Vortrag

Datum RR-Sitzung:	16. August 2023
Direktion:	Finanzdirektion
Geschäftsnummer:	2020.KAIO.134
Klassifizierung:	Nicht klassifiziert

Gesetz über die Informations- und Cybersicherheit (ICSG)

Inhaltsverzeichnis

1. Zusammenfassung

Mit der Digitalisierung der Verwaltung wird die Informations- und Cybersicherheit immer wichtiger, um die zunehmenden Angriffe von Cyberkriminellen auf Verwaltungssysteme abzuwehren. Dafür fehlen in der Kantonsverwaltung heute in vielen Punkten die technischen, organisatorischen und rechtlichen Grundlagen. Die Informations- und Cybersicherheit in der Verwaltung ist nur ansatzweise und auf tiefer Normebene geregelt. Zudem schreibt das neue Bundesgesetz vom 18. Dezember 2020 über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG)[1] den Kantonen bei der Bearbeitung von Bundesinformationen oder der Nutzung von ICT-Systemen des Bundes eine gleichwertige Gesetzgebung vor. Das ISG tritt am 1. April 2023 in Kraft.

Das hier vorgeschlagene Gesetz über die Informations- und Cybersicherheit (ICSG), das im Rahmen des gesamtstaatlichen Projekts Informationssicherheit Kanton Bern (IS BE) erarbeitet wurde, soll diese Lücken füllen. Es ergänzt die Gesetzgebung über die zentralen Personendatensammlungen (PDSG)[2], die digitale Verwaltung (DVG)[3] und die Revision des Datenschutzgesetzes (KDSG)[4]. Der Regierungsrat hat für diese Gesetzgebungsarbeiten mit den Richtlinien der Regierungspolitik 2019 bis 2022[5] und der Strategie Digitale Verwaltung (SDV)[6] die Grundsteine gelegt. Zudem beschloss der Strategische ICT-Ausschuss (SIA) der kantonsverwaltung die Informationssicherheitsstrategie BE 2022 bis 2025 (Strategie ISBE)[7].

Das ICSG soll auf die Risiken, Bedürfnisse und Möglichkeiten des Kantons Bern ausgerichtet werden. Es ist mit seinen 32 Artikeln deutlich schlanker als das ISG, welches über 100 Artikel umfasst. Für die Gemeinden und andere autonome Träger öffentlicher Aufgaben gilt das ICSG nur, soweit sie klassifizierte Informationen des Kantons oder des Bundes bearbeiten oder ihre ICT-Mittel nutzen.

Zu den wesentlichen Neuerungen gehören Regeln für die oberste Führung zur Prävention, für die Klassifizierung von Informationen und ICT-Mittel sowie für die Personensicherheitsprüfung (PSP). Die übergeordneten Koordinations- und Steuerungsaufgaben im Bereich der Informations- und Cybersicherheit sollen in die kantonalen Organe der digitalen Verwaltung und der ICT integriert werden.

Die Informations- und Cybersicherheit beschränkt sich nicht auf die ICT-Mittel. Massnahmen zur physischen und insbesondere zur personellen Sicherheit sind ebenso zu ergreifen. Denn der Mensch stellt das grösste Risiko für die Informations- und Cybersicherheit dar.

Das ICSG soll zusammen mit der dazugehörigen Verordnung im Verlauf des Jahres 2024 in Kraft gesetzt werden.

[1] BBl 2020 9975; https://www.fedlex.admin.ch/eli/fga/2020/2696/de
[2] PDSG, BSG 152.05; https://www.belex.sites.be.ch/frontend/versions/2140
[3] 2021.STA.1412: DVG, Unterlagen 2. Lesung Frühlingssession 2022
[4] KDSG, BSG 152.04; https://www.belex.sites.be.ch/frontend/versions/2000
[5] RRB 1311/2018
[6] RRB 719/2019
[7] Strategie ISBE: https://wwwin.kaio.fin.be.ch/intranet_kaio_fin/de/index/das_kaio/das_kaio/weisungen/1_1_strategie.assetref/dam/documents/intranet_kaio_fin/das_kaio/de/Weisungen/1_1_005_Informationssicherheitsstrategie%20BE%202022_2025.pdf

2. Informations- und Cybersicherheit

2.1 Risiken der digitalisierten Gesellschaft

Die Bedeutung von Informationen wird oft erst nach einem Vorfall und beim Eintreten negativer Auswirkungen erkannt. Sowohl für die Behörden als auch für Unternehmen und Privatpersonen kann der Verlust, der Diebstahl, die unberechtigte Preisgabe oder der Missbrauch von Informationen schwerwiegende Folgen haben. Die Informations- und Kommunikationsinfrastruktur sowie die einzelnen ICT-Mittel, die Behörden und Unternehmen zur Unterstützung ihrer Geschäftsprozesse einsetzen, sind verwundbar. Wenn ein Ausfall die Betreiberin einer kritischen Infrastruktur betrifft, die für das Funktionieren der Gesellschaft, der Wirtschaft, des Kantons oder des Bundes unerlässlich ist, kann dies katastrophale Auswirkungen, einschliesslich des Verlusts von Menschenleben, zur Folge haben.

Beispiele sind der Ausfall von ICT-Mitteln im Spitalbereich, wo die Patientendaten, Diagnosen oder medikamentösen Therapien hinterlegt oder lebenserhaltende Maschinen mit dem Internet verbunden sind; oder aber das Telekommunikationsnetz der Notrufzentrale Bern. Oder auch der öffentliche Verkehr oder die staatlichen oder privaten Energieversorger setzen für ihre Steuerungen ICT-Mittel ein, deren Ausfall sehr schwere Auswirkungen hat.

2.2 Strategische Ziele

Der Kanton Bern bewegt sich konsequent in Richtung E-Government und strebt das Primat der digitalen Verwaltungsführung an. Er verfolgt gemäss der Strategie Digitale Verwaltung (SDV) vom 26. Juni 2019, Ziff. 4, die folgende Vision (Ziff. 4):

> *Die digitale Verwaltung ist selbstverständlich: transparente, wirtschaftliche und medienbruchfreie elektronische Behördendienstleistungen für die Wirtschaft, Bevölkerung und Verwaltung.*

Das Primat der digitalen Verwaltung hat der Grosse Rat in Artikel 5 DVG verankert:

> *[1] Die Behörden handeln, informieren und kommunizieren digital, ausser wenn sie ihre Aufgaben in dieser Form nicht wirksam erfüllen können.*
> *[2] Rechtlich massgebend ist die digitale Form von Dokumenten.*
> *(…)*

Der Schutz von Informationen und Personendaten ist für die Staatsführung entscheidend, insbesondere für die Reputation und damit für das alles entscheidende Vertrauen in die Behörden. Daher legt die SDV ihrer Umsetzung u.a. das folgende Prinzip zu Grunde (Ziff. 6):

> *Vertrauenswürdigkeit und Sicherheit: Bei der Umsetzung neuer Lösungen ist dem Rechtssetzungsbedarf, dem Datenschutz und der Informationssicherheit frühzeitig Rechnung getragen.*

Die Informationssicherheitsstrategie BE 2022 bis 2025 vom 14. Dezember 2021 formuliert daher auch die folgende Vision einer Informationssicherheit für die Kantonsverwaltung:

> *Die Direktionen, Staatskanzlei und Justiz gewährleisten in allen Bereichen eine einheitliche und optimierte Informationssicherheit:*
>
> - *Sie handeln sicherheits- und verantwortungsbewusst in einer digitalisierten Umgebung;*
> - *Sie schützen ihre Informationen und Werte mit adäquaten, risikogemässen Massnahmen.*
>
> *Die erforderlichen Ressourcen zu Umsetzung der Ziele und Vorgaben betreffend Informationssicherheit werden durch die Direktionen, Staatskanzlei und Justiz zur Verfügung gestellt.*

Die Kantonsverwaltung setzt die in der Strategie formulierten Sicherheitsziele und strategischen Stossrichtungen – darunter auch das ICSG – seither um.

Weil im Kanton Bern aber alle kantonalen und kommunalen Behörden via ICT-Mittel miteinander vernetzt sind, kann die Informations- und Cybersicherheit nur mit einheitlichen, für alle Behörden geltenden Regeln gewährleistet werden. Zu diesem Zweck wird das ICSG erlassen.

2.3 Bedeutung und Inhalt

Die Informations- und Cybersicherheit wird nicht nur durch technische Schwächen von ICT-Mitteln, sondern vor allem durch menschliche Schwächen gefährdet; z.B. finanzielle Probleme oder kriminelle Neigungen. Deshalb muss das ICSG-Regelwerk nicht nur technische Sicherheitsmassnahmen, sondern auch Massnahmen für Mitarbeiterinnen und Mitarbeiter und deren Führungskräfte vorsehen.

Die Informationen und Personendaten sollen nach dem aktuellen Stand der Technik und der Praxis geschützt werden. Damit werden einerseits das störungsfreie Funktionieren des Staates gewährleistet (Sachinformationen), andererseits aber auch die Grundrechte und insbesondere der Privat- und Geheimbereich (Familienleben, Krankheiten, Sexualleben) natürlicher Personen geschützt (Personendaten).

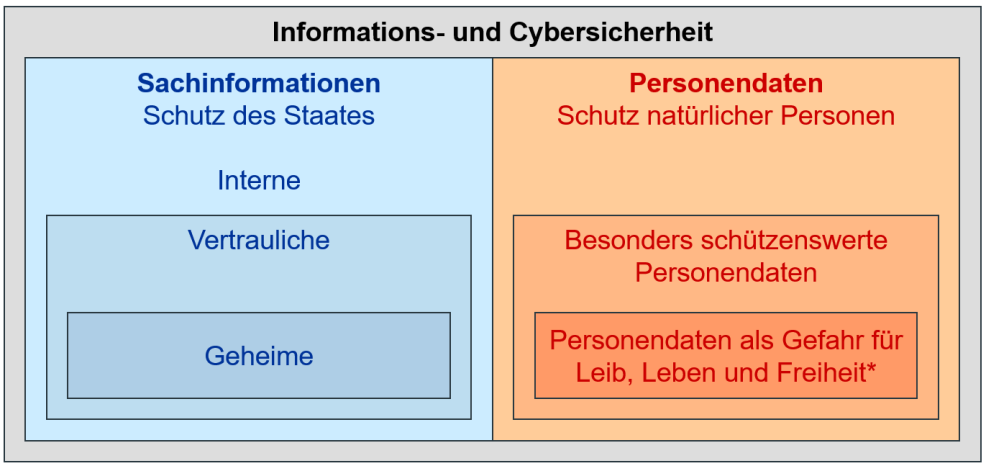

Abbildung 1: Wirkungsbereich, Ziele und Inhalt der Informations- und Cybersicherheit

*z.B. Angaben zu Personen des Kantons, die für den Nachrichtendienst des Bundes oder als verdeckte Ermittler gegen das organisierte Verbrechen arbeiten, oder zu Eltern, deren Kinder eine Entführung durch den anderen Elternteil befürchten müssen. Keine eigene Kategorie von Personendaten nach KDSG; erfordern jedoch infolge ihres Gefährdungspotentials besonders starken Schutz (Art. 14 Abs. 1 KDSG).

Der durch Verfassung und Gesetz garantierte Datenschutz ist nur realisiert, wenn die Informations- und Cybersicherheit dem aktuellen Stand der Technik sowie der Praxis entspricht und zudem die folgenden Elemente der Informations- und Cybersicherheit sichergestellt sind:

a) <u>Vertraulichkeit:</u>
   Auf Informationen dürfen nur Personen Zugriff haben, die dazu befugt sind. Eine unrechtmässige Bekanntmachung von Informationen kann das Amtsgeheimnis, das Berufsgeheimnis, das Geschäftsgeheimnis oder die Persönlichkeit Privater schwer verletzen; z.B. das Bekanntwerden von Vorerkrankungen eines COVID-Patienten oder die genauen Standorte der zentralen COVID-Impfstofflager.

b) Integrität:
Informationen müssen richtig, vollständig, aktuell und daher möglichst fälschungssicher sein. Andernfalls kann dies bis zum Tod führen; z.B. falsche Angaben über Vorerkrankungen eines COVID-Patienten oder der echte und fälschungssichere Ausweis der tatsächlich gegen COVID-geimpften Person.

c) Verfügbarkeit:
Informationen müssen im Moment ihres Bedarfs verfügbar sein, ansonsten wichtige Entscheidungen nicht oder falsch getroffen werden; z.B. Informationen als Grundlagen zum Entscheid von Swissmedic über die Zulassung von COVID-Impfstoffen oder die funktionstüchtige COVID-Zertifikat-Applikation auf dem Mobile.

d) Nachvollziehbarkeit:
Informationen müssen ihren Quellen, Wege und Bearbeitungszeitpunkten zugeordnet werden können. Es muss ersichtlich sein, wer wann welche Information bearbeitet hat; z.B. muss auf dem COVID-Zertifikat ersichtlich sein, wer die Impfung erhalten und wann diese stattgefunden hat sowie welche Behörde für die Ausstellung des COVID-Zertifikats verantwortlich ist. (Der Begriff der «Bearbeitung» hat im ICSG die gleiche breite Bedeutung wie im KDSG: «Das Bearbeiten von Personendaten umfasst jeden Umgang mit Personendaten, wie das Beschaffen, Aufbewahren, Verändern, Verknüpfen, Bekanntgeben oder Vernichten», Art. 2 Abs. 4 KDSG).

e) Cybersicherheit:
Sie ist gewährleistet, wenn die vorgenannten vier Anforderungen der Informationssicherheit bei der Bearbeitung oder beim Austausch von Informationen über die Informations- und Kommunikationsinfrastrukturen – insbesondere über das Internet – erfüllt sind (Art. 3 Bst. a Cyberrisikenverordnung des Bundes)[8]; z.B. muss der Server des Bundes über das Internet erreichbar sein, um die Gültigkeit des COVID-Zertifikats überprüfen zu können.

