



# Vortrag

Datum RR-Sitzung: 13. November 2024  
Direktion: Direktion für Inneres und Justiz  
Geschäftsnummer: 2019.JGK.647  
Klassifizierung: Nicht klassifiziert

## Kantonales Datenschutzgesetz (KDSG)

### Inhaltsverzeichnis

|       |                                                                                                                                                                                                                                     |    |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| 1.    | <b>Zusammenfassung</b>                                                                                                                                                                                                              | 2  |
| 2.    | <b>Ausgangslage</b>                                                                                                                                                                                                                 | 3  |
| 2.1   | Auswirkungen der europäischen Rechtsentwicklungen auf die Schweiz                                                                                                                                                                   | 3  |
| 2.2   | Umsetzung auf Bundesebene                                                                                                                                                                                                           | 4  |
| 2.3   | Umsetzung auf kantonaler Ebene                                                                                                                                                                                                      | 4  |
| 3.    | <b>Grundzüge der Neuregelung</b>                                                                                                                                                                                                    | 5  |
| 3.1   | Grundsatz                                                                                                                                                                                                                           | 5  |
| 3.2   | Geltungsbereich                                                                                                                                                                                                                     | 5  |
| 3.3   | Aktualisierung des Katalogs der besonders schützenswerten Personendaten                                                                                                                                                             | 6  |
| 3.4   | Transparenzbestimmungen                                                                                                                                                                                                             | 6  |
| 3.5   | Register der Datensammlungen und Verzeichnis der Bearbeitungstätigkeiten                                                                                                                                                            | 6  |
| 3.6   | Aufsichtsbereich                                                                                                                                                                                                                    | 7  |
| 3.7   | Gesetzessystematik                                                                                                                                                                                                                  | 7  |
| 3.8   | Revision weiterer Gesetze                                                                                                                                                                                                           | 8  |
| 3.8.1 | Revision Facherlasse                                                                                                                                                                                                                | 8  |
| 3.8.2 | Gesetz vom 7. März 2022 über die digitale Verwaltung (DVG)                                                                                                                                                                          | 8  |
| 3.8.3 | Gesetz vom 12. September 1985 über Niederlassung und Aufenthalt der Schweizerinnen und Schweizer (NAG) und das Einführungsgesetz vom 9. Dezember 2019 zum Ausländer- und Integrationsgesetz sowie zum Asylgesetz (EG AIG und AsylG) | 9  |
| 3.8.4 | Gesetz vom 20. Juni 1995 über die Organisation des Regierungsrates und der Verwaltung (Organisationsgesetz, OrG)                                                                                                                    | 9  |
| 3.9   | Verworfen Bestimmungen                                                                                                                                                                                                              | 9  |
| 3.9.1 | Versuchsverordnung                                                                                                                                                                                                                  | 9  |
| 3.9.2 | Datenschutzberaterin oder Datenschutzberater                                                                                                                                                                                        | 9  |
| 3.9.3 | Haftungsbestimmung                                                                                                                                                                                                                  | 10 |
| 4.    | <b>Erlassform</b>                                                                                                                                                                                                                   | 10 |
| 5.    | <b>Rechtsvergleich</b>                                                                                                                                                                                                              | 11 |
| 5.1   | Kanton Aargau                                                                                                                                                                                                                       | 11 |
| 5.2   | Kanton St. Gallen                                                                                                                                                                                                                   | 11 |
| 5.3   | Kanton Zürich                                                                                                                                                                                                                       | 11 |
| 5.4   | Kanton Luzern                                                                                                                                                                                                                       | 12 |
| 5.5   | Fazit                                                                                                                                                                                                                               | 12 |
| 6.    | <b>Umsetzung, geplante Evaluation des Vollzugs</b>                                                                                                                                                                                  | 12 |
| 7.    | <b>Erläuterungen zu den Artikeln</b>                                                                                                                                                                                                | 13 |
| 7.1   | Allgemeine Bestimmungen                                                                                                                                                                                                             | 13 |
| 7.2   | Bearbeiten von Personendaten                                                                                                                                                                                                        | 22 |
| 7.3   | Pflichten der Behörden und von beauftragten Dritten                                                                                                                                                                                 | 38 |
| 7.4   | Rechte der betroffenen Person                                                                                                                                                                                                       | 45 |

|         |                                                                                                                                                                                                                                                                        |           |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| 7.5     | Datenschutzbehörden .....                                                                                                                                                                                                                                              | 48        |
| 7.6     | Verfahren und Rechtsschutz .....                                                                                                                                                                                                                                       | 59        |
| 7.7     | Ausführungsbestimmungen .....                                                                                                                                                                                                                                          | 60        |
| 7.8     | Übergangs- und Schlussbestimmungen .....                                                                                                                                                                                                                               | 61        |
| 7.8.1   | Übergangsbestimmungen .....                                                                                                                                                                                                                                            | 61        |
| 7.9     | Änderungen anderer Erlasse .....                                                                                                                                                                                                                                       | 63        |
| 7.9.1   | Datenschutzgesetz (KDSG) vom 19. Februar 1986 .....                                                                                                                                                                                                                    | 63        |
| 7.9.2   | Gesetz vom 7. März 2022 über die digitale Verwaltung (DVG); indirekte<br>Änderung .....                                                                                                                                                                                | 63        |
| 7.9.3   | Gesetz vom 12. September 1985 über Niederlassung und Aufenthalt der<br>Schweizerinnen und Schweizer (NAG) und das Einführungsgesetz vom 9.<br>Dezember 2019 zum Ausländer- und Integrationsgesetz sowie zum<br>Asylgesetz (EG AIG und AsylG); indirekte Änderung ..... | 63        |
| 7.9.4   | Gesetz vom 20. Juni 1985 über die Organisation des Regierungsrates und<br>der Verwaltung (Organisationsgesetz, OrG); indirekte Änderung .....                                                                                                                          | 64        |
| 7.9.5   | Polizeigesetz (PolG) vom 10. Februar 2019; indirekte Änderung .....                                                                                                                                                                                                    | 64        |
| 7.9.6   | Gesetz vom 9. März 2021 über die sozialen Leistungsangebote (SLG) und<br>Kantonales Geldspielgesetz vom 10. Juni 2020 (KGSG); indirekte Änderung .....                                                                                                                 | 64        |
| 7.9.7   | Anpassungen an den neuen Erlassstitel (indirekte Änderungen) .....                                                                                                                                                                                                     | 65        |
| 7.9.8   | Anpassungen des französischen Begriffs für besonders schützenswerte<br>Personendaten (indirekte Änderungen) .....                                                                                                                                                      | 65        |
| 8.      | <b>Verhältnis zu den Richtlinien der Regierungspolitik<br/>(Rechtssetzungsprogramm) und anderen wichtigen Planungen .....</b>                                                                                                                                          | <b>67</b> |
| 9.      | <b>Finanzielle Auswirkungen .....</b>                                                                                                                                                                                                                                  | <b>67</b> |
| 10.     | <b>Personelle und organisatorische Auswirkungen .....</b>                                                                                                                                                                                                              | <b>68</b> |
| 11.     | <b>Auswirkungen auf die Gemeinden .....</b>                                                                                                                                                                                                                            | <b>68</b> |
| 12.     | <b>Auswirkungen auf die Volkswirtschaft .....</b>                                                                                                                                                                                                                      | <b>68</b> |
| 13.     | <b>Ergebnis des Vernehmlassungsverfahrens .....</b>                                                                                                                                                                                                                    | <b>68</b> |
| 13.1    | Geltungsbereich für juristische Personen .....                                                                                                                                                                                                                         | 68        |
| 13.2    | Begriffsdefinitionen .....                                                                                                                                                                                                                                             | 69        |
| 13.3    | Rechtsgrundlage für die Bearbeitung von Personendaten .....                                                                                                                                                                                                            | 70        |
| 13.4    | Bekanntgabe ins Ausland: Variantenvorschlag .....                                                                                                                                                                                                                      | 71        |
| 13.5    | Aufbewahrung, Vernichtung und Archivierung .....                                                                                                                                                                                                                       | 72        |
| 13.6    | Risikoanalyse bei geplanten, wiederkehrende Bearbeitungen .....                                                                                                                                                                                                        | 72        |
| 13.7    | Datensammlungen bzw. Registerpflicht .....                                                                                                                                                                                                                             | 72        |
| 13.8    | Meldepflichten bei Verletzungen der Datensicherheit .....                                                                                                                                                                                                              | 72        |
| 13.9    | Zentralisierung Datenschutzbehörden .....                                                                                                                                                                                                                              | 73        |
| 13.10   | Verwaltungsmassnahmen .....                                                                                                                                                                                                                                            | 73        |
| 13.10.1 | Rechtsmittelweg .....                                                                                                                                                                                                                                                  | 73        |
| 13.11   | Verfügungskompetenz gegenüber Gerichten und der Staatsanwaltschaft .....                                                                                                                                                                                               | 74        |
| 14.     | <b>Antrag .....</b>                                                                                                                                                                                                                                                    | <b>75</b> |

## 1. Zusammenfassung

Das Recht auf Datenschutz ist ein Grundrecht. Die Verfassung des Kantons Bern (KV)<sup>1</sup> konkretisiert das in Artikel 13 Absatz 2 der Bundesverfassung vom 18. April 1999 (BV)<sup>2</sup> enthaltene Recht auf informationelle Selbstbestimmung in Artikel 18 als Recht auf Datenschutz. Dies verdeutlicht seine Relevanz. Des- sen Ursprung ist auf die Angst vor der Kontrolle des Individuums durch den Staat («gläserner Mensch») zurückzuführen. Das Grundrecht auf Datenschutz ist verfassungskonform umgesetzt, wenn Behörden Personendaten sachgerecht und transparent bearbeiten, die betroffenen Personen um deren Bearbei- tung wissen und sie gegen widerrechtliche Bearbeitungen vorgehen können.

<sup>1</sup> BSG 101.1

<sup>2</sup> SR 101

Für Bundesbehörden und Private ist das Bundesgesetz vom 25. September 2020 über den Datenschutz (Datenschutzgesetz, DSG)<sup>3</sup> anwendbar; für kantonale und kommunale Behörden richtet sich die Bearbeitung von Personendaten nach deren Datenschutzgesetzen.

Beim Datenschutzrecht handelt es sich um eine Querschnittsmaterie. Folglich regelt das kantonale Datenschutzgesetz vom 19. Februar 1986 (KDSG)<sup>4</sup> 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 Geltungsauschluss 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 Behörden werden erweitert und die Rechte der betroffenen Personen klarer definiert. Der Aufwand der 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)<sup>5</sup> und die Richtlinie (EU) 2016/680<sup>6</sup>. Am 10. Oktober 2018 beschloss der Europarat ausserdem das Zusatzprotokoll<sup>7</sup> zum Übereinkommen vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (nachfolgend:

---

<sup>3</sup> SR 235.1

<sup>4</sup> BSG 152.04

<sup>5</sup> 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).

<sup>6</sup> 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.

<sup>7</sup> BBl 2020, S. 599

SEV Nr. 108+), das die Bundesversammlung am 19. Juni 2020 genehmigte.<sup>8</sup> 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 zum 1. August 2018. Der Kanton Bern setzte die Anforderungen mit der Einführungsverordnung vom 4. Juli 2018 zur EU-Datenschutzrichtlinie (EV EDS)<sup>9</sup> 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, DSG)<sup>10</sup> ist seit dem 1. September 2023 in Kraft. Gleichzeitig wurde das Schengen-Datenschutzgesetz<sup>11</sup> aufgehoben, welches bis dahin die Schengen-Acquis gewährleistet hat.

## **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»,

---

<sup>8</sup> BBl 2020, S. 5725

<sup>9</sup> BSG 152.043

<sup>10</sup> BBl 2020, S. 7639

<sup>11</sup> Vollständiger Name: Bundesgesetz über den Datenschutz im Rahmen der Anwendung des Schengen-Besitzstands in Strafsachen» (Schengen-Datenschutzgesetz, SDSG).

- 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.

### **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 mit hohem Risiko,
- 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**

Das Datenschutzgesetz gilt für jedes Bearbeiten von Personendaten sowohl von natürlichen als auch juristischen Personen durch Behörden. Sofern die Behörde Daten juristischer Personen bearbeitet, gelten jedoch gewisse Ausnahmen (Art. 3 Abs. 1 Bst. b E-KDSG).

Eine grundsätzliche Ausnahme für die Anwendung des Datenschutzgesetzes 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 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 auch gegenüber den Gerichten und der Staatsanwaltschaft Verwaltungsmassnahmen ergreifen, soweit das Datenschutzgesetz auf sie anwendbar ist.

### **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 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 Bearbeitung voraussichtlich ein hohes Risiko für die betroffene Person birgt und folglich eine Datenschutzfolgenabschätzung durchzuführen ist, 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 betroffenen Personen führt. Das kantonale Datenschutzrecht stellt mehrere Instrumente zur Verfügung, die solche Verletzungen verhindern sollen (Datenschutzfolgenabschätzung, 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 Behörde 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 kontrollierend 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 andere 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 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 Grösse 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 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 |                               | E-KDSG |                                                                                                                                                                                                                         |
|------|-------------------------------|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Allgemeine Bestimmungen       | 1      | Allgemeine Bestimmungen                                                                                                                                                                                                 |
| 2    | Bearbeiten von Personendaten  | 2      | Bearbeitung von Personendaten                                                                                                                                                                                           |
|      |                               |        | 2.1 Grundsätze<br>2.2 Besondere Bearbeitungsformen<br>2.3 Bearbeitung für nicht personenbezogene Zwecke                                                                                                                 |
| 3    | Datensammlungen               | 3      | Pflichten der Behörden und von beauftragten Dritten<br>3.1 Pflichten vor Inbetriebnahme<br>3.2 Register- und Verzeichnispflicht<br>3.3 Informationspflichten<br>3.4 Meldepflichten bei Verletzungen der Datensicherheit |
| 4    | Rechte der betroffenen Person | 4      | Rechte der betroffenen Person                                                                                                                                                                                           |
| 6    | Aufsicht                      | 5      | Datenschutzbehörden                                                                                                                                                                                                     |
|      |                               |        | 5.1 Kantonale Datenschutzbehörde<br>5.2 Gemeinderechtliche und landeskirchliche Datenschutzbehörde<br>5.3 Aufgaben                                                                                                      |
| 5    | Verfahren und Rechtsschutz    | 6      | Verfahren und Rechtsschutz                                                                                                                                                                                              |
|      |                               | 7      | Ausführungsbestimmungen                                                                                                                                                                                                 |
| 7    | Schlussbestimmungen           | 8      | Übergangs- und Schlussbestimmungen<br>8.1 Übergangsbestimmungen<br>8.2 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<sup>12</sup>.

Das kantonale Datenschutzgesetz ist ein sogenanntes Querschnittsgesetz. 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 E-KDSG). In folgenden Gesetzen hat die Revision inhaltliche Änderungen zur Folge:

#### 3.8.2 Gesetz vom 7. März 2022 über die digitale Verwaltung (DVG)<sup>13</sup>

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

<sup>12</sup> vgl. zum Ganzen Rechtsetzungstechnische Richtlinien, Modul 3, Ziff. 2.2.4.2.

<sup>13</sup> BSG 109.1



### **3.8.3 Gesetz vom 12. September 1985 über Niederlassung und Aufenthalt der Schweizerinnen und Schweizer (NAG)<sup>14</sup> und das Einführungsgesetz vom 9. Dezember 2019 zum Ausländer- und Integrationsgesetz sowie zum Asylgesetz (EG AIG und AsylG)<sup>15</sup>**

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 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 1995 über die Organisation des Regierungsrates und der Verwaltung (Organisationsgesetz, OrG)<sup>16</sup>**

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 geschaffen werden, der die kantonale Datenschutzbehörde als selbstständige Organisationseinheit bezeichnet. Aus der Systematik ergibt sich ausserdem, dass die kantonale Datenschutzbehörde zur Verwaltung gehört. Mehr dazu unter Ziff. 7.9.4.

## **3.9 Verworfenne 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)<sup>17</sup> 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 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

---

<sup>14</sup> BSG 122.11

<sup>15</sup> BSG 122.20

<sup>16</sup> BSG 152.01

<sup>17</sup> BSG 101.1

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)<sup>18</sup>, 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 DSG) und sollen mit der Revision der kantonalen Datenschutzverordnung künftig gleich bezeichnet werden. Gemäss Artikel 150 des Polizeigesetzes (PolG) vom 10. Februar 2019<sup>19</sup> 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 Justizverwaltungsleitung 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 KD SG). Es handelt sich dabei um eine spezialgesetzliche Norm, die grundsätzlich den allgemeinen Regeln vorgeht. Die Bestimmung stimmt inhaltlich jedoch mit dem allgemeinen Staatshaftungsrecht überein, weshalb ihr keine eigenständige Bedeutung zukommt.<sup>20</sup> Insbesondere haftet der Kanton gestützt auf Art. 100 des Personalgesetzes (PG)<sup>21</sup> auch für Schäden, die beauftragte Dritte verursacht haben. Das Verwaltungsgericht hat ausdrücklich entschieden, dass sich der Kanton das Handeln von Hilfspersonen auch ohne ausdrückliche gesetzliche Grundlage anrechnen lassen muss.<sup>22</sup> Die Bestimmung ist daher nicht ins neue Recht zu überführen. Die allgemeinen Staatshaftungsbestimmungen nach PG sind sinngemäss anwendbar.

## 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 der Bearbeitung 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.

---

<sup>18</sup> BSG 152.040.1

<sup>19</sup> BSG 551.1

<sup>20</sup> BVR 2008 S. 49 E. 6.6.2; Schwegler, Ivo (2021): Informations- und Datenschutzrecht. In: Müller, Markus /Feller, Reto (Hrsg.), Kommentar zum bernischen Verwaltungsverfahren. Bern: Stämpfli Verlag AG: S. 396.

<sup>21</sup> BSG 153.01

<sup>22</sup> BVR 2003 S. 241 E. 6e

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 Innerrhoden, Basel-Land, Freiburg, Luzern, St. Gallen, Schaffhausen, Schwyz, Zug und Zürich sind die Anpassungen an die europäischen Grundlagen per Mitte 2022 ebenfalls vollzogen worden. 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 übergeordnete 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 betroffene 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 Daten-

schutzfolgenabschätzung, 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 Bearbeitung 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 Bearbeitungen 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. Um eine wirksame Umsetzung des Gesetzes zu gewährleisten, soll dessen Wirkung evaluiert werden. Die Evaluation erfolgt mittels Bericht des Regierungsrates an den Grossen Rat vier Jahre nach Inkrafttreten dieses Gesetzes.

## 7. Erläuterungen zu den Artikeln

### 7.1 Allgemeine Bestimmungen

#### **Titel**

Es besteht eine gewisse Verwechslungsgefahr zum neuen Bundesgesetz über den Datenschutz, welches 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 die Kantonsverfassung in Artikel 18 KV als Recht auf Datenschutz konkretisiert hat. 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).

Anders als das Bundesdatenschutzgesetz ist das kantonale Datenschutzgesetz nicht auf Private anwendbar, weshalb der Schutz der Persönlichkeitsrechte im Zweckartikel des kantonalen Datenschutzgesetzes nicht erwähnt wird. Vielmehr wird ausdrücklich festgehalten, dass der Zweck des Gesetzes der Schutz des Grundrechts auf Datenschutz von Personen ist, über die Behörden Personendaten bearbeiten.

Anders als die internationalen Vorgaben (und die meisten europäischen Staaten) schützen die schweizerischen Datenschutzgesetze bisher juristische und natürliche Personen, was sich auch im Zweckartikel widerspiegelt. Das vom Bund verabschiedete Datenschutzgesetz verzichtet nun auf den Einbezug der juristischen Personen (Art. 1 und Art. 2 Abs. 1 DSG), führt jedoch für die Bearbeitung von deren Personendaten eine Reihe von Bestimmungen im Regierungs- und Verwaltungsorganisationsgesetz vom 21. März 1997 (RVOG)<sup>23</sup> 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 juristischer Personen einzufügen. Das wäre zudem nur mit grossem Aufwand umsetzbar. Im kantonalen Recht gibt es keinen Erlass, der auf sämtliche Behörden anwendbar ist: Das Organisationsgesetz ist auf Gemeinden nicht anwendbar, das Gemeindegesetz nicht auf gewisse kirchliche Institutionen. Auch für Private, die öffentliche Aufgaben übernehmen, gibt es keinen einheitlichen Erlass. Die Bestimmungen zum Schutz juristischer Personen müssten deshalb in diversen Erlassen eingefügt werden, wobei das Risiko bestünde, dass nicht sämtliche einschlägigen Erlasse entsprechend ergänzt würden. Nach Artikel 5 der Bundesverfassung ist die Grundlage staatlichen Handelns das Recht. Erliesse der Kanton Bern also keine spezialgesetzlichen Regelungen, die den Behörden die Bearbeitung von Daten juristischer Personen 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 sta-

---

<sup>23</sup> SR 172.010

tiert 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. Den Geltungsbereich auf natürliche Personen zu beschränken ist nicht sinnvoll. Ebenso verzichten beispielsweise die Kantone Zürich, Freiburg oder Schwyz darauf. Andere Kantone, die den Geltungsbereich auf natürliche Personen beschränken, führen gesonderte Bestimmungen in den Spezialgesetzen ein, so beispielsweise der Kanton Luzern.

