die betroffene Person die Information tatsächlich zur Kenntnis nehmen kann. Sicherzustellen ist damit die Möglichkeit, sich in einfach zugänglicher Weise zu informieren, nicht aber, dass sich die betroffene Person im konkreten Fall wirklich informiert. Bei der Datenbeschaffung bei Dritten kann sich aufdrängen, die betroffene Person direkt zu informieren.

Die Ausnahmen von der Informationspflicht sind im nachfolgenden Artikel geregelt.

Artikel 24 – Ausnahmen von der Informationspflicht

Absatz 1

In Übereinstimmung mit dem europäischen Recht kann auf die Information verzichtet werden, wenn

- die betroffene Person bereits über die Informationen verfügt (Bst. a) oder
- die Beschaffung der Personendaten gesetzlich vorgesehen ist (Bst. b).

Die Beschaffung von Personendaten ist gesetzlich vorgesehen, wenn die betroffene Person aus den gesetzlichen Grundlagen mit hinreichender Präzision herauslesen kann, welche Daten zu welchem Zweck bearbeitet werden. Folglich entfällt die Informationspflicht in den meisten Fällen. Durch den Gesetzesvorbehalt wird beispielsweise sichergestellt, dass etwa die Kantonspolizei die Möglichkeit hat, Auskünfte an die betroffenen Personen für die Datenbearbeitung der Zwangsmassnahmen nach Polizeigesetz zu verweigern bzw. nicht mitzuteilen, wenn dies die polizeilichen Vorermittlungen (Observation, verdeckte Vorermittlung oder verdeckte Fahndung) gefährden könnte.

Nicht übernommen wird auf den nach europäischem Recht möglichen Ausnahmetatbestand, wonach auf die Information verzichtet werden kann, wenn sie nicht oder nur mit unverhältnismässigem Aufwand möglich ist. Die Behörde kann die Informationen auch im Internet veröffentlichen. Daher ist kein Fall denkbar, in dem der Informationsaufwand unverhältnismässig wäre.

Absatz 2

Eine Einschränkung der Informationspflicht ist ausserdem unter den gleichen Voraussetzungen möglich, wie das Auskunftsrecht eingeschränkt werden kann, d.h. wegen besonderer gesetzlicher Geheimhaltungspflichten sowie überwiegenden öffentlichen oder privaten Interessen.

In Artikel 20 revDSG werden einzelne öffentlichen Interessen wie beispielsweise die öffentliche Sicherheit explizit genannt. In Übereinstimmung mit dem KdK-Leitfaden (Ziff. 5.6) verzichtet das KDSG auf die Nennung.

Artikel 25 – Meldung von Verletzungen der Datensicherheit an die Datenschutzbehörde

Absatz 1

Nach europäischem Recht muss die verantwortliche Behörde der Datenschutzbehörde melden, wenn die Datensicherheit verletzt worden ist (Art. 9 SEV 108+ zur Änderung von Art. 7 Abs. 2 SEV Nr. 108 und Art. 30 Abs. 1 Richtlinie (EU) 2016/680). Zum Begriff der Verletzung der Datensicherheit vgl. Artikel 2 Buchstabe h VE-revKDSG. Die Meldung hat unverzüglich, jedoch spätestens innerhalb von 72 Stunden seit Bekanntwerden des Datenschutzvorfalles zu erfolgen. Im Gegensatz zum revidierten Datenschutzgesetz des Bundes wird die 72-Stunden-Regel aus der Richtlinie übernommen. Die verantwortliche Behörde kann so vor einer allfälligen Meldung den Sachverhalt abklären und entscheiden, ob überhaupt eine Meldung erfolgen muss. Die Zeit, bis beauftragte Dritte die Datensicherheitsverletzung der verantwortlichen Behörde melden, muss sie sich nicht anrechnen lassen.

Das verabschiedete Datenschutzgesetz des Bundes sieht eine Meldepflicht nur vor, wenn voraussichtlich ein hohes Risiko für die Grundrechte der betroffenen Personen besteht. Nach dem kantonalen Datenschutzgesetz soll hingegen ein voraussichtliches Risiko genügen, da die Meldepflicht die Regel und nicht die Ausnahme sein soll. Ziel ist es, dass die Datenschutzbehörde die verantwortliche Behörde möglichst frühzeitig und umfassend bei der Gewährleistung der Datensicherheit unterstützen kann. Zudem erlaubt Artikel 30 Absatz 1 Richtlinie (EU) 2016/680 eine Ausnahme nur dann, wenn voraussichtlich kein Risiko besteht.

Absatz 2

Der Inhalt der Meldepflicht deckt sich mit demjenigen nach Artikel 24 Absatz 2 revDSG. Demnach enthält die Meldung eine Beschreibung der Verletzung und deren Auswirkungen sowie die ergriffenen und vorgesehenen Massnahmen. Die Meldung ist fortlaufend an den Wissensstand der Behörde anzupassen.

Absatz 3

Liegt eine Auftragsbearbeitung vor, ist die verantwortliche Behörde von den beauftragten Dritten über die Verletzung zu orientieren.

Artikel 26 – Meldung von Verletzungen der Datensicherheit an die betroffene Person

Absatz 1

Von der Meldepflicht an die Datenschutzbehörde ist die Meldung an die betroffene Person zu unterscheiden: Grundsätzlich muss die betroffene Person nicht benachrichtigt werden. Eine Benachrichtigung ist nur notwendig, wenn es die Umstände erfordern oder die Datenschutzbehörde es verlangt. Dabei besteht ein gewisser Ermessensspielraum.

Absatz 2

Bedeutsam für die Meldepflicht ist, ob durch die Benachrichtigung die Risiken einer missbräuchlichen Datenbearbeitung reduziert werden können. Dies ist insbesondere der Fall, wenn die betroffene Person entsprechende Vorkehren zu ihrem Schutz treffen kann, zum Beispiel indem sie ihre Zugangsdaten oder Passwörter ändert.

Artikel 27 – Ausnahmen von der Meldepflicht an die betroffene Person

Absatz 1

Es kann vorkommen, dass trotz eingetretener Verletzung der Datensicherheit im konkreten Fall die betroffene Person nicht geschädigt wird (Bst. a). Dies wäre etwa dann der Fall, wenn in Verletzung des Datenschutzes veröffentlichte Daten aufgrund von Sicherheitsvorkehrungen verschlüsselt sind.

Allenfalls können auch nachträgliche Massnahmen sicherstellen, dass für die Grundrechte der betroffenen Person aller Wahrscheinlichkeit nach kein hohes Risiko mehr besteht (Bst. b). Beispielsweise wenn die Person, die unbefugt Zugang zu den Daten erhalten hat, identifiziert werden kann und danach in einer schriftlichen Vereinbarung versichert, dass sie die Daten nicht weitergegeben und gelöscht hat.

Das Unterlassen der Meldung ist ebenfalls zulässig, wenn die Information unmöglich ist oder einen unverhältnismässigen Aufwand erfordert (Bst. c). Eine Information ist unmöglich, wenn die verantwortliche

Behörde gar nicht weiss, welche Personen von der Verletzung der Datensicherheit betroffen sind, weil beispielsweise die Logfiles, aus denen dies ersichtlich wäre, nicht mehr vorhanden sind. Ein unverhältnismässiger Aufwand würde vorliegen, wenn bei einer grossen Anzahl betroffener Personen diese einzeln informiert werden müssten und die dadurch verursachten Kosten im Verhältnis zum Informationsgewinn für die betroffenen Personen unverhältnismässig erscheinen. Insbesondere in solchen Konstellationen können die betroffenen Personen durch eine öffentliche Bekanntmachung informiert werden, sofern eine individuelle Information ihre Position nicht substantiell verbessert. Die öffentliche Bekanntmachung kann etwa auf der Internetseite der verantwortlichen Behörde erfolgen.

Absatz 2

Auf die Benachrichtigung ist zu verzichten, wenn besondere gesetzliche Geheimhaltungspflichten dies verlangen oder überwiegende öffentliche oder private Interessen der Benachrichtigung entgegenstehen (vgl. auch Art. 24 Abs. 5 Bst. a revDSG). Der Behörde obliegt hier jedoch kein Ermessen, weshalb die Bestimmung nicht als Kann-Vorschrift formuliert ist. Als milderes Mittel ist sie aufzuschieben oder einzuschränken.

7.4 Rechte der betroffenen Person

Artikel 28 – Auskunftsrecht

Absatz 1

Das Auskunftsrecht, ob und wenn ja, welche Daten über eine Person von einer verantwortlichen Behörde bearbeitet werden oder diese über sie bearbeiten lässt, ist einer der Kernpunkte des Datenschutzrechts und stellt den Ausgangspunkt für die weiteren Rechte und Ansprüche der betroffenen Person dar.

Das Auskunftsrecht ergänzt die Informationspflicht nach Artikel 23 bis 24 VE-revKDSG. Die betroffene Person kann auf Anfrage mehr erfahren, als die verantwortliche Behörde im Rahmen der Informationspflicht offenlegen muss.

Absatz 2

Das Auskunftsrecht ist ein subjektives höchstpersönliches Recht, das auch urteilsfähige handlungsunfähige Personen selbständig, ohne Zustimmung ihres gesetzlichen Vertreters, geltend machen können. Aus dem Charakter des höchstpersönlichen Rechts ergibt sich auch, dass niemand im Voraus auf das Auskunftsrecht verzichten kann.

Absatz 3

Die verantwortliche Behörde erteilt die Auskunft, selbst wenn die Bearbeitung im Auftrag erfolgt.

Artikel 29 – Inhalt und Modalität der Auskunft

Absatz 1

Die betroffene Person erhält diejenigen Informationen, die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann und damit eine transparente Datenbearbeitung gewährleistet ist.

Die Informationen sind dieselben wie diejenigen, über welche die verantwortliche Behörde bei der Beschaffung orientieren muss (Buchstabe a), zuzüglich die Angaben über die Aufbewahrungsdauer (Buchstabe b) und die Herkunft der Personendaten (Buchstabe c). Die zusätzlichen Angaben ergeben sich gestützt auf Artikel 11 SEV Nr. 108+ zur Änderung von Artikel 9 Absatz 1 Buchstabe b SEV Nr. 108 und auf Artikel 14 Absatz 1 Buchstabe d und g Richtlinie (EU) 2016/680.

Die Liste ist nicht abschliessend. Die Generalklausel im Einleitungssatz erlaubt der betroffenen Person gegebenenfalls weitere Informationen zu verlangen, wenn diese für die Geltendmachung ihrer Rechte erforderlich sind und eine transparente Datenbearbeitung nur so gewährleistet werden kann. Wenn die

verantwortliche Behörde grosse Datenmengen über die betroffene Person bearbeitet, kann sie gegebenenfalls verlangen, dass die betroffene Person präzisiert, auf welche Informationen oder welche Bearbeitungsvorgänge sich ihr Auskunftsgesuch bezieht.