Nur mit einer tatsächlich wirkungsvollen Informations- und Cybersicherheit können die Ziele des Datenschutzes erfüllt werden: Der Schutz und die Richtigkeit der persönlichen Daten als Teil des verfassungsmässigen Grundrechts auf Schutz der Privatsphäre (Art. 12 Abs. 3, Schutz der Privatsphäre, sowie Art. 18, Datenschutz, der Kantonsverfassung[9], vgl. nachfolgende Grafik):

[8] CyRV, SR 120.73; https://www.fedlex.admin.ch/eli/cc/2020/416/de#art_3
[9] KV, BSG 101.1; https://www.belex.sites.be.ch/frontend/versions/2420

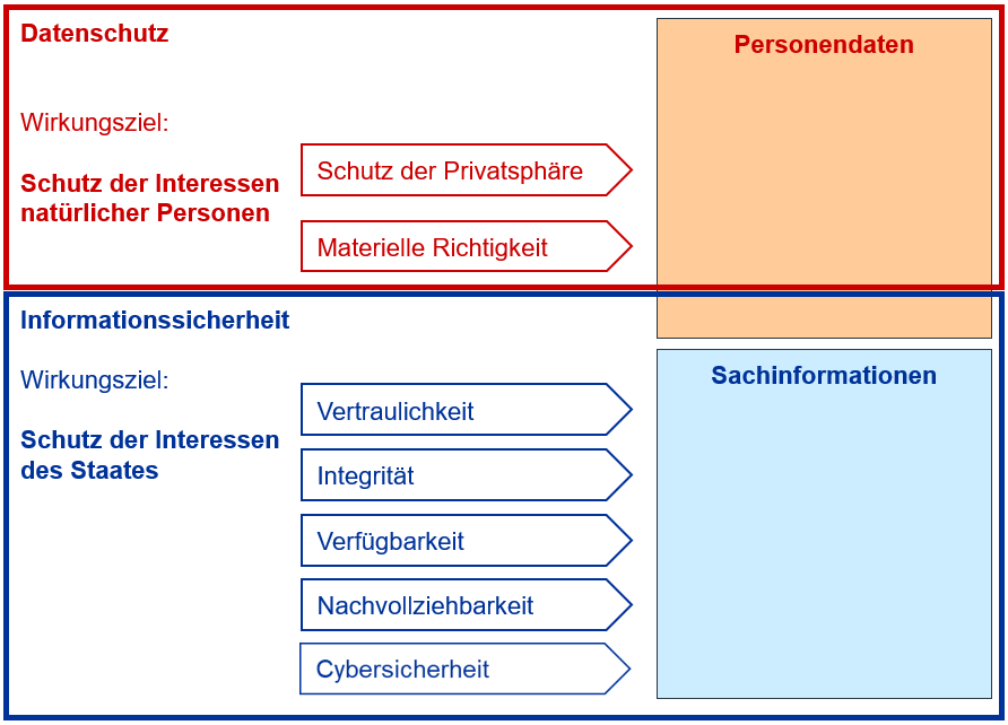

Abbildung 2: Informations- und Cybersicherheit als Voraussetzung des Datenschutzes

Obenstehende Ausführungen zeigen, dass die Informations- und Cybersicherheit nicht nur spezifische Anforderungen an die Technik, sondern auch an das Recht, die Organisation, die Prozesse und insbesondere auch an die Menschen und deren Führung stellt. Die Informations- und Cybersicherheit betrifft sämtliche Belange der Staatsführung und weist auch deshalb einen sehr hohen Grad an Komplexität auf.

3. Ausgangslage

3.1 Bund

Die Bundesversammlung hat am 18. Dezember 2020 das ISG verabschiedet, welches per 1. April 2023 in Kraft gesetzt wurde. Die Kantone arbeiten z.B. in den Bereichen Strassenverkehr, Strafverfolgung, Militär oder Nachrichtendienst mit Informationen und Personendaten des Bundes und verwenden dessen Applikationen. Daher verpflichtet das ISG die Kantone, entweder eigene Vorschriften mit gleicher Wirkung zu erlassen, oder aber die auf die weitreichenden Bundesaufgaben zugeschnittenen Regeln des ISG zu übernehmen (Art. 3 ISG, Geltung für die Kantone). Mit dem ICSG wird der erstere Weg gewählt und die Vorschriften des Bundes werden damit auf die Berner Verhältnisse zugeschnitten, was sie effektiver und effizienter macht. Für die Verwaltungsbereiche, in denen keine Bundesinformationen bearbeitet und keine Bundessysteme genutzt werden, ist der Kanton grundsätzlich frei, ob und wie er die Informationssicherheit regelt. Es wäre aber nicht praktikabel, dafür separate, inhaltlich unterschiedliche Sicherheitsvorschriften zu erlassen. Daher gilt das ICSG für alle Behörden einheitlich (zum Vorbehalt für den Grossen Rat siehe unten zu Art. 30 ICSG).

3.2 Kanton Bern

3.2.1 Heutige Situation

Mit der Analyse des Berner Rechts zur Informations- und Cybersicherheit wurde Folgendes festgestellt (Rechtsgrundlagenanalyse vom 30. Oktober 2019 zum Projekt Informationssicherheit BE):

1. Es bestehen keine formell-gesetzlichen, generell-abstrakten Vorschriften über die Ziele, den Inhalt, Aufbau und die Prozesse der Informations- und Cybersicherheit des Kantons Bern. Damit fehlen das gemeinsame Verständnis und die einheitliche Umsetzung der Informations- und Cybersicherheit durch die Berner Behörden.

2. Die Anforderungen an die Informations- und Cybersicherheit sind ausschliesslich auf die Personendaten ausgerichtet, erst ab Stufe Verordnung unvollständig sowie unsystematisch und nur im Kontext des Datenschutzes geregelt (Datenschutzverordnung vom 2008, DSV)[10]. Die Cybersicherheit sowie der Schutz von Sachinformationen sind nicht geregelt.

3. Die Klassifizierung von Dokumenten (nicht: Informationen) der Kantonsverwaltung ist mit der Verordnung über die Klassifizierung, die Veröffentlichung und die Archivierung von Dokumenten zu Regierungsratsgeschäften (Klassifizierungsverordnung, KRGV)[11] alleine auf die traktandierten Regierungsratsgeschäfte beschränkt. Für alle übrigen Informationen, unabhängig ob in analoger, elektronischer oder mündlicher Form, bestehen weder Klassifizierungs- noch Bearbeitungsvorschriften. Damit fehlt dem Kanton Bern das Rückgrat der Informations- und Cybersicherheit.

4. Der Schutz von Informationen oder Objekten, z.B. Spitäler oder Justizvollzugsanstalten, ist auch von der Direktionsverordnung über Informationssicherheit und Datenschutz von 2011 (ISDS DV)[12] nicht erfasst.

5. Die Regelung der verwaltungsweiten Sicherheitsorganisation beschränkt sich in der ISDS DV alleine auf das Nennen und Zuweisen der IT-Sicherheitsverantwortlichen pro DIR/STA/JUS (IT-SIVE) sowie des IT-Sicherheitsbeauftragten, der – analog zum Datenschutzbeauftragten – verwaltungsweite Zuständigkeit hat. Dem Kanton Bern fehlt eine effektive und effiziente Sicherheitsorganisation.

3.2.2 Angestrebte Situation

3.2.2.1 Motion «Sichere Kommunikation und Datenaustausch»

Die Motion «Sichere Kommunikation und Datenaustauch» vom 28. November 2018[13] befasst sich mit dem Austausch von Informationen und Personendaten in der Kantonsverwaltung. Der Grosse Rat beschloss am 10. November 2019 über die Motion wie folgt:

Der Regierungsrat wird beauftragt, dafür zu sorgen bzw. sicherzustellen, dass

1. *auf allen Ebenen der Verwaltung sowie bei Police Bern für die digitale Kommunikation immer die sicherste Software und die sichersten Applikationen verwendet werden:*
   Annahme und gleichzeitig Abschreibung.
2. *auch in Schulen sichere Kommunikationssoftware und -applikationen verwendet werden:*
   Annahme als Postulat.
3. *die Daten auf Schweizer Servern gespeichert und aufbewahrt werden:*
   Annahme.
4. *in der Kommunikation mit Externen, wenn es sich um schützenswerte Daten und Dokumente handelt, ebenfalls sichere Kommunikationssoftware und Applikationen verwendet werden:*
   Annahme und Abschreibung.

[10] DSV, BSG 152.040.1; https://www.belex.sites.be.ch/frontend/versions/2001
[11] KRGV, BSG 152.17; https://www.belex.sites.be.ch/frontend/versions/1578
[12] ISDS DV, BSG 152.040.2; https://www.belex.sites.be.ch/frontend/versions/835
[13] Motion 277-2018

3.2.2.2 Strategie Digitale Verwaltung – Schwerpunktplanung 2021

Mit Beschluss vom 20. Januar 2021 hat der Regierungsrat das ICSG sowie das Projekt Informationssicherheit BE (ISBE) als Vorhaben bezeichnet, welches «*die Digitalisierung wesentlich voranbringen, entscheidende Grundlagen für spezifische Digitalisierungsvorhaben bilden und damit einen herausragenden Beitrag zur Umsetzung der Strategie [Digitale Verwaltung] leisten*.».

Das ICSG ist die gesetzliche Grundlage und damit die Voraussetzung für die einheitliche, umfassende, effektive und effiziente Informations- und Cybersicherheit im Kanton Bern.

4. Grundzüge der Neuregelung

4.1 Normenarchitektur

Im Kanton Bern befinden sich die folgenden vier Gesetze bereits in Kraft oder in Erarbeitung:

- Gesetz über die zentralen Personendatensammlungen (PDSG)[14], welches am 1. März 2021 in Kraft getreten ist.
- Gesetz über die digitale Verwaltungsführung (DVG)[15], welches vom Grossen Rat in der Frühlingssession 2022 in zweiter Lesung beraten und verabschiedet wurde.
- Datenschutzgesetz (KDSG), dessen Revision im Sommer 2020 von der Direktion für Inneres und Justiz lanciert wurde.
- Gesetz über die Informations- und Cybersicherheit (ICSG), hiermit initiiert.

Diese Gesetze bilden die vier Säulen der Informationssicherheit und des Datenschutzes:

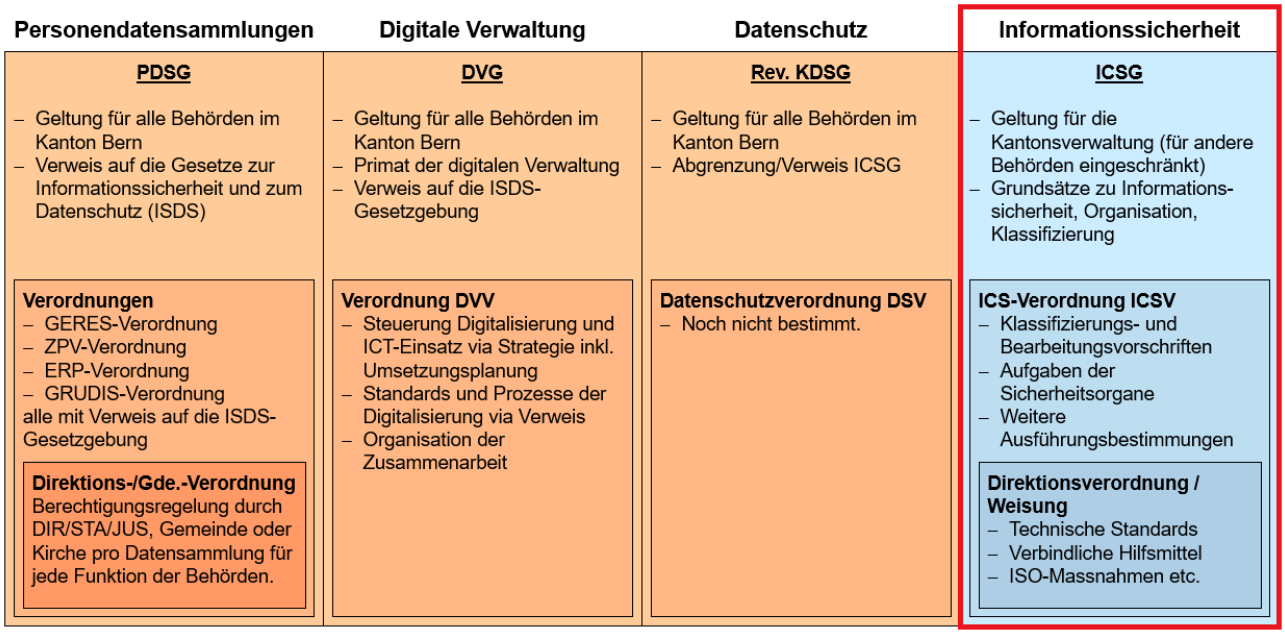

Abbildung 3: Die vier Säulen der Informationssicherheit und des Datenschutzes der Berner Gesetzgebung

[14] BSG 152.05; https://www.belex.sites.be.ch/frontend/fulltext_searches/258800
[15] RRB 750/2021: DVG, Antrag des Regierungsrates an den Grossen Rat vom 16. Juni 2021

4.2 Normenhierarchie

Das ICSG schafft die Grundlage für ein gesamtes Regelwerk zur Steuerung und Führung der Informations- und Cybersicherheit des Kantons Bern. Dieses erstreckt sich von der generell-abstrakten Ebene des ICSG, über die ICSV bis hin zur individuell-konkreten Realisierung eines Projekts, zur Umsetzung einer Massnahme bezüglich Risikominderung oder zur personellen Besetzung einer kritischen Funktion in der Berner Verwaltung:

Abbildung 4: Grundlagen zur Steuerung und Führung der Informations- und Cybersicherheit

4.3 Inhaltsübersicht

Das ICSG ist viel kürzer und übersichtlicher ausgestaltet als das ISG des Bundes mit über 100 Artikeln. Einerseits entfallen im ICSG Regelungsthemen, die nur für den Bund mit seinen besonderen Sicherheitsbedürfnissen (Armee, Nachrichtendienste, Aussenpolitik etc.) relevant sind. Andererseits wurden Detailbestimmungen ohne grundsätzliche, strategische Bedeutung oder Grundrechtseingriffe auf die Verordnungs- oder Weisungsebene verlagert, um eine rasche Anpassung der Vorschriften an die Entwicklung der Technik und Risiken zu ermöglichen. Auf Regeln über die physische Sicherheit der kritischen Infrastrukturen wird im ICSG verzichtet: Dies betrifft nicht Fragen der Informationssicherheit, und für die bereits ergriffenen risikobasierten Schutzmassnahmen ist keine besondere gesetzliche Grundlage nötig (die Videoüberwachung ist bereits im Polizeigesetz geregelt).