## **Artikel 2 – Begriffe**

Die Begriffe stimmen grösstenteils mit der bisherigen Gesetzgebung überein, wobei einige Begriffe gestützt auf die Vernehmlassung an den Wortlaut des Bundesdatenschutzgesetzes angeglichen werden. Auf Ergänzungen und Abweichungen wird im Folgenden hingewiesen. Neu ist der Begriff des Profilings mit hohem Risiko. 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 nach Buchstaben und nicht nach Absätzen unterteilt.

### *Buchstabe a*

Im Gegensatz zum Datenschutzgesetz des Bundes gelten auch Angaben zu bestimmten oder bestimm-  
baren juristischen Personen als Personendaten (vgl. Erläuterungen zu Art. 1 E-KDSG).

### *Buchstabe b*

Spricht das kantonale Datenschutzgesetz von betroffenen Personen, meint es Personen, über die Perso-  
nendaten bearbeitet werden.

### *Buchstabe c*

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 des-  
halb erhöhte Anforderungen gelten (vgl. Art. 4 Abs. 2 E-KDSG). Es ist durchaus umstritten, ob der Ge-  
setzgeber gewisse Personendaten als besonders schützenswert definieren soll. Massgeblich soll statt-  
dessen das Gefährdungspotential für das Grundrecht auf Datenschutz sein. Die europäischen Vorgaben  
und der Bundesgesetzgeber behalten die Kategorien aber bei. Für die Gesetzesanwendung ist es durch-  
aus sinnvoll, eine Kategorie von besonders schützenswerten Personendaten festzulegen, bei der kraft  
Gesetzes erhöhte Anforderungen gelten, ohne dass bei jeder Bearbeitung das Gefährdungspotential ein-  
zeln geprüft werden muss. Die Aufzählung ist aus Gründen der Rechtssicherheit abschliessend.

Im französischen Text wird der Begriff «données particulièrement dignes de protection» durch den vom  
Bund verwendeten Begriff «données personnelles sensibles (données sensibles)» ersetzt; auf Deutsch  
stimmt die verwendete Terminologie bereits jetzt überein. Daraus ergeben sich verschiedene indirekte  
Änderungen.

### *Ziffer 1*

Bisher erwähnte das Gesetz die gewerkschaftliche Ansicht und Betätigung nicht explizit, weil sie zur poli-  
tischen 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. Die Begriffe «Zuge-  
hörigkeit und Betätigung» werden in Angleichung an den Bundesgesetzestext mit «Tätigkeit» ersetzt.

## 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.<sup>24</sup> 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.

Der Begriff der «ethnischen Herkunft» hat nichts gemeinsam mit den Begriffen der «Gesundheit und Intimsphäre», weshalb er weiterhin in einer eigenen Ziffer erwähnt wird.

## 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.<sup>25</sup>

Das Bundesgericht unterscheidet nach der «Drei-Säulen-Theorie»<sup>26</sup> zwischen der Intim- 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.

## 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. I des Bundesgesetzes vom 8. Oktober 2004 über genetische Untersuchungen beim Menschen [GUMG])<sup>27</sup>.

## 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, Angaben zur Motorik, Gangart oder Aufnahmen der Stimme. Diese Daten müssen zwingend auf

<sup>24</sup> vgl. Rudin, Beat (2014): Praxiskommentar zum IDG des Kanton Basel-Stadt. Zürich, Basel, Genf: Schulthess Juristische Medien AG: § 3 N 37 Fn. 71.

<sup>25</sup> 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.

<sup>26</sup> BGE 97 II 100 f., E. 3; 118 IV 45; 119 II 222 ff., E. 2b.

<sup>27</sup> SR 810.12

einem spezifischen technischen Verfahren beruhen, das die eindeutige Identifizierung oder Authentifizierung einer Person erlaubt. Dies ist beispielsweise grundsätzlich nicht der Fall bei gewöhnlichen Fotografien.<sup>28</sup>

#### *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.<sup>29</sup>

Im Gegensatz zum Bund nennt das kantonale 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<sup>30</sup>. 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 Erwachsenenschutzes 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 oder die Beschlagnahme von Tieren darunter.

#### *Buchstabe d*

Bisher kennt das kantonale Datenschutz keine Definition für besonders schützenswerte Personendaten juristischer Personen. Hier wird die Definition des Bundesgesetzgebers übernommen. Inwiefern das kantonale Datenschutzgesetz auf juristische Personen anwendbar ist, ergibt sich aus dem Geltungsbereich (vgl. Erläuterungen zu Art. 3 Abs. 1 Bst. b E-KDSG).

#### *Buchstabe e*

Der Begriff der Datensammlung ist aus dem bisherigen Recht zu übernehmen. Die kantonalen Behörden melden ihre Datensammlungen der kantonalen Datenschutzbehörde, welche sie in einem Register veröffentlicht (Art. 42 Abs. 2 E-KDSG).

#### *Buchstabe f*

Der Begriff des «Bearbeitens» weicht in etlichen Punkten von demjenigen des Bundes ab. In Angleichung an das Bundesgesetz wird die Begriffsdefinition ergänzt mit «unabhängig von den angewendeten Mitteln» und mit weiteren Bearbeitungsformen wie das «Speichern», «Verwenden», «Archivieren» und

<sup>28</sup> BBl 2017, S. 7020 Ziff. 9.1.3.1

<sup>29</sup> vgl. Rudin, Beat (2015). In: Baeriswyl, Bruno/Pärli, Kurt (Hrsg.), Datenschutzgesetz (DSG). Bern: Stämpfli Verlag AG: Art. 3 N. 27.

<sup>30</sup> vgl. für den Kanton Basel-Stadt zum Begriff Massnahmen der sozialen Hilfe: Rudin, Beat (2014), s.o., § 3 N. 38.



«Löschen». Wie im aktuellen Recht ist die Liste der möglichen Bearbeitungsvorgänge nicht abschliessend, weitere, nicht ausdrücklich erwähnte Vorgänge sind denkbar wie z.B. Sortieren, Verändern, Auswerten von Daten.

Artikel 3 Ziffer 4 der Richtlinie (EU) 2016/680 regelt neu das «Profiling» als besondere, «gefährliche» Art der Bearbeitung. Es handelt sich dabei nicht um ein spezielles Personendatum, sondern um eine Bearbeitungsart. Der Begriff des Profiling mit hohem Risiko wird in Buchstabe h definiert.

Der Begriff «Vernichten» ist stärker als der Begriff «Löschen» und impliziert, dass die Daten unwiederbringlich zerstört werden. Wenn die Daten auf Papier vorhanden sind, ist dieses zu verbrennen oder zu schreddern. Schwieriger gestaltet sich die Datenvernichtung bei elektronischen Daten. Übliche Löschbefehle oder eine reine Umformatierung stellen keine Vernichtung, sondern eine Löschung dar.<sup>31</sup>

#### *Buchstabe g*

Der Begriff des «Bekanntgebens» wird an den Bundesgesetzgeber angeglichen. Statt lediglich «Zugänglichmachen» wird neu das «Übermitteln» als Bekanntgabe aufgeführt. Die beispielhafte Aufzählung wird beibehalten, um die Tragweite des Begriffs zu verdeutlichen.

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 h*

Das Profiling ist eine bestimmte Bearbeitungsart, 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 Bundesdatenschutzgesetz auf den ersten Blick für die beiden Profilingvarianten keine gesonderten Anforderungen. So verlangt es für ein Profiling eine Grundlage in einem Gesetz im formellen Sinn (Art. 34 Abs. 2 Bst. b DSG). Hingegen reicht eine Grundlage in einem Gesetz im materiellen Sinn aus, wenn die Bearbeitung für eine in einem Gesetz im formellen Sinn festgelegte Aufgabe unentbehrlich ist *und* der Bearbeitungszweck keine besonderen Risiken für die Grundrechte der betroffenen Person birgt (Art. 34 Abs. 3 DSG). Auch der Kanton Bern anerkennt, dass nicht jedes Profiling mit einem hohen Risiko für die betroffene Person verbunden ist. Die Vernehmlassungsvorlage sah eine entsprechende Einschränkung analog der Bundeslösung bei der Rechtsgrundlage vor, insoweit als nur Profilings mit besonderen Risiken für die betroffene Person eine qualifizierte Gesetzesgrundlage erforderten (Art. 4 Abs. 2 E-KDSG). Eleganter ist es jedoch, nur das Profiling mit einem hohen Risiko analog des Bundesgesetzgebers zu definieren und nur für diese Profilingart qualifizierte Anforderungen an die Gesetzesgrundlage zu stellen (vgl. Art. 4 E-KDSG). So sieht es beispielsweise auch die Vorlage des Kantons Zürich vor (vgl. Art. 5 Abs. 4 Bst. c und Art. 25 Abs. 1 Bst. a E-IDG ZH). Damit wird auch der Kritik in der Vernehmlassung begegnet, dass unklar sei, wann hohe Risiken für ein Profiling vorlägen und wie diese im Verhältnis zum Profiling mit hohem Risiko des Bundes stünden. Fällt ein Profiling nicht unter die Begriffsdefinition des kantonalen Datenschutzgesetzes, so gelten die allgemeinen Anforderungen an die gesetzliche Grundlage, da dabei Personendaten oder unter Umständen auch besonders schützenswerte Personendaten bearbeitet werden (Art 4 E-KDSG). Dies widerspricht auch nicht den europäischen Grundlagen, da sie nur bei besonders schützenswerten Personendaten verlangen, dass deren Bearbeitung für die öffentliche Aufgabe unbedingt erforderlich sein muss und folglich nur dafür qualifizierte Anforderungen gelten (Art. 10 Richtlinie (EU) 2016/680).

Im Interesse einer einfachen Formulierung und Verständlichkeit weicht die Definition im kantonalen Datenschutzgesetz vom Begriff auf Bundesebene ab, enthält aber die Elemente des «Profilings», jedoch

---

<sup>31</sup> Zum Ganzen: BBl 2017, S. 7021

ergänzt um die «wesentlichen» Aspekte des «Profilings mit hohem Risiko». Massgeblich ist eine automatisierte Auswertung mit dem Ziel «wesentliche» Aspekte der betroffenen Person zu analysieren oder vorherzusagen. Von einem Profiling mit hohem Risiko ist beispielsweise auszugehen, wenn die Behörde ein Profil für den idealen Stellenbewerber definiert und anhand der eingereichten Lebensläufe, Zeugnisse, Qualifikationen, Assessments etc. automatisiert beurteilen lässt, wer diesem am besten entspricht.

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

#### *Buchstabe i*

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 (vgl. Art. 3 Abs. 3 E-KDSG).

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])<sup>32</sup>.

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])<sup>33</sup>. Die Organe der Gemeinde sind in Artikel 10 GG aufgeführt. Für die Umsetzung der datenschutzrechtlichen Anforderung sind auch auf kommunaler Ebene die Verwaltungseinheiten 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 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 Informationssicher-

---

<sup>32</sup> BSG 151.21

<sup>33</sup> BVR 2013 S. 251 E. 4.3

heit, 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-rechtlichen Aufgabe bearbeitet. Dasselbe gilt für die Gemeinden. Zu nennen sind hier etwa die Verkehrsbetriebe Biel oder Energie Wasser Bern.<sup>34</sup>

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)<sup>35</sup> anwendbar. Ebenfalls ausgenommen sind die Stimmberechtigten.

#### *Buchstabe k*

Die kantonale Aufsichtsstelle nennt sich neu kantonale Datenschutzbehörde und übernimmt grundsätzlich die Aufgaben der bisherigen gemeinderechtlichen Aufsichtsstellen (vgl. Erläuterungen zu Ziff. 3.6). Weiterhin über eigene Datenschutzbehörden verfügen die vier bevölkerungsstärksten Gemeinden (Biel/Bienne, Bern, Köniz und Thun) sowie die Landeskirchen. Die Bestimmungen des kantonalen Datenschutzgesetzes gelten für sämtliche Datenschutzbehörden, es sei denn das Gesetz sehe ausdrücklich vor, dass nur die kantonale Datenschutzbehörde betroffen ist.

#### *Nicht übernommene Bestimmungen:*

Es wird darauf verzichtet, den Begriff «verantwortliche Behörde» in die Begriffsbestimmungen aufzunehmen, da dieser im materiellen Recht definiert und für eine Legaldefinition zu lang ist (vgl. Art. 11 E-KDSG). Ebenfalls nicht definiert wird der Begriff «Auftragsbearbeiter» wie ihn der Bund kennt, da er nicht geschlechterneutral ist. Das kantonale Gesetz spricht vom «beauftragten Dritten».

### **Artikel 3 – Geltungsbereich**

#### *Absatz 1*

##### *Buchstabe a*

Wie bisher gilt das kantonale Datenschutzrecht grundsätzlich für jede Bearbeitung von Personendaten, und zwar unabhängig von den dabei angewendeten Mitteln und Verfahren. Für die Bearbeitung von Personendaten natürlicher Personen hält das Artikel 3 Absatz 1 Buchstabe a fest.

##### *Buchstabe b*

Das kantonale Datenschutzgesetz gilt für die Bearbeitung von Personendaten juristischer Personen nur soweit es sich aus der bernischen Verfassung ergibt. An dieser Stelle ist darauf hinzuweisen, dass die Berner Verfassung relativ weit geht. Artikel 18 KV statuiert neben den Betroffenenrechte (Abs. 1) auch, dass jede Bearbeitung von Personendaten eine gesetzliche Grundlage voraussetzt und die Bearbeitung für die Aufgabenerfüllung (=festgelegter Zweck) geeignet und notwendig (=Verhältnismässig) sein muss (Abs. 2). Ferner verpflichtet der Verfassungsgeber die Behörden, dass sie sich vergewissern, dass die bearbeiteten Daten richtig sind, und sie diese vor missbräuchlicher Verwendung zu schützen hat (Abs. 3). Im Übrigen ist auch der Bundesgesetzgeber der Meinung, dass auch juristische Personen Betroffenenrechte geltend machen können, auch wenn er dies nicht explizit im RVOG normiert.<sup>36</sup>

<sup>34</sup> 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.

<sup>35</sup> BSG 410.11

<sup>36</sup> BBl 2017, S. 7120

Das heisst, die im 2. Titel festgehaltenen Grundsätze des kantonalen Datenschutzgesetzes gelten qua Kantonsverfassung. Ebenfalls gelten die im 4. Kapitel aufgelisteten Rechte der betroffenen Personen. Ausnahmen sind möglich im 3. Titel (Pflichten der verantwortlichen Behörden und von beauftragten Dritten) und im 5. Titel (Datenschutzbehörde). Deshalb werden diese Titel vom Geltungsbereich für Personendaten juristischer Personen ausgenommen.

#### Absatz 2

Wie bisher unterstehen persönliche Notizen, die ausschliesslich zum persönlichen Gebrauch verwendet werden, nicht den Bestimmungen dieses Gesetzes. Nicht unter den Ausnahmetatbestand fallen Notizen, welche vorgesetzten, stellvertretenden oder nachfolgenden Personen dienen sollen.

#### Absatz 3

Bereits heute gilt das kantonale Datenschutzrecht nicht für das privatwirtschaftliche Handeln der Behörden. Soweit sie privatrechtlich handeln, sollen deshalb 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. Am wirtschaftlichen Wettbewerb nimmt eine Behörde teil, wenn sie ihre Leistungen auf dem Markt in Konkurrenz zu anderen anbietet und mit ihrem Handeln Gewinn erzielt. Das heisst, deren Vertragspartnerinnen und -partner müssen beim Vertragsabschluss frei sein und ihre Rechte und Pflichten dürfen sich nicht aus einer Verfügung oder einem verwaltungsrechtlichen Vertrag ergeben.<sup>37</sup> 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 nun explizit im kantonalen Datenschutzgesetz erwähnt wird. Es ist bloss sinngemäss anwendbar, weil das kantonale Recht den Anwendungsbereich des Bundesgesetzes nicht erweitern kann.

Da solche Behörden aber nicht Private werden, sondern nur wie Private handeln, unterstehen sie auch für privates Handeln der kantonalen Aufsicht. Der EDÖB erachtet sich nämlich nur zuständig zur Aufsicht über Bundesorgane und Privatpersonen. Einen aufsichtsfreien Raum gibt es nicht.<sup>38</sup> Die Aufsicht richtet sich nach den kantonalen Bestimmungen.

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 E-KDSG). Die Bestimmung betrifft folglich öffentlich-rechtlich konstituierte Behörden (Art. 2 Abs. 1 Bst. h Ziff. 1 und 3 E-KDSG).

#### Absatz 4

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 betroffenen Person; bei ersteren handelt es sich indes um Grundsätze des rechtsstaatlichen Handelns nach der Verfassung, die das kantonale Recht beachten muss.

Beim kantonalen Datenschutzgesetz handelt es sich um ein Querschnittsgesetz, welches durch Fachgesetze zu ergänzen ist oder deren Regeln als spezielleres Recht davon abweichen können. In diesem Sinne ergänzen die Verfahrensgesetze als bereichsspezifisches (oder materielles) Datenschutzrecht bereits heute das formelle Datenschutzrecht: Beispielsweise verlangt das Datenschutzrecht zur Bearbei-

---

<sup>37</sup> Rudin, Beat (2014), s.o.: § 2 N. 13.

<sup>38</sup> Rudin, Beat (2014), s.o.: § 2 N. 17.

tung von Personendaten eine gesetzliche Grundlage, die das Fachrecht, also das anwendbare Verfahrensrecht, liefert. Es ist im Einzelfall zu entscheiden, inwieweit das Spezialgesetz die Regeln des kantonalen Datenschutzgesetzes derogiert.

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 sämtlichen Verfahren vor Gerichtsbehörden und verwaltungsinternen Verwaltungsjustizbehörden. Die Verfahren vor Gerichtsbehörden umfassen sämtliche Verfahren vor Gerichten im Kanton Bern: Zivilprozesse, Strafprozesse und Verwaltungsprozesse vor gerichtlichen Behörden, eingeschlossen Rekurskommissionen. Die Formulierung richtet sich nach dem Gesetz über die Organisation der Gerichtsbehörden und der Staatsanwaltschaft (GSOG)<sup>39</sup>. Zusätzlich aufzuführen ist die Staatsanwaltschaft. Für Verwaltungsprozesse reicht es aus, wenn die Ausnahme auch für verwaltungsinterne Verwaltungsjustizbehörden gilt, davon sind sowohl die internen Beschwerdeinstanzen als auch interne Klageinstanzen nach Art. 60-73 und 88 des Gesetzes vom 23. Mai 1989 über die Verwaltungsrechtspflege (VRPG)<sup>40</sup> erfasst.

Anzumerken ist, dass auch allfällige spezialgesetzliche Bestimmungen ausserhalb der eigentlichen Verfahrensgesetze unter den Begriff «anwendbares Verfahrensrecht» fallen. Zu nennen sind etwa das Gesetz vom 1. Februar 2012 über den Kindes- und Erwachsenenschutz (KESG)<sup>41</sup> 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. Diese Verfahrensordnungen stellen 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.

Die Bearbeitung von Personendaten und die Rechte der betroffenen Person richtet sich in Verfahren vor den aufgeführten Behörden nach den anwendbaren Verfahrensordnungen, insbesondere nach der Schweizerischen Zivilprozessordnung vom 19. Dezember 2008 (Zivilprozessordnung, ZPO)<sup>42</sup>, nach der Schweizerischen Strafprozessordnung vom 5. Oktober 2007 (Strafprozessordnung, StPO)<sup>43</sup> und nach dem VRPG. Das heisst, dass die Rechte der betroffenen Person (4. Titel E-KDSG) während dem Verfahren ruhen und für die Informationsansprüche beispielsweise Artikel 53 ZPO, Artikel 107 f. StPO und Artikel 23 VRPG gelten. Sowohl Bearbeitungen des Gerichts gegenüber den Verfahrensbeteiligten als auch solche, 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 einflussenden Personendaten und zur allfälligen Berichtigung derselben sowie für die Bearbeitung im Rahmen der gerichtlichen Verfahren im Allgemeinen. Das bedeutet namentlich, dass die verschiedenen Rechtsbehelfe nach dem kantonalen Datenschutzgesetz weder gegenüber Bearbeitungen des Gerichts im Rahmen des Verfahrens noch gegenüber Bearbeitungen 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 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

---

<sup>39</sup> BSG 161.1

<sup>40</sup> 155.21

<sup>41</sup> BSG 213.316

<sup>42</sup> SR 272

<sup>43</sup> SR 312.0

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.<sup>44</sup> 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.<sup>45</sup> 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 kantonale Datenschutzgesetz Anwendung (Art. 3 Abs. 1 Bst. b des Einführungsgesetzes zur Zivilprozessordnung, zur Strafprozessordnung und zur Jugendstrafprozessordnung vom 11. Juni 2009 [EG ZSJ]<sup>46</sup>). Dies gilt auch für Verwaltungsverfahren, 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<sup>47</sup>) oder in einem anderen Facherlass eine genügende gesetzliche Grundlage besteht.