Absatz 2

Der Regierungsrat regelt die Modalitäten des Auskunftsrechts auf Verordnungsstufe. Zu regeln ist beispielsweise, dass die Auskunft grundsätzlich schriftlich erteilt wird. Das bisherige Recht unterscheidet zwischen Auskunft und Einsicht, wobei das Einsichtsrecht eine Form des Auskunftsrechts darstellt. In Ausnahmefällen kann die Auskunft folglich durch Einsicht in die Personendaten an Ort und Stelle erteilt werden. Weiter zu regeln ist beispielsweise die Frist, innert derer die Auskunft zu erteilen ist.

Artikel 30 – Einschränkungen des Auskunftsrechts

Buchstabe a und b

Dieser Artikel regelt die Einschränkungen des Auskunftsrechts. Unter bisherigem Recht kann die Auskunft nur verweigert, eingeschränkt oder aufgeschoben werden, wenn ein Gesetz (gemeint sind besondere Geheimhaltungsvorschriften) es verlangt oder besonders schützenswerte Interessen Dritter dies erfordern. Nicht erwähnt sind – anders als bei der Einschränkung für die Einsichtnahme – wichtige und überwiegende öffentliche Interessen. Der Vortrag von 1985 verwies jedoch auf ebensolche öffentliche Interessen. In Angleichung an Artikel 26 revDSG verweigert die verantwortliche Behörde die Auskunft, schränkt sie ein oder schiebt sie auf, wenn überwiegender öffentlicher oder privaten Interessen entgegenstehen. In diesen Fällen ist die verantwortliche Behörde verpflichtet, die Auskunft einzuschränken.

Typische öffentliche Interessen sind die innere und äussere Sicherheit oder wenn die Auskunft Ermittlungen, Untersuchungen oder ein behördliches oder gerichtliches Verfahren gefährden könnte (vgl. auch Art. 26 Abs. 2 Bst. b revDSG).

Angaben über eine bestimmte Person können unter Umständen mit Angaben über eine andere Person verknüpft sein, beispielsweise, wenn Dritte über eine bestimmte Person Aussagen treffen. In solchen Fällen ist eine Interessensabwägung im Einzelfall vorzunehmen.

Buchstabe c

Neu ist ausserdem Buchstabe c. Die verantwortliche Behörde verweigert demnach die Auskunft, schränkt sie ein oder schiebt sie auf, wenn das Auskunftsgesuch offensichtlich unbegründet oder querulatorisch ist. Die Ausnahme ist eng auszulegen. Dies gilt in zweifacher Hinsicht: Einerseits darf die verantwortliche Behörde nicht leichthin annehmen, ein Auskunftsgesuch sei offensichtlich unbegründet oder querulatorisch. Andererseits hat sie selbst für den Fall, dass ein solches Gesuch vorliegt, die für die betroffene Person günstigste Lösung zu wählen. Sie muss daher, soweit als möglich, die Auskunft lediglich einschränken, darf sie allenfalls aufschieben und kann sie nur in den absolut eindeutigen, offensichtlichen Fällen verweigern.

Das Auskunftsrecht kann ohne Nachweis eines Partikularinteressens geltend gemacht werden. Daraus folgt, dass die verantwortliche Behörde grundsätzlich keine Begründung des Auskunftsbegehrens fordern darf. Das Bundesgericht hat jedoch entschieden, dass eine rechtsmissbräuchliche Geltendmachung des Auskunftsrechts in Betracht kommt, wenn es datenschutzwidrige Zwecke verfolgt, etwa wenn das Auskunftsbegehren einzig zum Zweck gestellt wird, die (spätere) Gegenpartei auszuforschen und Beweise zu beschaffen, an die eine Partei sonst nicht gelangen könnte.[55] Nur wenn bereits ohne vertiefte Prüfung feststeht, dass ein Auskunftsbegehren offensichtlich unbegründet ist, kann das Auskunftsrecht eingeschränkt werden.

[55] BGE 138 III 425 E. 5.5.

Querulatorisch sind Auskunftsgesuche, die beispielsweise ohne plausible Begründung häufig wiederholt werden, oder die sich an eine verantwortliche Behörde richten, von der die gesuchstellende Person bereits weiss, dass sie keine Daten über sie bearbeitet. Auch von einem querulatorischen Gesuch darf die verantwortliche Behörde nicht leichthin ausgehen.

Artikel 31 – Rechte bei widerrechtlicher Bearbeitung

Absatz 1

Im Gegensatz zum Bund listet das kantonale Datenschutzrecht die drei traditionellen Verteidigungsrechte (Unterlassungsanspruch, Beseitigungsanspruch und Feststellungsanspruch) nicht auf, sondern nennt exemplarisch das Recht der betroffenen Person, unrichtige Personendaten zu berichtigen, widerrechtlich bearbeitete Personendaten zu vernichten oder auf andere Weise die Folgen der Widerrechtlichkeit zu beseitigen. Das Bearbeiten von unrichtigen Personendaten ist ebenfalls widerrechtlich, da die Richtigkeit der Personendaten ein Grundsatz des Datenschutzrechts darstellt (Art. 8 VE-revKDSG). Eine widerrechtliche Bearbeitung liegt zudem vor, wenn beispielsweise für die Bearbeitung eine rechtliche Grundlage fehlt, die Bearbeitung unverhältnismässig ist oder sie zu einem Zweck erfolgt, der mit dem ursprünglichen Bearbeitungszweck unvereinbar ist. Die Folgen der Widerrechtlichkeit können unter anderem auch beseitigt werden durch Mitteilung an die Empfängerinnen oder den Empfänger der Personendaten, durch Veröffentlichung der Berichtigung oder mittels Schadenersatz und Genugtuung. Im Übrigen kann die betroffene Person die Bekanntgabe ihrer Personendaten sperren lassen, auch ohne dass deren Bearbeitung widerrechtlich sein muss (vgl. Art. 33 VE-revKDSG).

Die Rechte können von der betroffenen Person geltend gemacht werden. Dafür verzichtet das kantonale Datenschutzgesetz darauf, dass ein schutzwürdiges Interesse nachgewiesen werden muss. Es weicht somit von der Regelung in Artikel 41 Absatz 1 revDSG ab. Schliesslich ist das schutzwürdige Interesse Ausfluss des Grundrechts auf Datenschutz und dürfte bei einer widerrechtlichen Bearbeitung immer gegeben sein.

Absatz 2

Die verantwortliche Behörde trägt die Beweislast für die Richtigkeit der Daten, nicht die betroffene Person diejenige für deren Unrichtigkeit. Die Beweislastregel folgt dem Grundsatz, wonach Personendaten richtig sein müssen (Art. 8 VE-revKDSG).

Absatz 3

Dieser Absatz wurde an die Terminologie des Bundes angepasst (Art. 41 Abs. 4 revDSG): Die Gegendarstellung heisst neu Bestreitungsvermerk. Demnach kann bei Personendaten ein entsprechender Vermerk angebracht werden, wenn weder die Richtigkeit noch die Unrichtigkeit der Daten endgültig festgestellt werden kann. Die Bearbeitung ist danach insofern eingeschränkt, als die Personendaten nur noch zusammen mit dem Bestreitungsvermerk weitergegeben werden können.

Artikel 32 – Recht auf Bekanntgabe des Entscheids

Die Verteidigungsrechte enthalten wie nach geltendem Recht das Recht auf Bekanntgabe des Entscheids an von der betroffenen Person bezeichnete Behörden und Dritte, sofern dafür ein schützenswertes Interesse besteht.

Artikel 33 – Recht auf Sperrung der Bekanntgabe an Private

Die von behördlicher Datenbearbeitung betroffene Person kann von der verantwortlichen Behörde verlangen, dass sie die Bekanntgabe von bestimmten Personendaten an Private sperrt, wenn sie ein schutzwürdiges Interesse nachweist. Zu denken ist etwa an politische Flüchtlinge, die sich durch ausländische Verfolger bedroht fühlen. Die Sperre ist jedoch nicht zu gestatten, wenn die verantwortliche Behörde nach einer spezialgesetzlichen Regelung zur Bekanntgabe verpflichtet ist oder wenn die Sperrung rechtsmissbräuchlich ist, beispielsweise um sich einer Betreibung zu entziehen.

7.5 Datenschutzbehörden

Artikel 34 – Stellung

Absatz 1

Die kantonale Datenschutzbehörde ist wie die Finanzkontrolle fachlich unabhängig, nicht weisungsgebunden und nur der Verfassung und dem Gesetz verpflichtet. Dennoch hat sie nicht wie die Gerichte eine Stellung ausserhalb der Verwaltung. Ihre Unabhängigkeit darf nicht dazu führen, dass sie ihrerseits zu einer unkontrollierten «vierten Gewalt» oder gar zu einem «Staat im Staat» wird.[56] Sie ist damit eine der Verwaltung zugehörige, administrativ angelgliederte Verwaltungseinheit. Wenn die kantonale Datenschutzbehörde eine von der Verwaltung unabhängige Behörde sein soll, die aber nicht eine eigene vierte Gewalt im Staat bildet, muss sie einer der drei Gewalten «Legislative», «Judikative» und «Exekutive» zugeordnet werden, wobei sinnvollerweise nur Letztere in Frage kommt, also die Verwaltung (Exekutive). Am treffendsten ist die kantonale Datenschutzbehörde deshalb wie die Finanzkontrolle als eine selbständige Organisationseinheit der kantonalen Verwaltung zu bezeichnen. Sie soll im Organisationsgesetz wie die Finanzkontrolle nun explizit erwähnt werden (vgl. Erläuterungen zu Ziff. 7.9.4).

Absatz 2

Die heutige Stellung der Datenschutzbehörde bleibt unverändert. Mit dem neu geschaffenen Artikel soll jedoch deren Unabhängigkeit hervorgehoben werden. Zu übernehmen ist der bisher in Artikel 33a Absatz 1 KDSG festgehaltene Grundsatz der Unabhängigkeit. Die Bestimmung wird zudem redaktionell an Artikel 2 Absatz 2 des Gesetzes vom 17. März 2022 über die Finanzkontrolle (kantonales Finanzkontrollgesetz, KFKG)[57] angeglichen. Die selbständige Aufgabenerfüllung ergibt sich aus der Unabhängigkeit, weshalb sie nicht mehr explizit erwähnt werden soll. Die Datenschutzbehörde ist nicht nur bei ihrer Aufgabenerfüllung unabhängig, sondern auch bei organisatorischen und institutionellen Fragen.