Es ist notorisch, dass der Mensch für den Schutz von Informationen nach wie vor das grösste Risiko darstellt. Private Schulden oder charakterliche Schwächen können Menschen anfällig für Korruption oder andere kriminelle Handlungen machen. Aus diesen Gründen verlangen praxisgemäss schon heute z.B. das Amt für Informatik und Organisation (KAIO), das Personalamt (PA), die Steuerverwaltung (SV) oder das Strassenverkehrs- und Schifffahrtsamt (SVSA) teilweise von ihren Mitarbeitenden die Auszüge aus dem Straf- und dem Betreibungsregister. Ebenfalls verlangt werden diese bei allen Kandidierenden der Richterwahlen. Die Wahlen erfolgen sodann durch den Grossen Rat. Eine ausdrückliche gesetzliche Grundlage liegt heute nur für die Polizei mit den Artikeln 160 ff. Polizeigesetz (PolG)[16] vor. Zudem haben die Polizei sowie das Amt für Justizvollzug (AJV) für ihre Objekte (Führungsanlagen und Gefängnisse) und beauftragten Unternehmen Schutzbedürfnisse, die über die ICT-Sicherheit hinausgehen.

[16] BSG 551.1; https://www.belex.sites.be.ch/frontend/versions/2231

4.4 Wirkungsziele

Mit dem ICSG-Regelwerk sollen neben dem Hauptziel der Informations- und Cybersicherheit zudem die folgenden Wirkungsziele erreicht werden:

a) Gemeinsames Verständnis der Klassifizierungsstufen INTERN[17], VERTRAULICH und GEHEIM.
b) Reduktion der klassifizierten Informationen dank klaren und einheitlichen gesetzlichen Vorgaben zur Klassifizierung:

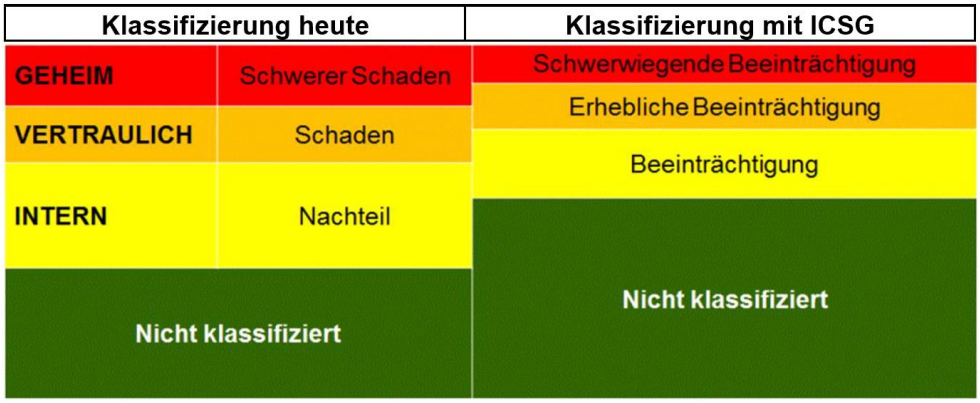

Abbildung 6: Reduktion der Klassifizierungen durch ICSG

c) Dank gezielter, risikobasierter Klassifizierung und damit dank der Reduktion klassifizierter Informationen können Kosten für Sicherungsmassnahmen gespart werden: «Gold in den Safe, Holz auf den Scheiterhaufen.».
d) Das ICSG schafft mit den Ausführungserlassen für alle Behörden und Bearbeitungsstufen konsistente Vorschriften über den Umgang mit klassifizierten Informationen.
e) Die nötige Aufmerksamkeit für die Informations- und Cybersicherheit des Personals und insbesondere der Führungskräfte wird sichergestellt («Awareness»).
f) Den Führungskräften werden Hilfsmittel zur Verfügung gestellt, um die für die Informations- und Cybersicherheit relevanten Schwächen der Mitarbeitenden zu erkennen.
g) Es wird eine Sicherheitsorganisation mit klaren Zuständigkeiten, Aufgaben und Kompetenzen geschaffen.

5. Erlassform

Die gesetzlichen Rahmenbedingungen der Informations- und Cybersicherheit sind einerseits wegen ihrer grundlegenden und strategischen Natur und andererseits wegen den schweren Grundrechtseingriffen bei der Personensicherheitsprüfung als Gesetz zu erlassen. Die Umsetzungsbestimmungen werden als Verordnungen, Direktionsverordnungen oder Weisungen erlassen (vgl. Ziff. 4.2 oben).

6. Rechtsvergleich

6.1 Bund

Das Parlament hat am 18. Dezember 2020 das ISG verabschiedet, welches am 1. April 2023 in Kraft getreten ist (s. Ziff. 3.1 oben).

[17] Gemäss der Praxis des Bundes werden die Klassifizierungsvermerke in Grossbuchstaben geschrieben, um sie vom entsprechenden Wort der Alltagssprache zu unterscheiden und um sie auf Dokumenten besser erkennbar zu machen. Auf Wunsch der Redaktionskommission werden die Bezeichnungen der Klassifizierungsstufen im Erlasstext dagegen nicht in Grossbuchstaben geschrieben. Die kantonalen Gestaltungsrichtlinien werden nötigenfalls näher regeln, auf welchen Dokumenten an welchen Stellen die Gross- oder Kleinschreibweise gewählt werden soll.

6.2 Kantone

Ein Vergleich mit der Gesetzgebung der anderen Kantone (Stand Anfang 2022) zeigt, dass es kein Regelungsmodell gibt, an dem sich der Kanton Bern orientieren könnte. Denn noch kein Kanton verfügt aktuell über ein analoges Gesetz. Zwei Kantone verfügen auf Verordnungsebene Informations- und Cybersicherheitsvorschriften, so der Kanton Zürich, der damit das umfassende Regelwerk der ISO-Norm 27'001 auf Stufe Kantonsverwaltung umsetzt. Das ISG sowie seine Absicht, auch die anderen Behörden einzubeziehen, lässt ihn den Erlass eines Gesetzes in Erwägung ziehen. Der Kanton Freiburg hat eine Verordnung nur über die Sicherheit der Personendaten erlassen.

7. Umsetzung, geplante Evaluation des Vollzugs

Die Umsetzungsprojekte und ihr Zeitplan richten sich nach der Umsetzungsplanung der Strategie IS BE (dort Abbildung 6, Seite 16):

Abbildung 7: Umsetzung ICSG inkl. Projekt ISBE

Die Evaluation des Vollzugs wird Gegenstand der im Rahmen der Umsetzung zu erarbeitenden kontinuierlichen Verbesserungsprozesse sein.

8. Erläuterungen zu den Artikeln

8.1 Allgemeine Bestimmungen

Artikel 1 – Zweck

Absatz 1 weist darauf hin, dass sowohl die Informationen als solche als auch die ICT-Mittel vom Gesetz erfasst werden. Das Gesetz macht grundsätzlich keinen Unterschied zwischen Informationen und Daten: Beide Begriffe werden unter dem Begriff Informationen subsumiert. Der Begriff ICT-Mittel wird in Artikel 4 Buchstabe d definiert.

Absatz 2: Sicherheit ist kein Selbstzweck. Der Schutz der Informationen dient den genannten öffentlichen Interessen. Geschützt werden hier also primär die Interessen der Behörden des Kantons Bern, deren Schutz jedoch mittelbare Wirkung auf das Vertrauen Dritter in die Behörden hat. Das ICSG schützt demnach die folgenden öffentlichen Interessen:

a) Der Schutz der Entscheidungs- und Handlungsfähigkeit der Behörden durch Massnahmen der Informations- und Cybersicherheit ist ein Kernzweck dieses Gesetzes (Bst. a). Die Behörden sind für die Erfüllung ihrer verfassungsmässigen und gesetzlichen Aufgaben von der Verfügbarkeit, Integrität und Nachvollziehbarkeit sowie, in ausgewählten Fällen, der Vertraulichkeit ihrer Informationen sowie vom zuverlässigen Funktionieren der Informatikinfrastruktur abhängig.

b) Mit Buchstabe b werden in erster Linie Informationen aus den Bereichen Polizei und Nachrichtendienst (im Auftrag des Bundes), Teile der Landesversorgung (kantonale Pflichtlager) sowie die Mittel, welche die Behörden zur Wahrung der Sicherheit einsetzen, geschützt. Derartige Informationen weisen oft einen erhöhten Bedarf an Vertraulichkeit auf, da ihr Missbrauch existenzgefährdende Folgen für den Staat, die Bevölkerung oder bestimmte Personen oder Personengruppen haben kann. Aus demselben Grund müssen die ICT-Mittel der Behörden, welche zur Unterstützung von kritischen Sicherheitsaufgaben eingesetzt werden, auch in Krisenzeiten stets verfügbar und funktionstüchtig bleiben.

c) Mit Buchstabe c wird die Einhaltung der gesetzlichen und vertraglichen Verpflichtungen der Behörden zum Schutz von Informationen erfasst, die nicht unter die Buchstaben a und b fallen. Damit soll die «Compliance» umgesetzt werden, also der gesetzes- und vertragsgemässe Schutz der Informationen.

   Die Behörden bearbeiten zur Erfüllung ihrer gesetzlichen Aufgaben sehr viele Informationen, die sie aufgrund verschiedenster gesetzlicher Bestimmungen schützen müssen (Datenschutzgesetz, Steuergesetz, Polizeigesetz, Anwaltsgesetz etc.) oder die sie von Dritten nur unter der Bedingung der Gewährleistung eines angemessenen Schutzes erhalten.

   Berufs-, Geschäfts- und Fabrikationsgeheimnisse oder die Wahrung der Vertraulichkeit und Integrität von Personendaten stellen zwar keine unmittelbaren Eigeninteressen der Behörden dar. Die Berhörden sind aber gesetzlich oder durch Vereinbarung verpflichtet, diese Informationen zu schützen. Wenn bekannt wird, dass die Behörden ihre Verpflichtungen zum Schutz dieser Informationen nicht einhalten, kann ihre Vertrauenswürdigkeit und damit ihre Handlungsfähigkeit erheblich darunter leiden. Zudem könnten deren Organe straf- oder zivilrechtlich zur Verantwortung gezogen werden.

   Buchstabe c stellt somit ein Auffangbecken für alle Informationen dar, welche die Behörden bearbeiten und schützen, aber nicht unbedingt klassifizieren müssen. Er schützt überdies das Interesse der Behörden an der Aufrechterhaltung ihrer hohen Vertrauenswürdigkeit.

Artikel 2 – Geltungsbereich

Das ICSG greift in Bezug auf den Geltungsbereich den Ansatz des ISG auf. Danach gelten aus dem ISG für die Kantone nur die Bestimmungen über klassifizierte Informationen, soweit sie klassifizierte Informationen des Bundes bearbeiten, und über die Sicherheit beim Einsatz von Informatikmitteln, soweit sie auf Informatikmittel des Bundes zugreifen (Art. 3 Abs. 1 ISG) – wobei auch diese Bestimmungen des ISG für die Kantone nicht gelten, wenn sie eine mindestens gleichwertige Informationssicherheit gewährleisten (Art. 3 Abs. 2 ISG), was vorliegend mit dem ICSG umgesetzt wird.

Dementsprechend gilt das ICSG vollumfänglich nur für die kantonalen Behörden. Für die Gemeinden sowie die anderen organisatorisch autonomen Behörden (Spitäler, Hochschulen, Staatsunternehmen etc.) gilt es im Sinne der Subsidiarität nur in dem Umfang, wie sie mit Informationen und Systemen des Kantons oder des Bundes interagieren. Für die restlichen Informationen liegt es an den betroffenen Behörden, sich dem Schutzbedarf ihrer Informationen angemessene Sicherheitsvorschriften zu geben. Artikel 17 KDSG verpflichtet sie zudem zur Sicherung von Personendaten (s. unten zu Art. 3).

Artikel 3 – Verhältnis zu anderen Gesetzen

Absatz 1 regelt den potenziellen Konflikt zwischen dem ICSG (Informationsschutz) und dem im Gesetz über die Information der Bevölkerung und die Medienförderung (IMG; BSG 107.1) geregelten Öffentlichkeitsprinzip. Wie auf Bundesebene wird dieser Konflikt dadurch gelöst, dass die Regeln des IMG vorgehen. Das heisst, dass eine Klassifizierung die Akteneinsicht gemäss IMG nicht ausschliesst, sondern nur als Element der Interessenabwägung nach Artikel 27 ff. IMG berücksichtigt wird.

Absatz 2 regelt dagegen nicht einen Konflikt zwischen Gesetzen, sondern bringt zum Ausdruck, dass die Methoden des ICSG, wie das Risikomanagement gemäss Artikel 5, auch zum Schutz von Informationen, der von anderen Gesetzen vorgeschrieben ist, massgeblich sind. Besondere Erlasse, z.B. das Datenschutzgesetz, das Gesetz über den Grossen Rat, das Steuergesetz, das Gesundheitsgesetz oder das Anwaltsgesetz beinhalten nämlich eigene Vorschriften über Geheimhaltungspflichten. Soweit abweichend, gehen diese Vorschriften vor (Abs. 2). Ein besonderes Augenmerk gilt es dabei auf die Abgrenzung von Informationen gemäss ICSG und Personendaten gemäss KDSG zu richten. Das KSDG regelt für die kantonalen Behörden den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden (Art. 1, Zweck). Es legt unter anderem fest, dass Personendaten nur rechtmässig, verhältnismässig, zweckmässig und für die betroffenen Personen möglichst transparent bearbeitet werden dürfen (Art. 5, Zulässigkeit der Datenbearbeitung). Personendaten werden weiterhin nach den Regeln des KDSG bearbeitet.

Soweit das KDSG jedoch Anforderungen an den *tatsächlichen Schutz* der Vertraulichkeit, Verfügbarkeit und Integrität von Personendaten stellt, kommt das ICSG als ergänzendes Recht zur Anwendung. Konkret verlangt Artikel 17 KDSG nämlich, dass wer Personendaten bearbeitet, für deren Sicherung zu sorgen hat. Artikel 4 bis 6 DSV konkretisieren dabei Anforderungen an den Schutz von Personendaten, namentlich sollen die technischen und organisatorischen Massnahmen dem gegenwärtigen Stand der Technik Rechnung tragen. Es wird jedoch nicht bestimmt, was Stand der Technik ist, oder wer für dessen Umschreibung zuständig ist. Hier kommt künftig das ICSG mit seinen Ausführungsbestimmungen, insbesondere der dazugehörigen Verordnung, zur Anwendung. Personendaten sind hinsichtlich ihrer Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit ebenfalls zu schützen. In der Regel werden Personendaten aber nicht formell klassifiziert, denn eine Klassifizierung ist den enger gefassten öffentlichen Interessen des Kantons gemäss Artikel 1 Absatz 2 ICSG vorbehalten. Personendaten werden ausnahmsweise dann klassifiziert, wenn nicht nur die natürliche Person gemäss KDSG, sondern mit ihr auch die öffentlichen Interessen nach ICSG zu schützen sind; z.B. die besonders schützenswerten Personendaten von Bundesrätinnen und Bundesräten.