Im Umkehrschluss zu Absatz 4 ergibt sich, dass das kantonale Datenschutzrecht anwendbar ist auf Bearbeitungen 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.

In Verwaltungsverfahren (Verfahren auf Erlass einer Verfügung) gelten weiterhin die Bestimmungen des kantonalen Datenschutzgesetzes, weshalb die Verwaltungsbehörden nicht aufgeführt werden. Nach Buchstabe c gilt die Ausnahme vom kantonalen Datenschutzgesetz nur für Verfahren vor verwaltungsinternen Verwaltungsjustizbehörden.

## 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 «Rechtsgrundlage».

Jede Bearbeitung 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 die Bearbeitung 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

---

<sup>44</sup> Vgl. BBl 2017, S. 7013 Ziff. 9.1.2

<sup>45</sup> Vortrag des Regierungsrates zum Polizeigesetz (2017): S. 39 zu Art. 72.

<sup>46</sup> BSG 271.1

<sup>47</sup> SR 312.3

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.<sup>48</sup> Zu beachten ist, dass die Bearbeitung von besonders schützenswerten Personendaten und das Profiling mit hohem Risiko eine Grundlage in einem Gesetz bzw. einem Reglement erfordert (vgl. Abs. 2).

Die gesetzliche Grundlage kann unmittelbar oder mittelbar ausgestaltet sein: Die unmittelbare gesetzliche Grundlage regelt die Bearbeitung explizit, d.h. sie verpflichtet oder ermächtigt die Behörde, bestimmte Personendaten zu bearbeiten.<sup>49</sup> So regelt beispielsweise Artikel 39 Absatz 3 des Gesetzes vom 3. Dezember 2020 über die Leistungen für Kinder mit besonderem Förder- und Schutzbedarf (KFSG)<sup>50</sup>, 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 Behörde eine Aufgabe zu, welche sie nur durch das Bearbeiten von Personendaten erfüllen kann.<sup>51</sup> 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 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 fest. Im Unterschied zum geltenden Recht und zugunsten der Lesefreundlichkeit sind die unmittelbare und mittelbare gesetzliche Grundlage in zwei separate Buchstaben unterteilt.

Personendaten dürfen nach Buchstabe a nur bearbeitet werden, wenn dies gesetzlich vorgesehen ist (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 darf, wenn es der Erfüllung einer gesetzlichen Aufgabe dient (mittelbare gesetzliche Grundlage).

#### *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 das Profiling mit hohem Risiko (vgl. Erläuterungen zu Art. 2 Bst. h E-KDSG). Falls die Behörde nicht Personendaten auswertet, um wesentliche Aspekte einer natürlich Person zu analysieren oder vorherzusagen, bearbeitet sie dennoch Personendaten und sie benötigt dazu eine unmittelbare oder mittelbare Rechtsgrundlage nach Absatz 1. Die Behörde hat dies im Einzelfall zu beurteilen.

Zusätzlich zu den Anforderungen nach Absatz 1 darf eine Behörde besonders schützenswerte Personendaten nur bearbeiten oder ein Profiling mit hohem Risiko nur betreiben, wenn dazu eine Grundlage im Gesetz ermächtigt. Die Regelung auf Gesetzesstufe darf sich auf die Grundsätze beschränken, d.h. daraus muss sich ergeben, welche Behörde zu welchem Zweck welche besonderen Datenkategorien bearbeitet bzw. ein Profiling mit hohem Risiko betreibt. Die Gesetzesbestimmung muss aber nicht jeden Datenbearbeitungszweck oder sämtliche Datenbearbeitungen einzeln aufzählen. Das würde zu einer

<sup>48</sup> Wichtermann, Jürg (1999). In: Kommentar zum Gemeindegesetz des Kantons Bern. Bern: Stämpfli Verlag AG: Vorbem. zu Art. 50-60 N. 12.

<sup>49</sup> Rudin, Beat (2014), s.o.: § 9 N. 16.

<sup>50</sup> BSG 213.319

<sup>51</sup> Rudin, Beat (2014), s.o.: § 9 N. 17.

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. Je höher das Risiko für die betroffene Person ist, desto höher sind die Anforderungen an die Konkretisierung in der Verordnung.

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 Profiling mit einem hohen Risiko betreibt. Die Bearbeitung muss für die Aufgabenerfüllung «unentbehrlich» sein. Der Begriff «unentbehrlich» wird aus dem Bundesrecht übernommen (vgl. Wortlaut nach Art. 34 Abs. 3 Bst. a DSG). Eine materielle Änderung zum bisherigen Begriff «zwingend erforderlich» ergibt sich dadurch nicht. Der Bund fordert in diesen Fällen zusätzlich, dass der Bearbeitungszweck für die Grundrechte der betroffenen Person «keine besonderen Risiken» birgt. Diesbezüglich ist die Bestimmung weniger streng als Art. 34 Abs. 3 DSG. Die betroffenen Personen müssen gestützt auf die Aufgabennormen und Zuständigkeitsvorschriften auf Gesetzesstufe abschätzen können, welche besonders schützenswerten Personendaten die Behörde zu welchem Zweck über sie bearbeitet oder zu welchem Zweck sie ein Profiling betreibt. Folglich muss die Aufgabennorm hinreichend bestimmt ausgestaltet sein. Müssen die betroffenen Personen nicht mit solchen Bearbeitungen rechnen, dann ist eine 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 Profiling mit hohem Risiko gelten.

Ebenfalls beizubehalten ist, dass eine Grundlage auf niedrigerer Stufe (Dekret oder Verordnung) genügt, wenn die betroffene Person in eine oder mehrere bestimmte Datenbearbeitungen ausdrücklich eingewilligt hat (Bst. c). Der Umfang und Zweck der Datenbearbeitungen muss hinreichend bestimmt sein. Nur so ist es möglich in mehrere gleichgelagerte oder verschiedene Bearbeitungen einzuwilligen. Ebenso ist es möglich, dass ein Bearbeitungszweck verschiedene Bearbeitungen erfordert. Die betroffene Person muss aber die Risiken abschätzen können. Generelle Einwilligungserklärungen oder Blanko-Einwilligungen sind ausgeschlossen. 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 Bearbeitungen, die zu einem schweren Eingriff in die Grundrechte führen können (Art. 34 Abs. 2 Bst. c DSG). Diese Anforderung ergibt sich aus der eidgenössischen und kantonalen Verfassung (Art. 36 Abs. 1 BV und Art. 28 Abs. 1 KV).

Der bisherige allgemeine Vorbehalt des Amtsgeheimnisses oder besonderer Geheimhaltungspflichten (Art. 5 Abs. 5 KDSG) entfällt. Soweit eine Behörde nach Art. 14 Abs. 1 und 2 zur Datenbekanntgabe gesetzlich ermächtigt ist, stellt weder das Amtsgeheimnis nach Art. 58 PG noch jenes nach Art. 320 StGB ein Hindernis für die Datenbekanntgabe dar (vgl. Art. 58 Abs. 5 PG und Art. 14 StGB).

Die besonderen Geheimhaltungspflichten nach der Spezialgesetzgebung (z.B. Sozialhilfegeheimnis) inkl. Berufsgeheimnisse (z.B. Arztgeheimnis) werden neu in den einzelnen Bestimmungen adressiert, bei denen sie zu beachten sind, so beispielsweise bei der Datenbekanntgabe.



## **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 Artikel 12 Absatz 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 DSG). Die Einzelfallbewilligung einer Bearbeitung 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 inhaltlich 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 E-KDSG). Dieser ergibt sich aus den für die Aufgabenerfüllung anwendbaren Rechtsgrundlagen.

Personendaten dürfen nur zu dem Zweck bearbeitet werden, für den sie ursprünglich beschafft worden sind. Die Bearbeitung zu einem anderen Zweck ist jedoch unter gewissen im Gesetz ausdrücklich erwähnten Voraussetzungen zulässig. Dies ist der Fall, wenn es eine Rechtsgrundlage nach Art. 4 E-KDSG oder eine ausdrückliche Einwilligung in eine oder mehrere bestimmte Bearbeitungen erlaubt. Hinzuweisen ist auf das Gesetz über die zentralen Personendatensammlungen (Personendatensammlungsgesetz, PDSG<sup>52</sup>). Das PDSG regelt, welche Behörde auf welche Personendaten im Abrufverfahren zugreifen können.

Zulässig ist eine Bearbeitung zu einem anderen Zweck auch, wenn die betroffene Person in eine oder mehrere bestimmte Bearbeitungen eingewilligt hat.

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 Behörden und den Privaten. Folglich dürfen 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 oder eben zur Erfüllung der gesetzlichen Aufgaben geeignet und erforderlich sein muss und der betroffenen Person zugemutet werden kann. Entsprechend wird der Wortlaut der Bestimmung angepasst. Hierfür muss der Zweck der Datenbearbeitung bestimmt sein (Artikel 6 E-KDSG).

---

<sup>52</sup> BSG 152.05

## **Artikel 8 – Richtigkeit und Vollständigkeit**

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 E-KDSG). 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 datenschutzfreundliche 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 DSGVO.

### **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.<sup>53</sup>

### **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 Bearbeitung sowie der Eintrittswahrscheinlichkeit und Schwere der Risiken angemessen sein, welche die fragliche Bearbeitung für die betroffenen Personen mit sich bringt. Der Stand der Technik ist massgebend in Bezug auf den Informationsträger und die zu treffenden Massnahmen (bspw. auf Zugangsbeschränkungen). Der Kanton Bern erlässt ein neues Informations- und Cybersicherheitsgesetz (ICSG)<sup>54</sup> mit entsprechender Verordnung, welches die Informationssicherheit datenschutzübergreifend regelt und sich dazu äussert wird. Das E-KDSG schützt gemäss dessen Zweckartikel das Grundrecht auf Datenschutz (Art. 1 E-KDSG). In den folgenden Bestimmungen weist das Gesetz mehrfach auf «das Risiko für die betroffene Person» hin, ohne das Grundrecht auf Datenschutz explizit zu nennen. «Das Risiko für die betroffene Person» bezieht sich jedoch auf den Zweckartikel und damit auf das Grundrecht auf Datenschutz.

Die Norm bringt den risikobasierten Ansatz zum Ausdruck. Das Risiko für die betroffenen Personen, das mit einer Bearbeitung einhergeht, muss zu den technischen Möglichkeiten in Beziehung gesetzt werden,

<sup>53</sup> vgl. Rosenthal David (2020): Das neue Datenschutzgesetz. In: Jusletter vom 16. November 2020, Rz. 44.

<sup>54</sup> BSG [noch zu bestimmen]

um dieses zu verringern. Je höher das Risiko für die betroffenen Personen, je grösser die Eintrittswahrscheinlichkeit und je umfangreicher die Bearbeitung ist, umso höher sind die Anforderungen an die technischen Vorkehrungen, damit sie im Sinne der vorliegenden Bestimmung als angemessen gelten können.<sup>55</sup>

#### *Absatz 3*

Dieser Absatz führt die Verpflichtung ein, durch 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 Bearbeitung durch Behörden eine untergeordnete Rolle, da die Bearbeitung 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 Behörde bei einem Service, einer Software oder einem Gerät mehrere 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 Bearbeitung 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 Behörde kann also bestimmen, dass eine bestimmte Bearbeitung nur gewählt werden kann, wenn zugleich auch andere Bearbeitungen zugelassen werden. Eingeschränkt wird dies höchstens durch den Grundsatz der Verhältnismässigkeit oder der Freiwilligkeit der Einwilligung.<sup>56</sup>

### **Artikel 10 – Datensicherheit**

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

#### *Absatz 1*

Der Wortlaut von Absatz 1 wird an das Datenschutzgesetz des Bundes 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 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 der betroffenen Person stehen. Es ist Aufgabe der 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*

Wie beschrieben, erlässt der Kanton Bern ein neues Informations- und Cybersicherheitsgesetz (ICSG) 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 Behörden ergreifen entsprechend dem festgelegten Schutzbedarf Massnahmen bezüglich der Vertraulichkeit, Verfügbarkeit, Integrität und

---

<sup>55</sup> BBl 2017, S. 7029 f. Ziff. 9.1.3.1

<sup>56</sup> vgl. Rosenthal, David (2020), s.o.: Rz. 50.

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 Bearbeitungen, 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 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 Bearbeitung 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 Bearbeitung 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 Bearbeitungen 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 Bearbeitungen 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 Bearbeitung 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 Bearbeitung ebenfalls mit, indem es mit der ICT-Grundversorgung technische Mittel dafür zur Verfügung stellt. Es regelt in seinen technischen Weisungen, wel-

ches Datenschutz- und Datensicherheitsniveau mit diesen Mitteln sichergestellt ist, so dass die nutzen- den 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 Daten- bearbeitung beteiligt ist, kann sie auch bei dieser anfragen, wie die Verantwortlichkeiten aufgeteilt sind.

Entsprechend der bundesrechtlichen Regelung (Art. 33 DSG) verzichtet das kantonale Datenschutzge- setz 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 ein- holen (vgl. Art. 45 Abs. 2 Bst. a E-KDSG).

### **Artikel 12 – Bearbeitung durch beauftragte Dritte**

Artikel 22 und Artikel 23 der Richtlinie (EU) 2016/680 enthalten detaillierte Vorschriften, unter welchen Voraussetzungen eine Bearbeitung durch Dritte zulässig ist. Die Richtlinie stellt insbesondere Anforde- rungen an die Auftragsnehmerin bzw. den Auftragsnehmer, enthält Formvorschriften und inhaltliche An- forderungen an die Auftragserteilung sowie Voraussetzungen für das Unterauftragsverhältnis. Der Bund hat den Begriff der Auftragsbearbeiterin bzw. des Auftragsbearbeiters übernommen und die europäi- schen Anforderungen inhaltlich in Artikel 9 DSG umgesetzt. Neu regelt das DSG insbesondere die Unter- auftragsbearbeitung (Art. 9 Abs. 3 DSG). Der Kanton Bern kennt mit Artikel 28 DVG ebenfalls eine Be- stimmung zur Datenbearbeitung durch Dritte, die sich – mit einer Ausnahme – am DSG orientiert. Die einzige Abweichung zum neuen DSG korrigiert ein vermutliches Versehen des DSG-Gesetzgebers: Das DSG 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 tat- sächliche Sicherheit, nicht die potenzielle. Das DVG sieht deshalb vor, dass die Behörde sich vergewis- sern muss, dass die oder der Dritte die Datensicherheit gewährleistet. Diese Regelung ist in das kanto- nale Datenschutzgesetz zu übernehmen und gleichzeitig die provisorische Regelung im DVG aufzuhe- ben (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, beispielsweise 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 in- nerhalb einer Verwaltungseinheit stellt dagegen keine Auftragsbearbeitung dar. Werden Daten in einer sogenannten Cloud aufbewahrt, handelt es sich dabei grundsätzlich um einen Anwendungsfall der Auf- tragsbearbeitung, bei der die entsprechenden Voraussetzungen gelten. Die Datenherrschaft verbleibt bei der Behörde, weshalb sie die Personendaten nicht im Sinne des Datenschutzgesetzes bekanntgibt. Den- noch gelten die Bestimmungen zur Bekanntgabe von Personendaten ins Ausland sinngemäss, wenn die Auftragsbearbeitung im Ausland stattfindet (vgl. Erläuterungen zu Art. 15 E-KDSG).

### *Absatz 1*

Absatz 1 begründet eine Sorgfaltspflicht für die 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 Behörde muss Verstösse gegen die Datenschutzgesetzgebung verhindern. Infolgedessen ist sie ver- pflichtet, die beauftragten Dritten sorgfältig auszuwählen, sie angemessen zu instruieren und – soweit als

möglich – zu überwachen. Nicht mehr erwähnt ist, dass der Auftrag mittels Gesetz oder Vertrag zu erteilen ist. Sofern das Gesetz dazu ermächtigt, die Bearbeitung von Personendaten Dritten zu übertragen, werden die beauftragten Dritten regelmässig mit der Erfüllung der öffentlichen Aufgabe betraut, womit sie selbst zur Behörde im Sinne des kantonalen Datenschutzgesetzes werden.

Einer Auftragsbearbeitung können sowohl gesetzliche als auch vertragliche Geheimhaltungspflichten entgegenstehen (Bst. b). Nicht jede Geheimhaltungspflicht schliesst indes eine Auslagerung aus. Als gesetzliche Geheimhaltungspflichten gelten das Amtsgeheimnis, Spezialgeheimnisse wie spezielle Schweigepflichten und Berufsgeheimnisse. Beim Amtsgeheimnis ist die Auslagerung in der Regel möglich, wenn die Behörde die Verschwiegenheitspflicht vertraglich dem beauftragten Dritten überbindet. Bei der Auslagerung von Spezial- und Berufsgeheimnissen kommt es auf die technischen und organisatorischen Massnahmen an, die von der Behörde ergriffen werden. Dazu zählen beispielsweise die Pseudonymisierung oder Verschlüsselung.

Das kantonale Datenschutzgesetz spricht entgegen dem Bundesgesetzgeber von «entgegenstehen» statt «verbieten», da eine Auslagerung trotz Geheimhaltungspflichten mit entsprechenden organisatorischen und/oder technischen Massnahmen möglich ist. Inhaltlich entspricht die Regelung derjenigen auf Bundesebene.

Die Vernehmlassungsvorlage sprach die Geheimhaltungspflichten noch in einem separaten Absatz 2 an. Demnach sollte die Behörde den Zugang des Beauftragten Dritten bei Geheimhaltungspflichten auf das notwendige Minimum beschränken. Für die Teilnehmerinnen und Teilnehmer der Vernehmlassung war die Unterscheidung zu Absatz 1 Buchstabe b zu wenig klar bzw. kritisierten sie die rein deklaratorische Natur der Bestimmung. Es ist zuzustimmen, dass sich die Zugangsbeschränkung auf das Minimum bereits aus dem Verhältnismässigkeitsgrundsatz ergibt, weshalb die Bestimmung gestrichen wird.

#### *Absatz 2*

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 3*

Dieser Absatz sieht vor, dass die beauftragten Dritten die Bearbeitung nur mit vorgängiger Genehmigung der Behörde an Dritte übertragen dürfen. Die Genehmigung hat grundsätzlich 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 die Beschaffung oder die Bekanntgabe von Personendaten. Die besonderen Bestimmungen ändern nichts daran, dass die Grundsätze zur Bearbeitung von Personendaten immer einzuhalten sind (Art. 4 bis 12 E-KDSG).

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 anderen privaten Personen als der betroffenen erhoben werden. «In der Regel» 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 Behörde auf die Freiwilligkeit der Auskunft hinweisen.

Die Informationspflichten (Art. 9 Abs. 4 KDSG) sind neu unter dem 3. Titel «Pflichten der Behörden 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. 7.9.3). 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 der Bearbeitung 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 Vollzugsverordnung. «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 E-KDSG).

Wie bereits ausgeführt, kann die Behörde Personendaten auch gestützt auf eine Einwilligung nicht ohne jegliche gesetzliche Grundlage bearbeiten (vgl. Erläuterungen zu Art. 4 E-KDSG). Hingegen ist es möglich, dass die Behörde Personendaten bekanntgibt, die sie rechtmässig erhoben hat, wenn die betroffene Person in eine oder mehrere bestimmte Bearbeitungen ausdrücklich eingewilligt hat oder ihre Personendaten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat (Bst. b). 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 E-KDSG einen entsprechenden Vorbehalt für die Bekanntgabe vor.

Die 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 reicht es aus, dass die verlangende Behörde zur Datenbearbeitung befugt ist. In diesem Fall soll die bekanntgebende Behörde 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).

Ob eine besondere Geheimhaltungspflicht der Bekanntgabe im konkreten Fall entgegensteht, muss die Behörde im Einzelfall mittels einer Gesetzesauslegung prüfen.<sup>57</sup> Daraus kann sich ergeben, dass Behörden zur Bekanntgabe von Personendaten trotz besonderer Geheimhaltungspflicht befugt sind.

Zur Veranschaulichung folgendes Beispiel: Die GSI beauftragt einen Leistungsvertragspartner 1 zur Durchführung eines Krebscreening-Programms mit wiederkehrenden Untersuchungen der teilnehmenden Personen. Nach einiger Zeit beenden die Parteien diesen Vertrag und ein Leistungsvertragspartner 2 führt das Krebscreening-Programm fort. Die Auslegung der gesetzlichen Normen zur Aufgabenerfüllung kann in diesem konkreten Fall (d.h. nach der Natur der Aufgabe) zum Ergebnis führen, dass der Leistungsvertragspartner 1 Personendaten an den Leistungsvertragspartner 2 bekannt geben darf, da ansonsten die Aufgabe nicht bestimmungsgemäss weitergeführt werden kann (vgl. etwa Art. 2 der Verordnung über die Qualitätssicherung bei Programmen zur Früherkennung von Brustkrebs durch Mammographie; SR 832.102.4).