Auch die Ergänzung, dass die Datenschutzbehörde weisungsungebunden ist, ist Ausdruck ihrer Unabhängigkeit. Weisungsungebunden ist, wer seine Tätigkeit frei gestalten kann. Das heisst, die Datenschutzbehörde kann ihren Arbeitsinhalt frei wählen. Sie arbeitet somit frei von fachlichen Weisungen oder Verhaltensanweisungen. Ihr können keine Weisungen zum Arbeitsgegenstand oder zur Erledigungsart erteilt werden. So legt sie auch ihr eigenes Prüfprogramm fest. Die Datenschutzbehörde ist allerdings wie alle staatlichen Stellen der Verfassung und dem Gesetz verpflichtet.

Absatz 3

Die Datenschutzbehörde ist bisher der Direktion für Inneres und Justiz administrativ zugeordnet. Die Zuordnung hat sich bewährt und bringt folgende Vorteile mit sich: Mit der Anbindung an eine Direktion wird der Kommunikationsfluss zur Regierung sichergestellt. Trotz ihrer unabhängigen Stellung können und sollen Anliegen der Datenschutzbehörde von der Direktionsvorsteherin oder dem Direktionsvorsteher in den Regierungsrat eingebracht werden. Zudem wird sie von der Stabstelle der Direktion beim Personalmanagement, insbesondere bei der Zeiterfassung, bei Änderungen von Anstellungsbedingungen oder bei der Rechnungsadministration unterstützt. Die Unabhängigkeit der Datenschutzbehörde in Bezug auf ihre Ressourcen und ihre Tätigkeit bleibt bestehen.

Geprüft und wieder verworfen wurde die administrative Anbindung an das Büro des Grossen Rates, weil die Datenschutzbehörde keine parlamentarische Tätigkeit ausübt. Sie pflegt denn auch keinen ständigen Kontakt zum Grossen Rat, sondern ist nur zur jährlichen Berichterstattung verpflichtet (Art. 48 VE-revKDSG). Sie gehört organisatorisch zur Verwaltung und nicht zur Legislative (vgl. Erläuterungen zu Abs. 1). Bei einer anderen Zuordnung würde sie zudem den niederschwelligen Informationsaustausch mit der Regierung verlieren.

Prinzipiell wäre die Anbindung an die Staatskanzlei möglich, womit die Verbindung zum Regierungsrat ebenfalls hergestellt werden könnte. Im Sinne einer pragmatischen Anpassung sieht der Entwurf aber die

[56] Vortrag des Regierungsrates zur Änderung des KDSG (2008): S. 14.
[57] BSG 622.1

bisherige administrative Zuordnung an die Direktion für Inneres und Justiz vor und trägt damit auch der Motion Vogt Rechnung. Eine Neuzuordnung wäre mit administrativem und finanziellem Aufwand verbunden und brächte keinen ersichtlichen Mehrwert.

Artikel 35 – Leitung kantonale Datenschutzbehörde

Absatz 1 und 2

Nach europäischen Vorgaben muss die oder der Beauftragte für Datenschutz über die zur Aufgabenerfüllung erforderliche Qualifikation, Fachkenntnis und Erfahrung im Bereich des Datenschutzes verfügen. Diese Anforderungen sind neu in Absatz 2 verankert. Die bisher statuierte Voraussetzung zu den Amtssprachen erfährt eine geringfügige redaktionelle Anpassung.

Absatz 3

Die oder der Beauftragte für Datenschutz wird auf eine Amtsdauer von vier Jahren gewählt (Art. 36 Abs. 1 VE-revKDSG). Sie oder er ist damit nicht Angestellte, sondern hauptamtliches Behördenmitglied. Der Verweis auf die Personalgesetzgebung dient der erleichterten Auffindbarkeit.

Artikel 36 – Wahl und Wiederwahl der oder des Beauftragten für Datenschutz

Absatz 1

Seit der Revision 2008 wählt der Grosse Rat auf Antrag des Regierungsrates die Beauftragte oder den Beauftragten für Datenschutz, und nicht mehr der Regierungsrat.

In den Kantonen ist das Wahlverfahren unterschiedlich ausgestaltet: Bis heute wählt in den meisten Kantonen die Exekutive die Beauftragte oder den Beauftragten für Datenschutz, teilweise unter dem Zustimmungsvorbehalt der Legislative. Eine Wahl durch die Legislative stärkt demgegenüber die Unabhängigkeit der oder des Beauftragten für Datenschutz, da die Wahl nicht mehr durch die Beaufsichtigten erfolgt. Die Beteiligung der Exekutive stellt dagegen sicher, dass die Fachkompetenz der Kandidatinnen und Kandidaten im Vordergrund steht und nicht die politische Zugehörigkeit. Mit der Beteiligung beider Gewalten sind die unterschiedlichen Interessen ausgewogen vertreten, weshalb am heutigen Berner System – Wahl durch den Grossen Rat auf Antrag des Regierungsrates – grundsätzlich festgehalten werden soll.

Im Gegensatz zum Staatsschreiber bzw. zur Staatsschreiberin oder dem Generalsekretär bzw. der Generalsekretärin des Grossen Rates handelt es sich bei der oder dem Beauftragten für Datenschutz nicht um ein politisches Amt, weshalb sich die Amtsdauer nicht zwingend an der Legislatur orientieren muss. So ist beispielsweise auch die Amtsdauer der Vorsteherin oder des Vorstehers der Finanzkontrolle nicht an die Legislatur geknüpft (Art. 3 KFKG). Anlässlich der Revision ist aus Praktikabilitätsgründen jedoch gewünscht worden, die Amtsdauer an die Legislatur anzubinden, was in den Übergangsbestimmungen umgesetzt worden ist (vgl. Erläuterungen zu Art. 58 VE-revKDSG).

Absatz 2

Bereits heute ist die Wiederwahl der oder des Beauftragten für Datenschutz möglich. Auf eine Amtszeitbeschränkung soll weiterhin verzichtet werden. Zum einen ist eine gewisse Erfahrung und ein Netzwerk innerhalb der Verwaltung für die Ausübung des Amtes unabdingbar und zum anderen muss sich die gewählte Person alle vier Jahre der Wiederwahl stellen.

Artikel 37 – Vorbereitung der Wahl oder Wiederwahl der oder des Beauftragten für Datenschutz

Absatz 1 und 2

Der Wahlvorschlag des Regierungsrates zur Beauftragten oder zum Beauftragten für Datenschutz wird nach geltendem Recht von der Justizkommission vorberaten (Art. 38 Abs. 2 Bst. d der Geschäftsordnung vom 4. Juni 2013 des Grossen Rates [GO[58]]). Die Beteiligung der Legislative am Auswahlverfahren ist

[58] BSG 151.211

bisher nicht vorgesehen. Für einen reibungslosen Ablauf ist es indes wichtig, dass sich die Legislative bei der Auswahl der Kandidatinnen und Kandidaten beteiligen und sich zu deren Befähigung äussern kann. Anlässlich der letzten Wahl des seit März 2019 amtierenden Beauftragten für Datenschutz fungierte ein ad-hoc eingesetztes Wahlgremium, bestehend aus

- dem Präsidenten der Geschäftsprüfungskommission,
- dem Staatsschreiber und
- einer Vertretung aus der Direktion für Inneres und Justiz, bestehend aus einem Mitglied des Generalsekretariats und dem Personalverantwortlichen.

Die Erfahrungen mit dem eingesetzten Wahlgremium waren positiv. Mit der Beteiligung aus Politik und Verwaltung konnten die unterschiedlichen Kompetenzen angemessen berücksichtigt werden. Der Vorschlag für die Zusammensetzung des Wahlgremiums orientiert sich deshalb am 2018 ad-hoc eingesetzten Wahlgremium. Es besteht mindestens aus den genannten Vertreterinnen und Vertretern. Die Direktion für Inneres und Justiz kann bei Bedarf weitere Personen beiziehen.

Der Wahlvorschlag des Regierungsrates wird heute von der Justizkommission für den Grossen Rat vorbereitet. Eine solche Wahlvorbereitung ist nicht mehr notwendig, zumal für die Wahlvorbereitung eigens ein Wahlgremium eingerichtet werden soll, das aus Mitgliedern der Exekutive und Legislative besteht. Artikel 38 Absatz 2 Buchstabe d GO, der die Wahlvorberatung durch die Justizkommission vorsieht, ist deshalb aufzuheben. Der Wahlvorschlag soll künftig direkt vom Büro des Grossen Rates entgegengenommen werden, entsprechend dem Vorschlag für die Wahl der Staatsschreiberin oder des Staatsschreibers (Art. 31 Abs. 2 und Art. 82 Abs. 1 Bst. b GO). Ein untergeordneter Erlass kann nicht indirekt abgeändert werden (Parallelität von Erlassänderungen). Deshalb erfolgt die Änderung der Geschäftsordnung des Grossen Rates mit einer separaten Vorlage.

Auch die Wiederwahl soll vom Wahlgremium vorgeschlagen werden. Ist sie unbestritten, können die Mitglieder des Wahlgremiums schriftlich konsultiert werden.

Die Normierung eines Stichentscheides ist nicht notwendig. Es ist durchaus möglich, dass das Wahlgremium mehrere Kandidaten vorschlägt. Das Wahlorgan ist der Grosse Rat. Somit obliegt ihm die Entscheidung.

Artikel 38 – Aufsichtsbehörde über die Beauftragte oder den Beauftragten für Datenschutz

Absatz 1

Absatz 1 wiederholt Artikel 38 Absatz 1 Buchstabe d des Personalgesetzes vom 16. September 2004 (PG)[59], wonach die Geschäftsprüfungskommission die Beauftragte oder den Beauftragten für Datenschutz beaufsichtigt. Damit soll dem Grundsatz Rechnung getragen werden, dass ein Erlass möglichst vollständig zu formulieren ist. Zudem wurde diskutiert, ob die Geschäftsprüfungskommission statt der Aufsicht die Oberaufsicht ausübt. Dies wäre jedoch nicht kongruent mit der Personalgesetzgebung, weshalb eine entsprechende Anpassung des Gesetzestextes wieder verworfen wurde.

Absatz 2

Betont wird hier nochmals die Unabhängigkeit der oder des Beauftragten für Datenschutz, d.h. die Geschäftsprüfungskommission ist nicht weisungsbefugt (vgl. Erläuterungen zu Artikel 34 Absatz 2 VE-revKDSG). Die Aufsicht gegenüber der bzw. dem Beauftragten für Datenschutz muss der Kontrolle über die Gerichte entsprechen. Dies bedeutet namentlich, dass eine inhaltliche Kontrolle der Tätigkeit ausgeschlossen ist, sei dies in Bezug auf die Zweckmässigkeit, die Rechtmässigkeit, auf die Art und Weise der Ausübung der Tätigkeit oder auf das Fachliche, insbesondere die Beurteilung von datenschutzrechtlicher Fragen. Die Rechte der Geschäftsprüfungskommission ergeben sich wie gegenüber den Gerichten sinngemäss aus der Grossratsgesetzgebung, insbesondere aus Kapitel 4 des Grossratsgesetzes. Die Aufsichtstätigkeit beschränkt sich auf die Beauftragte bzw. den Beauftragten für Datenschutz und erstreckt sich keinesfalls auf das übrige Personal der Datenschutzbehörde.