Die Ausführungsbestimmungen zum ICSG werden demnach sowohl Informationen als auch Personendaten je nach Schutzbedarf einem bestimmten Schutzniveau, abhängig von Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit, zuweisen (vgl. dazu das Konzept gemäss Abbildung 8 zu Art. 8). Die Standardisierung der Massnahmen nach dem Stand von Wissenschaft und Technik, die mit den jeweiligen Schutzniveaus verknüpft wird, wird damit auch dazu dienen, die Anforderungen der Datenschutzgesetzgebung an die Datensicherheit zu erfüllen, und somit den Datenschutz beim Kanton erhöhen.

Artikel 4 – Begriffe

Der Begriff *ICT-Mittel* nach Buchstabe d wird als Oberbegriff für alle Mittel der Informations- und Kommunikationstechnik verwendet und ist identisch mit demjenigen nach Artikel 4 Absatz 3 Buchstabe a DVG. Auf Verordnungs- und Weisungsstufe werden detailliertere Begriffe (Informationssystem, Netzwerk, Anwendung, Sprachübermittlung, Telefonie usw.) verwendet und definiert. Ein ICT-Mittel kann auch aus mehreren Systemen oder Mitteln bestehen, die eine funktionale Einheit bilden.

8.2 Grundsätze

Artikel 5 – Pflichten der Behörden

Absatz 1 Buchstabe a verpflichtet die Behörden ausdrücklich, in ihrem Verantwortungsbereich den Schutzbedarf ihrer Informationen zu prüfen. Dies setzt vorab voraus, dass sie überhaupt wissen, über welche Informationen sie verfügen. Sie müssen also über ein vollständiges und aktuelles Inventar ihrer Informationen und Daten verfügen; heute ist ein solches Inventar identisch mit demjenigen aller ICT-Mittel, welche Informationen oder Daten beinhalten. Erst wenn der Schutzbedarf im Lichte der zu wahrenden öffentlichen Interessen ermittelt ist, kann auch über deren risikoorientierten, effektiven und effizienten Schutzmassnahmen entschieden werden, nach dem Motto: «Holz auf die Scheiterbeige, Gold in den Safe.». Mit einem vollständigen Inventar, welches das «Gold» vom «Holz» unterscheidet, und einer richtigen Schutzbedarfsanalyse werden nicht nur die öffentlichen Interessen geschützt, sondern die Behörden können damit auch viele Steuergelder sparen. Denn es ist offensichtlich unwirtschaftlich, Holz im Safe aufzubewahren.

Buchstabe b nennt die vier Schutzkriterien der Informationssicherheit, nämlich die Vertraulichkeit, Integrität, Verfügbarkeit und die Nachvollziehbarkeit der Information, die oben in Ziff. 2.3 beschrieben sind.

Obwohl sich die Anforderung nach einem angemessenen Schutz der ICT-Mittel vor Missbrauch und Störungen grundsätzlich bereits aus Buchstabe b ergibt, wird sie in Buchstabe c noch ausdrücklich erwähnt; dies, weil die Unterstützung der Geschäftsprozesse durch die Technik immer mehr an Bedeutung gewonnen hat. Ihr gutes Funktionieren stellt heute eine unentbehrliche Voraussetzung für die effiziente Aufgabenerfüllung der Behörden dar.

Das Risikomanagement (*Absatz 2*) ist die zentrale Methode der Informationssicherheit. Dazu gehört, dass die Risiken für die Informationssicherheit laufend erkannt und beurteilt werden, dass die Risiken vermieden oder auf ein tragbares Mass reduziert werden, und dass die tragbaren Risiken und ihre Inkaufnahme dokumentiert werden. Dies erfolgt zweckmässigerweise als Teil des gesamten Risikomanagements der Behörde.

Die Beurteilung der Risiken setzt folgendes voraus: Gute Kenntnisse der gesetzlichen Aufgaben und der entsprechenden Geschäftsprozesse, regelmässige Beurteilung der Bedrohungen, Analyse der Schwachstellen, sowie die Einschätzung der Eintrittswahrscheinlichkeit und des potenziellen Schadensausmasses. Risiken können vermieden werden, indem auf eine bestimmte, zu riskante Tätigkeit ganz verzichtet wird. Sie können mit technischen, organisatorischen oder rechtlichen Massnahmen reduziert werden. Oder sie können bewusst in Kauf genommen werden. Solche Restrisiken müssen klar ausgewiesen und von den Entscheidträgerinnen und -trägern akzeptiert werden.

Absatz 3 trägt der Tatsache Rechnung, dass die absolute Sicherheit ein unerreichbares Ideal ist. Der Aufwand für die Behebung verbleibender kleinerer Sicherheitslücken kann unverhältnismässig hoch werden. Die zuständigen Behörden müssen daher darauf achten, dass ihre Massnahmen risikoorientiert, effektiv und effizient sind. Entsprechend ist bei der Verfolgung der Schutzmassnahmen von den übergeordneten Stellen eine Güterabwägung zwischen Sicherheitskosten und -nutzen vorzunehmen. Erschweren Sicherheitsmassnahmen die Aufgabenerfüllung der Mitarbeitenden zu sehr, ist die Wahrscheinlichkeit gross, dass sie entweder nicht eingehalten oder gar absichtlich umgegangen werden.

Artikel 6 – Beauftragte Dritte

Die Behörden sind für ihre Aufgabenerfüllung häufig auf Leistungen der Privatwirtschaft oder anderer Stellen angewiesen. Die auftragserteilenden Behörden haben in diesem Fall dafür zu sorgen, dass bei

der Auftragserteilung und -ausführung die gesetzlich vorgesehenen Massnahmen eingehalten werden. Die einzuhaltenden Sicherheitsmassnahmen werden in der Regel vertraglich geregelt. Grundsätzlich sollten Beauftragte erst dann Zugang zu Informationen oder zu ICT-Mitteln der Behörden erhalten, wenn sie selbst die erforderlichen Massnahmen umgesetzt haben. Das ICSG verlangt von den Behörden auch, dass sie die Umsetzung der Massnahmen angemessen (d. h. risikoorientiert) überprüfen. Dies kann zum Beispiel im Rahmen eines Besuchs vor Ort oder mittels schriftlicher Bestätigung durch die Drittpartei erfolgen. Schliesst der Auftrag die Ausübung einer sicherheitsempfindlichen Tätigkeit ein, so können die Behörden die erforderlichen PSP einleiten (Art. 21 Abs. 1 Bst. c).

Artikel 7 – Reaktionsfähigkeit und Vorsorge

Zu Vorfällen im Bereich der Informations- und Cybersicherheit wird es immer wieder kommen. Es ist deshalb nötig, einen einheitlichen und effektiven Ansatz für den Umgang mit solchen Vorfällen anzuwenden.

Die Behörden müssen nach Buchstabe a die erforderlichen Massnahmen treffen, um Informations- und Cybersicherheitsvorfälle überhaupt und frühzeitig identifizieren zu können (z. B. regelmässige Kontrollen, Sensoren, Alarmanlagen, Netzwerküberwachung, regelmässige Auswertung von Log-Files). Sie müssen zudem ein Verfahren festlegen, welches anzuwenden ist, wenn Vorfälle oder Schwachstellen identifiziert werden, und zudem klare Zuständigkeiten für die Behandlung der Vorfälle zuweisen. Interne und externe Mitarbeitende müssen im Weiteren wissen, wie sie beim Eintreten eines Ereignisses zu reagieren haben, damit dessen Auswirkungen minimiert werden können. Damit aus Vorfällen gelernt wird, müssen die Behörden auch dafür sorgen, dass die Ursachen eines Vorfalls abgeklärt und ausgewertet werden.

Die Behörden und insbesondere die Exekutiven müssen darüber hinaus alle notwendigen Vorkehrungen treffen, damit sie ihre Kernaufgaben selbst in ausserordentlichen Situationen termingerecht erfüllen können (sog. Business-Continuity-Management, BCM). Es ist heute davon auszugehen, dass die Erfüllung aller Aufgaben der Behörden von grosser Wichtigkeit für die Bevölkerung vom zuverlässigen Einsatz von ICT-Mitteln abhängt. Daher ist gemäss Buchstabe b erforderlich, dass die Behörden die aus ihrer strategischen Sicht unverzichtbaren Aufgaben identifizieren und für den Fall einer schwerwiegenden Verletzung der Informations- und Cybersicherheit (z. B. dauernder Ausfall eines Systems) Vorsorgeplanungen erstellen und soweit risikoangemessen entsprechende Übungen durchführen lassen. Weil sich die Risiken und die daraus folgenden Verletzungen der Informationssicherheit laufend ändern können, sind auch die Vorsorgeplanungen periodisch zu überprüfen und zu aktualisieren (Bst. c).

8.3 Organisatorische Massnahmen

Artikel 8 – Klassifizierung

Mit der Klassifizierung von Informationen legen die Behörden fest, wie wichtig es ist, die Informationen vor der Kenntnisnahme durch Unberechtigte zu schützen. Die Massnahmen dafür werden auf Verordnungsebene geregelt.

Absatz 1: Massgeblich für die Klassifizierung ist das öffentliche Interesse am Schutz von Informationen, mit Ausnahme des Schutzes des öffentlichen Interesses nach Artikel 1 Absatz 2 Buchstabe c, welches keinen eigenständigen Grund zur Klassifizierung darstellt (vgl. die Bemerkungen dazu). Personendaten nach dem KDSG oder Geschäfts-, Fabrikations- oder Berufsgeheimnisse werden demnach grundsätzlich nicht klassifiziert, es sei denn, dass einzelne Informationen zum Schutz des öffentlichen Interesses nach Artikel 1 Absatz 2 Buchstaben a und b klassifiziert werden müssen. Dasselbe gilt für Informationen, die bei den Gerichten oder Staatsanwaltschaften im Rahmen ihrer ordentlichen

Verfahren bearbeitet werden. Die Mehrheit dieser Informationen sind Personendaten, die zwar schützenswert sind, die aber aufgrund des vorliegenden Gesetzes nicht klassifiziert werden müssen. Hingegen können die besonderen Massnahmen, die zum Schutz solcher Informationen getroffen werden, klassifiziert werden (zum Beispiel ein Informationssicherheits- und Datenschutzkonzept, ISDS-Konzept).

Dieser Unterscheidung liegt das folgende Konzept zu Grunde:

Informations- und Cybersicherheitsgesetz ICSG		**Informations- und Cybersicherheits-verordnung ICSV**	**Datenschutzgesetz KDSG**
Schutz der Interessen des Staates		*Vollzug und Massnahmen für Informations- und Cybersicherheit (analog auch für KDSG)*	*Schutz der Interessen natürlicher Personen*
ICT-Mittel	**Informationen**	**Schutzmassnahmen nach Stand der Technik**	**Personendaten**
Sehr hoher Schutz	GEHEIM	Schutzniveau 3	Personendaten als schwere Gefahr für die Sicherheit Einzelner (Leib, Leben, Freiheit)
Hoher Schutz	VERTRAULICH	Schutzniveau 2	Besonders schützenswerte Personendaten und Personendaten mit besonderer Geheimhaltung (Berufs-, Steuergeheimnis etc.)
Grundschutz	INTERN	Schutzniveau 1	Allgemeine Personendaten
	Nicht klassifiziert	Schutzniveau 0	Nicht personenbezogene Daten (ausserhalb des Schutzbereichs des KDSG)
PSP nach ICSG durch zentrale Fachstelle oder dezentrale Behörde.		Vollzugsvorschriften für ICSG und – per Verweis – auch für KDSG	Prüfung der Vertrauenswürdigkeit der Personen nach *Personalgesetz* durch dezentrale Behörde

Abbildung 8: Konzept Schutz der Vertraulichkeit; Abgrenzung ICSG–KDSG; ICSV als «Interface»

Wichtig ist die Unterscheidung der Schutzziele des ICSG sowie des KDSG:

Das ICSG schützt primär den Staat vor ungesetzlichem Stören seines Handelns. Das KDSG hingegen schützt Personen vor ungesetzlichen Eingriffen in ihre Persönlichkeit. Beide Interessenslagen verfügen daher über eigene Schutzstufen aus der spezifischen Gesetzgebung (ICSG und KDSG). Diese werden über die vier Schutzniveaus in der zu definierenden Informations- und Cybersicherheitsverordnung (ICSV) synchronisiert. Die Schutzziele sind zwar verschieden, die Schutzmassnahmen jedoch die gleichen. Somit sind nur Personen, welche regelmässig mit als VERTRAULICH oder GEHEIM klassifizierten Informationen arbeiten, einer PSP zu unterziehen. Die dezentralen Anstellungsbehörden, welche besonders schützenswerte Personendaten bearbeiten, können jedoch zur Prüfung der Vertrauenswürdigkeit von Personen gestützt auf das Personalgesetz (PG)[18] selbst eine PSP vornehmen (Ziff. **Fehler! Verweisquelle konnte nicht gefunden werden.** unten).

Absatz 2: Für die Klassifizierungsstufe sind die Schwere und das Ausmass des Schadens massgebend, der durch eine Kenntnisnahme durch Unberechtigte den zu schützenden öffentlichen Interessen zugefügt werden kann. Obschon die Kriterien der Schwere und des Ausmasses der potenziellen Beeinträchtigung für die Klassifizierung massgebend sind, genügen sie alleine nicht. Es muss auch eine vernünftige kausale Verbindung zwischen der unberechtigten Kenntnisnahme der Information und der potenziellen Beeinträchtigung der geschützten Interessen geben. Erforderlich ist somit, dass auch die Häufigkeit bzw. Eintrittswahrscheinlichkeit des Schadens berücksichtigt wird.