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**

Nach Art. 15 E-KDSG muss ein Empfängerstaat das Grundrecht auf Datenschutz der betroffenen Person angemessen schützen. Dies gilt auch bei der Nutzung von Cloud-Dienstleistungen. Der Regierungsrat schickte bezüglich der Ausnahmetatbestände zwei Varianten in die Vernehmlassung, welche sich bezüglich der Ausnahmetatbestände unterscheiden. Die Variante 1 sah vor, dass die Behörde davon nur in klar definierten Einzelfällen davon abweichen kann. Die Variante 2 sah einen weiteren Ausnahmetatbestand vor, bei dem unabhängig vom Datenschutzniveau lediglich die Voraussetzungen der Auftragsbearbeitung nach Art. 12 erfüllt sein müssen (Art. 15 Abs. 3 Bst. d VE-KDSG).

Der Regierungsrat entschied, dass parallel zum Vernehmlassungsverfahren in einem Gutachten zu klären sei, ob die Variante 2 mit übergeordnetem Recht vereinbar bzw. rechtmässig ist. Dementsprechend hat das Rechtsamt der DIJ eine geeignete Gutachterin bzw. einen geeigneten Gutachter gesucht und schliesslich Frau Prof. Dr. Astrid Epiney beauftragt, zu dieser Frage ein Rechtsgutachten zu erstellen. Sie ist ordentliche Professorin für Völkerrecht, Europarecht und schweizerisches öffentliches Recht an der Universität Freiburg und verantwortet jeweils die Datenschutztagung der Universität Freiburg. Frau Prof. Dr. Epiney qualifiziert sich durch ihre Expertise in Datenschutzfragen, insbesondere auch im internationalen Kontext, und publiziert regelmässig zu diesen Themen.

Im auf Oktober 2023 datierten Gutachten kommt Frau Prof. Dr. Astrid Epiney gemeinsam mit Frau Dr. Nula Frei zum Ergebnis, dass die Variante sowohl völker- und verfassungsrechtlich unzulässig als auch «nutzlos» ist. Der Regierungsrat hat sich deshalb entschieden, Variante 2 nicht weiterzuverfolgen.

#### **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 DSG, Art. 17 SEV108+ und Art. 36 Abs. 1 Richtlinie (EU) 2016/680).

<sup>57</sup> Vgl. Ehrensperger, Jennifer (2024): Bekanntgabe von Personendaten. In: Blehta, Gabor P. / Vasella David (Hrsg.), Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz, Basel: Helbing Lichtenhahn Verlag: Art. 36 N. 62; u.a. mit Verweis auf BGE 124 III 170).



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 Rechtsgrundlage.
- 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.

Damit nicht bei jeder Auslandsbekanntgabe 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 DSG 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 DSG 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.<sup>58</sup> Hier handelt es sich um eine klare Erleichterung für die Behörden. Liegt nämlich ein entsprechender Angemessenheitsbeschluss des Bundesrates vor, so ist es nicht mehr an der Behörde zu prüfen, ob ein Drittstaat ein angemessenes Datenschutzniveau bietet. Es handelt sich um eine Vereinfachung und trägt damit der Motion Vogt Rechnung.

In Bezug auf die USA gilt Folgendes: 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 bisher nicht auf der Positivliste des Bundesrates befand (Anhang 1 zur

<sup>58</sup> BBl 2017, S. 7039

Datenschutzverordnung, die am 23. September 2023 in Kraft getreten ist). Die Behörden mussten 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 2 stützen können. Es ist zulässig, wenn Bearbeitungen 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.

Nun ermöglicht das neue Swiss-U.S. Data Privacy Framework nach dem Bundesrat einen sicheren Austausch von Personendaten zwischen der Schweiz und zertifizierten US-Unternehmen. Der Bundesrat passt in der Folge die Datenschutzverordnung per 15. September 2024 an und setzt die USA in diesem Umfang auf die Liste der Länder mit einem angemessenen Datenschutzniveau. Sobald und solange zertifizierten Unternehmen der USA auf der Positivliste in Anhang 1 der Datenschutzverordnung sind, ist eine Bekanntgabe von Personendaten in diesem Rahmen auch nach Art. 15 Abs. 1 Bst. b E-KDSG zulässig.

#### *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 DSG) 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 SEV 108 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 45 Absatz 2 Bst. a E-KDSG Auskünfte einholen kann, muss dies hier nicht explizit geregelt werden. In Angleichung an das Bundesrecht wird auf die Informationspflicht verzichtet. Es handelt sich dabei um eine Erleichterung für die Behörde, weshalb die Nichtübernahme auch der Umsetzung der Motion Vogt dient.

#### *Absatz 2*

Personendaten dürfen auch ins Ausland bekanntgegeben werden, wenn zwar kein angemessenes Schutzniveau vorliegt, aber eine Voraussetzung nach Absatz 2 gegeben ist. Gegenüber dem heutigen Recht wird die Bestimmung stark gestrafft, da die Regelungen auf private Personen zugeschnitten waren und Anwendungsfälle für 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 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 kann die betroffene Person für eine oder für mehrere bestimmte Bekanntgaben erteilen (vgl. auch Art. 4 Abs. 2 Bst. c E-KDSG). Die ausdrückliche Zustimmung ergibt sich aus Artikel 17 SEV 108+. 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 DSG. 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 E-KDSG).

#### *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 DSG. 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.

### **Artikel 16 – Vernichtung, Aufbewahrung und Archivierung**

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

Die von der Behörde festgelegte Aufbewahrungsfrist in Absatz 2 ist eine pauschalisierte Anwendung des Verhältnismässigkeitsprinzips. Ist sie abgelaufen, muss die Behörde die Daten vernichten oder im Einzelfall gemäss Absatz 3 begründen, (a) warum sie die Daten weiterhin zu Sicherungs- und Beweis Zwecken (d.h. immer noch im Rahmen der primären Aufgabenerfüllung, zum ursprünglichen Zweck und gestützt auf die ursprüngliche Rechtsgrundlage) benötigt oder (b) dass jetzt eine neue Rechtsgrundlage / ein neuer Zweck die weitere Aufbewahrung rechtfertigt. Die vorliegende Regelung nimmt also Bezug auf den Lebenszyklus von Daten.

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 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)<sup>59</sup> und werden zu diesem Zweck weiterhin benötigt. Der Zugriff auf die Daten ist nur noch zu den in der Archivgesetzgebung vorgesehenen Zwecken zulässig.

### *Titel*

Der Artikel regelt neben der Vernichtung und Archivierung auch die Aufbewahrung von Personendaten, weshalb dieser Tatbestand in den Titel aufzunehmen ist.

### *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).

Personendaten gelten dann als vernichtet im Sinne dieser Bestimmung, wenn es ausserhalb des Wahrscheinlichen liegt, dass der Personenbezug wiederhergestellt werden kann. Dies kann bei einer Anonymisierung der Fall sein.

### *Absatz 2*

In Absatz 2 verpflichtet der Gesetzgeber die Behörden eine Aufbewahrungsfrist festzulegen und zu definieren, 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)<sup>60</sup>, 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 Beweis Zwecken 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

---

<sup>59</sup> BSG 108.1

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 – Bearbeitung 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.

Im Unterschied zum bisherigen Recht wird der Titel der Bestimmung neutraler formuliert und lautet neu «Bearbeitung 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 Behörde die Ergebnisse nicht bekanntgeben, sondern nur sicherstellen muss, dass die betroffenen Personen im Zeitpunkt der Bekanntgabe nicht bestimmbar sind.

Die Voraussetzungen in Buchstaben a und b sind kumulativ zu erfüllen.

#### **Absatz 2**

Die 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.<sup>61</sup>

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 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 E-KDSG durch «Datensicherheit» ersetzt.

Die Voraussetzungen in Buchstaben a bis d sind kumulativ zu erfüllen.

---

<sup>61</sup> vgl. Art. 32 GERES-Verordnung (gegenüber Behörden mit eigener Rechtspersönlichkeit).

## 7.3 Pflichten der Behörden und von beauftragten Dritten

### **Artikel 18 – Risikoanalyse bei geplanten, wiederkehrende Bearbeitungen**

Bei jeder geplanten, wiederkehrenden Bearbeitung schätzt die Behörde selbst die Risiken für die betroffenen Personen ab (Stufe 1, Art. 18 E-KDSG). Sofern ein hohes Risiko für sie besteht, führt die Behörde eine Datenschutzfolgenabschätzung durch (Stufe 2, Art. 18 Abs. 3 und Art. 19 E-KDSG). Gleich wie das Datenschutzgesetz des Bundes regelt die Bestimmung die Tatbestände, aus denen sich ein hohes Risiko für die betroffene Person ergibt, nicht abschliessend. Wenn zusätzlich eine grosse Anzahl Personen betroffen ist, legt die Behörde die Bearbeitung ihrer Datenschutzbehörde zur Stellungnahme vor (Stufe 3, Art. 20 E-KDSG).

#### *Absatz 1*

Abs. 1 regelt die Risikoanalyse. 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 den Behörden 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 Behörde. Die Beurteilung erfolgt nicht für jede einzelne Bearbeitung, weshalb das kantonale Datenschutzgesetz in Abweichung vom Bund nicht von «Bearbeitung» und «Bearbeitungsvorgängen» spricht, sondern von «geplanten, wiederkehrenden Bearbeitungen». Der Zusatz «geplant» verdeutlicht, dass die Risikoanalyse vor der Inbetriebnahme erfolgt. «Wiederkehrend» stellt klar, dass einmalige Bearbeitungen nicht von der Risikoanalyse erfasst sind.

An die Risikobeurteilung werden keine hohen formellen Anforderungen gestellt. Eine Aktennotiz im Projekt reicht, sofern in diesem Projekt keine hohen Risiken für die betroffenen Personen bestehen und folglich keine formelle Datenschutzfolgenabschätzung durchgeführt werden muss. Im bisherigen Recht ist eine solche Risikoanalyse nicht explizit verankert. Gedanklich war sie aber bereits im Rahmen der Vorabkontrolle vorzunehmen. Zur Vorabkontrolle waren bereits bisher sämtliche Behörden verpflichtet.

Auf Kantonsebene gilt bisher zudem die Direktionsverordnung vom 3. Januar 2011 über die Informationssicherheit und Datenschutz, ISDS DV<sup>62</sup>). Diese soll durch die neue Gesetzgebung zur Informationssicherheit ausser Kraft gesetzt werden. Beim Einsatz von ICT durch die Kantonsverwaltung muss die kantonale Behörde bereits heute in der Phase «Voranalyse» mit einer Informations- und Datenschutzsicherheitsanalyse (ISDS-Analyse) prüfen, ob erhöhte ISDS-Anforderungen bestehen (Art. 5 Abs. 1 bis 4 ISDS DV und neu Art. 18 E-KDSG). Lagen solche vor, musste die Behörde in der Phase «Konzept» ein ISDS-Konzept erstellen, welches die zusätzlichen zu ergreifenden organisatorischen und technischen Massnahmen festlegte (Art. 5 Abs. 5 ISDS DV und neu Art. 19 E-KDSG). 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 nach Absatz 3 durchzuführen ist. Die Aufzählung ist gestützt auf die Vernehmlassung nicht mehr abschliessend formuliert. Massgeblich ist das Risiko, das ohne Massnahmen zum Schutz der Rechte der betroffenen Personen besteht (sog. Brutto-Risiko). In der Datenschutzfolgenabschätzung ist darzulegen, wie das Risiko mit geeigneten technischen und organisatorischen Massnahmen (vgl. Art. 10 Abs. 1 E-KDSG) beseitigt oder auf ein tragbares Restrisiko (netto) gesenkt werden kann.

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 Bearbeitung. So auch

---

<sup>62</sup> BSG 152.040.2

Artikel 22 Absatz 2 DSG. Dieses Element ist ins kantonale Recht zu übernehmen. Die Aspekte Art, Umfang, Umstände und Zweck sind entsprechend insbesondere bei der Verwendung neuer Technologien zu würdigen und können dort zu einem hohen Risiko führen.

Namentlich bei der Bearbeitung von besonders schützenswerten Personendaten und bei systematisch umfangreicher Überwachung im öffentlichen Bereich besteht ein erhöhtes Risiko (Bst. a und b).

#### *Absatz 3*

Stellt die Behörde mittels Selbstkontrolle fest, dass bei einem Vorhaben ein hohes Risiko besteht, so nimmt sie formell eine Datenschutzfolgenabschätzung vor.

### **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 betroffenen Personen (Bst. b) sowie die Schutzmassnahmen (Bst. c) enthalten.

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

### **Artikel 20 – Vorabkontrolle**

#### *Absatz 1*

Ergibt die Risikoanalyse, dass die geplante Datenbearbeitung ein hohes Risiko für die betroffenen Personen birgt und werden zudem Personendaten einer grösseren Anzahl von Personen elektronisch bearbeitet, so unterbreitet die Behörde die Bearbeitung vor deren Beginn der Datenschutzbehörde zur Stellungnahme. Die Bestimmung orientiert sich an der Vorabkontrolle wie sie im Entwurf zum DSG 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 betroffenen Personen besteht und nicht nur, wenn trotz den von der Behörde ergriffenen Massnahmen ein erhöhtes Risiko für die betroffenen Personen besteht. In diesem Punkt weicht das kantonale Datenschutzgesetz von der Regelung in Artikel 23 DSG 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 DSG) 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 Behörde effizienter, da mögliche datenschutzrechtliche Problemfelder bereits in einem frühen Stadium der Bearbeitung 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 DSG enthält eine zweimonatige Frist, innert welcher die Datenschutzbehörde Einwände gegen die geplante Bearbeitung mitteilen kann. Aus Sicht des Kantons 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 intern «angemessener Frist» durchzuführen.

## **Artikel 21 – Registerpflicht**

Artikel 24 der Richtlinie (EU) 2016/680 verpflichtet die Behörde, 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 Behörden ihr Verzeichnis der Datenschutzbehörde zu melden, die ein Register über alle Verzeichnisse führt (Art. 12 und 56 DSG).

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 es zukünftig aber auf Datensammlungen beschränkt werden, die besonders schützenswerte Personendaten enthalten. Dadurch wird sich der Aufwand für Behörden verringern. Besonders heikel kann ausserdem sein, wenn die Behörden ein Profiling betreiben oder algorithmische Entscheidungssysteme (AES oder s.g. Künstliche Intelligenz) nutzen. Wie bereits erläutert, ist nicht jedes Profiling für die betroffenen Personen heikel. Dasselbe gilt für den Einsatz von Künstlicher Intelligenz, weshalb die Meldung auf Anwendungen mit einem hohen Risiko für die betroffene Person beschränkt wird.

Die Beschränkung des Registers gilt jedoch nicht im Anwendungsbereich der Richtlinie (EU) 2016/680, da hier eine Verzeichnispflicht besteht (vgl. Erläuterungen zur Verzeichnispflicht nach Art. 22 E-KDSG).

Die Ausführungsbestimmungen werden konkretisieren, inwieweit Behörden weitere Datensammlungen zur Aufnahme im Register melden können.

### **Absatz 1**

Die kantonale Datenschutzbehörde führt und veröffentlicht ein Register der kantonalen Datensammlungen (vgl. auch Art. 42 Abs. 2 E-KDSG).

### **Absatz 2**

Damit sie das Register führen kann, müssen die kantonalen Behörden ihre Datensammlungen anmelden. Die Pflicht wird in Absatz 1 statuiert. Mit der Meldepflicht einher geht auch die Pflicht, Mutationen zu melden. Neben Datensammlungen mit besonders schützenswerten Personendaten melden die Behörden auch, wenn sie ein Profiling mit hohem Risiko betreiben oder AES mit einem hohen Risiko für die betroffene Person nutzen. Künstliche Intelligenz, Algorithmen oder algorithmische Systeme werden oft synonym verwendet. Künstliche Intelligenz im Sinne einer eigenständig und «menschengleich» denkenden und handelnden Maschine gibt es bisher nicht und wird es auch in absehbarer Zeit nicht geben. Was es gibt, sind von Menschen entwickelte Entscheidungssysteme, die Daten analysieren und Lösungen für bestimmte Probleme oder Bereiche entwickeln oder vorschlagen.<sup>63</sup> Besonders wenn AES ein Entscheidungsspielraum zusteht, und sie nicht lediglich nach festen Regeln handeln, dürfte das Risiko für die betroffenen Personen hoch sein. Dies ist jedoch im Einzelfall zu entscheiden.

Die kantonale Datenschutzbehörde wird eine Eingabemaske gestalten, in welche die kantonalen Behörden ihre Datensammlungen bzw. die angewendeten Profiling und AES mit hohen Risiken eingeben können. Insofern melden sie die notwendigen Angaben nach den Vorgaben der Datenschutzbehörde. Nachdem sie diese geprüft hat, wird sie diesen Teil des Registers veröffentlichen. Das Register soll einer betroffenen Person ermöglichen, sich darüber zu informieren, wo über sie allenfalls entsprechende Daten

<sup>63</sup> Öktem Rosa (2021): Algorithmische Entscheidungssysteme, menschenrechtliche Vorgaben und Entwicklungen auf internationaler Ebene. In: Deutsches Institut für Menschenrechte (Hg.)



bearbeitet werden. Die Informationsmöglichkeit stellt den Ausgangspunkt dar, dass eine betroffene Person ihre Rechte geltend machen kann, die ihr nach der Datenschutzgesetzgebung zustehen.

#### *Absatz 3*

Die gemeinderechtlichen und landeskirchlichen Behörden müssen ihre Register selber führen. Wie sie dies organisatorisch lösen, ist ihnen überlassen. Es ist jedoch darauf hinzuweisen, dass öffentlich zugängliche und umfangreiche Register in der Regel dazu führen, dass weniger Auskunftsbegehren gestellt werden.

#### *Absatz 4*

Die einzelnen Angaben zu den Datensammlungen werden auf Verordnungsstufe aufgelistet. Aus der Meldung ergibt sich jedoch bereits, wer die Datensammlung betreibt, die Kategorien der Personendaten (die Art der besonders schützenswerten Personendaten wie Religionszugehörigkeit). Deshalb wird explizit nur noch der Zweck im Gesetz erwähnt, woraus sich in der Regel auch der Empfängerkreis ergibt.

Der Zweck des Bearbeitens kann beispielsweise lauten «Prüfen des Anspruchs auf Prämienverbilligung», «Durchführen eines Profilings mit hohem Risiko» oder «Weiterentwicklung von algorithmischen Entscheidungssystemen». Auf Verordnungsstufe werden die Inhalte analog dem Bundesdatenschutzgesetz einzeln aufgelistet werden. Damit handelt es sich um eine Vollzugsverordnung, weshalb keine explizite Gesetzesdelegation notwendig ist.

Dem bisherigen Recht entsprechend, sollen kurzfristig geführte und bereits anderweitig veröffentlichte Datensammlungen von der Registerführungspflicht ausgenommen werden. Erstere liegen vor, wenn sie auf höchstens zwei Jahre angelegt sind. Letztere sind Datensammlungen, die beispielsweise im Staats- oder Gemeindearchiv archiviert worden sind oder in Form von Jahreshüchern der Öffentlichkeit zugänglich gemacht werden. Eine Ausnahme ist jedoch nur möglich, wenn für die betroffenen Personen keine Risiken bestehen.

### **Artikel 22 – Verzeichnispflicht für Strafverfolgungsbehörden und Strafgerichte**

Artikel 24 der Richtlinie (EU) 2016/680 verlangt, dass Behörden, die im Bereich der Strafverfolgung und Strafvollstreckung tätig sind 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 Bearbeitungstätigkeiten an und umfasst Angaben zum Bearbeitungszweck, zu den Kategorien von Empfängern der Personendaten und den Kategorien der betroffenen Personen. Eine Kategorie einer Bearbeitungstätigkeit könnte beispielsweise «Videoüberwachung mit Aufzeichnung» sein. Auf Verordnungsstufe werden die Inhalte einzeln aufgelistet werden. Damit handelt es sich um eine Vollzugsverordnung, weshalb keine explizite Gesetzesdelegation notwendig ist. Die Ausnahmen des Verzeichnisses regelt der Regierungsrat ebenfalls durch 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 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 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 KdK-Leitfaden Folgendes zu regeln:

- Die Feststellung, dass die Informationspflicht für sämtliche Arten von Personendatenbearbeitungen gilt,
- eine Erweiterung der Liste der zu erteilenden Informationen 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 sie sämtliche Informationen erhält, die sie braucht, um ihre Rechte geltend zu machen. Absatz 2 enthält die Mindestinformationen, was durch den Zusatz «mindestens» ausgedrückt wird. Die Informationspflicht wird im Einklang mit der Registerpflicht und der Transparenz willen um algorithmische Entscheidungssysteme mit einem hohen Risiko für die betroffene Person ergänzt. Das Profiling ergibt sich aus dem Bearbeitungszweck.

Zusätzliche Angaben können sich beispielsweise zur Speicherdauer aufdrängen, wenn die Behörde besonders schützenswerten Personendaten beschafft.

Die Informationspflicht gilt nur insoweit, als die 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 Beschaffung.