[59] BSG 153.01

Bei schweren Amtspflichtverletzungen kann die Geschäftsprüfungskommission das Abberufungsverfahren nach Artikel 41 PG einleiten. Voraussetzungen hierfür sind Unfähigkeit, dauerhaft ungenügende Leistungen, schwere oder wiederholte Pflichtverletzung oder wenn ein anderer wichtiger Grund die Fortsetzung der Amtsführung unzumutbar macht. Mit dieser Regelung ist dem Erfordernis der Unabhängigkeit der Datenschutzbehörde genügend Rechnung getragen.

Artikel 39 – Budget, Aufgaben- und Finanzplan

Wie bisher verfügt die kantonale Datenschutzbehörde über ein eigenes Budget, auf das Regierung und Verwaltung keinen Einfluss nehmen dürfen. Das Budget für die Datenschutzbehörde muss indes in das Gesamtbudget des Kantons integriert werden, was in administrativer Hinsicht durch die Verwaltung erfolgt. Es soll dem Regierungsrat weiterhin möglich sein, den Voranschlag zu kommentieren. Die Bestimmung ist redaktionell an Artikel 7 KFKG der Finanzkontrolle angeglichen worden.

Artikel 40 – Haushaltsführung

Die Bestimmungen zur Haushaltführung (Art. 33a Abs. 4 KDSG und Art. 33b KDSG) werden in einem Artikel zusammengefasst und an die Finanzkontrollgesetzgebung angeglichen. Wie bisher gilt für die Haushaltsführung die Finanzhaushaltsgesetzgebung.

Die kantonale Datenschutzbehörde verfügt selbst über die mit dem Budget bewilligten Mittel. Diese Mittel können sowohl zur Anstellung von Personal als auch für andere Zwecke, beispielsweise für den «Einkauf» von Leistungen spezialisierter Personen, verwendet werden. Explizit verzichtet wird in diesem Zusammenhang auf das Erfordernis der Leistungsvereinbarung. Eine solche Leistungsvereinbarung würde dem Grundsatz der Unabhängigkeit der Datenschutzaufsicht widersprechen.

Wie bisher stellt das Gesetz klar, dass die kantonale Datenschutzbehörde eine besondere Rechnung führt und der Grosse Rat die Art und Weise der Rechnungsführung durch Dekret regelt, nämlich das Dekret vom 1. Februar 2011 über die Besondere Rechnung der kantonalen Aufsichtsstelle für Datenschutz (BRDD)[60].

Artikel 41 – Organisation und Stellung

Die kantonale Aufsichtsstelle wird neu als kantonale Datenschutzbehörde bezeichnet und ihre Funktion gestärkt. Diverse Aufgaben im Aufsichtsbereich, die bisher von Gemeinden und andere gemeinderechtliche Körperschaften erfüllt wurden, werden neu von der kantonalen Datenschutzbehörde wahrgenommen (Abs. 3). Folglich bezeichnen nur noch Gemeinden und andere gemeinderechtliche Körperschaften mit mehr als 25’000 Einwohnerinnen und Einwohnern sowie Landeskirchen und ihre regionalen Einheiten eine eigene Datenschutzbehörde, welche die Aufgaben nach diesem Gesetz ausübt. Aktuell sind dies Biel/Bienne, Bern, Köniz und Thun. Die Neuverteilung der Aufgaben soll über den Lastenausgleich finanziert werden (vgl. Erläuterungen zu Art. 57 VE-revKDSG).

Artikel 42 – Aufgaben

Absatz 1

Dieser Artikel listet sämtliche Aufgaben der Datenschutzbehörden in konzentrierter Form auf. Er gilt auch für Datenschutzbehörden von Gemeinden und anderen gemeinderechtlichen Körperschaften, soweit sie eine eigene Behörde bezeichnen müssen.

Die Datenschutzbehörden unterstützen die verantwortlichen Behörden bei der Anwendung des Datenschutzrechts. Die Hauptaufgaben der Datenschutzbehörden sind die Beratung und die Überwachung der Datenschutzbestimmungen inkl. der Datensicherheit. Mit der Beratung soll darauf hingewirkt werden, dass die verantwortlichen Behörden mit Personendaten datenschutzkonform umgehen und mit der Überwachung soll überprüft werden, ob sie die datenschutzrechtlichen Bestimmungen einhalten. Im Vordergrund steht die Beratung. Der Aufgabenkatalog ist neu strukturiert; in Buchstabe a bis c sind Aufgaben

[60] BSG 620.03

aufgelistet, die thematisch zur Überwachung der Datenschutzbestimmungen gehören, wobei die Vorabkontrolle einer tatsächlichen Datenbearbeitung vorangestellt ist. Die Buchstaben d bis h thematisieren die beratende Tätigkeit der Aufsichtsbehörden. Die weiteren Aufgaben betreffen die Öffentlichkeitsarbeit und die Veröffentlichung des Registers der Datensammlungen. Sämtliche Aufgaben in einem Katalog aufzulisten, führt zwar zu Wiederholungen im weiteren Gesetzestext, ist jedoch sinnvoll, da die Datenschutzbehörden i.d.R. über keine eigene Organisationsverordnung bzw. über kein eigenes Organisationsreglement verfügen. Bei der Zusammenarbeit mit anderen Behörden dient der Aufgabenkatalog dazu, die Handlungsfelder der Datenschutzbehörde zu erläutern.

Buchstabe a

Die Datenschutzbehörde wird entweder von sich aus tätig und überprüft die Einhaltung des Gesetzes nach ihrem autonom festgelegten Prüfungsprogramm oder handelt auf Anzeige hin (vgl. Art. 44 VE-revKDSG). Ziel der Überwachung ist es, allfällige Missstände zu eruieren und aufzuzeigen, wo Massnahmen ergriffen werden müssen, damit ein rechtskonformer Zustand hergestellt werden kann. Die Überwachung der Datensicherheit gehört zur Überwachung der Datenschutzbestimmungen, weshalb sie nicht mehr als eigenständige Aufgabe aufgeführt ist.

Buchstabe b

Die Vorabkontrolle ist eine weitere Hauptaufgabe der Datenschutzbehörden. Im Gegensatz zum geltenden Recht wird der explizite Verweis auf den Artikel gestrichen, da sich dieser aus dem Gesetzestext ergibt. Die Vorabkontrolle bezieht sich auf eine geplante, systematische Bearbeitung von Personendaten, die wegen der bearbeiteten Personendaten oder der Art der Bearbeitung, ein hohes Risiko für die Grundrechte der betroffenen Personen birgt und eine grössere Anzahl von Personen betrifft (vgl. Art. 20 VE-revKDSG). Im Gegensatz zur Überwachung bezieht sich die Vorabkontrolle nicht auf eine stattfindende oder bereits stattgefundene Bearbeitung von Personendaten, sondern auf eine zukünftige Bearbeitung von Personendaten.

Buchstabe c

Artikel 52 der Richtlinie (EU) 2016/680 verlangt, dass jede betroffene Person (...) das Recht auf Beschwerde bei einer Datenschutzbehörde hat, wenn sie der Ansicht ist, dass die Bearbeitung der sie betreffenden Personendaten gegen die nach dieser Richtlinie erlassenen Vorschriften verstösst. Es besteht kein Grund zur Annahme – und davon geht auch der KdK-Leitfaden aus –, dass letztere Vorschrift mehr verlangt als die im kantonalen Recht bereits geregelte aufsichtsrechtliche Anzeige (Art. 101 VRPG). Es besteht daher kein Anlass, einen neuen Rechtsbehelf einzuführen, der bei der Datenschutzbehörde erhoben werden kann. Insofern handelt es sich bei Buchstabe c um eine Handlungsanweisung an die Datenschutzbehörden. Über das Ergebnis der Abklärungen müssen die Datenschutzbehörden die anzeigende Person innerhalb von drei Monaten informieren (vgl. Art. 44 Abs. 4 VE-revKDSG).

Buchstabe d

Die Datenschutzbehörde versteht sich hauptsächlich als beratende Behörde. So berät sie die verantwortlichen Behörden bei der Anwendung des Gesetzes sowie die betroffenen Personen über ihre Rechte. In diesem Sinn vermittelt sie auch zwischen den beiden Akteuren, weshalb die beiden Aufgaben zusammengefasst werden.

Buchstabe e

Das Auskunftsrecht der betroffenen Person kann in bestimmten Fällen, insbesondere wegen überwiegender öffentlicher oder privater Interessen verweigert, eingeschränkt oder aufgeschoben werden (vgl. Art. 30 VE-revKDSG). In solchen Fällen wahren die zuständigen Datenschutzbehörden die Rechte der betroffenen Personen.

Buchstabe f

Unter Erlassentwürfen sind Gesetzes- und Verordnungsentwürfe zu verstehen sowie deren Änderungen. Wesentliche Massnahmen sind beispielsweise Vorkehrungen zur Sicherstellung der Informatiksicherheit,

Umfragen, Aus- und Umgestaltung von Prozessen wie etwa die Ausstellung von elektronischen Zertifikaten. Für Erlassentwürfe und andere Massnahmen von Gemeinden und anderen gemeinderechtlichen Körperschaften ohne eigene Datenschutzbehörden besteht eine Einschränkung (vgl. Abs. 3).

Buchstabe g

Auf Anfrage von Verfügungs- und Rechtmittelbehörden reichen die Datenschutzbehörden ausserdem Vernehmlassungen zu Datenschutzfragen ein.

Buchstabe h

Die Datenschutzbehörden sind zudem verpflichtet, mit anderen Aufsichtsstellen zusammenzuarbeiten und Amtshilfe zu leisten (vgl. Art. 47 VE-revKDSG).

Buchstabe i

Die Datenschutzbehörden informieren die Öffentlichkeit einerseits periodisch mit dem öffentlichen Tätigkeitsbericht sowie bei Bedarf, nämlich in Fällen von allgemeinem Interesse (vgl. Art. 48 VE-revKDSG).

Absatz 2

Die kantonale Datenschutzbehörde führt und veröffentlicht zudem das kantonale Register der Datensammlungen (vgl. Art. 21 VE-revKDSG).

Absatz 3

Aus praktischen Gründen äussert sich die kantonale Datenschutzbehörde nur zu gewissen Erlassentwürfen und anderen Massnahmen von Gemeinden und anderen gemeinderechtlichen Körperschaften ohne eigene Datenschutzbehörde. Das Organisationsreglement und teilweise auch andere kommunale Erlasse unterliegen der Vorprüfung durch das Amt für Gemeinden und Raumordnung, das sich zu untergeordneten datenschutzrechtlichen Fragen äussern kann. Es kann auf Wunsch die kantonale Datenschutzbehörde konsultieren.