Diese Risikobeurteilung kann graphisch wie folgt dargestellt werden:

[18] PG BSG 153.01: https://www.belex.sites.be.ch/frontend/versions/2253

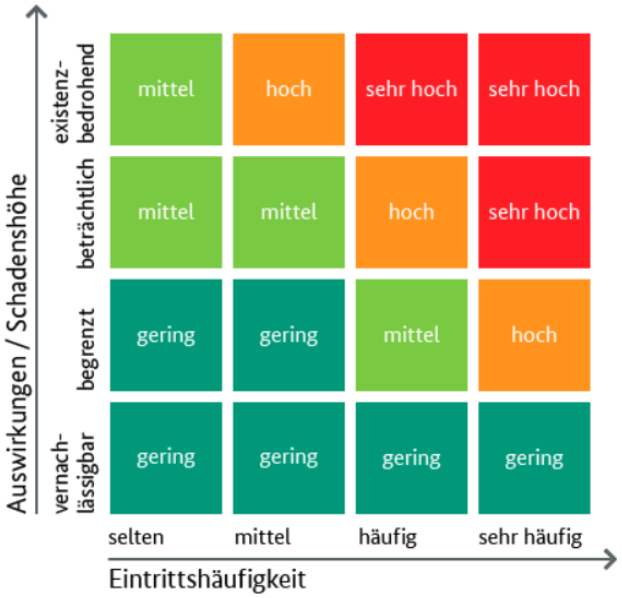

Abbildung 9: Risikomatrix nach BSI-Standard 200-3

Die Klassifizierung einer Information entspricht also dem Ergebnis einer Risikobeurteilung und soll somit den tatsächlichen Schutzbedarf dieser Information wiedergeben.

Bei der Beurteilung des Schutzbedarfs von Informationen politischer Natur ist besondere Zurückhaltung erforderlich. Zwar wird der Schutz der freien Meinungs- und Willensbildung der Behörden von Artikel 1 Absatz 2 Buchstabe a, Entscheidungsfähigkeit, erfasst. In einer modernen Demokratie gehört es aber zur normalen Regierungstätigkeit, dass politische Ideen, Vorschläge, Konzepte und Entscheide in der Öffentlichkeit besprochen und gegebenenfalls auch heftig kritisiert werden. Die Klassifizierung darf also nicht dazu dienen, bestimmte Sachverhalte der öffentlichen Debatte zu entziehen, wenn kein überwiegendes öffentliches Interesse dafür besteht.

Buchstabe a: Als Grenzkriterium zwischen «nicht klassifiziert» und «klassifiziert» gilt, dass qualifizierte Anhaltspunkte vorliegen müssen, welche die Klassifizierung «INTERN» zu begründen vermögen. So darf der potenzielle Schaden nicht einfach vernachlässigbar sein: Die Beeinträchtigung der öffentlichen Interessen muss vielmehr spürbar sein. Wenn es um sicherheitsrelevante Informationen im Sinne von Artikel 1 Absatz 2 Buchstabe b geht, kann der Schwellenwert für die Klassifizierung «INTERN» relativ rasch erreicht werden. Diese wird für derartige Fälle am häufigsten verwendet. So werden einzelne Sicherheitsunterlagen zu ICT-Mitteln oder einfache Einsatzpläne von Sicherheitskräften in der Regel als «INTERN» klassifiziert.

Buchstabe b: Die Klassifizierung «VERTRAULICH» erfordert gegenüber «INTERN» eine erhöhte Schutzanforderung. Es wird ein deutlicher und gewichtiger Schaden verlangt, beispielsweise:

- Die freie Meinungs- und Willensbildung der Behörden wird vorübergehend unrechtmässig erschwert.
- Eine Behörde wird vorübergehend handlungsunfähig.
- Die Erfüllung bestimmter Aufgaben einer Behörde wird über längere Zeit erheblich erschwert.
- Bestimmte Ressourcen der Polizei oder der Sanitätspolizei sind vorübergehend einsatzunfähig.
- Die Sicherheit von Personen oder Gruppen von Personen wird gefährdet.
- Sicherheitsempfindliche Funktionen der Hochwasserregulierung in Thun werden sabotiert.
- Dem Kanton entsteht ein erheblicher finanzieller Schaden.

Buchstabe c: Mit der für «GEHEIM» gewählten Formulierung wird ein besonders grosser, katastrophaler Schaden für die Behörden verlangt, beispielsweise:

- Eine Behörde ist vorübergehend entscheidungs- oder handlungsunfähig oder ihre Entscheidungs- oder Handlungsfähigkeit ist über längere Zeit besonders ernsthaft erschwert.
- Die Erfüllung unverzichtbarer Aufgaben einer Behörde wird vorübergehend verhindert oder über längere Zeit ernstlich erschwert.
- Wesentliche Ressourcen der Polizei oder der Sanitätspolizei sind einsatzunfähig.
- Leib und Leben von ganzen Bevölkerungsgruppen werden gefährdet.
- Das Erbringen unverzichtbarer Dienstleistungen durch kritische Infrastrukturen wird unterbrochen, z.B. im Sicherheits- oder Gesundheitsbereich.
- Eine Gemeinde oder der Kanton erleidet einen schwerwiegenden finanziellen Schaden.

Die Klassifizierung muss sofort ersichtlich und darf nicht mit anderen Vermerken verwechselbar sein. Im internationalen Rahmen hat sich die Regel durchgesetzt, dass die Klassifizierung immer in Grossbuchstaben vermerkt wird.

Absatz 3: Die Klassifizierung ist zwingend, sofern die Kriterien dafür erfüllt sind. Sie muss angesichts des Öffentlichkeitsprinzips und des mit der Klassifizierung verbundenen Aufwands jedoch die Ausnahme bleiben. Daher ist sie auf das erforderliche Mindestmass zu beschränken, d.h., es sind nur so wenige Dokumente zu klassifizieren wie nötig, und es ist nur eine so hohe Klassifizierungsstufe zu wählen wie nötig.

Der Schutzbedarf von Informationen nimmt mit der Zeit oftmals ab oder erübrigt sich nach einem bestimmten Ereignis (z.B. Veröffentlichung eines Berichts oder Abschluss einer bestimmten Massnahme). Die Klassifizierung derartiger, z.B. nicht mehr aktueller, Informationen rechtfertigt sich dann nicht mehr. Sie würde bloss unnötigen Aufwand verursachen. Informationen, die für längere Zeit klassifiziert bleiben müssen, erfordern zudem zunehmend andere technische Schutzvorkehrungen als jene, die nur eine befristete Schutzwürdigkeit haben. Soweit eine Klassifizierung auf Zeit im Voraus nicht möglich ist, muss sichergestellt werden, dass Informationen nicht unnötig klassifiziert bleiben. Eine Überprüfung des Schutzbedarfs soll mindestens im Rahmen der Anbietepflicht nach Artikel 9 des Gesetzes über die Archivierung (ArchG)[19] an das Staatsarchiv erfolgen.

Absatz 4: In der Kantonsverwaltung wird die Zuständigkeit zur Klassifizierung heute der Verfasserin oder dem Verfasser eines Dokuments überlassen, weil sie oder er am besten den Schutzbedarf der Informationen sowie allfällige Risiken einschätzen kann. Die Behörden können aber auch beschliessen, dass die Klassifizierung beispielsweise durch die Behördenleitung, durch eine zentrale zuständige Stelle oder ausschliesslich durch die Linie erfolgen muss. Der Regierungsrat wird dies auf Verordnungsebene näher regeln, einschliesslich der Entklassifizierung von Informationen durch vorgesetzte Stellen und der Entklassifizierung von Archivgut. Er beabsichtigt, wie im Bundesrecht vorzusehen, dass jede Behörde für die Dokumente in ihrem Aufgabenbereich einen Klassifizierungskatalog erlässt, der die einheitliche Klassifizierung der in der Behörde anfallenden Dokumente regelt, und dass die Sicherheitsfachorgane der Verwaltung durch Weisungen regeln können, wie Informationen, die in der ganzen Verwaltung häufig bearbeitet werden, einheitlich zu klassifizieren sind (Art. 17 Abs. 2 des Vernehmlassungsentwurfs zur Informationssicherheitsverordnung, ISV[20]).

Auf Verordnungsebene zu regeln wird auch sein, unter welchen Bedingungen die vor dem Inkrafttreten dieses Gesetzes geschaffenen Informationen klassifiziert werden. Dies, weil es in den Behörden sehr viele bestehende Informationen gibt, die nie auf ihre Klassifizierung hin überprüft wurden. Es wäre wohl in vielen Fällen sehr aufwändig, dies nachzuholen. Der Regierungsrat kann dies daher auf Verordnungsebene differenziert regeln, z.B. mit einer Vorschrift, wonach bestehende Informationen erst dann klassifiziert werden müssen, wenn sie erneut bearbeitet werden (z.B. auf ein Einsichtsgesuch hin).

[19] ArchG, BSG 108.1: https://www.belex.sites.be.ch/frontend/versions/2264
[20] Abrufbar unter: https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-90051.html

Artikel 9 – Zugang zu klassifizierten Informationen

Absatz 1 umschreibt die Voraussetzungen für den Zugang zu klassifizierten Informationen, der wiederum Voraussetzung für das Bearbeiten der entsprechenden Informationen ist. Der Grundsatz «Kenntnis nur, wenn nötig» gilt für jede einzelne klassifizierte Information. Es besteht also kein allgemeines Recht, Zugang zu allen klassifizierten Informationen zu haben. Die Regelung des Zugangs zu klassifizierten Informationen umfasst auch den Zugang zu den Systemen, in denen sich die Informationen befinden.

Bei einem vertraglich vereinbarten Zugangsrecht müssen die entsprechenden Verträge den Zugang zu klassifizierten Informationen vorsehen und deren Bearbeitung regeln. «Gewähr bieten» für einen sachgerechten Umgang setzt voraus, dass die Personen, die klassifizierte Informationen bearbeiten sollen, entsprechend ausgebildet wurden. Ferner müssen sie gegebenenfalls den Nachweis für die Fähigkeit erbringen, die erforderlichen technischen und physischen Sicherheitsmassnahmen einhalten zu können. Für «VERTRAULICH» oder «GEHEIM» klassifizierte Informationen kann zudem die Durchführung einer PSP eine weitere Bearbeitungsvoraussetzung darstellen.

Wegen des Vorrangs des IMG (s. oben zu Art. 3) sind diese Voraussetzungen nicht verbindlich, wenn über die Akteneinsicht nach Artikel 27 ff. IMG entschieden werden soll. Sie können aber im Rahmen der Interessenabwägung nach Artikel 27 Absatz 1 IMG berücksichtigt werden.

Artikel 10 – Zugang in besonderen Verfahren

Absatz 1: Das Verfahrensrecht des Grossen Rates, z.B. betreffend die Öffentlichkeit seiner Organe sowie die Information der Öffentlichkeit nach Artikel 11 ff. des Gesetzes über den Grossen Rat (GRG)[21], sowie dasjenige der Gerichte und der Staatsanwaltschaften bleiben vorbehalten. Für den Zugang zu klassifizierten Informationen (z. B. im Rahmen der Verwendung derselben als Entscheidgrundlage oder als Beweismittel) soll das jeweilige Verfahrensrecht zur Anwendung kommen. Die Verfahrensgesetze des Kantons enthalten selbst Regelungen darüber, wie weit solche Informationen den Verfahrensbeteiligten zur Einsicht freigegeben werden bzw. wie weit sie im Rahmen öffentlicher Verfahren bekannt werden dürfen oder wie weit Zeugen die Aussage unter Hinweis auf gesetzliche Geheimhaltungspflichten verweigern können.

Absatz 2: Vor dem Entscheid über eine Bekanntgabe klassifizierter Informationen an Dritte muss allerdings der klassifizierenden Stelle Gelegenheit gegeben werden, sich zu den Klassifizierungsgründen zu äussern und zu den allfälligen Auswirkungen einer Bekanntgabe angehört zu werden. Das zuständige Organ bzw. Gericht entscheidet dann unter Würdigung der Stellungnahme über das weitere Vorgehen. Wenn also z.B. eine parlamentarische Aufsichtskommission in einem veröffentlichten Bericht aus einem klassifizierten Dokument zitieren will, oder ein Gericht dies in einem veröffentlichten Urteil tun will, oder der Regierungsrat in einer Vorstossantwort auf Aussagen, die seine Mitglieder vor einer Kommission des Grossen Rates gemacht haben, Bezug nehmen will, dann muss vorher die Stellungnahme der klassifizierenden Stelle dazu eingeholt werden. Um zu verdeutlichen, dass diese Anhörungspflicht zwischen Behörden aller Staatsgewalten gilt, spricht die Bestimmung ausdrücklich parlamentarische, Justiz- und Verwaltungsbehörden an.

[21] BSG 151.21: https://www.belex.sites.be.ch/frontend/versions/1628

8.4 Technische Massnahmen

8.4.1 Sicherheitsverfahren

Artikel 11 – Zweck

Die Zeiten sind vorbei, als beispielsweise die Ämter oder die Gerichte ihre eigenen ICT-Mittel im eigenen Haus betrieben. Heute beziehen die Behörden des Kantons in der Regel ihre Informatikleistungen bei hochspezialisierten externen Beauftragten, vorab bei der kantonseigenen Bedag Informatik AG, aber auch bei privaten Unternehmen. Dadurch ist eine organisatorische Trennung zwischen Einsatz und Betrieb von ICT-Mitteln entstanden, die auch wesentliche Auswirkungen auf die Sicherheit hat. Dies ist insbesondere auch der Fall, weil die Informations- und Cybersicherheit meistens fälschlicherweise als reine technische Angelegenheit betrachtet wird, für welche die Beauftragten verantwortlich sind. Das Gesetz legt im Grundsatz fest, welche Aufgaben die auftraggebenden Behörden erfüllen müssen, um ihre Verantwortung in Bezug auf die Sicherheit wahrzunehmen (vgl. Art. 5, Pflichten der Behörden). Der Regierungsrat muss diese Aufgaben in einem standardisiertenn Sicherheitsverfahren für alle Behörden näher umschreiben. Alle kantonalen Behörden haben bereits heute gestützt auf die Direktionsverordnung über Informationssicherheit und Datenschutz (ISDS DV) aus dem Jahr 2011 ein solches Verfahren einzusetzen. Die vorhandenen Vorschriften müssen aber systematisiert und an die Anforderungen der heutigen Technik und Risiken angepasst werden. Die wichtigsten Verfahrensetappen müssen auf Verordnungsebene für alle Behörden, nicht nur diejenigen der Kantonsverwaltung, vereinheitlicht werden. Das Sicherheitsverfahren muss insbesondere die sicherheitsmässigen Aufgaben, Kompetenzen und Verantwortungen derjenigen Stellen festlegen, die den Einsatz von ICT-Mitteln planen und beschliessen.