Es ist der Behörde überlassen, wie sie ihrer Informationspflicht nachkommt. Sofern sie besonders schützenswerte Personendaten bearbeitet, ein Profiling mit hohem Risiko betreibt oder algorithmische Entscheidungssysteme mit einem hohen Risiko einsetzt, erfüllt sie die Pflicht, indem sie die Informationen im Register der Datensammlungen veröffentlicht. Werden andere Personendaten bei der betroffenen Person selbst beschafft, kann die Veröffentlichung im Internet genügen. Die Behörde muss sicherstellen, dass die betroffene Person die Information ohne grossen Aufwand tatsächlich zur Kenntnis nehmen kann, jedoch nicht, dass sich die betroffene Person im konkreten Fall wirklich informiert. Bei der Datenbeschaffung bei Dritten kann es 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*

Eine Einschränkung der Informationspflicht ist 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 DSG werden einzelne öffentlichen Interessen wie beispielsweise die öffentliche Sicherheit explizit genannt. In Übereinstimmung mit dem KdK-Leitfaden (Ziff. 5.6) verzichtet das KDSG darauf.

## Absatz 2

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

- die betroffene Person bereits über die Angaben verfügt (Bst. a) oder
- diese aus der Rechtsgrundlage nach Artikel 4 E-KDSG hervorgehen (Bst. b).

Andere Kantone verwenden die Wendung, dass die Informationspflicht entfällt, wenn die Bearbeitung gesetzlich «ausdrücklich» vorgesehen ist. Demgegenüber sieht Art. 24 Abs. 2 Bst. b E-KDSG vor, dass aus der Rechtsgrundlage mit hinreichender Präzision herausgelesen werden kann, welche Behörde, welche Daten zu welchem Zweck bearbeitet. Die Rechtsgrundlage muss die Informationen enthalten, über die die Behörde sonst informieren müsste (Artikel 23 Absatz 2 E-KDSG). Dabei müssen sich die Informationen weder aus einem Artikel noch zwingend aus einem Gesetz ergeben.

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 übernommene Bestimmung:*

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. Die Behörde kann sich nicht auf ein öffentliches Interesse stützen, wenn sie einen unverhältnismässigen Aufwand geltend macht.

## **Artikel 25 – Meldung von Verletzungen der Datensicherheit an die Datenschutzbehörden**

Im Gegensatz zur EV EDS lautet der Titel Verletzung der Datensicherheit und nicht des Datenschutzes, da die Bestimmung nur den Teilaspekt der Datensicherheit betrifft.

### *Absatz 1*

Nach europäischem Recht muss die 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). Der Begriff wird in Absatz 2 definiert. Die Meldung hat möglichst innert 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 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 Behörde melden, muss sie sich nicht anrechnen lassen.

Im Europäischen Recht sind die Meldepflichten unterschiedlich geregelt. Nach Art. 9 SEV 108+ zur Änderung von Art. 7 Abs. 2 SEV Nr. 108 besteht eine Meldepflicht erst bei einem schweren Eingriff bzw. hohem Risiko für die betroffenen Personen, nach Art. 30 Abs. 1 Richtlinie (EU) 2016/680 bereits bei einem gewöhnlichen Risiko. Das Datenschutzgesetz des Bundes verlangt ein hohes Risiko für die betroffene Person. Dies soll verhindern, dass selbst unbedeutende Verletzungen gemeldet werden müssen. Die Behörde muss dafür die Auswirkungen für die betroffenen Personen beurteilen.<sup>64</sup> Die Kantone regeln die Meldepflicht ebenfalls unterschiedlich: So verlangen beispielsweise der Kanton Zürich oder Luzern ebenfalls ein hohes bzw. grosses Risiko für die betroffene Person und im Kanton Basel-Land entfällt die Meldepflicht nur, wenn die Datenschutzverletzung voraussichtlich nicht zu einem Risiko für die Grundrechte der betroffenen Personen führt. Die Vernehmlassungsvorlage verlangte ebenfalls kein hohes Risiko für die betroffene Person, da die Meldepflicht die Regel und nicht die Ausnahme sein sollte. Ziel war es, dass die Datenschutzbehörde die Behörde möglichst frühzeitig und umfassend bei der Gewährleistung der Datensicherheit unterstützen kann.

---

<sup>64</sup> BBl 2017, S. 7064

Was die Meldung an die Datenschutzbehörde beinhalten muss, wird im Verordnungsrecht konkretisiert (vgl. Art. 24 Abs. 2 DSG).

#### *Absatz 2*

Absatz 2 definiert, wann eine Verletzung der Datensicherheit im Sinne dieser Bestimmung vorliegt. Die Bestimmung entspricht inhaltlich Artikel 5 Buchstabe h DSG. Im Gegensatz zum Datenschutzgesetz des Bundes spricht das KDSG in dieser Bestimmung nicht von «widerrechtlich», sondern verwendet den Begriff «unberechtigt». Damit wird die Definition an das zu erlassende kantonale Informations- und Cybergesetz angeglichen. Angeknüpft wird damit an Art 10 Abs. 2 E-KDSG, wonach bei der Bearbeitung von Personendaten eine dem Risiko für die betroffene Person angemessene Datensicherheit mit geeigneten technischen und organisatorischen Massnahmen gewährleistet werden muss.

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

- 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.

#### *Absatz 3*

Liegt eine Auftragsbearbeitung vor, ist die Behörde von den beauftragten Dritten über die Verletzung zu orientieren. Die Behörde wird dies vertraglich absichern müssen.

### **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 Vorkehrungen zu ihrem Schutz treffen kann, beispielsweise indem sie ihre Zugangsdaten oder Passwörter ändert.

### **Artikel 27 – Ausnahmen von der Meldepflicht an die betroffene Person**

#### *Absatz 1*

Auf die Benachrichtigung der betroffenen Person 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 DSG). Der Behörde obliegt hier jedoch kein Ermessen, weshalb die Bestimmung nicht als Kann-Vorschrift formuliert ist. Als milderer Mittel ist sie aufzuschieben oder einzuschränken.

#### *Absatz 2*

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 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.

Die Meldung an die betroffene Person ist nicht erforderlich, wenn sie mit einem unverhältnismässigen Aufwand verbunden ist (Bst. c). Das kann sein, 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 Behörde erfolgen. Da die Meldung durch öffentliche Bekanntgabe erfolgen kann, ist sie nie unmöglich, weshalb die Vorlage hier vom Bundesgesetz abweicht.

## **7.4 Rechte der betroffenen Person**

### ***Artikel 28 – Auskunftsrecht***

#### ***Absatz 1***

Das Auskunftsrecht darüber, welche Daten über eine Person von einer 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 E-KDSG. Die betroffene Person kann auf Anfrage mehr erfahren, als die 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 Behörde erteilt die Auskunft, selbst wenn die Bearbeitung im Auftrag erfolgt.

### ***Artikel 29 – Inhalt und Modalitäten 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 Bearbeitung gewährleistet ist.

Die Information umfasst einerseits die Personendaten als solche (Buchstabe a). Weiter umfasst die Information jene Informationen, über welche die Behörde nach Artikel 23 E-KDSG bei der Beschaffung orientieren muss (Buchstabe b), zuzüglich die Angaben über die Aufbewahrungsdauer (Buchstabe c) und die Herkunft der Personendaten (Buchstabe d). 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 Bearbeitung nur so gewährleistet werden kann. Wenn die 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 Behörde die Auskunft grundsätzlich schriftlich erteilt, auch in digitaler Form. Das bisherige Recht unterscheidet zwischen Auskunft und Einsicht, wobei das Einsichtsrecht eine Form des Auskunftsrechts darstellt. In Ausnahmefällen kann die Auskunft 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.

Nicht auf Gesetzesstufe geregelt wird die Auskunftserteilung durch eine Gesundheitsfachperson, wie sie der Bund kennt (Art. 25 Abs. 3 DSG). Die betroffene Person kann im Einzelfall einwilligen, dass die Behörde ihrer Auskunftspflicht über eine Drittperson wahrnimmt (vgl. Art. 14 Abs. 1 Bst. b E-KDSG). Näheres dazu wird auf Verordnungsstufe geregelt.

### **Artikel 30 – Einschränkungen des Auskunftsrechts**

Dieser Artikel regelt die Einschränkungen des Auskunftsrechts. Das allgemeine Amtsgeheimnis nach Personalrecht verpflichtet über Angelegenheiten zu schweigen, die Mitarbeiterinnen und Mitarbeiter in ihrer dienstlichen Stellung zur Kenntnis gelangen (vgl. Art. 58 PG)<sup>65</sup>. Besteht jedoch eine gesetzliche Verpflichtung zur Bekanntgabe der Daten wie bei der Auskunft über eigene Personendaten, liegt keine Amtsgeheimnisverletzung vor.

Unter bisherigem Recht kann die Behörde die Auskunft nur verweigern, einschränken oder aufschieben, 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 DSG verweigert die Behörde die Auskunft, schränkt sie ein oder schiebt sie auf, wenn überwiegende öffentliche oder private Interessen entgegenstehen. In diesen Fällen ist die 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 DSG).

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 oder in Anzeigesituationen. In solchen Fällen ist eine Interessensabwägung im Einzelfall vorzunehmen.

#### *Nicht übernommene Bestimmungen:*

Das Bundesdatenschutzgesetz sieht vor, dass die Behörde die Auskunft verweigern, einschränken oder aufschieben kann, wenn das Auskunftsgesuch offensichtlich unbegründet ist, namentlich wenn es einen datenschutzwidrigen Zweck verfolgt (Art. 26 Abs. 1 Bst. c DSG). Auf Verfahren nach dem kantonalen Datenschutzgesetz und insbesondere bei Gesuchen um Akteneinsicht ist das Gesetz über die Verwaltungspflege (VRPG) anwendbar. Demnach tritt die Behörde auf Eingaben nicht ein, die auf querulatorischer oder rechtsmissbräuchlicher Prozessführung beruhen (Art. 45 Abs. 1 VRPG). Folglich braucht es im kantonalen Datenschutzgesetz keine spezialgesetzliche Regelung, wie sie der Bund vorsieht.

Das Auskunftsrecht kann ohne Nachweis eines Partikularinteressens geltend gemacht werden. Daraus folgt, dass die Behörde grundsätzlich keine Begründung des Auskunftsbegehrens fordern darf. Das Bundesgericht hat jedoch entschieden, dass eine rechtsmissbräuchliche Geltendmachung des Auskunfts-

---

<sup>65</sup> BSG 153.01

rechts in Betracht kommt, wenn es datenschutzwidrige Zwecke verfolgt, etwa wenn das Auskunftsbeglehen einzig zum Zweck gestellt wird, die (spätere) Gegenpartei auszuforschen und Beweise zu beschaffen, an die eine Partei sonst nicht gelangen könnte.<sup>66</sup>

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

Eine widerrechtliche Bearbeitung liegt beispielsweise vor, wenn 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 Bearbeitung von unrichtigen Personendaten ist ebenfalls widerrechtlich, da die Richtigkeit der Personendaten ein Grundsatz des Datenschutzrechts darstellt (Art. 8 E-KDSG). 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 E-KDSG).

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 DSG ab. Schliesslich ist das schutzwürdige Interesse Ausfluss des Grundrechts auf Datenschutz und dürfte bei einer widerrechtlichen Bearbeitung immer gegeben sein.

### **Absatz 2**

Die 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 E-KDSG). Lässt sich die Richtigkeit der bisher bearbeiteten Daten nicht beweisen, hat die Behörde sie grundsätzlich zu berichtigen oder zu vernichten. Insoweit trifft die Behörde die Beweislast. Hingegen hat die betroffene Person die von ihr verlangten Berichtigungen zu beweisen. Unter Umständen kann sie die vorgeschlagene Berichtigung nicht einwandfrei beweisen, aber die Behörde kann ihre Aufgabe ohne die Datenbearbeitung nicht erfüllen. Für solche Fälle gibt es den Bestreitungsvermerk (Abs. 3).

### **Absatz 3**

Dieser Absatz wurde an die Terminologie des Bundes angepasst (Art. 41 Abs. 4 DSG): 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. Danach können die Personendaten nur noch zusammen mit dem Bestreitungsvermerk weitergegeben werden.

## **Artikel 32 – Recht auf Bekanntgabe des Entscheids**

---

<sup>66</sup> BGE 138 III 425 E. 5.5.

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 schutzwürdiges Interesse besteht.

### **Artikel 33 – Recht auf Sperrung der Bekanntgabe an Private**

Die von einer Bearbeitung betroffene Person kann von der Behörde verlangen, dass sie die Bekanntgabe von bestimmten Personendaten an Private sperrt, wenn sie ein schutzwürdiges Interesse nachweist (vgl. auch Art. 50 Abs. 2 VRPG). Zu denken ist etwa an politische Flüchtlinge, die sich durch ausländische Verfolger bedroht fühlen.

Die Sperre ist jedoch nicht zu gestatten, wenn die Behörde nach einer spezialgesetzlichen Regelung zur Bekanntgabe verpflichtet ist oder wenn die Privatperson ohne die Personendaten Rechtsansprüche gegenüber der betroffenen Person nicht durchsetzen kann.

Die bisher in Artikel 13 Absatz 3 KDSG enthaltene Regelung, um die Bekanntgabe von Personendaten durch die Einwohnerkontrolle zu sperren, findet sich im Spezialgesetz (vgl. Ziff. 7.9.3).

## **7.5 Datenschutzbehörden**

Heute führt jede Gemeinde und andere gemeinderechtliche Körperschaft für ihren Bereich eine eigene Aufsichtsstelle, die die Aufgaben der Datenschutzbehörde wahrnimmt. Mit der Revision soll das Aufsichtswesen zentralisiert und die Gemeinden entlastet werden. Die kantonale Datenschutzbehörde hat zusammen mit dem Amt für Gemeinden und Raumordnung, dem Verband Bernischer Gemeinden (VBG), der Geschäftsleitung der Regierungsstatthalterinnen und Regierungsstatthalter sowie unter Einbezug verschiedener Gemeinden 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) und andere gemeinderechtlichen Körperschaften. Der Fokus der kantonalen Datenschutzbehörde liegt dabei auf der Beratung, Anleitung und Ausbildung der Behörden. Das Datenschutzniveau soll dadurch gestärkt und die Ressourcen effizienter eingesetzt werden.

Die Kantone organisieren die Datenschutzaufsicht sehr unterschiedlich, jedoch gibt es nur sehr wenige, die eine zwingende kommunale Datenschutzaufsicht kennen, so beispielsweise der Kanton St. Gallen. Die dezentralisierte Variante wird nicht weiterverfolgt, da damit weder ein erhöhtes Datenschutzniveau noch eine effizientere Ressourcennutzung erreicht wird. Die nun gewählte Teilzentralisierung hat den Vorteil, dass nicht hauptsächlich die grösseren Gemeinden die kantonale Datenschutzbehörde beanspruchen. Zudem verfügen die grösseren Gemeinden über gut etablierte und professionelle Aufsichtsstellen, die bereits heute ein hohes Datenschutzniveau gewährleisten. Eine ähnliche Lösung kennt der Kanton Zürich, in dem lediglich die Städte Zürich und Winterthur über eine eigene Aufsichtsstelle verfügen. Die übrigen Gemeinden können im Gegensatz zur Vorlage des Kantons Bern wählen, ob sie eine eigene Aufsichtsstelle führen. Diese Wahlmöglichkeit wurde jedoch verworfen, da damit eine kantonal zersplitterte Lösung mit qualitativ unterschiedlicher Datenschutzpraxis riskiert würde. Die in die Vernehmlassung geschickte Variante stärkt das Datenschutzniveau und bleibt damit sachgerecht.

### **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.<sup>67</sup> Sie ist damit eine

<sup>67</sup> Vortrag des Regierungsrates zur Änderung des KDSG (2008): S. 14.



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 selbstständige 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)<sup>68</sup> angeglichen. Die selbstständige 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 an ihr Wahlorgan verpflichtet (Art. 50 E-KDSG). Sie gehört organisatorisch zur Verwaltung und nicht zur Legislative (vgl. Erläuterungen zu Abs. 1). Bei einer anderen Zuordnung würde sie zudem den niederschweligen 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 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**

#### *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.

---

<sup>68</sup> BSG 622.1

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 E-KDSG). 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 und nicht mehr der Regierungsrat die Beauftragte oder den Beauftragten für Datenschutz.

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 durch die Beaufsichtigten erfolgt. Mit der Beteiligung beider Gewalten sind die unterschiedlichen Interessen ausgewogen vertreten, weshalb an der Wahlvorbereitung weiterhin beide Gewalten beteiligt sein sollen (vgl. Art. 37 E-KDSG).

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. 60 E-KDSG).

#### *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 – Findungskommission**

Auf Bundesebene wählt entgegen des bundesrätlichen Vorschlags die Vereinigte Bundesversammlung die Beauftragte oder den Beauftragten (Art. 43 Abs. 1 DSG). Die Gerichtskommission der Vereinigten Bundesversammlung bereitet sowohl den Wahlvorschlag als auch Anträge betreffend Amtsenthebung vor (Art. 2 Entwurf zur Verordnung der Bundesversammlung über das Arbeitsverhältnis der Leiterin oder des Leiters des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten).<sup>69</sup>

Seit der Teilrevision des kantonalen Datenschutzgesetzes 2008 ist die Geschäftsprüfungskommission (damals Oberaufsichtskommission) Aufsichtsbehörde über die kantonale Beauftragte oder den kantonalen Beauftragten für Datenschutz. Sie bereitete auch den Wahlvorschlag vor. 2013 anlässlich der Revision des Grossratsgesetzes und der dazugehörigen Geschäftsordnung hat der Gesetzgeber in Anlehnung an die Richterwahlen die Wahlvorbereitung der Justizkommission übertragen<sup>70</sup>. Weitere Ausführungen dazu finden sich nicht. Den Wahlvorschlag für die Staatsschreiberin oder den Staatsschreiber nimmt das Büro des Grossen Rates entgegen (vgl. Art. 31 Abs. 2 GO GR)<sup>71</sup>. Die oder den Vorsteher der Finanzkontrolle wählt der Grosse Rat auf Vorschlag des Finanzkontrollgremiums, das für die Wahlvorberei-

<sup>69</sup> BBl 2022 348.

<sup>70</sup> Vortrag zum Gesetz über den Grossen Rat (Grossratsgesetz, GRG), Geschäftsordnung des Grossen Rates (GO) vom 3. Dezember 2012, zu Art. 38 GO, S. 47.

<sup>71</sup> BSG 151.211

tung aus folgenden Personen besteht: Präsidentin oder Präsident der Finanzkommission und der Geschäftsprüfungskommission, der Finanzdirektorin oder dem Finanzdirektor und einem weiteren Mitglied des Regierungsrats (Art. 34 Abs. 1 KFKG<sup>72</sup>). Also aus einem paritätischen Wahlvorbereitungsgremium aus Exekutive und Legislative. Die Stellung der oder des Beauftragten für Datenschutz ist vergleichbar mit derjenigen des Finanzkontrollorgans, was sich neu auch in der Organisationsgesetzgebung ersichtlich ist (vgl. Ziff. 7.9.4). Die Findungskommission wird analog ausgestaltet. Ein Einsitz der Gemeinden ist deshalb nicht vorgesehen. Eine überproportionale Besetzung der Exekutive wäre auch schwer mit der funktionellen Unabhängigkeit vereinbar.

#### *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<sup>73</sup>]). Die Beteiligung der Legislative am Auswahlverfahren ist 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. Die Zusammensetzung der Findungskommission orientiert sich an derjenigen des Finanzkontrollorgans, das die Wahl des Finanzkontrollorgans vorbereitet.

Der Wahlvorschlag wird heute von der Justizkommission für den Grossen Rat vorberaten. Eine solche Wahlvorberatung ist nicht mehr notwendig, zumal für die Wahlvorbereitung eigens eine Findungskommission 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 oder auch des Finanzkontrollorgans (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 schlägt die Findungskommission vor. Ist sie unbestritten, können die Mitglieder der Findungskommission schriftlich konsultiert werden.

Die Findungskommission kann weitere Personen beratend beiziehen. Denkbar ist etwa die Staatsschreiberin oder den Staatsschreiber beizuziehen oder bei einer Neuwahl auch den Verband der Bernischen Gemeinden (VBG) anzuhören.

### **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)<sup>74</sup>, 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. Ausserdem übt bereits die kantonale Datenschutzbehörde die Oberaufsicht über die gemeinderechtlichen und landeskirchlichen Datenschutzbehörden aus und eine zweifache Verwendung des Begriffs «Oberaufsicht» in einem unterschiedlichen Kontext ist zu vermeiden.

#### *Absatz 2*

Betont wird hier nochmals die Unabhängigkeit der oder des Beauftragten für Datenschutz, d.h. die Geschäftsprüfungskommission ist nicht weisungsbefugt (vgl. Erläuterungen zu Art. 34 Abs. 2 E-KDSG). Die Aufsicht gegenüber der bzw. dem Beauftragten für Datenschutz muss der Kontrolle über die Gerichte

---

<sup>72</sup> BSG 622.1

<sup>73</sup> BSG 151.211

<sup>74</sup> BSG 153.01

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.