Artikel 43 – Schweigepflicht bei der Aufgabenerfüllung

Das Recht der Datenschutzbehörde, ungeachtet von Geheimhaltungspflichten, Auskünfte von Behörden zu verlangen, erfordert auf der anderen Seite die gleiche Verpflichtung zur Geheimhaltung, wie sie die Behörde zu beachten hat.

Artikel 44 – Überprüfung der Einhaltung von Datenschutzbestimmungen und der Datensicherheit

Gestützt auf die Richtlinie (EU) 2016/680 und des Übereinkommens SEV Nr. 108+ erhält die oder der Beauftragte für den Datenschutz erweiterte Kontrollbefugnisse als bis anhin. Die erweiterten Kontrollbefugnisse sind ins kantonale Recht zu übernehmen. Der sehr ausführliche Artikel 35 des geltenden Rechts wird in drei Artikel unterteilt: Überwachung der Einhaltung von Datenschutzbestimmungen inkl. der Datensicherheit (Art. 44 VE-revKDSG; bisher: Arbeitsweise und Verfahren), Empfehlungen (Art. 45 VE-revKDSG) und Verwaltungsmassnahmen (Art. 46 VE-revKDSG).

Absatz 1

Vor der Inbetriebnahme prüft die Datenschutzbehörde geplante Informatikvorhaben auf ihre Datenschutzkonformität und Datensicherheit. Das geschieht im Rahmen der Vorabkontrolle nach Artikel 20 VE-revKDSG. Im Unterschied zur Vorabkontrolle – bei der die Datenschutzbehörde in Zusammenarbeit mit der Behörde den Soll-Zustand in Bezug auf die Datenschutzbestimmungen und die Datensicherheit festlegt – nimmt die Datenschutzbehörde auch Prüfungen in der Betriebsphase vor (Prüfung des Ist-Zustandes). Die Prüfung durch die Aufsichtsbehörde erfolgt gestützt auf das autonom festgelegte Prüfungsprogramm oder gestützt auf eine Anzeige.

Absatz 2

Dieser Absatz beschreibt die Form der Überwachung. Das geltende Recht erwähnt lediglich die Auskunft, die Einsicht in Unterlagen und die Besichtigung, weshalb der Artikel mit «Nachweise einholen» und «weitere Prüfungshandlungen» ergänzt wird.

Sinnvollerweise werden die Anforderungen an den Nachweis bei bedeutenden Anwendungen mit grossen Auswirkungen höher sein als bei kleineren Anwendungen. Als Instrumente zum Nachweis der Einhaltung der Datenschutzbestimmungen kommen etwa Datenschutzmanagementsysteme (DSMS) oder datenschutzrechtliche Audits in Frage. DSMS basieren auf den ISO-Standards des Qualitätsmanagements (ISO 9001) und der Informationssicherheit (ISO 27001). Denkbar ist auch ein blosser Bericht, der sich über die Umsetzung von Massnahmen äussert. Die Vorabkontrolle durch die Datenschutzbehörde (Art. 20 VE-revKDSG) und das Verfahren zur Umsetzung von Informationssicherheit und Datenschutz (ISDS) sind jedoch kein genügender Nachweis. Sie kommen vielmehr zum Einsatz, bevor die Datenbearbeitung einsetzt (Feststellung des Soll-Zustandes). Hier muss jedoch nachgewiesen werden, dass die Bearbeitung der Personendaten dem bei der Vorabkontrolle festgelegten Soll-Zustand entspricht.

Typischerweise erfolgt die Prüfung mit einem Datenschutz-Audit. Dabei wird der Umgang mit den Personendaten standardisiert geprüft. Kontrolliert wird, ob bei den untersuchten Datenbearbeitungsprozessen, die datenschutzrechtlichen Bestimmungen eingehalten werden oder ob beispielsweise die Rechte der betroffenen Person gewährleistet sind. Ferner kann geprüft werden, ob die Personendaten mit geeigneten technischen und organisatorischen Massnahmen dem Risiko angemessen geschützt sind (vgl. Art. 10 VE-revKDSG).

Die weiteren Befugnisse der Datenschutzbehörde und das Verfahren bei festgestellten Mängeln ergeben sich aus den nachfolgenden Artikeln.

Absatz 3

Wie bisher ist die verantwortliche Behörde verpflichtet, bei den Prüfungshandlungen mitzuwirken.

Absatz 4

Es bestehen keine Vorschriften, innerhalb welcher Frist Anzeigen von der Datenschutzbehörde behandelt werden müssen. Der bisherige Artikel 34 Absatz 2 KDSG enthält bloss eine allgemeine Orientierungspflicht der Betroffenen durch die Datenschutzbehörde. Hingegen bestehen Richtlinien des Regierungsrats vom 14. November 2012 (RRB 1616) für die Behandlung aufsichtsrechtlicher Anzeigen. Nach deren Ziffer 3 sind solche Anzeigen – vorbehältlich besonders aufwendiger Abklärungen – in der Regel innert längstens sechs Monaten zu behandeln.

Artikel 53 Absatz 2 der Richtlinie (EU) 2016/680 enthält die Bestimmung, dass jede betroffene Person (...) das Recht auf einen wirksamen gerichtlichen Rechtsbehelf hat, wenn die (...) Datenschutzbehörde sich nicht mit der Beschwerde befasst oder die betroffene Person nicht innerhalb von drei Monaten über den Stand oder das Ergebnis der gemäss Artikel 52 erhobenen Beschwerde in Kenntnis gesetzt hat. Diese dreimonatige Frist ist in das kantonale Recht zu übernehmen. Sie gilt nicht für alle aufsichtsrechtlichen Anzeigen nach Artikel 101 VRPG, sondern nur für die an die Datenschutzbehörde gerichteten. Im Gegensatz zu der aufsichtsrechtlichen Anzeige nach Art. 101 VRPG informiert die Datenschutzbehörde nicht nur über die Erledigung der Anzeige, sondern auch über das Ergebnis der Abklärungen.

Artikel 45 – Empfehlungen

Das bisherige System, wonach die Datenschutzbehörde ihre Empfehlung lediglich in Form eines mit einer Begründung versehenen Antrags abgeben kann, ist gemäss den europäischen Vorgaben nicht mehr ausreichend. Die Datenschutzbehörde erhält die Kompetenz, zu verfügen (vgl. Art. 46 VE-revKDSG). Es soll aber weiterhin möglich sein, dass sie gegenüber der verantwortlichen Behörde Empfehlungen aussprechen kann.

Mit der Begründungspflicht kann die verantwortliche Behörde zu den Empfehlungen Stellung nehmen, womit ihr das rechtliche Gehör gemäss Artikel 21 Absatz 1 VRPG gewährt wird, bevor allenfalls verfügt wird. Die Verfügungskompetenz der Behörde entfällt.

Artikel 46 – Verwaltungsmassnahmen

Absatz 1

Gestützt auf Artikel 47 Absatz 2 Buchstabe b und c der Richtlinie (EU) 2016/680 und Artikel 19 SEV Nr. 108+ zur Änderung von 15 Ziffer 2 Buchstabe c SEV Nr. 108 muss die Datenschutzbehörde bei Verstössen gegen das Datenschutzrecht verbindliche Anordnungen in Form einer Verfügung treffen können. Diese Verfügungsmöglichkeit ist ins kantonale Datenschutzrecht zu übernehmen. Die Verfügung könnte beispielsweise darauf lauten, eine widerrechtliche Datenbearbeitung einzustellen oder auf eine widerrechtliche Datenbearbeitung zu verzichten. Die Verfügungskompetenz ist jedoch auf Fälle zu beschränken, bei denen die Bestimmungen über den Datenschutz erheblich verletzt werden.

Der Vollständigkeit halber ist hier zu erwähnen, dass betroffene Personen, die sich gegen die Datenbearbeitung verantwortlicher Behörden zur Wehr setzen wollen, deren Handlungen direkt anfechten können. Dazu steht ihnen der normale Rechtsmittelweg zur Verfügung. Die oder der Beauftragte für den Datenschutz ist an diesem Verfahren nicht beteiligt. Ausnahmeweise reicht die Datenschutzbehörde auf Ersuchen von einer Verfügungs- oder Rechtsmittelbehörden im Rahmen der Zusammenarbeit eine Vernehmlassung zu Datenschutzfragen ein.

Absatz 2

Die Datenschutzbehörde ist keiner Direktion untergeordnet; Artikel 34 Absatz 3 VE-revKDSG sieht lediglich die administrative Zuordnung an die Direktion für Inneres und Justiz vor. Daher muss der Rechtsmittelweg unmittelbar an das Verwaltungsgericht führen. Dieser Rechtsmittelweg entspricht dem Vorschlag des KdK-Leitfadens.

Absatz 3

Gemäss Artikel 80 Absatz 1 VRPG verfügt das Verwaltungsgericht nur über beschränkte Kognition, d.h. es kann nur die unrichtige oder unvollständige Feststellung des Sachverhalts überprüfen sowie andere Rechtsverletzungen, einschliesslich Rechtsfehlern bei der Ausübung des Ermessens. Die Unangemessenheit entzieht sich indes der Überprüfung durch das Verwaltungsgericht, ausser wenn die Gesetzgebung diese Rüge vorsieht (Art. 80 Abs. 1 Bst. c VRPG). Da hier das Verwaltungsgericht als einzige Rechtsmittelinstanz vorgesehen ist, muss es mindestens über volle Kognition verfügen. Deshalb ist in Absatz 3 die Unangemessenheitsrüge vorgesehen.

Artikel 47 Absatz 2 Buchstabe c der Richtlinie (EU) 2016/680 und der KdK-Leitfaden verlangen eine Regelung für den Erlass vorsorglicher Massnahmen. Falls schutzwürdige Interessen offensichtlich gefährdet oder verletzt werden, muss die Datenschutzbehörde die Befugnis haben, vorsorglich eine Datenbearbeitung einzuschränken oder zu untersagen. Eine explizite Regelung im kantonalen Datenschutzgesetz erübrigt sich jedoch, da auf das Verfahren die Bestimmungen des VRPG anwendbar sind und in Artikel 27 VRPG der Erlass von vorsorglichen Massnahmen bereits vorgesehen ist.

Absatz 4

Die Aufsicht kann nur dort greifen, wo das kantonale Datenschutzgesetz anwendbar ist (vgl. Art. 3 Abs. 3 VE-revKDSG). Die Bearbeitung von Personendaten in einem hängigen Verfahren der Gerichtsbehörden oder der Staatsanwaltschaft kann die Datenschutzbehörde nicht beaufsichtigen. Hingegen müssen sie geplante, systematische Bearbeitungen von Personendaten der Datenschutzbehörde zur Vorabkontrolle vorlegen; dabei werden die allgemeinen Fragen zur Datenbearbeitung thematisiert, etwa die Frage, wie mit Daten über andere als die Zielpersonen umgegangen wird. Die Datenschutzbehörde soll jedoch ihnen gegenüber keine verbindlichen Anordnungen treffen können, weshalb die Datenschutzbehörde keine Verwaltungsmassnahmen erlassen darf. Im Vordergrund steht die Beratungstätigkeit.