Weil das Sicherheitsverfahren regelmässig neuen Techniken und Risiken angepasst werden muss, kann der Regierungsrat seine Festlegung an ein gesamtkantonales Fachorgan delegieren, voraussichtlich die Konferenz Digitale Verwaltung und ICT (KDI; s. dazu Ziff. 11 unten).

Artikel 12 – Inhalt

Artikel 12 führt die wichtigsten Eckpunkte des Sicherheitsverfahrens auf:

Buchstabe a: Schutzbedarf

ICT-Mittel werden für bestimmte Zwecke und für eine geplante Lebensdauer eingesetzt. Der erste Schritt besteht darin, bei der Bestimmung des Einsatzzwecks des ICT-Mittels die Geschäftsprozesse zu bestimmen, die mit dem einzusetzenden ICT-Mittel unterstützt werden sollen, sowie die Informationen zu identifizieren, die damit bearbeitet werden sollen. Zu diesem Zeitpunkt – also in der Planungsphase – muss die Behörde den Schutzbedarf der Informationen nach Artikel 5 Absatz 1 erheben sowie die potenziellen Auswirkungen einer Störung oder eines Missbrauchs des einzusetzenden ICT-Mittels auf die öffentlichen Interessen nach Artikel 1 Absatz 2 beurteilen. Diese «Business-Impact-Analyse» muss von der für den Geschäftsprozess verantwortlichen Stelle durchgeführt werden. Bei der Beurteilung des Schutzbedarfs muss auch berücksichtigt werden, dass ICT-Mittel Teil einer technischen und geschäftlichen Umgebung (sog. Architektur) sind. Die frühzeitige Identifizierung von Vernetzungen und Abhängigkeiten hilft auch, die Massnahmen dort umzusetzen, wo sie am wirksamsten sind. Aus der Schutzbedarfsanalyse ergeben sich die Anforderungen an den Schutz der Informationen sowie die Sicherheitseinstufung gemäss Buchstabe b (nachfolgend) des ICT-Mittels.

Buchstabe b: Sicherheitsstufe und Sicherheitsmassnahmen

Vgl. die Bemerkungen zu Artikel 13 unten.
Buchstabe c: Umsetzung und Überprüfung der Sicherheitsmassnahmen

Die Behörden haben festzulegen, welche Massnahmen umgesetzt werden müssen und wie die Umsetzung dieser Massnahmen zu prüfen ist. Grundsätzlich sollen standardisierte Massnahmen zur Anwendung kommen, die das entsprechende Schutzniveau gemäss ICSV gewährleisten (vgl. Abbildung 8 oben). Die Überprüfung der Umsetzung der Massnahmen ist in diesem Zusammenhang besonders wichtig.

Buchstabe d: Sicherheitsfreigabe

Mit der Sicherheitsfreigabe soll sichergestellt werden, dass die verantwortliche Behörde vor dem Einsatz eines ICT-Mittels die identifizierten Restrisiken kennt und auch bereit ist, diese zu tragen. Ist sie der Meinung, die Restrisiken seien noch zu hoch, kann sie die Freigabe verweigern und die Umsetzung ergänzender risikomindernder Massnahmen verlangen.

Buchstabe e: Risikoüberprüfung

Informations- und Cybersicherheit verändert sich kontinuierlich. Die Behörden müssen deshalb ein Vorgehen festlegen, um eine Veränderung der Risiken bei bereits eingesetzten ICT-Mitteln zu berücksichtigen.

Artikel 13 – Sicherheitsstufe

Die ICT-Mittel werden je nachdem, wie schädlich eine Verletzung der Sicherheit der mit ihnen bearbeiteten Informationen ist, in Sicherheitsstufen eingeteilt. Sie entsprechen der Regelung in Artikel 17 ISG:

- Die Sicherheitsstufe «Grundschutz» gilt für alle ICT-Mittel, die keine besonderen Schutzanforderungen aufweisen, und erlaubt die Bearbeitung von Informationen bis und mit der Klassifizierung INTERN.
- Die Sicherheitsstufe «hoher Schutz» ist für ICT-Mittel mit erhöhtem Schadenpotenzial vorgesehen, und erlaubt die Bearbeitung von Informationen bis und mit der Klassifizierung VERTRAULICH.
- Die Sicherheitsstufe «sehr hoher Schutz» ist für ICT-Mittel mit sehr hohem Schadenpotenzial vorgesehen, und erlaubt die Bearbeitung von Informationen bis und mit der Klassifizierung GEHEIM.

Für jede Sicherheitsstufe werden risikoangemessene standardisierte Schutzmassnahmen festgelegt, etwa zu Anmeldeverfahren, zur Verschlüsselung und zum Umgang mit Datenträgern bzw. Geräten.

Artikel 14 – Zuständigkeit

Die Zuständigkeit für die Durchführung des Sicherheitsverfahrens liegt bei derjenigen Behörde, die den Einsatz von ICT-Mitteln beschliesst und Dritten z.B. mittels Rahmenverträgen in Auftrag gibt. Dies ist die Behörde, die gemäss dem in Artikel 32 Absatz 2 DVG verankerten «Dreischichtenmodell» für das ICT-Mittel zuständig ist: das Amt für Informatik und Organisation (KAIO) für die ICT-Grundversorgung des Kantons und die jeweilige Fachdirektion bzw. das jeweilige Fachamt für die Fach- und Konzernapplikationen.

Die beauftragende Behörde ist allein für die Geschäftsprozesse sowie für die Umsetzung der Sicherheitsanforderungen verantwortlich. Sie muss deshalb ihre Geschäfts- und Sicherheitsanforderungen ihren Beauftragten, welche die ICT-Mittel betreiben, klar, nachvollziehbar und verbindlich kommunizieren. Behörden, welche gestützt auf Rahmenverträge die ICT-Mittel bei den Beauftragten beziehen, können sich auf das Ergebnis des durchgeführten Sicherheitsverfahrens verlassen.

Artikel 15 – Delegation

Mit der Bestimmung wird die Absicht verdeutlicht, auf Verordnungsebene einheitliche Schutzstufen und damit einheitliche Schutzmassnahmen für vergleichbar schützenswerte ICT-Mittel, Informationen und Personendaten festzulegen, wie in Abbildung 8 oben als mögliche Umsetzung gezeigt.

8.4.2 Sicherheit beim Betrieb

Artikel 16

Mit diesem Artikel wird klargestellt, dass die Verantwortung für die Sicherheit im Betrieb von ICT-Mitteln auch mit dessen Outsourcing bei der zuständigen Behörde (Art. 32 Abs. 2 DVG, s. oben) verbleibt. Unter den am Betrieb beteiligten Behörden kann die Verantwortung im Rahmen der Ausführungsbestimmungen oder durch Weisungen differenziert geregelt werden (vgl. auch Art. 29 Abs. 2 DVG). Bei der Nutzung der ICT-Grundversorgung beispielsweise ist das KAIO dafür verantwortlich, dass die Arbeitsplätze, Server, Drucker etc. der Verwaltung sicher ausgestaltet sind, und die nutzenden Behörden sind dafür verantwortlich, dass ihr Personal diese ICT-Mittel in einer sicheren Weise nutzt.

Die Hauptverantwortung für die Sicherheit beim Einsatz von ICT-Mitteln liegt bei den Auftraggebern, also den Behörden. Die Beauftragten sind ihrerseits dafür zuständig, beim Betrieb dieser ICT-Mittel die Sicherheit nach dem Stand der Wissenschaft und Technik zu gewährleisten. Sie müssen die Anforderungen und Massnahmen nach diesem Gesetz sowie die vereinbarten zusätzlichen Anforderungen der Behörden berücksichtigen und umsetzen.

Behördeninterne Beauftragte fallen als Behörden alle unter den Anwendungsbereich dieses Gesetzes und müssen es deshalb für ihre Tätigkeiten anwenden.

Externe Beauftragte werden zwar mit Artikel 16 KDSG den Behörden gleichgestellt, wenn sie Personendaten in deren Auftrag bearbeiten. Für nicht personenbezogene Informationen müssen sie aber zudem vertraglich verpflichtet werden, die Massnahmen dieses Gesetzes einzuhalten. Jeder Beauftragte steht in der Pflicht, seine Netzwerke zu überwachen. Anomalien, Angriffe und Störungen müssen frühzeitig entdeckt, beurteilt und dem Auftraggeber mitgeteilt werden, um darauf reagieren zu können. Bei Verdacht auf Gefährdung oder bei konkreten Verletzungen der Informations- und Cybersicherheit kann es vorkommen, dass die elektronischen Aktivitäten bestimmter interner oder externer Mitarbeitender (oder Maschinen) detailliert geprüft werden müssen. Ist in diesem Zusammenhang die namentliche Identifizierung einer Person erforderlich, dann sind die Vorschriften der Randdatenverordnung (RDV)[22] über die Bearbeitung von Personendaten, die im Rahmen der Benutzung der Informatikinfrastruktur anfallen, anwendbar.

8.5 Physische Massnahmen

Artikel 17 – Grundsatz

Bei den physischen Schutzmassnahmen geht es darum, die Risiken durch physische Bedrohungen zu reduzieren. Zu diesen Risiken gehören unter anderem menschliche Handlungen (z. B. Spionage, Diebstahl, Vandalismus oder Sabotage). Dazu gehören aber auch Elementarschäden (z. B. Hitze, Feuer, Wasser, Staub, Vibrationen usw.). Artikel 17 legt den Grundsatz fest, dass die Behörden den physischen Schutz ihrer Informationen und ICT-Mittel gewährleisten müssen. Zu verhindern ist insbesondere der unberechtigte Zugang zu den Informationen oder ICT-Mitteln etwa durch Zugangskontrollen, Videokameras, Schliesssysteme, Sicherheitsbehältnisse, Aktenvernichtungsgeräte usw. Gegen

[22] RDV BSG 153.011.5: https://www.belex.sites.be.ch/frontend/versions/1781

Elementarschäden werden beispielsweise Brandmeldeanlagen und automatische Löschanlagen eingesetzt. Die Massnahmen des physischen Schutzes betreffen sowohl Informationen und ICT-Mittel, die sich in den Räumlichkeiten der betroffenen Behörde oder Organisation befinden, als auch solche, die öffentlich zugänglich sind. Es handelt sich beim zweiten Fall einerseits um Informationen und ICT-Mittel, die von ihrem üblichen Standort (Büro) mitgenommen werden und die anschliessend – ausserhalb des üblichen Sicherheitsperimeters, z.B. im Homeoffice – geschützt werden müssen. Es handelt sich aber auch um Informationen und Einrichtungen, Verkabelungen und Versorgungsleitungen, die nicht unter der ständigen Kontrolle der Behörde oder Organisation stehen. Besondere Aufmerksamkeit muss beispielsweise Zugangspunkten wie Anlieferungs- und Ladezonen geschenkt werden.

Artikel 18 – Sicherheitszonen

Die Ausscheidung bestimmter Räume bzw. Bereiche als Sicherheitszone stellt eine physische Massnahme der Informations- und Cybersicherheit dar, die bereits heute bei der Polizei oder beim Amt für Justizvollzug (AJV) ergriffen wird, insbesondere zum Schutz von Server-, Arbeits- oder Führungsräumen. Eine Sicherheitszone muss vordefiniert werden, identifizierbar sein und entsprechend geschützt werden. Sie kann einzelne Räume, einen Komplex von Räumen oder ein Gebäude umfassen. Die Massnahmen in den Sicherheitszonen werden risikoorientiert auszugestalten sein. Über ihre tatsächliche Einrichtung entscheidet die Behörde nach einer Risikobeurteilung.

Absatz 2 regelt die besonderen Befugnisse der Behörde oder Organisation, die eine Sicherheitszone einrichtet:

- Das Mitführen bestimmter Gegenstände in eine Sicherheitszone kann eingeschränkt werden. Das Mitführen von Bild- oder Tonaufnahmegeräten (inkl. Smartphones oder Notebooks mit entsprechenden Funktionen) ist in der Regel nur mit besonderer Bewilligung erlaubt.

- Bereiche der Sicherheitszone, die für die Informations- und Cybersicherheit besonders wichtig sind (z. B. die Zutrittszone zu einem besonderen Serverraum, der Administratorarbeitsplatz oder der Archivraum mit «GEHEIM» klassifizierten Informationen), können mittels Videoaufnahmegeräten überwacht werden. Die Ausgestaltung der allfälligen Videoüberwachung und die Aufbewahrungsdauer der Aufzeichnungen (die auf Verordnungsebene zu regeln sein wird) muss verhältnismässig sein (s. dazu die «Erläuterungen zur Videoüberwachung am Arbeitsplatz» des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten, EDÖB[23]).

- Beim Ein- oder Ausgang kann die Behörde oder Organisation Taschen- oder Personenkontrollen durchführen lassen. Damit soll verhindert werden, dass Personen ohne Bewilligung Geräte in die Sicherheitszone mitnehmen oder Informationen (z. B. mit einem USB-Memorystick) entwenden. Taschenkontrollen benötigen als risikobasierte Sicherheitsmassnahmen einen konkreten Anlass, sind grundsätzlich anzukündigen und in verhältnismässiger Weise umzusetzen.[24] Die Bestimmung stellt keinen Eingriff in das von der der Kantonspolizei ausgeübte staatliche Gewaltmonopol dar. Sollte zur Durchsetzung von Kontrollen die Anwendung von Zwang notwendig sein, ist daher zwingend die Kantonspolizei beizuziehen. Die Bestimmung stellt mit anderen Worten keine Rechtsgrundlage für die Anwendung von Zwang z.B. durch private Sicherheitsorgane oder Behördenmitarbeitende dar.

- Zur Durchsetzung der Vorschriften sollen auch Bürokontrollen möglich sein. Dabei wird unter anderem die Einhaltung der sogenannten «Clean-Desk-Policy» überprüft: Es dürfen keine schutzwürdigen Informationen auf dem Schreibtisch oder anderswo herumliegen, der PC muss gesperrt oder ausgeschaltet sein, Datenträger müssen unter Verschluss gehalten werden, die Schubladen müssen geschlossen sein, der Abfallkorb darf keine klassifizierten Informationen enthalten usw.