Bei schweren Amtspflichtverletzungen kann die Geschäftsprüfungskommission das Abberufungsverfahren nach Artikel 41 Personalgesetz 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 Haushaltsführung (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)<sup>75</sup>.

### **Artikel 41 – gemeinderechtliche und landeskirchliche Datenschutzbehörde**

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 (Art. 43 Abs. 2 E-KDSG). Folglich bezeichnen nur noch Gemeinden und andere gemeinderechtliche Körperschaften mit mehr als 25'000 Einwohnerinnen und Einwohnern bzw. Angehörigen sowie Landeskirchen und ihre regionalen Einheiten eine eigene Datenschutzbehörde, welche die Aufgaben nach diesem Gesetz ausübt. Mehr als 25'000 Einwohnerinnen und Einwohner haben die Gemeinden Biel/Bienne, Bern, Köniz und Thun (vgl. auch Ziff. 3.6).

Das Gesetz schreibt vor, dass die Gemeinden die Wahl und Organisation ihrer Datenschutzbehörden in einem Reglement regeln müssen, da es sich hier um grundlegende organisationsrechtliche Normen handelt (Abs. 2).

### **Artikel 42 – Aufgaben**

---

<sup>75</sup> BSG 620.03

## *Absatz 1*

Dieser Artikel listet sämtliche Aufgaben der Datenschutzbehörden in konzentrierter Form auf. Dieser Artikel und die Aufgaben der folgenden Artikel gelten auch für die gemeinderechtlichen und landeskirchlichen Datenschutzbehörden.

Die Datenschutzbehörden unterstützen die Behörden bei der Anwendung des Datenschutzrechts. Die Hauptaufgaben der Datenschutzbehörden sind die Beratung und die Überwachung der Datenschutzbestimmungen, insbesondere der Datensicherheit. Mit der Beratung soll darauf hingewirkt werden, dass die 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 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. 45 E-KDSG). 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 betroffenen Personen birgt und eine grössere Anzahl von Personen betrifft (vgl. Art. 20 E-KDSG). Im Gegensatz zur Überwachung bezieht sich die Vorabkontrolle nicht auf eine stattfindende oder bereits stattgefundene Bearbeitung von Personendaten, sondern auf eine zukünftige Bearbeitung.

## *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. 45 Abs. 4 E-KDSG).

## *Buchstabe d*

Die Datenschutzbehörde versteht sich hauptsächlich als beratende Behörde. So berät sie die 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 E-KDSG). 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 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. 49 E-KDSG).

#### *Buchstabe i*

Die Datenschutzbehörden informieren die Öffentlichkeit einerseits periodisch mit dem öffentlichen Tätigkeitsbericht sowie bei Bedarf, nämlich in Fällen von allgemeinem Interesse (vgl. Art. 50 E-KDSG).

#### *Absatz 2*

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

#### *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 – Aufsicht im Allgemeinen**

Die Datenschutzbehörde beaufsichtigt die Bearbeitung von Personendaten durch Behörden, natürlich nur soweit die Datenbearbeitung in den Zuständigkeitsbereich der jeweiligen Datenschutzbehörde fällt.

### **Artikel 44 – Schweigepflicht**

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 45 – Überprüfung der Einhaltung von Datenschutzbestimmungen**

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 (Art. 45 E-KDSG; bisher: Arbeitsweise und Verfahren), Empfehlungen (Art. 46 E-KDSG) und Verwaltungsmassnahmen (Art. 47 E-KDSG).

### *Absatz 1*

Vor der Inbetriebnahme prüft die Datenschutzbehörde geplante Informatikvorhaben auf ihre Datenschutzkonformität einschliesslich der Datensicherheit. Das geschieht im Rahmen der Vorabkontrolle nach Artikel 20 E-KDSG. 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 aufsichtsrechtliche 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 zur Umsetzung von Massnahmen äussert. Die Vorabkontrolle durch die Datenschutzbehörde (Art. 20 E-KDSG) 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 für die betroffene Person angemessen geschützt sind (vgl. Art. 10 E-KDSG).

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

### *Absatz 3*

Wie bisher ist die 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 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 46 – 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. 47 E-KDSG). Es soll aber weiterhin möglich sein, dass sie gegenüber der Behörde Empfehlungen aussprechen kann.

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

## **Artikel 47 – 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 der Behörden zur Wehr setzen wollen, deren Handlungen direkt anfechten können. Dazu steht ihnen der normale Rechtsmittelweg offen. Die Datenschutzbehörde 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**

Auf Bundesebene sind die eidgenössischen Gerichte von der Aufsicht insgesamt ausgenommen (Art. 4 Abs. 2 Bst. c DSG). Begründet wird die Ausnahme damit, dass die Aufsicht die Gewaltenteilung und die Unabhängigkeit der Justiz beeinträchtigen würde. Dazu kommt, dass das Bundesverwaltungsgericht und das Bundesgericht Beschwerdeinstanzen für Verfügungen des Datenschutzbeauftragten sind. Um den europäischen Anforderungen gerecht zu werden, richtet jedes eidgenössische Gericht eine eigene unabhängige Datenschutzaufsicht mittels Verordnung ein.<sup>76</sup> Die Verwaltungskommission des Bundesgerichts übt die Datenschutzaufsicht über das Bundesstraengericht, das Bundesverwaltungsgericht und das Bundespatentgericht aus (Art. 1 Abs. 2 und Art. 3 Bst. cbis Aufsichtsreglement des Bundesgerichts [AufRB-Ger])<sup>77</sup>. Die Gerichte müssen ihr einen Datenschutzbericht einreichen (Art. 6a AufRBGer). Sie kann Untersuchungen (Art. 7 AufRBGer) durchführen und Weisungen im Datenschutz erlassen (Art. 10 AufRBGer).

Die Kantone regeln die Aufsicht über die Gerichte sehr unterschiedlich. Teilweise werden die Gerichte von der Aufsicht ausgenommen und gleichzeitig eigene Aufsichtsorgane eingerichtet (z.B. Kanton Zürich), teilweise darf die Datenschutzbehörde gegenüber ihnen keine Verwaltungsmassnahmen verhängen (z.B. Kanton Basel-Land und Basel-Stadt) oder die Aufsicht gilt vollumfänglich (z.B. Kanton Luzern, wobei unklar ist, ob sich ein Gericht gegen eine Massnahme wehren kann, da Entscheide der Datenschutzbehörde ansonsten beim Kantonsgericht anfechtbar sind).

Die kantonale Datenschutzbehörde kann im Anwendungsbereich des kantonalen Datenschutzgesetzes (vgl. Art. 3 Abs. 4 E-KDSG) auch gegenüber Gerichtsbehörden und der Staatsanwaltschaft Verfügungen erlassen (vgl. Art. 47 Abs. 2 E-KDSG). Damit ist die Verfügungskompetenz der kantonalen Datenschutzbehörde gegenüber den Behörden einheitlich geregelt.

---

<sup>76</sup> BBl 2017, S. 7018.

<sup>77</sup> SR 173.110.132



Massgebend ist, ob ein Verfahren von einer Verfahrensordnung geregelt ist. Die Bearbeitung von Personendaten in einem hängigen Verfahren der Gerichtsbehörden oder der Staatsanwaltschaft kann die Datenschutzbehörde nicht beaufsichtigen. Hingegen müssen Gerichtsbehörden 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. Insgesamt wird mit der Vorlage der Gewaltenteilung genügend Rechnung getragen.

## **Artikel 48 – Zuständigkeit für Beschwerden**

### **Absatz 1**

Verfügt eine gemeinderechtliche Datenschutzbehörde gegenüber einer Gemeinde oder einer anderen gemeinderechtlichen Körperschaft, könnte sowohl das zuständige Regierungsstatthalteramt als auch die kantonale Datenschutzbehörde Beschwerdeinstanz sein. Die kantonale Datenschutzbehörde übt die Obergericht aus (Art. 43 Abs. 2 E-KDSG). Diese beinhaltet jedoch gerade nicht die Befugnis, anstelle der beaufsichtigten Stellen zu handeln, Entscheide abzuändern oder aufzuheben (vgl. auch Art. 4 GRG). Sie ist als Beschwerdeinstanz ungeeignet.

Nach dem geltenden Recht wäre für Verfügungen der Gemeinden oder der anderen gemeinderechtlichen Körperschaften das zuständige Regierungsstatthalteramt Rechtsmittelbehörde (Art. 26 KDSG und Art. 63 Abs. 1 Bst. a VRPG). Sie üben die kantonale Aufsicht aus (Art. 87 GG). An diesem Instanzenzug wird auch für Verfügungen der gemeinderechtlichen Datenschutzbehörden festgehalten.

### **Absatz 2**

Die kantonale Datenschutzbehörde ist keiner Direktion untergeordnet. Sie gilt wie die Finanzkontrolle als selbstständige Organisationseinheit innerhalb der Verwaltung (vgl. Ziff. 7.9.4). Unabhängig davon, ob die kantonale Datenschutzbehörde gegenüber einer Gemeinde, einer anderen gemeinderechtlichen Körperschaft (inkl. Kirchgemeinden) oder einer kantonalen Behörde verfügt, sind ihre Verfügungen direkt beim Verwaltungsgericht anfechtbar. Diese Lösung entspricht dem KdK-Leitfaden und dem bernischen Rechtsmittelsystem. So sind namentlich auch Verfügungen der kantonalen Finanzkontrolle beim Verwaltungsgericht anfechtbar.<sup>78</sup> Sofern die kantonale Datenschutzbehörde verfügt, wird an der Vorlage festgehalten.

Ebenfalls zu regeln ist die Beschwerde gegen Verfügungen der landeskirchlichen Datenschutzbehörde. Kirchgemeinden als gemeinderechtliche Körperschaften fallen nicht darunter. Bei letzteren übt die kantonale Datenschutzbehörde die Aufsicht aus. Verfügungen der landeskirchlichen Behörden, die ausschliesslich oder ergänzend zum landeskirchlichen Recht auch auf staatliches Recht ergangen sind, müssen direkt bei den staatlichen Rechtsmittelbehörden gemäss VRPG angefochten werden (Art. 23 des Gesetzes über die bernischen Landeskirchen [Landeskirchengesetz]<sup>79</sup>). Erste Rechtsmittelinstanz gegen diese Verfügungen ist demzufolge das Verwaltungsgericht (Artikel 74 VRPG).

### **Nicht übernommene Bestimmungen:**

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.

Auf die Unangemessenheitskontrolle durch das Verwaltungsgericht wird verzichtet. Geht es um vorwiegend technische Materien, wie bei Massnahmen des Datenschutzes und der Datensicherheit, sind Ge-

---

<sup>78</sup> BVR 2023 S. 201. E. 1.1.

<sup>79</sup> BSG 410.11

richte oft nicht in der Lage die Zweckmässigkeit zu prüfen, weshalb sie sich in der Regel auf die Fachkenntnisse der verfügenden Behörde abstützen. Mit der Sachverhalts- und Rechtskontrolle wird ein genügender Rechtsschutz gewährt.

#### *Absatz 3*

Verfügungen und Beschwerdeentscheide der kantonalen Datenschutzbehörde sind innert 30 Tagen grundsätzlich beim Verwaltungsgericht anfechtbar. Dies ist nicht möglich, wenn das Verwaltungsgericht Verfügungsadressat ist, weshalb das Gesetz für diesen Fall ausdrücklich das Obergericht als Rechtsmittelbehörde bestimmt.

### **Artikel 49 – 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 E-KDSG). Dies kann ein Hindernis für die Zusammenarbeit darstellen. Wenn beispielsweise 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 Datenschutzaufsichtsstellen anderer öffentlich-rechtlicher Körperschaften Aufgaben der Datenschutzaufsicht im Kanton Bern wahrnehmen, soweit dies schriftlich vereinbart ist. So kann etwa die kantonale Datenschutzbehörde einer ausserkantonalen Datenschutzaufsichtsstelle das Recht einräumen, im Kanton Bern Kontrollaufgaben zu erledigen, **wenn Behörden mehrerer Kantone gemeinsam Personendaten bearbeiten oder bei Befangenheit der Mitarbeitenden der kantonalen Datenschutzbehörde.**

#### *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 (Bst. a).

Für die Datenschutzaufsicht über Vorhaben, die die Nutzung kantonal 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, beispielsweise mit einer Software der Gemeinden, vorgenommen werden (Bst. b).

### **Artikel 50 – Berichterstattung und Information der Öffentlichkeit**

Dieser Artikel regelt sowohl die jährliche Berichterstattung ans Wahlorgan und bei Bedarf an die beaufsichtigten Gemeinden und anderen gemeinderechtlichen Körperschaften der kantonalen Datenschutzbehörde 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 der kantonalen Datenschutzbehörde richtet sich formell ans Wahlorgan sowie bei Bedarf an die beaufsichtigten Gemeinden und anderen gemeinderechtlichen Körperschaften.

Soweit Gemeinden, andere gemeinderechtliche Körperschaften sowie Landeskirchen und ihre regionalen Einheiten über eine eigene Datenschutzbehörde verfügen, regeln sie die Berichterstattung selbst (Abs. 2). Ein Verzicht ist nicht zulässig.

Die kantonale Datenschutzbehörde publiziert den Tätigkeitsbericht 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 E-KDSG) und der Informationsgesetzgebung, weshalb dazu keine explizite Regelung notwendig ist.

Bei Bedarf kann die Datenschutzbehörde die Öffentlichkeit informieren. Die Pflicht der kantonalen Datenschutzbehörde, vorgängig die Direktionsvorsteherin oder den Direktionsvorsteher 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 E-KDSG 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 51 – Anwendbare Bestimmungen**

Der in diesem Artikel 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 die kantonale Datenschutzbehörde, das Verwaltungsgericht oder das Obergericht zuständig (vgl. Art. 48 E-KDSG).

### **Artikel 52 – Prozessvertretung**

Nach Artikel 15 Absatz 4 VRPG sind ausser auf dem Gebiet des Sozialversicherungsrechts und vorbehaltlich 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 Vertretung durch gemeinnützige Organisationen ist nur im Geltungsbereich der Richtlinie möglich. Zudem müssen die Organisationen Sitz in der Schweiz haben.

Die Richtlinie sieht vor, dass gegen eine aufsichtsrechtliche Anzeige, gegen Anordnungen der Datenschutzbehörde und gegen Anordnungen der Behörde ein Rechtsmittel 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, wobei die Vertretung von Personen in Datenschutzfragen statutarisch vorgesehen sein muss.

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, sofern sie von der Richtlinie erfasst sind. Betroffen sind in erster Linie die Verfahren in Anwendung der Artikel 28 ff. E-KDSG, 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 53 – Anfechtungsobjekt**

Es ist fraglich, ob ein förmlicher Entscheid über ein Auskunftsgesuch oder über ein Gesuch bei widerrechtlicher Bearbeitung (vgl. Art. 28 und 31 E-KDSG) 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. Gleiches gilt für die Bekanntgabe von Personendaten.

### **Artikel 54 – 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 55 – 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. Hingegen kann die Behörde Gebühren erheben, wenn die betroffene Person ihre Rechte mutwillig oder leichtfertig ausübt. Die Ausnahme zielt hauptsächlich auf querulatorische Gesuche ab und übernimmt eine im bernischen Recht gängige Formulierung.

Die Gebührenfreiheit gilt nur für die Ansprüche gegenüber der verantwortlichen Behörde und nicht für das Rechtsmittelverfahren. Für das Verwaltungsjustizverfahren verweist Artikel 51 auf die anwendbare Verfahrensordnung.

## **7.7 Ausführungsbestimmungen**

### **Artikel 56 – Ausführungsbestimmungen**

Diese Bestimmung ermächtigt den Regierungsrat zum Erlass der erforderlichen Vollzugsvorschriften.

Die Subdelegation für technische und untergeordnete Regelungsgegenstände ist nicht mehr erforderlich, da die Bestimmungen der Direktionsverordnung über Informationssicherheit und Datenschutz in die Verordnung zum künftigen Gesetz über Informations- und Cybersicherheit überführt werden.

## 7.8 Übergangs- und Schlussbestimmungen

### 7.8.1 Übergangsbestimmungen

#### **Artikel 57 – Laufende Bearbeitungen**

Die Übergangsbestimmung betrifft Datenbearbeitungen, die bereits von der kommunalen oder kantonalen Datenschutzbehörde vorabkontrolliert oder die nach bisherigem Recht begonnen worden sind und nach Inkrafttreten dieses Gesetzes fort dauern. 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 Behörden im Vorfeld einer Datenbearbeitung. Sie sollen nicht nachträglich und damit rückwirkend die Pflichten erfüllen müssen. Es kann sein, dass eine Bearbeitung bis zum Inkrafttreten des Gesetzes bereits von einer Datenschutzbehörde vorabkontrolliert worden ist, aber erst danach begonnen wird. Auch solche Bearbeitungen sollen nicht erneut geprüft werden müssen. Da eine Vorabkontrolle nicht für jede Bearbeitung Pflicht ist, muss die Ausnahme auch für andere Bearbeitungen gelten, die bereits begonnen worden sind.

#### **Artikel 58 – 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 Inkrafttretens des künftigen Datenschutzgesetzes hängig sind, sowie Beschwerden gegen Verfügungen dem bisherigen Recht unterstehen. Dies betrifft sowohl die materiellen Datenschutzvorschriften als auch die Befugnisse der Datenschutzbehörde und die weiteren anwendbaren Verfahrensvorschriften.

#### **Artikel 59 – Lastenausgleich**

Infolge der Zentralisierung der datenschutzrechtlichen Aufgaben der Gemeinden muss die Lastenverteilung 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 <sup>80</sup> :                        | 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, anderen gemeinderechtlichen Körperschaften und Kleinstkörperschaften per Ende 2021 umgerechnet, ergeben sich folgende Ausgabenbefugnisse:

- |                                  |         |         |
|----------------------------------|---------|---------|
| - Bei 530 Kleinstkörperschaften: | 530'000 | Franken |
|----------------------------------|---------|---------|

<sup>80</sup> Unterabteilungen, Bürgergemeinden, bürgerliche Korporationen, Gemeindeverbände und Schwellenkorporationen (Art. 64a Gemeindeverordnung [GV; BSG 170.111]).

- 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 Artikel 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 anderen 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 Stellenprozenten. 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 kantonale 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.

Die Lastenverschiebung zwischen den Gemeinden und dem Kanton als Folge der Zentralisierung der Datenschutzbehörden wird ab dem Zeitpunkt des Inkrafttretens dieses Gesetzes dem Lastenausgleich gemäss Artikel 29b des Gesetzes vom 27. November 2000 über den Finanz- und Lastenausgleich (FILAG)<sup>81</sup> angerechnet.

Mit dem Lastenausgleich nach Art. 29b FILAG wurde ein Instrument geschaffen, welches es ermöglicht, Lastenverschiebungen zwischen dem Kanton und den Gemeinden aufgrund einer neuen Aufgabenteilung zu kompensieren.<sup>82</sup> Gerade bei einer Lastenverschiebung im vorliegenden Ausmass bietet Art. 29b FILAG ein passendes Ausgleichsgefäss. Die entsprechenden Lastenverschiebungen sind von sämtlichen Gemeinden zu tragen. Einzelne Gemeinden aus dem Lastenausgleich nach Art. 29b FILAG auszunehmen ist mit der Bestimmung nicht vereinbar und auch nicht vollziehbar, weshalb die Lastenverschiebung von sämtlichen Gemeinden zu tragen ist.

### **Artikel 60 – Amtsdauer der oder des Beauftragten für Datenschutz**

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.

<sup>81</sup> BSG 631.1

<sup>82</sup> Lienhard, Andreas/ Engel Gerhard/ Schmutz Andreas (2021) Finanzrecht. In: Müller, Markus /Feller, Reto (Hrsg.), Kommentar zum bernischen Verwaltungsrecht. Bern: Stämpfli Verlag AG: S. 1002.

## **Artikel 61 – Evaluation**

Um eine wirksame Umsetzung des Gesetzes zu gewährleisten, soll dessen Wirkung evaluiert werden. Die Evaluation erfolgt mittels Bericht des Regierungsrates an den Grossen Rat vier Jahre nach Inkrafttreten.

### **7.9 Änderungen anderer Erlasse**

#### **7.9.1 Datenschutzgesetz (KDSG) vom 19. Februar 1986<sup>83</sup>**

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)<sup>84</sup>; 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. 49 E-KDSG). 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 Schweizerinnen und Schweizer (NAG)<sup>85</sup> und das Einführungsgesetz vom 9. Dezember 2019 zum Ausländer- und Integrationsgesetz sowie zum Asylgesetz (EG AIG und AsylG)<sup>86</sup>; 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 E-KDSG.

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 E-KDSG kann die betroffene Person die Bekanntgabe von zusätzlichen Personendaten, die gestützt auf das Gemeindereglement zulässig wäre, ohne Nachweis eines schutzwürdigen Interesses sperren lassen.