Artikel 47 – Zusammenarbeit

Absatz 1

Auch der Datenschutz ist vom Schweizer Föderalismus geprägt: Der Bund und die Kantone haben je eigene Datenschutzgesetze, und im Kanton Bern haben einige Gemeinden ihre eigene Datenschutzbehörde (Art. 41 VE-revKDSG). Dies kann ein Hindernis für die Zusammenarbeit darstellen. Wenn z.B. eine gemeinsame Plattform der Kantone, die auch von den Gemeinden genutzt werden soll, von Dutzenden unterschiedlichen Datenschutzbehörden nach unterschiedlichen Kriterien und in unterschiedlichen Verfahren geprüft wird, können die sich daraus ergebenden Differenzen und allfälligen Beschwerdeverfahren das Projekt für lange Zeit blockieren oder die Kantone zum Vornherein von der Zusammenarbeit abhalten – ganz abgesehen vom Mehraufwand für die vielen parallelen Prüfverfahren.

Um solche Friktionen möglichst zu vermeiden, äussert Absatz 1 den Grundsatz, dass die Datenschutzbehörden untereinander sowie mit anderen Aufsichtsstellen zusammenarbeiten sollen. Letztere können Aufsichtsstellen anderer Kantone, des Bundes oder ausländische Aufsichtsstellen sein, sowohl Datenschutzaufsichtsstellen als auch Behörden mit anderen Aufsichtsfunktionen wie beispielsweise Regierungsstatthalter oder die kantonale Finanzkontrolle. Besonders Vorabkontrollverfahren sind zeitlich und inhaltlich so zu koordinieren, dass sie das Zusammenarbeitsprojekt möglichst wenig behindern. Die Datenschutzbehörden sollen sich dazu miteinander austauschen, so dass sie nach Möglichkeit einen gemeinsamen oder gleichlautenden Prüfbericht abgeben oder auch Prüfungshandlungen anderer Datenschutzbehörden berücksichtigen können.

Absatz 2

Wie bisher können Datenschutzbehörden anderer öffentlich-rechtlicher Körperschaften Aufgaben der Datenschutzaufsicht im Kanton Bern wahrnehmen, soweit dies vereinbart ist.

Absatz 3

Die kantonale Datenschutzbehörde übernimmt beispielsweise für das interkantonale Geldspielkonkordat Aufsichtshandlungen, für das sonst keine Datenschutzbehörde zuständig wäre. Denkbar sind beispielsweise auch die Übernahme von Prüfungshandlungen (Audits) oder Vorabkontrollen in Gemeinden oder anderen Kantonen auf deren Anfrage hin.

Absatz 4

Für die Datenschutzaufsicht über Vorhaben, die die Nutzung kantonaler digitaler Leistungen betrifft (wie der Basisdienste), ist die kantonale Datenschutzbehörde allein zuständig. Dies gilt auch für Datenbearbeitungen von Gemeinden, die über eine eigene Datenschutzbehörde verfügen. Sie stellt so eine einheitliche und effiziente Beurteilung auf kantonaler Ebene sicher. Sonst bestünde das Risiko, dass voneinander abweichende Meinungen der kommunalen Datenschutzbehörden ein Projekt verzögern oder eine einheitliche Nutzung und Sicherung der digitalen Leistungen verhindern. Festzuhalten ist, dass der Kanton nur soweit verantwortlich ist, als er die Leistung auch tatsächlich zur Verfügung stellt. Für die Weiterverarbeitung bleibt die Gemeinde zuständig. Zudem sind nur Datenbearbeitungen mit den kantonalen digitalen Leistungen betroffen, nicht aber die Datenbearbeitungen, die ausserhalb dieser Leistungen, z.B. mit einer Software der Gemeinden, vorgenommen werden.

Artikel 48 – Berichterstattung und Information der Öffentlichkeit

Dieser Artikel regelt sowohl die jährliche Berichterstattung ans Wahlorgan als auch die Information an die Öffentlichkeit. Im Tätigkeitsbericht soll sich die Datenschutzbehörde auf die für die Öffentlichkeit wichtigen Sachverhalte beschränken. Auf Verordnungsstufe wird dies ausdrücklich festgehalten.

Der Tätigkeitsbericht richtet sich formell an das Wahlorgan. Die kantonale Datenschutzbehörde publiziert ihn aber bereits heute im Internet. Die Öffentlichkeit des Berichts ergibt sich aus der Pflicht der Datenschutzbehörde zur periodischen Information der Öffentlichkeit (Art. 42 Abs. 1 Bst. i VE-revKDSG) und der Informationsgesetzgebung, weshalb dazu keine explizite Regelung notwendig ist.

In Fällen von allgemeinem Interesse kann die Datenschutzbehörde die Öffentlichkeit informieren. Die Pflicht der kantonalen Datenschutzbehörde, vorgängig die Direktionsvorsteherin oder den Direktionsvor-

steher bzw. die Staatsschreiberin oder den Staatsschreiber zu informieren, findet bewusst keinen Eingang mehr im Gesetz. Damit soll der Unabhängigkeit der Datenschutzbehörde Rechnung getragen werden. Im Übrigen erfolgt ein Austausch zwischen den Behörden und der Datenschutzbehörde nach den Bestimmungen von Artikel 44-46 VE-revKDSG oder im Rahmen der informellen Zusammenarbeit. Vorfällen von öffentlichem Interesse geht in der Regel ein solches Verfahren voraus. Demnach kann sich die betroffene Behörde zu Empfehlungen der Datenschutzbehörde äussern, womit ihr das rechtliche Gehör gewährt wird.

7.6 Verfahren und Rechtsschutz

Artikel 49 – Anwendbare Bestimmungen

Der in Artikel 49 verankerte Grundsatz bedeutet, dass der ordentliche Rechtsmittelweg auch im Datenschutzrecht gilt. Rechtsmittelbehörde ist demnach wie bisher nicht die Datenschutzbehörde. Eine Ausnahme vom ordentlichen Rechtsmittelweg ist die Eskalation zwischen den Behörden und der Datenschutzbehörde, wenn die Datenschutzbehörde eine Verfügung erlässt. In diesen Fällen ist das Verwaltungsgericht zuständig (vgl. Art. 46 Abs. 2 VE-revKDSG).

Artikel 50 – Prozessvertretung

Nach Artikel 15 Absatz 4 VRPG sind ausser auf dem Gebiet des Sozialversicherungsrechts und vorbehältlich anderslautender Gesetzgebung vor den Verwaltungsjustizbehörden zur Prozessvertretung nur Anwältinnen und Anwälte zugelassen. Sie müssen nach der Anwaltsgesetzgebung zur Parteivertretung im Kanton Bern berechtigt sein.

Artikel 55 der Richtlinie (EU) 2016/680 sieht eine Ausnahme vom Anwaltsmonopol für die Prozessvertretung vor, welche in Artikel 11 EV EDS abgebildet worden ist und nun ins ordentliche Recht überführt werden muss. Die Richtlinie sieht vor, dass gegen eine aufsichtsrechtliche Anzeige, gegen Anordnungen der Datenschutzbehörde und gegen Anordnungen der verantwortlichen Behörde ein Rechtmittel ergriffen werden kann. Zweck der Bestimmung ist, dass sich Betroffene bei der Ergreifung der genannten Rechtsmittel von gemeinnützigen Organisationen vertreten lassen können. Weil nach dem VRPG in verwaltungsinternen und –externen Beschwerdeverfahren das Anwaltsmonopol besteht, ist die Ausnahme davon spezialgesetzlich im KDSG aufzunehmen (vgl. Art. 15 Abs. 4 VRPG). Voraussetzung für die Vertretungsbefugnis ist, dass die Organisation gemeinnützig, d.h. nicht gewinnorientiert ist. Ausserdem muss sie sich statutengemäss mit den Anliegen des Datenschutzes befassen. Zur Auslegung des letztgenannten Punktes kann auf die Rechtsprechung zum Verbandsbeschwerderecht verwiesen werden.

Die Ausnahme vom Anwaltsmonopol gilt für sämtliche verwaltungsinternen Beschwerdeverfahren und die Verfahren vor dem Verwaltungsgericht und den anderen verwaltungsunabhängigen Justizbehörden im Sinne von Artikel 85 VRPG in Angelegenheiten des Datenschutzes. Betroffen sind in erster Linie die Verfahren in Anwendung der Artikel 28 ff. VE-revKDSG, d.h. Verfügungen der Behörde über Auskunftsgesuche sowie deren Verweigern und Verzögern. Weil das Anwaltsmonopol bei der aufsichtsrechtlichen Anzeige an die Datenschutzbehörde nicht gilt, braucht es hier keine Ausnahme.

Artikel 51 – Anfechtungsobjekt

Es ist fraglich, ob ein förmlicher Entscheid über ein Auskunftsgesuch oder über ein Gesuch bei widerrechtlicher Bearbeitung (vgl. Art. 28 und 31 VE-revKDSG) alle Merkmale einer Verfügung erfüllt. Mit dieser Bestimmung soll klargestellt werden, dass sämtliche Entscheide über solche Gesuche inkl. deren Verweigerung, Einschränkung und Aufschub anfechtbar sind.

Artikel 52 – Behördenbeschwerde

Verlangt eine Behörde von einer anderen Behörde die Bekanntgabe von Personendaten und lehnt diese die Auskunft ab, so muss sich die abgewiesene Behörde dagegen zur Wehr setzen können, wenn sie gestützt auf die Bestimmungen dieses Gesetzes Anspruch auf die Bekanntgabe der Personendaten hat.

Artikel 53 – Gebühren

Das Recht auf Auskunft ist einer der wichtigsten Ausflüsse des Grundrechts auf Datenschutz, weshalb die Auskunftserteilung und die sich daraus ergebenden weiteren Rechte der betroffenen Person, grundsätzlich kostenlos sind. Folglich können sämtliche Rechte, die eine betroffene Person nach dem 4. Titel dieses Gesetzes geltend machen kann, gebührenfrei ausgeübt werden. Eine Ausnahme ist hingegen zulässig, wenn Gesuche exzessiven Charakter haben oder querulatorisch sind.

Für Berichtigungsgesuche und weitere Schutzansprüche sieht die Verordnung vom 22. Februar 1995 über die Gebühren der Kantonsverwaltung (Gebührenverordnung; GebV)[61] bereits heute die Erhebung von Gebühren vor, wenn die ersuchende Person zur widerrechtlichen Bearbeitung Anlass gegeben hat (Art. 33 Abs. 2 GebV). Diese Ausnahme soll nun auf Gesetzesstufe verankert und gleichzeitig auf Auskunftsgesuche ausgeweitet werden. So kann missbräuchlichen Auskunftsgesuchen vorgebeugt werden. Absatz 2 gibt dem Regierungsrat deshalb die Möglichkeit, Ausnahmen von der Kostenlosigkeit vorzusehen. Dabei wird der Tatsache Rechnung tragen, dass gewisse Auskunftsersuchen für den Verantwortlichen mit einem grossen Aufwand verbunden sind.