[23] Abrufbar unter: https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/arbeitsbereich/ueberwachung-am-arbeitsplatz/erlaeuterungen-zur-videoueberwachung-am-arbeitsplatz.html (zuletzt besucht am 8.1.2023).
[24] Vgl. dazu näher: Stefanie Meier-Gubser, Mitarbeiterüberwachung: Rechte, Pflichten und Verbote, TREX 2020 S. 286–291.

Die Kontrolle darf auch in Abwesenheit der betroffenen Personen, beispielsweise während der Nacht, stattfinden.

- Die Behörde kann eine störende Fernmeldeanlage betreiben, wenn die Sicherheitszone besonders kritisch ist. Der tatsächliche Bedarf sowie die Bedingungen für den Betrieb einer solchen Störanlage werden nach dem FMG beurteilt.

8.6 Personelle Massnahmen

8.6.1 Auswahl, Instruktion und Berechtigung

Artikel 19

Personen, die Zugang zu Informationen, ICT-Mitteln oder Infrastrukturen der Behörden haben, müssen gemäss Buchstabe a bestimmte Anforderungen erfüllen. Es liegt in der Verantwortung des Arbeit- bzw. des Auftraggebers, dafür zu sorgen, dass die Arbeit- bzw. Auftragnehmerinnen und -nehmer diese Anforderungen erfüllen.

a. Bei der Auswahl der anzustellenden oder zu beauftragenden Personen müssen die Auswahlkriterien dem Schutzbedarf der Informationen beziehungsweise der Kritikalität der ICT-Mittel entsprechen. Die Arbeitgeber sind für ihre Personalentscheide verantwortlich. Die Unterstellung einer Person unter die PSP entbindet sie nicht von dieser Verantwortung.

b. Die Verwaltung des Zugangs zu Informationssystemen, Räumlichkeiten und Infrastrukturen erfolgt zunehmend elektronisch. Personen, die auf ICT-Mittel der Behörden zugreifen wollen, müssen sich elektronisch identifizieren lassen (Authentisierung), damit über ihre Zugangsberechtigung entschieden werden kann. Je nach Kritikalität des Zugangs werden stärkere oder schwächere Authentisierungssysteme eingesetzt. Beispielsweise wird zusätzlich zu einem Passwort eine Smartcard oder die Überprüfung eines biologischen Merkmals (Fingerabdruck, Augenscan usw.) verlangt (vgl. Art. 31 Abs. 2 Bst. c DVG).

c. Die Behörden müssen ihre Angestellten und Beauftragten ausreichend ausbilden. Im Bereich der Informations- und Cybersicherheit genügt eine einmalige Ausbildung nicht. Die Arbeit- und Auftragnehmerinnen und -nehmer müssen regelmässig geschult und sensibilisiert werden. Besondere Aufmerksamkeit ist der Schulung der Vorgesetzten sowie derjenigen Personen, die eine sicherheitsempfindliche Tätigkeit ausüben, zu schenken.

   Angestellte der Behörden müssen aufgrund der Artikel 58 PG und 320 des Schweizerischen Strafgesetzbuches (StGB)[25] das Amtsgeheimnis wahren. Bei Beauftragten ist vertraglich darauf hinzuweisen, dass diese als Hilfspersonen vorübergehend amtliche Funktionen ausüben und daher ebenso dem Amtsgeheimnis unterstehen. Dies wurde mit der Revision von Artikel 320 StGB, welche mit dem ISG erfolgte, klargestellt.

Buchstabe b stellt einen zentralen Grundsatz der Informations- und Cybersicherheit auf. Wer für eine Behörde arbeitet oder einen Auftrag ausführt, braucht zur Aufgabenerfüllung unter Umständen einen Zugang zu bestimmten Informationen, ICT-Mitteln oder Räumlichkeiten. Die Arbeit- und Auftragnehmerinnen und -nehmer sollen nur diejenigen Berechtigungen erhalten, die sie zur Erfüllung ihrer Aufgaben tatsächlich benötigen. Das Risiko eines Missbrauchs kann wesentlich reduziert werden, wenn eine Person nicht ohne Grund Informationen eines anderen Bereichs bearbeiten kann.

[25] StGB, SR 311.0: https://www.fedlex.admin.ch/eli/cc/54/757_781_799/de

Es kommt nicht selten vor, dass ehemalige Angestellte oder Beauftragte nach Beendigung des Vertragsverhältnisses nicht aufgefordert werden, ihren Schlüssel oder ihren Badge zurückzugeben, oder dass ihr Benutzerkonto nicht gesperrt werden. Solche ungültigen Berechtigungen können in der Folge benutzt werden, um gegen die Interessen des Arbeit- oder Auftraggebers zu handeln. Wenn eine Anstellung oder ein Auftrag beendet ist, müssen die entsprechenden Berechtigungen entzogen werden. Besteht Grund zur Annahme, dass eine Gefährdung der Informations- und Cybersicherheit vorliegt, müssen die Berechtigungen sofort gesperrt oder entzogen werden. Beide Massnahmen sollen insbesondere dazu beitragen, das Risiko einer Innentat zu reduzieren.

8.6.2 Personensicherheitsprüfung (Art. 20–27)

Mit der Regelung der Personensicherheitsprüfung (PSP) erhalten alle Behörden eine ausdrückliche gesetzliche Grundlage dafür, die Vertrauenswürdigkeit anzustellender oder bestehender Mitarbeitenden sowie beauftragter Dritter zu überprüfen, welche sicherheitsrelevante Tätigkeiten ausüben (wie Führungspersonen oder Systemadministratoren). Die Behörden können so namentlich feststellen, ob eine Person wegen Vorstrafen als weniger vertrauenswürdig erscheint oder wegen Schulden potenziell erpressbar ist. Mit dieser organisatorischen Massnahme können die Behörden das Risiko, dass Sicherheitslücken durch vorsätzliches Fehlverhalten der eigenen Mitarbeitenden entstehen, reduzieren. Es liegt in der Verantwortung der einzelnen Behörden, gestützt auf ihre Risikobeurteilung (Art. 5 Abs. 2) festzulegen, welche Personen sie wie oft einer PSP unterziehen wollen.

Anstelle der relativ komplizierten und aufwändigen PSP, die das Bundesrecht vorsieht (Art. 27–48 ISG) übernimmt das ICSG mit geringfügigen Anpassungen die heute bereits für die Kantonspolizei geltende Regelung des Polizeigesetzes (Art. 149 Abs. 4 und Art. 160–162 PolG). Danach führt nicht wie in der Bundesverwaltung eine separate Fachstelle die PSP durch, sondern jede einzelne Behörde selbst, und zwar meist dadurch, dass sie sich aktuelle Straf- und Betreibungsregisterauszüge vorlegen lässt. Für die Erläuterungen kann daher grundsätzlich auf den Vortrag zum total revidierten PolG verwiesen werden.[26] Das ICSG sieht folgende Anpassungen dieser Regelungen vor:

- In Artikel 20 wird der Zweck der PSP konkretisiert.

- Gemäss Artikel 21 können neben Angestellten (Art. 160 PolG) und Beauftragten (Art. 149 Abs. 4 PolG) nun auch zu wählende Behördenmitglieder (wie Richterinnen und Richter, die Generalstaatsanwältin oder der Generalstaatsanwalt) vor der Wahl einer PSP unterzogen werden. Zuständig für den Entscheid, eine PSP durchzuführen, ist bei vom Grossen Rat gewählten Personen die Kommission, die die Wahl vorbereitet und den Wahlantrag stellt, und bei vom Regierungsrat gewählten Personen die antragstellende Direktion. Mit der Bestimmung wird damit auch eine ausdrückliche Rechtsgrundlage für die bisherige Praxis der Justizkommission des Grossen Rates geschaffen, welche von Kandidatinnen und Kandidaten für Justizämter schon heute jeweils Straf- und Betreibungsregisterauszüge verlangt. Nicht möglich ist eine PSP mangels einer Wahlbehörde bei vom Volk gewählten Behördenmitgliedern, wie Mitgliedern des Grossen Rates und des Regierungsrates oder Regierungsstatthalterinnen und -statthaltern.

- In Artikel 22 werden die Voraussetzungen der PSP gegenüber dem PolG ausgedehnt. Sie ist nicht nur in abschliessend aufgezählten (polizeispezifischen) Fällen möglich, sondern auch dann, wenn die PSP eine dem Sicherheitsrisiko, das mit dem Einsatz der geprüften Person verbunden ist, angemessene Schutzmassnahme ist. Dies entspricht dem risikobasierten Ansatz des ICSG. Die entsprechende Risikobeurteilung ist von der verantwortlichen Behörde im Rahmen ihres Risikomanagements (Art. 5 Abs. 2) vorzunehmen. Die Anwendungsfälle gemäss PolG werden als Beispielfälle wieder aufgegriffen und erweitert: eine PSP ist neu namentlich auch möglich, wenn die geprüfte Person bei ihrer Tätigkeit häufig oder in grossem Umfang Zugang zu als VERTRAULICH

[26] Vortrag zum PolG, S. 73 f.

oder GEHEIM klassifizierten Informationen hat (vgl. analog Art. 5 Bst. b ISG), weitreichenden Einblick in wichtige politische oder sicherheitsrelevante Geschäfte hat und darauf Einfluss nehmen kann, oder regelmässig oder unbegleitet Zugang zu sicherheitsrelevanten Anlagen oder Räumlichkeiten oder zu Sicherheitszonen gemäss Artikel 18 hat. Soweit sich ein Risiko aus der Bearbeitung von Personendaten ergibt, setzt eine PSP unverändert voraus, dass diese Daten nicht nur besonders schützenswert gemäss KDSG sind, sondern dass ihre Offenbarung die Persönlichkeitsrechte der Betroffenen schwerwiegend beeinträchtigen könnte (vgl. bisher Art 160 Abs. 1 Bst. a PolG).

- In Artikel 24 wird klargestellt, dass Personen, die von Bundesrechts wegen einer PSP des Bundes unterstehen, sich dieser weiterhin unterziehen müssen.

- In Artikel 25 wird bei den Datenquellen der PSP das Register der Einwohnerkontrollen (Art. 161 Abs. 2 Bst. c PolG) gestrichen, weil nicht klar ist, welche sicherheitsrelevanten Daten es enthalten soll. Stattdessen wird das Strafregister (ausdrücklich) mit aufgeführt, um klarzumachen, dass die Behörden sich im Rahmen der PSP einen Strafregisterauszug vorlegen lassen können. Soweit andere Behörden als die Kantonspolizei im Rahmen der PSP ausnahmsweise auf Daten aus den polizeispezifischen Datensammlungen gemäss Artikel 143 bzw. Artikel 147 PolG zugreifen wollen, müssen sie dies auf dem Amtshilfeweg bei der Kantonspolizei beantragen. Die Kantonspolizei ist dazu nicht verpflichtet. Sie wird diesen Anträgen nur stattzugeben haben, wenn dargelegt wird, wieso die Vorlage des Straf- und Betreibungsregisterauszugs nicht genügt.

- Gemäss Artikel 26 müssen den Geprüften nur negative Ergebnisse der PSP mitgeteilt werden. Das reduziert den Verwaltungsaufwand.

Zu diesen Bestimmungen bleibt im Übrigen zu bemerken:

- Artikel 26 Absatz 2: Das Verfahren zur Berichtigung falscher Daten richtet sich nach der Datenschutzgesetzgebung (Art. 23 KDSG).

- Artikel 27 Absatz 1 Buchstabe b: Der Rücktritt von einer schriftlichen Zusage kann auch durch eine aufschiebenden Bedingung im Arbeitsvertrag umgesetzt werden. Besser ist es jedoch, den Arbeitsvertrag erst nach der PSP abzuschliessen und in einer allfälligen früheren Zusage die PSP ausdrücklich vorzubehalten.

- Die PSP und ihre möglichen Folgen werden auf Verordnungsebene näher zu regeln sein. Dort wird etwa festzuhalten sein, dass, wer die Zustimmung zur PSP verweigert, personalrechtliche Konsequenzen zu gewärtigen hat. Dazu kann die Nichtanstellung oder die Versetzung auf eine weniger sensitive Funktion gehören, oder gegebenenfalls, wenn das nicht möglich ist, die Kündigung.

- Weil der Aufwand, der bei der Kantonspolizei für ihre Mitwirkung an der PSP anfällt, noch nicht abschätzbar ist, ist vorgesehen, aufgrund der Erfahrungen der ersten Jahre auf Verordnungs- oder Weisungsebene die nötigen Regelungen zu erlassen, um den Aufwand für die Kantonspolizei gegebenenfalls auf ein tragbares Mass zu reduzieren.

8.7 Sicherheitsorganisation

Die Informationssicherheitsorganisation des Kantons ist heute nur punktuell und weitgehend bereichsspezifisch geregelt. Weil die Gewährleistung der Informationssicherheit eine ständige Führungsaufgabe der Regierung und der Verwaltung ist, schafft das ICSG die Grundlage für eine direktions- und

fachthemenübergreifende Sicherheitsorganisation auf Verwaltungsebene. Dadurch sollen die Führungsaufmerksamkeit für Sicherheitsbelange gestärkt und das Sicherheitsbewusstsein der Fach- und Führungspersonen der Verwaltung erhöht werden.

Artikel 28 – Sicherheitsorganisation des Kantons und der kantonalen Verwaltung

Mit dem Gesetz und der Verordnung über die digitale Verwaltung (DVG/DVV[27]) hat der Regierungsrat Organe eingerichtet, welche die Steuerung und Führung der Digitalisierung und der ICT sowohl kantonsweit (einschliesslich der Belange der Gemeinden und der autonomen Träger öffentlicher Aufgaben) wie auch innerhalb der Kantonsverwaltung sicherstellen. Weil sich Informationssicherheitsfragen primär im Zusammenhang mit ICT-Systemen und Digitalisierungsvorhaben stellen, erlaubt es das ICSG, die Sicherheitsorganisation des Kantons in die Organe gemäss DVG und DVV zu integrieren. Dies vereinfacht es, die Sicherheit als integralen Teil der Digitalisierung der öffentlichen Verwaltung zu berücksichtigen, und es erlaubt den Verzicht auf die Schaffung neuer Fachgremien.