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

---

<sup>83</sup> BSG 152.04

<sup>84</sup> BSG 109.1

<sup>85</sup> BSG 122.11

<sup>86</sup> BSG 122.20

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

#### **7.9.4 Gesetz vom 20. Juni 1995 über die Organisation des Regierungsrates und der Verwaltung (Organisationsgesetz, OrG)<sup>87</sup>; 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 selbstständige 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 geschaffen werden, der die kantonale Datenschutzbehörde als selbstständige Organisationseinheit bezeichnet. Aus der Systematik ergibt sich ausserdem, dass die kantonale Datenschutzbehörde zur Verwaltung gehört.

#### **7.9.5 Polizeigesetz (PolG) vom 10. Februar 2019<sup>88</sup>; 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.

#### **7.9.6 Gesetz vom 9. März 2021 über die sozialen Leistungsangebote (SLG)<sup>89</sup> und Kantonales Geldspielgesetz vom 10. Juni 2020 (KGSG)<sup>90</sup>; 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.<sup>91</sup> Dazu zählen etwa Angaben über eine fürsorgerische Unterbringung. In der bernischen Gesetzgebung ist der Begriff bereits teilweise angepasst worden, so beispielsweise in Artikel 57d Absatz 4 des Gesetzes über die öffentliche Sozialhilfe (Sozialhilfegesetz, SHG)<sup>92</sup>. Mit der Revision soll die fürsorgerische Betreuung auch in Artikel 71 des Kantonalen

---

<sup>87</sup> BSG 152.01

<sup>88</sup> BSG 555.1

<sup>89</sup> BSG 860.2

<sup>90</sup> BSG 935.52

<sup>91</sup> vgl. Rudin, Beat (2014), s.o. § 3 N. 38.

<sup>92</sup> BSG 860.1



Geldspielgesetzes (KGSG)<sup>93</sup> und in Artikel 111 Absatz 2 des Gesetzes über die sozialen Leistungsangebote (SLG)<sup>94</sup> mit Massnahmen des Kindes- und Erwachsenenschutzes ersetzt werden (vgl. Art. 2 Abs. 1 Ziff. 6 E-KDSG).

### 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)<sup>95</sup>
- Artikel 9a, Artikel 14 und Artikel 20 des Gesetzes vom 31. März 2009 über die Archivierung (ArchG)<sup>96</sup>
- 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 Personendatenansammlungen (PDSG)<sup>97</sup>
- Artikel 12a des Personalgesetzes vom 16. September 2004 (PG)<sup>98</sup>
- Artikel 35 des Gesetzes vom 18. Mai 2014 über die Pensionskassen (PKG)<sup>99</sup>
- Artikel 23 des Gesetzes vom 23. Mai 1989 über die Verwaltungsrechtspflege (VRPG)<sup>100</sup>
- Artikel 55 des Gesetzes vom 1. Februar 2012 über den Kindes- und Erwachsenenschutz (KESG)<sup>101</sup>
- Artikel 3 des Einführungsgesetzes vom 11. Juni 2009 zur Zivilprozessordnung, zur Strafprozessordnung und zur Jugendstrafprozessordnung (EG ZSJ)<sup>102</sup>
- Artikel 38 des Kantonalen Finanzkontrollgesetzes vom 7. März 2022 (KFKG)<sup>103</sup>
- Artikel 130 des Spitalversorgungsgesetzes vom 13. Juni 2013 (SpVG)<sup>104</sup>
- Artikel 57g und Artikel 80g des Gesetzes vom 11. Juni 2001 über die Sozialhilfe (SHG)<sup>105</sup>
- Artikel 46 und Artikel 51 des Gesetzes vom 3. Dezember 2019 über die Sozialhilfe im Asyl- und Flüchtlingsbereich (SAFG)<sup>106</sup>
- Artikel 71 des Kantonalen Geldspielgesetz vom 10. Juni 2020 (KGSG)<sup>107</sup>

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

### 7.9.8 Anpassungen des französischen Begriffs für besonders schützenswerte Personendaten (indirekte Änderungen)

Im französischen Text wird der Begriff «données particulièrement dignes de protection» durch den vom Bund verwendeten Begriff «données personnelles sensibles (données sensibles)» ersetzt. Dadurch ergeben sich folgende indirekte Änderungen:

---

<sup>93</sup> BSG 935.52

<sup>94</sup> BSG 860.2

<sup>95</sup> BSG 107.1

<sup>96</sup> BSG 108.1

<sup>97</sup> BSG 152.05

<sup>98</sup> BSG 153.01

<sup>99</sup> BSG 153.41

<sup>100</sup> BSG 155.21

<sup>101</sup> BSG 213.316

<sup>102</sup> BSG 271.1

<sup>103</sup> BSG 622.1

<sup>104</sup> BSG 812.11

<sup>105</sup> BSG 860.1

<sup>106</sup> BSG 861.1

<sup>107</sup> BSG 935.52

- Artikel 28 und Artikel 29 des Gesetzes vom 2. November 1993 über die Information und die Medienförderung (IMG)<sup>108</sup>
- Artikel 31 des Gesetzes vom 7. März 2022 über die digitale Verwaltung (DVG)<sup>109</sup>
- Artikel 25 des Gesetzes vom 13. Juni 2017 über das Kantons- und Gemeindebürgerrecht (Kantonales Bürgerrechtsgesetz, KBüG)<sup>110</sup>
- Artikel 37 und Artikel 38 des Einführungsgesetzes vom 9. Dezember 2019 zum Ausländer- und Integrationsgesetz sowie zum Asylgesetz (EG AIG und AsylG)<sup>111</sup>
- Artikel 4, Artikel 5, Artikel 7, Artikel 18 und Artikel 24 des Gesetzes vom 10. März 2020 über die zentralen Personendatensammlungen (Personendatensammlungsgesetz, PDSG)<sup>112</sup>
- Artikel 11a des Gesetzes vom 28. März 2006 über die Regierungsstatthalterinnen und Regierungsstatthalter (RStG)<sup>113</sup>
- Artikel 12a, Artikel 12 f und Artikel 12g des Personalgesetzes vom 16. September 2004 (PG)<sup>114</sup>
- Artikel 20a des Notariatsgesetzes vom 22. November 2005 (NG)<sup>115</sup>
- Artikel 38 und Artikel 39 des Gesetzes vom 3. Dezember 2020 über die Leistungen für Kinder mit besonderem Förder- und Schutzbedarf (KFSG)<sup>116</sup>
- Artikel 23, Artikel 24, Artikel 25 und Artikel 26 des Gesetzes vom 23. Januar 2018 über den Justizvollzug (Justizvollzugsgesetz, JVG)<sup>117</sup>
- Artikel 19 und Artikel 21 des Gesetzes vom 21. März 2018 über die bernischen Landeskirchen (Landeskirchengesetz, LKG)<sup>118</sup>
- Artikel 6, Artikel 7 des Gesetzes vom 28. Januar 1997 über die jüdischen Gemeinden<sup>119</sup>
- Artikel 21d und Artikel 73 des Volksschulgesetzes vom 19. März 1992 (VSG)<sup>120</sup>
- Artikel 67 des Mittelschulgesetzes vom 27. März 2007 (MiSG)<sup>121</sup>
- Artikel 57a des Gesetzes vom 14. Juni 2005 über die Berufsbildung, die Weiterbildung und die Berufsberatung (BerG)<sup>122</sup>
- Artikel 24 des Kantonalen Sportförderungsgesetzes vom 7. Dezember 2021 (KSpöFöG)<sup>123</sup>
- Artikel 66, Artikel 141, Artikel 144, Artikel 145, Artikel 146, Artikel 148 und Artikel 160 des Polizeigesetzes vom 10. Februar 2019 (PoIG)<sup>124</sup>
- Artikel 14 des Gesetzes vom 13. Juni 2018 über das Erbringen von Sicherheitsdienstleistungen durch Private (SDPG)<sup>125</sup>
- Artikel 66 des Finanzhaushaltsgesetzes vom 15. Juni 2022 (FHG)<sup>126</sup>
- Artikel 28 des Kantonalen Finanzkontrollgesetzes vom 7. März 2022 (KFKG)<sup>127</sup>
- Artikel 34a des Baugesetzes vom 9. Juni 1985 (BauG)<sup>128</sup>
- Artikel 17b1 des Gesundheitsgesetzes vom 2. Dezember 1984 (GesG)<sup>129</sup>
- Artikel 4 des Einführungsgesetzes vom 6. September 2018 zur eidgenössischen Krebsregistrierungsgesetzgebung (EG KRG)<sup>130</sup>
- Artikel 14 des Arbeitsmarktgesetzes vom 23. Juni 2003 (AMG)<sup>131</sup>

---

<sup>108</sup> BSG 107.1

<sup>109</sup> BSG 109.1

<sup>110</sup> BSG 121.1

<sup>111</sup> BSG 122.20

<sup>112</sup> BSG 152.05

<sup>113</sup> BSG 152.321

<sup>114</sup> BSG 153.01

<sup>115</sup> BSG 169.11

<sup>116</sup> BSG 213.319

<sup>117</sup> BSG 341.1

<sup>118</sup> BSG 410.11

<sup>119</sup> BSG 410.51

<sup>120</sup> BSG 432.210

<sup>121</sup> BSG 433.12

<sup>122</sup> BSG 435.11

<sup>123</sup> BSG 437.11

<sup>124</sup> BSG 551.1

<sup>125</sup> BSG 551.4

<sup>126</sup> BSG 620.0

<sup>127</sup> BSG 622.1

<sup>128</sup> BSG 721.0

<sup>129</sup> BSG 811.01

<sup>130</sup> BSG 815.21

<sup>131</sup> BSG 836.11

- Artikel 4 und Artikel 21a des Gesetzes vom 6. Juni 2000 betreffend die Einführung der Bundesgesetze über die Kranken-, die Unfall- und die Militärversicherung (EG KUMV)<sup>132</sup>
- Artikel 57e des Gesetzes vom 11. Juni 2001 über die öffentliche Sozialhilfe (Sozialhilfegesetz, SHG)<sup>133</sup>
- Artikel 56, Artikel 102 und Artikel 111 des Gesetzes vom 9. März 2021 über die sozialen Leistungsangebote (SLG)<sup>134</sup>
- Artikel 46, Artikel 47 und Artikel 49 des Gesetzes vom 13. Juni 2023 über die Leistungen für Menschen mit Behinderungen (BLG)<sup>135</sup>
- Artikel 45, Artikel 46, Artikel 47 und Artikel 48 des Gesetzes vom 3. Dezember 2019 über die Sozialhilfe im Asyl- und Flüchtlingsbereich (SAFG)<sup>136</sup>
- Artikel 44a des Kantonalen Landwirtschaftsgesetzes vom 16. Juni 1997 (KLwG)<sup>137</sup>
- Artikel 71 und Artikel 72 des Kantonalen Geldspielgesetzes vom 10. Juni 2020 (KGSG)<sup>138</sup>
- Artikel 21 und Artikel 23 des Gesetzes vom 7. Juni 2012 über das Prostitutionsgewerbe (PGG)<sup>139</sup>

## 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. 59 E-KDSG).

Die eingeführte Datenschutzfolgenabschätzung entspricht grösstenteils der bereits heute durchzuführenden ISDS-Analyse und dem ISDS-Konzept, weshalb hier kein bedeutender Mehraufwand entstehen sollte. Zwar müssen gestützt auf die neue Regelung auch Behörden eine Datenschutzfolgeabschätzung durchführen, die bisher dazu nicht verpflichtet waren. Zusätzlicher Aufwand wird dadurch aber letztlich nicht verursacht, weil sie bereits heute eine Vorabkontrolle durchführen und die Risiken einer Bearbeitung abschätzen mussten. Mit der formalisierten Risikoanalyse und der Datenschutzfolgenabschätzung wird lediglich das Verfahren standardisiert und auf Gesetzesstufe verankert.

<sup>132</sup> BSG 842.11

<sup>133</sup> BSG 860.1

<sup>134</sup> BSG 860.2

<sup>135</sup> BSG 860.3

<sup>136</sup> BSG 861.1

<sup>137</sup> BSG 910.1

<sup>138</sup> BSG 935.52

<sup>139</sup> BSG 935.90

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. Zudem ist es an den Behörden durch geeignete technische und organisatorische Massnahmen Zwischenfälle zu verhindern.

## **10. Personelle und organisatorische Auswirkungen**

Infolge der Zentralisierung der gemeinderechtlichen Aufsicht benötigt die kantonale Datenschutzbehörde ca. 400 zusätzliche Stellenprozent. Der Mehraufwand wird über das Lastenausgleichssystem abgerechnet (Erläuterungen zu Art. 59 E-KDSG).

## **11. Auswirkungen auf die Gemeinden**

Für die Gemeinden – mit Ausnahme der vier bevölkerungsstärksten 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 die Behörde 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**

Der Regierungsrat ermächtigte die Direktion für Inneres und Justiz am 21. Juni 2023, für die Totalrevision des kantonalen Datenschutzgesetzes (KDSG) eine Vernehmlassung durchzuführen. Das Vernehmlassungsverfahren dauerte vom 23. Juni 2023 bis zum 29. September 2023. Von den 65 Teilnehmerinnen und Teilnehmern gingen teilweise sehr umfangreiche Rückmeldungen ein, die sich grundsätzlich auf wenige Kernthemen fokussierten.

### **13.1 Geltungsbereich für juristische Personen**

Ob das KDSG weiterhin Personendaten juristischer Personen schützen soll, ist in der Vernehmlassung umstritten. Dabei sprechen sich die IG ländlicher Raum, die SVP, Thun und die Piratenpartei für deren Schutz aus und etwa die Inselgruppe sowie der BAV dagegen aus. Letztere verweisen in der Regel auf den Bundesgesetzgeber, der die Anwendbarkeit seines Gesetzes auf natürliche Personen beschränkt. Der Bundesgesetzgeber hält dazu in seiner Botschaft Folgendes fest<sup>140</sup>:

---

<sup>140</sup> BBl 2017, S. 6972

*Im Bereich der Datenbearbeitung durch Bundesorgane hätte die Aufhebung des Schutzes von Daten juristischer Personen zur Folge, dass die bundesrechtlichen Gesetzesgrundlagen, mit denen die Bundesorgane zur Bearbeitung von Personendaten ermächtigt werden, nicht mehr anwendbar wären, wenn diese Daten juristischer Personen bearbeiten. Nach Artikel 5 BV ist die Grundlage staatlichen Handelns jedoch das Recht. Des Weiteren unterstehen auch juristische Personen dem Schutz der Privatsphäre, selbst wenn sie nicht Trägerinnen sämtlicher Schutzgehalte gemäss Artikel 13 BV sind. Der Bundesrat schlägt deshalb vor, für Bundesorgane im Regierungs- und Verwaltungsorganisationsgesetz vom 21. März 1997 (RVOG) eine Reihe von Bestimmungen zu schaffen, die deren Umgang mit Daten juristischer Personen regeln (vgl. Ziff. 9.2.8). Ausserdem soll eine Übergangsbestimmung während fünf Jahren mögliche Rechtslücken verhindern (vgl. Art. 66 DSG sowie die Erläuterungen unter Ziff. 9.1.11).*

Im Unterschied zur kantonalen Vorlage gilt das Bundesgesetz auch für Privatpersonen, wenn sie Personendaten bearbeiten. Soweit Bundesorgane Daten juristischer Personen bearbeiten, schafft der Bundesgesetzgeber **parallele Datenschutzbestimmungen**. Als Bundesbehörden gelten auch Private, denen Bundesaufgaben übertragen worden sind.

Es ist wenig sinnvoll, eine parallele Gesetzgebung zu schaffen. Daraus ergeben sich auch praktische Schwierigkeiten. Im kantonalen Recht gibt es keinen Erlass, der auf sämtliche Behörden anwendbar ist: Das Organisationsgesetz ist beispielsweise auf Gemeinden nicht anwendbar, das Gemeindegesetz nicht auf gewisse kirchliche Institutionen. Für Private, die öffentliche Aufgaben übernehmen, gibt es keinen einheitlichen Erlass. Somit fänden sich die Bestimmungen zum Schutz von Daten juristischer Personen in diversen Erlassen verstreut. Es ist hingegen zuzustimmen, dass in der Vorlage bisher eine **Definition** fehlte, was **besonders schützenswerte Personendaten juristischer Personen** sind. Dies wird neu in Artikel 2 Absatz 1 Buchstabe d E-KDSG definiert bzw. wird die Definition des Bundesgesetzgebers übernommen. Ausserdem werden einige **Ausnahmen vom Geltungsbereich** normiert, sofern die Bestimmungen des Datenschutzes nicht qua bernische Verfassung sowieso gelten. An dieser Stelle ist darauf hinzuweisen, dass die Berner Verfassung relativ weit geht. Artikel 18 KV statuiert neben den Betroffenenrechten (Abs. 1), dass jede Bearbeitung von Personendaten eine gesetzliche Grundlage voraussetzt (=Rechtsgrundlage) und die Bearbeitung für die Aufgabenerfüllung (=festgelegter Zweck) geeignet und notwendig (=Verhältnismässigkeit) sein muss (Abs. 2). Ferner verpflichtet der Verfassungsgeber die Behörde, dass sie sich vergewissern muss, dass die bearbeiteten Daten richtig sind, und sie diese vor missbräuchlicher Verwendung zu schützen hat (Abs. 3). Im Übrigen ist auch der Bundesgesetzgeber der Meinung, dass auch juristische Personen Betroffenenrechte ausüben können, auch wenn er dies nicht explizit im RVOG normiert<sup>141</sup>. Das heisst, die im 2. Titel festgehaltenen Grundsätzen des KDSG gelten qua Kantonsverfassung. Ebenfalls gelten die im 4. Kapitel aufgelisteten Rechte der betroffenen Personen. Ausnahmen sind möglich im 3. Titel (Pflichten der Behörden und von beauftragten Dritten) und im 5. Titel (Datenschutzbehörde). Deshalb werden diese Titel vom Geltungsbereich für Daten juristischer Personen ausgenommen.

## 13.2 Begriffsdefinitionen

Im Gegensatz zur Vernehmlassung spricht das Gesetz nicht mehr von der «verantwortlichen Behörde», sondern verwendet lediglich den Begriff «Behörde». Inhaltlich regelt Artikel 11 weiterhin, wer für den Datenschutz verantwortlich ist. Ebenfalls spricht die Vorlage nun durchgehend von «Bearbeitung» und «Beschaffung» statt teilweise von «Bearbeiten» oder «Beschaffen».

Von mehreren Teilnehmerinnen und Teilnehmer der Vernehmlassung wird gefordert, die Begriffsbestimmungen näher an diejenigen des **Bundes anzugleichen**. Soweit sinnvoll, wird dies umgesetzt (vgl. Erläuterungen zu Art. 2 E-KDSG bei den einzelnen Begriffen). Ausgenommen sind folgende Begriffe:

Massnahmen der sozialen Hilfe: Hier muss sich die Vorlage an der kantonalen Gesetzgebung orientieren. Im Kanton Bern sind Massnahmen der sozialen Hilfe schlicht nicht dasselbe wie auf Bundesebene.

---

<sup>141</sup> BBl 2017, S. 7120

Bewusst verzichtet wird auf den Begriff der «Rassenzugehörigkeit», da dieser nicht mehr zeitgemäss ist. Der Begriff «Daten über die ethnische Herkunft» bleibt weiterhin in einer eigenen Ziffer normiert, da er nichts mit den Begriffen «Gesundheit und Intimsphäre» gemeinsam hat.

An der vereinfachten Definition des Profilings wird festgehalten, damit der Text verständlicher bleibt. Ausserdem ist für kantonale Behörden nur der Profiling-Begriff mit hohem Risiko massgebend.

Der Behördenbegriff muss zwingend anders lauten, da das Gesetz nicht auf die gleichen Behörden anwendbar ist.

Die Verletzung der Datensicherheit ist nicht mehr in den Begriffsbestimmungen normiert, sondern bei der materiellen Bestimmung (Art. 25 Abs. 2 E-KDSG).

### 13.3 Rechtsgrundlage für die Bearbeitung von Personendaten

Zur Rechtsgrundlage stellten die Teilnehmerinnen und Teilnehmer der Vernehmlassung sehr unterschiedliche und teilweise auseinanderfallende Anträge. Die FDP forderte für sämtliche Bearbeitungen von Personendaten eine Grundlage auf Gesetzesstufe. Etwa die Stadt Bern sprach sich für die bisherige Regelung aus. Die DJB und Grünen forderten, die Anforderungen aus Art. 18 Abs. 2 KV, wonach die Bearbeitung für die Aufgabenerfüllung geeignet und notwendig sein muss, bereits bei der Rechtsgrundlage festzuhalten. Der VBG und die Stadt Thun beantragen hingegen, dass es bei der mittelbaren gesetzlichen Grundlage ausreichen soll, wenn die Bearbeitung der Erfüllung einer gesetzlichen Aufgabe dient, da die gewählte Formulierung die Anforderung verschärfe.