7.7 Ausführungsbestimmungen

Artikel 54 – Ausführungsbestimmungen

Diese Bestimmung ermächtigt den Regierungsrat zum Erlass der erforderlichen Vollzugsvorschriften. Ausserdem darf er Befugnisse auf die Direktionen übertragen, die eher technischer und operativer Natur sind, oder primär die Zuständigkeiten der einzelnen verantwortlichen Stellen betreffen.

7.8 Übergangs- und Schlussbestimmungen

7.8.1 Übergangsbestimmungen

Artikel 55 – Laufende Bearbeitungen

Die Übergangsbestimmung betrifft Datenbearbeitungen, die nach bisherigem Recht begonnen wurden und nach Inkrafttreten des Gesetzes fortdauern. Folgende Artikel finden für solche Bearbeitungen keine Anwendung, wenn sich die Bearbeitung nicht wesentlich ändert:

- Artikel 9: Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen
- Artikel 18: Risikoanalyse
- Artikel 19: Datenschutzfolgenabschätzung
- Artikel 20: Vorabkontrolle

Diese Artikel betreffen die Pflichten der verantwortlichen Behörden im Vorfeld einer Datenbearbeitung. Sie sollen nicht nachträglich und damit rückwirkend die Pflichten erfüllen müssen.

Artikel 56 – Laufende Verfahren

Zur Gewährleistung der Rechtssicherheit und Einhaltung des Grundsatzes von Treu und Glauben schreibt diese Bestimmung vor, dass Untersuchungen der Datenschutzbehörde, die im Zeitpunkt des In-

[61] BSG 154.21

krafttretens des künftigen Datenschutzgesetzes hängig sind, sowie Beschwerden gegen hängige erstinstanzliche Entscheide dem bisherigen Recht unterstehen. Dies betrifft sowohl die materiellen Datenschutzvorschriften als auch die Befugnisse der Datenschutzbehörde und die weiteren anwendbaren Verfahrensvorschriften.

Artikel 57 – Lastenausgleich

Infolge der Zentralisierung der datenschutzrechtlichen Aufgaben der Gemeinden muss die Lastenneuverteilung geregelt werden. Die bisher von den Gemeinden geführten bzw. beauftragten Datenschutzbehörden werden neu grossenteils im Kanton zentralisiert und folglich auch finanziert. Die finanzielle Mehrbelastung des Kantons Bern infolge Übernahme der gemeinderechtlichen Aufsichtsfunktion wurde wie folgt ermittelt:

Das geltende Recht verlangt in Art. 33a Abs. 5 KDSG, dass die gemeinderechtlichen Datenschutzbehörden sowie die Datenschutzbehörden der Landeskirchen und ihrer regionalen Einheiten über hinreichende Ausgabenbefugnisse verfügen müssen. Um diese Vorgaben zu konkretisieren, hält Artikel 14 der geltenden kantonalen Datenschutzverordnung (die jährlichen Ausgabenbefugnisse fest, über welche die Datenschutzbehörden verfügen müssen. Die Ausgabenbefugnisse sind nach Grösse der Körperschaft abgestuft:

- Kleinstkörperschaften[62]: 1’000 Franken
- Andere Körperschaften: 5’000 Franken
- Gemeinden mit mehr als 10’000 Einwohnerinnen und Einwohnern: 10’000 Franken

Werden die Ausgabenbefugnisse auf die Anzahl der Gemeinden, gemeinderechtlichen Körperschaften und Kleinstkörperschaften per Ende 2021 umgerechnet, ergeben sich folgende Ausgabenbefugnisse:

- Bei 530 Kleinstkörperschaften: 530’000 Franken
- Bei 335 politische Gemeinden (abzgl. Gemeinden mit 25 000 Einwohnern): 1'740’000 Franken
- Bei 243 Kirchgemeinden: 1’215’000 Franken

Der zusätzliche Aufwand für den Kanton Bern entspricht jedoch nicht den normierten Beträgen in Art. 14 DSV, die zusammengezählt rund 3.5 Millionen Franken ausmachen würden. In zahlreichen Gemeinden und anderen gemeinderechtlichen Körperschaften nimmt die datenschutzrechtliche Aufsicht eine externe Revisionsstelle und in grösseren Gemeinden Kommissionen des Parlaments (Geschäftsprüfungskommission, Aufsichtskommission) wahr. Der tatsächliche Aufwand entspricht in der Regel nicht dem Aufwand gemäss kantonaler Datenschutzverordnung. In kleinen und mittleren Gemeinden und gemeinderechtlichen Körperschaften dürfte sich der Aufwand auf weniger als 1 000 Franken pro Jahr belaufen. Dazu kommt, dass die kantonale Datenschutzbehörde von Synergien aus dem zentralen Wissensaufbau und –erhalt profitieren kann. Dennoch wird die kantonale Aufsichtstätigkeit ihre Ressourcen wegen des Mehraufwands aufstocken müssen. Per 31. Dezember 2021 verfügt die kantonale Datenschutzbehörde über einen Personalbestand von 570 Vollzeitstellen. Gemäss Geschäftsbericht 2021 beträgt der Personalaufwand für das Jahr 2021 1’067‘775 Franken und der Sach- und übrige Betriebsaufwand 174’048 Franken (recte gemäss Jahresbericht kantonalen Datenschutzbehörde 2021: 243’000 Franken). Die kantonale Datenschutzbehörde rechnet mit einer Mehrbelastung von ca. 400 Stellenprozenten. Die Zentralisierung der Aufgaben darf nicht dazu führen, dass der Kanton diese Mehrkosten ohne gleichzeitige Kompensation tragen muss. Die Mehrbelastung für den zusätzlichen Personalaufwand und erhöhten Betriebsaufwand dürfte rund 1 Million Franken betragen und ist über das Lastausgleichssystem auszugleichen.

Artikel 58 –Die oder der Beauftragte für Datenschutz

[62] Unterabteilungen, Burgergemeinden, burgerliche Korporationen, Gemeindeverbände und Schwellenkorporationen (Art. 64a Gemeindeverordnung [GV; BSG 170.111]).

Die Übergangsbestimmung betrifft insbesondere die Wahlvorbereitung zur Wahl der oder des Beauftragten für Datenschutz und ihre bzw. seine Amtsdauer. Die Amtsdauer soll an die Legislatur angepasst werden. So wählt der Grosse Rat an seiner konstituierenden Sitzung ebenfalls die Staatsschreiberin oder den Staatsschreiber. Die Übergangsbestimmung bringt zum Ausdruck, dass die oder der gewählte Beauftragte für Datenschutz bis zum Ende ihrer bzw. seiner Amtsdauer gewählt bleibt. Bei der erstmaligen Wahl oder Wiederwahl nach Inkrafttreten des Gesetzes verkürzt sich die vierjährige Amtsdauer um neun Monate, da die oder der Beauftragte für Datenschutz nur bis zum Ende der aktuellen Legislaturperiode gewählt wird.

Daraus folgen Anpassungen in der Geschäftsordnung des Grossen Rates. Ein untergeordneter Erlass kann nicht indirekt abgeändert werden (Parallelität von Erlassänderungen). Deshalb erfolgt die Änderung der Geschäftsordnung mit einer separaten Vorlage. Hierfür soll die Wahl der oder des Beauftragten für Datenschutz in Artikel 1 GO mit einem Buchstaben m1 (Wahl an der konstituierenden Sitzung des Grossen Rates) und in Artikel 109 Absatz 1 GO mit einem Buchstaben f (Zeitpunkt der Wahlen) ergänzt werden.

7.9 Änderungen anderer Erlasse

7.9.1 Datenschutzgesetz (KDSG) vom 19. Februar 1986[63]

Da das kantonale Datenschutzgesetz totalrevidiert wird, muss das aktuelle Gesetz aufgehoben werden.

7.9.2 Gesetz vom 7. März 2022 über die digitale Verwaltung (DVG)[64]; indirekte Änderung

Die Bestimmungen zur Datenbearbeitung durch Dritte (Art. 28 DVG), zur Datenschutzverantwortung bei gemeinsamer Bearbeitung von Personendaten durch mehrere Behörden (Art. 29 DVG) und zur Datenschutzaufsicht bei der Zusammenarbeit unter Behörden (Art. 30 DVG) werden in leicht geänderter Fassung ins kantonale Datenschutzgesetz überführt (Art. 12 und Art. 47 VE-revKDSG). Somit kann der gesamte 5. Titel im DVG gestrichen werden. Der Verweis auf das kantonale Datenschutzgesetz ist nicht notwendig, da seine Bestimmungen ungeachtet des Verweises für sämtliche Bearbeitungen von Personendaten durch Behörden gelten.

7.9.3 Gesetz vom 12. September 1985 über Niederlassung und Aufenthalt der Schweizer (GNA)[65] und das Einführungsgesetz vom 9. Dezember 2019 zum Ausländer- und Integrations- sowie zum Asylgesetz (EG AIG und AsylG)[66]; indirekte Änderung

Mit der Revision werden die Bestimmungen zur Bekanntgabe von Personendaten zusammengefasst und die Bekanntgabe durch die Einwohnergemeinde in die Spezialgesetze verschoben. Bei letzterer Bestimmung handelt es sich um materielles Datenschutzrecht, welches nicht im Datenschutzrecht als Querschnittsmaterie zu regeln ist und bisher ein Fremdkörper im Gesetz darstellte.

Im revidierten Artikel 12 ist nur die Bekanntgabe an private Personen zu regeln. Die Bekanntgabe an Behörden richtet sich nach den allgemeinen Grundsätzen des kantonalen Datenschutzgesetzes, insbesondere nach Artikel 14 VE-revKDSG.

[63] BSG 152.04
[64] BSG 109.1
[65] BSG 122.11
[66] BSG 122.20

Gemäss der Aufzählung in Absatz 1 gibt die Einwohnerkontrolle neben dem Datum des Zu- und Wegzuges nun auch den neuen Wohnort bekannt, was der gängigen Praxis der Gemeinden entspricht. Die restlichen Angaben entsprechen dem bisherigen Artikel 12 Absatz 1 KDSG.

In Abweichung zu Artikel 33 VE-revKDSG kann die betroffene Person die Bekanntgabe von zusätzlichen Personendaten, die gestützt auf das Gemeindereglement zulässig wäre, ohne Nachweis eines schutzwürdigen Interessens sperren lassen.

Der Verweis auf die datenschutzrechtlichen Bestimmungen in Artikel 12 Absatz 1 GNA ist mit der Einführung der spezialgesetzlichen Regelung zu streichen.