Ausgangslage für das kantonale Datenschutzgesetz ist die Verfassung. Jede Bearbeitung von Personendaten durch Behörden stellt einen **Eingriff in die Grundrechte** der betroffenen Personen dar. Als Ausfluss des verfassungsrechtlichen Legalitätsprinzips (Art. 5 Abs. 1 und Art. 36 Abs. 1 BV, Art. 28 KV) verlangt auch die Bearbeitung von Personendaten eine gesetzliche Grundlage. Artikel 18 Absatz 2 KV BE lautet wie folgt:

*Behörden dürfen Personendaten nur bearbeiten, wenn eine **gesetzliche Grundlage** besteht (=Rechtsgrundlage) und die Daten **für die Erfüllung ihrer Aufgaben geeignet und notwendig** (=Verhältnismässigkeit) sind.*

**Schwerwiegende Einschränkungen eines Grundrechts müssen im Gesetz selbst vorgesehen werden.** Das kantonale Datenschutzgesetz definierte die Begriffe bisher uneinheitlich bzw. sogar falsch. So verlangt heute Artikel 5 Absatz 1 KDSG, dass auch das Bearbeiten von gewöhnlichen Personendaten durch eine Grundlage **im Gesetz** ermächtigt sein muss. Das widerspricht dem oben aufgeführten Verfassungsartikel. Das geltende Recht ist deshalb zu revidieren.

Als **Grundsatz** gilt, was folgt: Ob die Bearbeitung von Personendaten eine Grundlage im Gesetz oder eine gesetzliche Grundlage verlangt, hängt von der Schwere des Grundrechtseingriffs ab. Der **Gesetzgeber nimmt hier eine Wertung vor**. Demnach gilt die Bearbeitung von besonders schützenswerten Personendaten als schwerer Eingriff und verlangt nach einer Grundlage im Gesetz (vgl. Art. 4 Abs. 2 E-KDSG und Art. 34 Abs. 2 DSG). Diese kann **unmittelbar** oder **mittelbar** sein. Unmittelbar ist sie, wenn sich die Bearbeitung direkt daraus ergibt und mittelbar, wenn sich die Bearbeitung aus der Aufgabenerfüllung ergibt. Sofern eine Behörde Personendaten bearbeitet, muss sie ausserdem den Verhältnismässigkeitsgrundsatz beachten. Die Verhältnismässigkeit wird jedoch in Artikel 7 E-KDSG adressiert und nicht in der Rechtsgrundlage. Deshalb wird dem Antrag der Stadt Thun und dem VGB gefolgt und es reicht zur Bearbeitung von Personendaten wie bisher aus, wenn sie der Erfüllung der gesetzlichen Aufgabe dient. Die Bearbeitung muss aber weiterhin für die Aufgabenerfüllung geeignet und erforderlich sowie für die betroffene Person zumutbar sein (=Verhältnismässigkeitsgrundsatz).

Die Inselgruppe und die UPD beantragen auf die unterschiedlichen Anforderungen an die Gesetzesstufe beim **Profiling** zu verzichten, da die Unterscheidung zu wenig klar sei. Die Vorlage definiert den Profilingbegriff gegenüber der Vernehmlassung neu und orientiert sich dabei am «Profiling mit hohem Risiko»

des Bundes. Für dieses Profiling ist immer eine Grundlage im Gesetz notwendig. Bei jedem Profiling bearbeitet die Behörde jedoch Personendaten, weshalb sie auch hierfür mindestens eine materiell-rechtliche Grundlage benötigt (vgl. Art. 4 E-KDSG). Das trägt der bereits zu Beginn angestellten Überlegung Rechnung, dass nicht jedes Profiling potentiell gefährlich ist. Die Lösung ist jedoch wesentlich eleganter als auf Bundesstufe, die übrigens erst in der parlamentarischen Debatte eingeflossen ist.

Die Stadt Langenthal fordert, dass bei einer **Einwilligung** gänzlich auf eine gesetzliche Grundlage verzichtet werden kann. Wie bereits in der Vernehmlassungsvorlage dargelegt, sind die Behörden aus Sicht des Kantons bei der Bearbeitung von Personendaten an das Legalitätsprinzip gebunden. Deshalb kann eine Einwilligung nicht von jeglicher gesetzlichen Grundlage befreien. Die Piratenpartei verlangt, dass öffentlich zugänglich gemachte besonders schützenswerte Personendaten nur mit Zustimmung der betroffenen Person von einer Grundlage im Gesetz befreien soll. Der Antrag wird nicht umgesetzt, da die Bestimmung nicht von der Bundesbestimmung abweichen soll.

Dem Antrag der Stadt Thun und des VBG folgend, **verzichtet die Vorlage auf den Vorbehalt des Amtsgeheimnisses**, der sich bisher in Artikel 5 Absatz 5 KDSG fand. Das Amtsgeheimnis verpflichtet Mitarbeiterinnen und Mitarbeiter, über Angelegenheiten zu schweigen, die ihnen in ihrer dienstlichen Stellung zur Kenntnis gelangen (Art. 58 PG)<sup>142</sup>.

### 13.4 Bekanntgabe ins Ausland: Variantenvorschlag

Der Europäische Gerichtshof (EuGH) entschied im Urteil «Schrems II» vom 16. Juli 2020, dass die USA kein dem europäischen Datenschutzrecht gleichwertiges Schutzniveau gewährleistet. Das führte zu Unsicherheiten, wie in der Schweiz Cloud-Lösungen wie Microsoft 365 eingesetzt werden können, bei denen unter Umständen Personendaten ins Ausland bekanntgegeben werden. Der Regierungsrat schickte deshalb für die Bekanntgabe von Personendaten ins Ausland zwei Varianten in die Vernehmlassung. Grundsätzlich dürfen Behörden Personendaten ins Ausland bekanntgeben, wenn sie ein angemessenes Datenschutzniveau gewährleisten, ausser sie können sich auf einen Ausnahmetatbestand berufen (Variante 1). Ein weiterer Ausnahmetatbestand sah vor, dass unabhängig vom Datenschutzniveau lediglich die Voraussetzungen der Auftragsbearbeitung erfüllt sein mussten (Variante 2). Frau Prof. Dr. Astrid Epiney und Dr. Nula Frei schlussfolgerten in ihrem Gutachten vom Oktober 2023, dass die Variante 2 sowohl völker- und verfassungsrechtlich unzulässig als auch «nutzlos» ist. Wegen der Gesetzeslage in den USA kann eine beauftragte Dritte Personendaten unter Umständen nicht nur so bearbeiten, wie es die Behörde selbst tun dürfte. Für eine Risikoanalyse, mit welcher Wahrscheinlichkeit eine andere Bearbeitung tatsächlich stattfinden könnte, bleibt kein Raum. Denn ob das Recht eingehalten wird oder nicht, ist keine Frage des Risikos, sondern eine Rechtsfrage, die bei staatlichen Behörden anders zu beantworten sein kann als bei Privaten. Für die Variante 2 gibt es keine überzeugenden rechtlichen Argumente, weshalb diese nicht weiterverfolgt wird. Anzuführen bleibt, dass sich die Ausgangslage hinsichtlich der USA aktuell ändert. Das neue Swiss-U.S. Data Privacy Framework ermöglicht nach dem Bundesrat einen sicheren Austausch von Personendaten zwischen der Schweiz und zertifizierten US-Unternehmen. Der Bundesrat passt in der Folge die Datenschutzverordnung per 15. September 2024 an und setzt die USA in diesem Umfang auf die Liste der Länder mit einem angemessenen Datenschutzniveau. Sobald und solange zertifizierten Unternehmen der USA auf der Positivliste in Anhang 1 der Datenschutzverordnung sind, ist eine Bekanntgabe von Personendaten in diesem Rahmen auch nach Art. 15 Abs. 1 Bst. b E-KDSG zulässig.

---

<sup>142</sup> BSG 153.01

### 13.5 Aufbewahrung, Vernichtung und Archivierung

Die Vernehmlassung zeigte, dass der Unterschied zwischen der behördlich zum Voraus festgelegten Aufbewahrungsfrist und der darüber hinaus möglichen Aufbewahrung zu Sicherungs- und Beweis Zwecken oder für die wissenschaftliche Forschung für einige Vernehmlassungsteilnehmende unklar ist. Es gilt: Die Aufbewahrung dient dem Nachweis, dass die Behörde ihre primäre Aufgabe ordnungsgemäss erfüllt hat; sie stützt sich auf die ursprüngliche Rechtsgrundlage und dient dem ursprünglichen Zweck. Die von der Behörde festgelegte Aufbewahrungsfrist ist eine pauschalisierte Anwendung des Verhältnismässigkeitsprinzips. Ist sie abgelaufen, muss die Behörde die Daten vernichten *oder* sie kann im Einzelfall begründen, warum sie Daten weiterhin zu Sicherungs- und Beweis Zwecken (d.h. immer noch im Zusammenhang mit der primären Aufgabenerfüllung und gestützt auf die ursprüngliche Rechtsgrundlage) benötigt. Oder aber die Daten werden jetzt einem neuen Zweck zugeführt, der sich auf eine neue Rechtsgrundlage stützt (Art. 17 E-KDSG für die Forschung oder Archivierungsgesetz) und zu dessen Erreichung die Daten wiederum benötigt werden.

### 13.6 Risikoanalyse bei geplanten, wiederkehrende Bearbeitungen

Bei jeder geplanten, wiederkehrenden Bearbeitung schätzt die Behörde selbst die Risiken für die betroffenen Personen ab (Stufe 1, Art. 18 E-KDSG). Sofern ein hohes Risiko für sie besteht, führt die Behörde eine Datenschutzfolgenabschätzung durch (Stufe 2, Art. 19 E-KDSG). In der Vernehmlassung forderten diverse Teilnehmerinnen und Teilnehmer (UPD, Grüne, DJB, Privatlinik Wyss), dass die Bestimmung ans Bundesrecht angeglichen wird und die Tatbestände nicht abschliessend formuliert werden, aus denen sich ein hohes Risiko für die betroffenen Personen ergibt. Die Bestimmung wird in dieser Hinsicht ans Bundesrecht angeglichen. Gleich wie das Datenschutzgesetz des Bundes regelt die Bestimmung die Tatbestände, aus denen sich ein hohes Risiko für die betroffene Person ergibt, nicht abschliessend. Wenn zusätzlich eine grosse Anzahl Personen betroffen ist, legt die Behörde die Bearbeitung ihrer Datenschutzbehörde zur Stellungnahme vor (Stufe 3, Art. 20 E-KDSG).

### 13.7 Datensammlungen bzw. Registerpflicht

In der Vernehmlassung war das Register sehr umstritten. Einige begrüsst die Beschränkung auf besonders schützenswerte Personendaten (VBG, IG ländlicher Raum, Worb, Bern), andere forderten, dass im Register auch das Betreiben eines Profilings ersichtlich sein sollte (DJB, Grüne). Wenige beantragten, das Register wie bisher umfassend beizubehalten (BAV, digitale Gesellschaft, Thun) oder ganz abzuschaffen (Langenthal, Inselgruppe). Verschiedene Kantone behalten das Register in umfassender Form bei (so etwa der Kanton Zürich oder Basel-Stadt), andere beschränken die Verzeichnispflicht auf Strafbehörden (so etwa Basel-Land oder Luzern). Kritisiert wurden etwa Aufwand und Schwierigkeit der Aktualität bei der Führung des Registers. Der Datenschutzbeauftragte kann jedoch die Behörden sensibilisieren und sowohl die Erfassung als auch die Nachführung einfach gestalten. Um den Aufwand zu reduzieren, werden die Register ausserdem auf besonders schützenswerte Personendaten beschränkt. Aus Transparenzgründen soll daran festgehalten werden. Besonders heikel kann ausserdem sein, wenn die Behörden **Profilings mit hohem Risiko** betreiben oder **algorithmische Entscheidungssysteme** (AES oder s.g. Künstliche Intelligenz) mit einem hohen Risiko für die betroffene Person nutzen. Deshalb sollen diese Bearbeitungen ebenfalls von den Behörden offengelegt werden.

### 13.8 Meldepflichten bei Verletzungen der Datensicherheit

Eine Meldepflicht besteht nach europäischen Recht teilweise erst bei einem schweren Eingriff bzw. hohen Risiko für die betroffenen Personen und teilweise bereits bei einem Risiko. Das Datenschutzgesetz



des Bundes verlangt ein hohes Risiko für die betroffene Person. Dies soll verhindern, dass selbst unbedeutende Verletzungen gemeldet werden müssen. Die Behörde muss dafür die Auswirkungen für die betroffenen Personen beurteilen. Die Kantone regeln die Meldepflicht ebenfalls unterschiedlich: So verlangen beispielsweise die Kantone Zürich oder Luzern ebenfalls ein hohes bzw. grosses Risiko für die betroffene Person und im Kanton Basel-Land entfällt die Meldepflicht nur, wenn die Datenschutzverletzung voraussichtlich nicht zu einem Risiko für die Grundrechte der betroffenen Personen führt. Die Vernehmlassungsvorlage verlangte ebenfalls kein hohes Risiko für die betroffene Person, da die Meldepflicht die Regel und nicht die Ausnahme sein sollte. Ziel war es, dass die Datenschutzbehörde die Behörde möglichst frühzeitig und umfassend bei der Gewährleistung der Datensicherheit unterstützen kann. Mehrere Teilnehmerinnen und Teilnehmer der Vernehmlassung verlangen jedoch, dass die Meldepflicht nur greifen soll, wenn durch den Vorfall «voraussichtlich ein **hohes** Risiko für die Grundrechte der betroffenen Person» besteht. Da die Begriffsdefinition die meldepflichtigen Fälle offenbar zu wenig einschränkt, wird die Bestimmung ans Bundesrecht angeglichen.

### 13.9 Zentralisierung Datenschutzbehörden

In der Vernehmlassung bewerteten die Teilnehmerinnen und Teilnehmer die vorgeschlagene Teilzentralisierung unterschiedlich. Neun begrüßten diese (FDP, Verein eGov, Thun, Worb, VBG, Lyss, DJB, Grüne, Bern), drei weitere sprachen sich für eine komplette Zentralisierung aus (Burgdorf, Langenthal und Köniz, jedoch mit Wahlfreiheit). Lediglich drei (IG ländlicher Raum, SVP, GPK Muri) befürworteten, dass sämtliche Gemeinden und gemeinderechtliche Körperschaften weiterhin eigene Datenschutzbehörden führen.

Die Kantone organisieren die Datenschutzaufsicht sehr unterschiedlich, jedoch gibt es nur sehr wenige, die eine zwingende kommunale Datenschutzaufsicht kennen, so beispielsweise der Kanton St. Gallen. Die dezentralisierte Variante wird nicht weiterverfolgt, da sich nur eine Minderheit dafür ausspricht und damit weder ein erhöhtes Datenschutzniveau noch eine effizientere Ressourcennutzung erreicht wird. Die im Entwurf gewählte Variante der **Teilzentralisierung** hat den Vorteil, dass nicht hauptsächlich die grösseren Gemeinden die kantonale Datenschutzbehörde beanspruchen. Zudem verfügen diese über gut etablierte und professionelle Aufsichtsstellen, die bereits heute ein hohes Datenschutzniveau gewährleisten. Eine ähnliche Lösung kennt der Kanton Zürich, in dem lediglich die Städte Zürich und Winterthur über eine eigene Aufsichtsstelle verfügen. Die übrigen Gemeinden können im Gegensatz zur Vorlage des Kantons Bern wählen, ob sie eine eigene Aufsichtsstelle führen. Diese Wahlmöglichkeit wurde jedoch bereits zu Beginn des Gesetzgebungsprozesses verworfen, da damit eine kantonal zersplitterte Lösung mit qualitativ unterschiedlicher Datenschutzpraxis riskiert würde. Die in die Vernehmlassung geschickte Variante stärkt das Datenschutzniveau und **bleibt** damit **sachgerecht**.

### 13.10 Verwaltungsmassnahmen

#### 13.10.1 Rechtsmittelweg

In der Vernehmlassung war der Rechtsmittelweg an das Verwaltungsgericht umstritten. Da sowohl gemeinderechtliche und landeskirchliche Datenschutzbehörden als auch die kantonale Datenschutzbehörde verfügen können, ist der Instanzenzug differenziert zu betrachten.

Verfügt eine gemeinderechtliche Datenschutzbehörde gegenüber einer Gemeinde oder einer anderen gemeinderechtlichen Körperschaft, könnte sowohl das zuständige Regierungsstatthalteramt als auch die kantonale Datenschutzbehörde Beschwerdeinstanz sein. Die kantonale Datenschutzbehörde übt die Oberaufsicht aus (Art. 43 Abs. 2 E-KDSG). Diese beinhaltet jedoch gerade nicht die Befugnis, anstelle der beaufsichtigten Stellen zu handeln, Entscheide abzuändern oder aufzuheben (vgl. auch Art. 4 GRG). Sie ist als Beschwerdeinstanz ungeeignet.

Nach dem geltenden Recht wäre für Verfügungen der Gemeinden oder der anderen gemeinderechtlichen Körperschaften das zuständige Regierungsstatthalteramt Rechtsmittelbehörde (Art. 26 KDSG und Art. 63 Abs. 1 Bst. a VRPG). Sie üben die kantonale Aufsicht aus (Art. 87 GG). An diesem Instanzenzug sollte auch für Verfügungen der gemeinderechtlichen Datenschutzbehörden festgehalten werden. Zwei Gemeinden und der Verband Bernischer Gemeinden sprechen sich für diese Lösung aus, die umgesetzt wird.

Die kantonale Datenschutzbehörde ist keiner Direktion untergeordnet. Sie gilt wie die Finanzkontrolle als selbstständige Organisationseinheit innerhalb der Verwaltung (vgl. Ziff. 7.9.4). Entsprechend sah der Vernehmlassungsentwurf als Rechtsmittelinstanz unmittelbar das Verwaltungsgericht vor. Unabhängig davon, ob die kantonale Datenschutzbehörde gegenüber einer Gemeinde, einer anderen gemeinderechtlichen Körperschaft (inkl. Kirchgemeinden) oder einer kantonalen Behörde verfügt. Diese Lösung entspricht dem KdK-Leitfaden und dem bernischen Rechtsmittelsystem. So sind namentlich auch Verfügungen der kantonalen Finanzkontrolle beim Verwaltungsgericht anfechtbar.<sup>143</sup> Sofern die kantonale Datenschutzbehörde verfügt, wird an der Vorlage festgehalten.

Ebenfalls zu regeln ist die Beschwerde gegen Verfügungen der landeskirchlichen Datenschutzbehörde. Damit sind nicht die Kirchgemeinden als gemeinderechtliche Körperschaft gemeint. Bei letzteren übt die kantonale Datenschutzbehörde die Aufsicht aus. Verfügungen der landeskirchlichen Behörden, die ausschliesslich oder ergänzend zum landeskirchlichen Recht auch auf staatliches Recht ergangen sind, müssen direkt bei den staatlichen Rechtsmittelbehörden gemäss VRPG angefochten werden (Art. 23 des Gesetzes über die bernischen Landeskirchen [Landeskirchengesetz]<sup>144</sup>). Erste Rechtsmittelinstanz gegen diese Verfügungen ist demzufolge das Verwaltungsgericht (Art. 74 VRPG).

### **13.11 Verfügungskompetenz gegenüber Gerichten und der Staatsanwaltschaft**

Mehrfach wurde im Vernehmlassungsverfahren die fehlende Verfügungskompetenz der kantonalen Datenschutzbehörde gegenüber den Gerichten und der Staatsanwaltschaft kritisiert (DJB, GLP, Grüne, Gewerbeverband Berner KMU, HIV).

Gestützt auf die Vernehmlassung sieht die Vorlage nun vor, dass die kantonale Datenschutzbehörde im Anwendungsbereich des kantonalen Datenschutzgesetzes (vgl. Art. 3 Abs. 4 E-KDSG) auch gegenüber Gerichtsbehörden und der Staatsanwaltschaft Verfügungen erlassen kann (vgl. Art. 47 Abs. 2 E-KDSG). Dabei sind die Verfügungen und Beschwerdeentscheide der kantonalen Datenschutzbehörde innert 30 Tagen grundsätzlich beim Verwaltungsgericht anfechtbar. Damit ist Verfügungskompetenz der kantonalen Datenschutzbehörde gegenüber den Behörden einheitlich geregelt.

Im Sinne einer Ausnahme des Instanzenzugs ist eine Verfügung beim Obergericht anfechtbar, für den Fall, dass die kantonale Datenschutzbehörde gegenüber dem Verwaltungsgericht verfügt.

Anzumerken ist, dass die Aufsicht nur dort greifen kann, wo das kantonale Datenschutzgesetz anwendbar ist (vgl. Art. 3 Abs. 3 E-KDSG). Massgebend ist, ob ein Verfahren von einer Verfahrensordnung geregelt ist. 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.

Zu erwähnen bleibt, dass die kantonale Datenschutzbehörde bisher noch nie einen Entscheid provoziert hat und auch künftig nicht zu erwarten ist, dass sie viele Verfügungen erlässt. Ihr Ziel ist es, vorwiegend beratend tätig zu sein.

---

<sup>143</sup> BVR 2023 S, 201. E. 1.1.

<sup>144</sup> BSG 410.11

#### **14. Antrag**

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