Die Bestimmung soll ebenfalls für die Bekanntgabe von Personendaten ausländischer Personen gelten, weshalb im EG AIG und AsylG auf das GNA zu verweisen ist.

7.9.4 Gesetz vom 20. Juni 1985 über die Organisation des Regierungsrates und der Verwaltung (Organisationsgesetz, OrG)[67]; indirekte Änderung

Anlässlich der Revision stellte sich die Frage nach der organisationsrechtlichen Stellung der kantonalen Datenschutzbehörde. Ihre Stellung ist vergleichbar mit derjenigen der Finanzkontrolle: Beide Organisationseinheiten sind organisatorisch und institutionell unabhängig. Sie sind nur der Verfassung und dem Gesetz verpflichtet. Ihre Angliederung an die Verwaltung ist lediglich administrativ, ihre Leitung wird durch den Grossen Rat gewählt und hat die personalrechtliche Stellung eines hauptamtlichen Behördenmitglieds. Die Leitung untersteht der Aufsicht des Grossen Rates und führt eine separate Rechnung. Die kantonale Datenschutzbehörde ist in fachlicher, organisatorischer, personeller und finanzieller Hinsicht weisungsungebunden, was ihr eine von der Verwaltung unabhängige Stellung verleiht. Das könnte darauf hindeuten, dass ihr eine eigene Stellung ausserhalb der Verwaltung zukommt, ähnlich der Gerichte. Wie bereits der Vortrag zur Änderung des KDSG 2008 aber zu Recht festhält, soll die Unabhängigkeit der kantonalen Datenschutzbehörde nicht dazu führen, dass sie zu einer unkontrollierten «vierten Gewalt» oder gar zu einem «Staat im Staat» werde. Folgerichtig muss die kantonale Datenschutzbehörde einer der drei Gewalten Legislative, Judikative und Exekutive zugeordnet werden, wobei sinnvollerweise nur die Exekutive in Frage kommt. Demzufolge kann die kantonale Datenschutzbehörde als selbständige Organisationseinheit der Verwaltung bezeichnet werden. Sie steht nicht ausserhalb der Verwaltung, sondern gehört als eigenständiger Teil zur Verwaltung.

In Angleichung an die Finanzkontrolle soll der Titel 2a mit «kantonale Datenschutzbehörde» ergänzt und ein zusätzlicher Artikel 40b analog zu demjenigen der Finanzkontrolle geschafften werden, der die kantonale Datenschutzbehörde als selbständige Organisationseinheit bezeichnet. Aus der Systematik ergibt sich ausserdem, dass die kantonale Datenschutzbehörde zur Verwaltung gehört.

7.9.5 Polizeigesetz (PolG) vom 10. Februar 2019[68]; indirekte Änderung

In Angleichung an das übergeordnete Recht soll die oder der Datenschutzverantwortliche gemäss Artikel 150 Absatz 1 PolG neu als Datenschutzberaterin oder Datenschutzberater bezeichnet werden.

In Artikel 141 PolG ist ausserdem der Verweis auf die kantonale Datenschutzgesetzgebung anzupassen.

[67] BSG 152.01
[68] BSG 555.1

7.9.6 Gesetz vom 9. März 2021 über die sozialen Leistungsangebote (SLG)[69] und Kantonales Geldspielgesetz vom 10. Juni 2020 (KGSG)[70]; indirekte Änderung

Das geltende Recht nennt lediglich Massnahmen über die fürsorgerische Betreuung als besonders schützenswerte Personendaten, jedoch fielen bereits nach heutigem Verständnis grundsätzlich Massnahmen des Kindes- und Erwachsenenschutzes darunter[71]. Dazu zählen etwa Angaben über eine fürsorgerische Unterbringung. In der bernischen Gesetzgebung ist der Begriff bereits teilweise angepasst worden, so beispielsweise in Art. 57d Abs. 4 des Gesetzes über die öffentliche Sozialhilfe (Sozialhilfegesetz, SHG)[72]. Mit der Revision soll die fürsorgerische Betreuung auch in Art. 71 des Kantonalen Geldspielgesetzes (KGSG)[73] und in Art. 111 Abs. 2 des Gesetzes über die sozialen Leistungsangebote (SLG)[74] mit Massnahmen des Kindes- und Erwachsenenschutzes ersetzt werden (vgl. Art. 2 Abs. 1 Ziff. 6 VE-revKDSG).

7.9.7 Anpassungen an den neuen Erlasstitel (indirekte Änderungen)

Folgende Gesetze verweisen pauschal auf das kantonale Datenschutzgesetz oder auf bestimmte Bestimmungen desselben. Mit der Änderung des Erlasstitels sind diese Verweise anzupassen. Soweit möglich, soll der Verweis mittels Sprache und dynamisch erfolgen, ohne sich auf den bestimmten Artikel zu beziehen. Dies vereinfacht spätere Gesetzesänderungen. Folgende indirekten Änderungen sind nötig:

- Artikel 29 des Informations- und Medienförderungsgesetzes vom 2. November 1993 (IMG)[75]
- Artikel 14 und Artikel 20 des Gesetzes vom 31. März 2009 über die Archivierung (ArchG)[76]
- Artikel 2, Artikel 4, Artikel 7, Artikel 11, Artikel 13, Artikel 15 und Art. A1-1 des Gesetzes vom 10. März 2020 über die zentralen Personendatensammlungen (PDSG)[77]
- Artikel 12a des Personalgesetzes vom 16. September 2004 (PG)[78]
- Artikel 35 des Gesetzes vom 18. Mai 2014 über die Pensionskassen (PKG)[79]
- Artikel 23 des Gesetzes vom 23. Mai 1989 über die Verwaltungsrechtspflege (VRPG)[80]
- Artikel 55 des Gesetzes vom 1. Februar 2012 über den Kindes- und Erwachsenenschutz (KESG)[81]
- Artikel 3 des Einführungsgesetzes vom 11. Juni 2009 zur Zivilprozessordnung, zur Strafprozessordnung und zur Jugendstrafprozessordnung (EG ZSJ)[82]
- Artikel 130 des Spitalversorgungsgesetzes vom 13. Juni 2013 (SpVG)[83]
- Artikel 57g und Artikel 80g des Gesetzes vom 11. Juni 2001 über die Sozialhilfe (SHG)[84]
- Artikel 46 und Artikel 51 des Gesetzes vom 3. Dezember 2019 über die Sozialhilfe im Asyl- und Flüchtlingsbereich (SAFG)[85]

Zu den indirekten Änderungen des DVG, GNA, EG AIG und AsylG, OrG SLG und KGSG vgl. Ziff. 7.9.1 bis 7.9.6.

[69] BSG 860.2
[70] BSG 935.52
[71] vgl. Rudin, Beat (2014), s.o. § 3 N. 38.
[72] BSG 860.1
[73] BSG 935.52
[74] BSG 860.2
[75] BSG 107.1
[76] BSG 108.1
[77] BSG 152.05
[78] BSG 153.01
[79] BSG 153.41
[80] BSG 155.21
[81] BSG 213.316
[82] BSG 271.1
[83] BSG 812.11
[84] BSG 860.1
[85] BSG 861.1

8. Verhältnis zu den Richtlinien der Regierungspolitik (Rechtsetzungsprogramm) und anderen wichtigen Planungen

Die Revision entspricht dem Ziel 2 der Richtlinien der Regierungspolitik, wonach der Kanton Bern die digitale Transformation nutzt, um wirkungsvolle, qualitativ hochstehende und effiziente Dienstleistungen zu erbringen. Zu diesem Ziel trägt das kantonale Datenschutzgesetz bei, indem die kantonale Datenschutzbehörde die Aufgaben der kommunalen Datenschutzbehörden – mit Ausnahme der vier bevölkerungsstärksten Gemeinden – übernimmt. Dabei werden die Gemeinden von den heute bestehenden und künftigen Herausforderungen der Digitalisierung entlastet und die Aufsicht professionalisiert. Das gebündelte Know-how führt nicht nur zu mehr Effizienz, sondern auch zu einer professionellen Anlaufstelle für Gemeindebehörden und Bürger.

9. Finanzielle Auswirkungen

Die zwingenden Anpassungen ans übergeordnete Recht ziehen Kosten nach sich. Insbesondere die Möglichkeit der Datenschutzbehörde Verfügungen zu erlassen und die überwiegende Zentralisierung der gemeinderechtlichen Aufsicht beim Kanton werden zu einem grösseren Mittelbedarf führen. Die zusätzlichen Aufwendungen beim Kanton werden jedoch durch den Lastenausgleich abgegolten (vgl. Erläuterungen zu Art. 57 VE-revKDSG). Die eigeführte Datenschutzfolgenabschätzung entspricht grösstenteils der bereits heute durchzuführenden ISDS-Analyse und dem ISDS-Konzept, weshalb hier kein bedeutender Mehraufwand entstehen sollte. Die neuen Informations- und Meldepflichten können im Einzelfall zwar zusätzliche Aufwendungen bei den Behörden auslösen. Die Kosten sollten jedoch mit den bestehenden Mitteln abgedeckt werden können.

10. Personelle und organisatorische Auswirkungen

Infolge der Zentralisierung der gemeinderechtlichen Aufsicht benötigt die kantonale Datenschutzbehörde ca. 400 zusätzliche Stellenprozente. Der Mehraufwand wird über das Lastenausgleichssystem abgerechnet (Erläuterungen zu Art. 57 VE-revKDSG).

11. Auswirkungen auf die Gemeinden

Für die Gemeinden – mit Ausnahme der vier bevölkerungsstärkten Gemeinden – verringert sich der Aufwand mit der Zentralisierung der kantonalen Datenschutzbehörde. In finanzieller Hinsicht tragen sie die Mehraufwände des Kantons über das Lastenausgleichssystem mit. Der anfallende Betrag dürfte jedoch deutlich geringer sein als bisher.

12. Auswirkungen auf die Volkswirtschaft

Das kantonale Datenschutzgesetz richtet sich direkt nur an die Behörden des Kantons Bern. Dritte, insbesondere Unternehmen, werden nur indirekt vom Gesetz erfasst, wenn sie im Auftrag des Kantons handeln. In diesem Fall dürfen die beauftragten Dritten Personendaten nur so bearbeiten, wie es ihr Auftraggeber tun dürfte. Insofern müssen sie sich ebenfalls an die datenschutzrechtlichen Bestimmungen halten. Die Beurteilung anhand der Regulierungscheckliste hat ergeben, dass die Vorlage keine relevanten Auswirkungen auf die administrative oder finanzielle Belastung von Unternehmen oder auf die Volkswirtschaft insgesamt hat.

13. Ergebnis des Vernehmlassungsverfahrens

[Text folgt nach Vernehmlassungsverfahren]

14. Antrag

Der Regierungsrat beantragt dem Grossen Rat, den Entwurf des Datenschutzgesetzes (KDSG) zu beschliessen.