Zukünftig sollen damit namentlich folgende Verwaltungsorgane auch Sicherheitsaufgaben wahrnehmen: Das Kontaktgremium Digitale Verwaltung Kanton–Gemeinden (KDKG) dient dem Austausch zwischen dem Kanton und den Gemeinden auf politischer Ebene. Die Konferenz Digitale Verwaltung und ICT (KDI) sowie ihre Fachgruppe Informationssicherheit (FG IS) erarbeiten und erlassen Sicherheitsgrundlagen wie Weisungen, Standards und Prozesse. Artikel 27 Absatz 3 ICSG wiederholt die bereits im DVG und in der DVV vorgesehene Regel, dass die Gemeinden, soweit sie betroffen sind, in die Entscheide der kantonalen Organe angemessen mit einbezogen werden müssen.

Artikel 29 – Sicherheitsorganisation der anderen Behörden

Die Behörden, die nicht Teil der kantonalen Verwaltung sind, müssen sich eine ihren Aufgaben und Risiken angemessene Sicherheitsorganisation geben. Zu diesen Behörden gehören alle Träger öffentlicher Aufgaben, die nicht dem Regierungsrat hierarchisch unterstellt sind, wie namentlich der Grosse Rat, die Justizbehörden, die autonomen kantonalen Anstalten, Staatsunternehmen, die Gemeinden sowie die Träger kommunaler Aufgaben.

Diese Behörden müssen mindestens eine Person mit angemessenen Kompetenzen und Ressourcen bezeichnen, die auch Kontaktperson für die kantonalen und Bundessicherheitsbehörden ist. Es ist möglich, dass kleinere Gemeinden oder Behörden eine gemeinsame Person bezeichnen oder diese Aufgabe einer externen Fachperson übertragen.

8.8 Ausführungsbestimmungen

Artikel 30 – Regierungsrat

Wie bereits Artikel 34 DVG erlaubt das ICSG die Subdelegation des Erlasses fachlicher Ausführungsbestimmungen sowie weiterer Grundlagen der Umsetzung des ICSG an die zuständigen Organe der Kantonsverwaltung (vgl. Art. 20 ICSG). Die von diesen Organen erlassenen Vorschriften sind nicht Rechtsverordnungen, sondern Weisungen (Verwaltungsverordnungen), die sich an andere Behörden richten.

Die zur Umsetzung des Gesetzes erforderlichen Übergangsfristen werden auf Verordnungsebene zu bestimmen sein. Dazu gehören angemessene Fristen für die erstmalige Klassifizierung aller Informationen (unter Vorbehalt von Art. 8 Abs. 3) sowie die Anpassung der ICT-Systeme und der Organisation an das ICSG und die sich daraus ergebenden Sicherheitsvorgaben. Die zuständigen Fachorgane werden diese Fristen und das Einführungsvorgehen im Dialog mit den betroffenen Behörden erarbeiten.

[27] www.be.ch/dvg

Artikel 31 – Grosser Rat

Die Bestimmung übernimmt sinngemäss Artikel 84 Absätze 2 und 3 ISG. Damit hat der Grosse Rat die Möglichkeit, bei Bedarf von den für die Verwaltung geltenden Ausführungsbestimmungen abzuweichen. Anders als im ISG ist die direkte Delegation dieser Kompetenz an das Büro des Grossen Rates nicht möglich (Art. 69 Abs. 3 Satz 2 KV).

Bei der Ausübung dieser Kompetenz wird der Grosse Rat beachten müssen, dass Abweichungen von den Ausführungsbestimmungen des Regierungsrates zur Folge haben können, dass der Grosse Rat die ICT-Grundversorgung der Kantonsverwaltung nur eingeschränkt nutzen kann (Art. 32 DVG). Dies, weil die ICT-Grundversorgung auf die gesamtkantonalen Sicherheitsvorschriften ausgerichtet ist und ihre Nutzung daher voraussetzt, dass sich die Nutzenden an diese Sicherheitsvorschriften halten.

8.9 Schlussbestimmungen

Artikel 32 – Änderung eines Erlasses

Im Polizeigesetz werden die Bestimmungen über die Personensicherheitsprüfung (Art. 17 Abs. 4, Art. 149 Abs. 4, Art. 160–162) gestrichen, weil sie in die Artikel 20 bis 26 ICSG überführt werden.

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

Das Gesetz entspricht den Richtlinien der Regierungspolitik 2023 – 2026. Diese sehen als zweites Ziel vor, dass der Kanton Bern die digitale Transformation nutzt, um wirkungsvolle, qualitativ hochstehende und effiziente Dienstleistungen zu erbringen. Dies setzt voraus, dass auch die Sicherheit dieser Leistungen als ein Aspekt ihrer Qualität sichergestellt wird. Die Sicherheit ist auch eine Voraussetzung dafür, dass die Bevölkerung und die Wirtschaft bereit sind, den Behörden ihre Personendaten und vertraulichen Informationen anzuvertrauen.

Das Gesetz entspricht auch der vom Regierungsrat 2019 beschlossenen Strategie Digitale Verwaltung (s. Ziff. 2.2 und 3.2.2.2 oben).

10. Finanzielle Auswirkungen

Das Gesetz wird grundsätzlich mit den bestehenden bzw. geplanten, für die ICT und die Digitalisierung vorgesehenen Finanzmitteln umzusetzen sein. Dies aus folgenden Gründen:

- Bereits heute sind die Behörden durch Artikel 17 des Datenschutzgesetzes (KDSG) zur Gewährleistung der Datensicherheit verpflichtet. Das ICSG führt damit keine neue staatliche Aufgabe ein, sondern konkretisiert lediglich eine bereits bestehende Aufgabe.

- Die Digitalisierung der Verwaltung ist zwar ein Kostentreiber für die ICT und damit auch für die Informations- und Cybersicherheit, namentlich vor dem Hintergrund zunehmender Cybersicherheitsbedrohungen. Das DVG und das ICSG geben den verantwortlichen Behörden aber mehrere Mittel in die Hand, um ICT- und sicherheitsbedingte Mehrkosten zu reduzieren oder zu kompensieren:

    - Wenn im Verkehr mit Behörden, Unternehmen und Berufsleuten (vgl. Art. 8 DVG) die Geschäftsprozesse konsequent nur noch digital ausgestaltet und stärker als bisher automatisiert

werden, erlaubt dies die Einsparung von Material- und Personalkosten (für Sachbearbeitung, Sekretariat, Datenerfassung, Porto, Papier und Druck, etc.).

- Wenn Behörden bei der Digitalisierung zusammenarbeiten (Art. 20 DVG), etwa wenn sie Systeme interkantonal oder interkommunal gemeinsam beschaffen und betreiben, oder indem sie bestehende kantonale Basisdienste nutzen (Art. 16 ff. DVG), können sie die mit der Digitalisierung verbundenen Sicherheitskosten stark reduzieren oder vermeiden.

- Wenn Behörden ein angemessenes Risikomanagement betreiben (Art. 5 Abs. 2 ICSG), können sie ihre Sicherheitsmassnahmen gezielt auf die risikoreichen Aspekte ihrer Tätigkeit ausrichten und Risiken in weniger sensiblen Tätigkeitsbereichen bewusst in Kauf nehmen (Art. 12 Abs. 2 Bst. d ICSG). Wenn sie nur soviele Informationen wie nötig klassifizieren (Art. 8 Abs. 3 ICSG), reduzieren sie damit den Umfang der Systeme mit erhöhter Sicherheitsstufe (Art. 12 Abs. 2 Bst. b ICSG) und die damit verbundenen Kosten.

11. Personelle und organisatorische Auswirkungen

Aufgrund der finanziellen und personalpolitischen Rahmenbedingungen wird die Informationssicherheitsgesetzgebung in der Kantonsverwaltung grundsätzlich mit den bestehenden personellen Ressourcen umzusetzen sein. Dazu kann auf das oben zu Ziff. 10 Gesagte verwiesen werden. Die personellen Auswirkungen werden auch dadurch möglichst klein gehalten, dass die Fachorgane der Informationssicherheit in die bestehende Governance der digitalen Verwaltung und der ICT integriert werden (vgl. Art. 28 ICSG).

12. Auswirkungen auf die Gemeinden und die anderen Träger öffentlicher Aufgaben

Wie für den Kanton ist die Aufgabe der Informationssicherheit für die Gemeinden und die anderen Träger öffentlicher Aufgaben nicht neu (Art. 17 KDSG). Das ICSG gilt für sie aber nur in dem beschränkten Umfang, wie sie mit dem Kanton oder dem Bund bzw. deren Systemen und Informationen interagieren (Art. 2 Abs. 2 ICSG). In diesem Kontext müssen sie die Regeln über die Klassifizierung bzw. den Umgang mit klassifizierten Informationen und ICT-Systemen einhalten.

Die Gemeinden und die anderen Träger öffentlicher Aufgaben sind darüber hinaus frei, sich selber Informationssicherheitsregeln zu geben bzw. das ICSG auf sich integral für anwendbar zu erklären, was im Interesse eines einheitlichen Sicherheitsraums im Kanton Bern von Vorteil wäre. Auch sie können die Kosten der Informationssicherheit im Griff behalten, indem sie gezielte, risikoangemessene Sicherheitsmassnahmen ergreifen und Synergien mit anderen Gemeinden sowie mit der Kantonsverwaltung realisieren.

13. Auswirkungen auf die Volkswirtschaft

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.

14. Ergebnis des Vernehmlassungsverfahrens

Im Vernehmlassungsverfahren fand das ICSG verbreitet Zustimmung. Keine Stellungnahme lehnte es ab. Häufig wurde die Notwendigkeit der Informationssicherheit in einer Zeit der zunehmenden Cyberbedrohungen unterstrichen.

Die wesentlichen Anliegen der Vernehmlassungsteilnehmenden waren folgende:

- **Umsetzungsaufwand:** Für die EDU löst das ICSG zuviel Aufwand aus. Die Grünen wollen, dass mehr Mittel zur Umsetzung bereitgestellt werden.

  Der Regierungsrat ist sich bewusst, dass der Aufwand für die Sicherheit als Folge der Digitalisierung und der steigenden Sicherheitsbedrohung steigen wird. Er will jedoch den Zusatzaufwand für die Digitalisierung einschliesslich der Sicherheit primär mit den dank der Digitalisierung möglichen Effizienzgewinnen decken (s. Ziff. 10 oben).

- **Aufgaben der Gemeinden:** Der Verband Bernischer Gemeinden (VBG) verlangt, dass die Verordnung näher regelt, welche Aufgaben die Gemeinden im Rahmen ihrer Betroffenheit vor allem bei der Klassifizierung und bei der Sicherheit beim Einsatz von ICT-Mitteln erfüllen müssen.

  Die Verordnung wird diese Fragen näher regeln, und eine Vertretung der Gemeinden wird an der Erarbeitung dieser Regeln mitwirken können.

- **Geltungsbereich:** Das Büro des Grossen Rates und die EDU lehnen die Unterstellung des Grossen Rates unter das ICSG ab. Die Klassifizierungsregeln passten nicht zum Ratsbetrieb, und die bisherige Unterscheidung «öffentlich»/»nicht öffentlich» habe sich bewährt.

  Der Regierungsrat hält daran fest, dass das ICSG auch für den Grossen Rat gelten soll, so wie das ISG auch für die Bundesversammlung gilt. Dies aus folgenden Gründen:
  - Um die Sicherheit der ICT-Systeme der Kantonsverwaltung zu gewährleisten, müssen alle, die sie nutzen, die gleichen Sicherheitsregeln einhalten, also auch die Ratsmitglieder und die Parlamentsdienste. Sonst können Rats-PCs zum Einfallstor für Cyberangreifer werden.
  - Der Grosse Rat hat viel Spielraum, das ICSG im Sinne seiner Risikobeurteilung und seiner bisherigen Praxis umzusetzen, etwa indem er selbst regelt, welche seiner Dokumente wie klassifiziert werden. Dank einer neu vorgeschlagenen Bestimmung kann der Grosse Rat, analog zum Bundesrecht, bei Bedarf auch eigene Ausführungsbestimmungen erlassen.
  - Weiter macht es für die zu schützenden öffentlichen Interessen (Art. 2 ICSG) keinen Unterschied, ob die zu schützenden Informationen vom Grossen Rat oder von einer anderen Behörde bearbeitet werden, denn dies ändert nichts an den Risiken, die sich als Folge eines unsicheren Umgangs mit Informationen verwirklichen können. Daher ist der Grosse Rat ja wie alle Behörden auch dem Amtsgeheimnis und dem Datenschutzgesetz unterstellt.

- **Personensicherheitsprüfungen (PSP):** Das Büro des Grossen Rates, die Justizleitung, die EDU und die Grünen lehnen PSP für angehende Mitglieder von Justizbehörden ab. Diese sei für Regierungs- und Grossratsmitglieder auch nicht vorgesehen, und sie könnte ein Vehikel der politischen Einflussnahme sein. Mit einer PSP müsste das ganze Wahlverfahren überdacht werden.

  Der Regierungsrat hät daran fest, dass die Wahlbehörde auch in diesen Fällen eine PSP durchführen können soll:

  - Wie das Büro schreibt, lässt sich die Justizkommission schon heute die Straf- und Betreibungsregisterauszüge der Kandidierenden für Justizämter vorlegen. Damit nimmt sie schon

heute (und noch ohne gesetzliche Grundlage) jeweils eine PSP vor. Mit dem Erlass des ICSG muss sie ihre Praxis nicht ändern, denn weiter als die Prüfung der Registerauszüge geht eine PSP nach ICSG in der Regel nicht.

- Mitglieder der Justizbehörden üben staatliche Macht in einer Weise aus, welche sich auf die Rechtsunterworfenen sehr einschneidend auswirken kann, und sie haben Zugang zu vielen sehr schützenswerten Informationen über die Rechtsunterworfenen. Daher haben diese ein legitimes Interesse daran, darauf vertrauen zu können, dass die Personen, die über sie urteilen, vertrauenswürdige und integre Menschen sind.

- Bei Regierungs- und Grossratswahlen ist keine PSP möglich, weil dies Volkswahlen sind und das Privatleben der Kandidierenden nicht in der Öffentlichkeit ausgebreitet werden kann.

Das Büro des Grossen Rates und die Grünen bringen zudem viele Vorbehalte zur Ausgestaltung der PSP an und verlangen in verschiedenen Punkten eine ausführlichere Regelung. Darauf verzichtet der Regierungsrat, denn er übernimmt bewusst die schlanke Regelung des Polizeigesetzes, die in der Praxis problemlos angewendet wird. Allfälliger weiterer Regelungsbedarf kann auf Verordnungsebene adressiert werden.

- **Klassifizierung:** Die Grünen verlangen ausgebaute Klassifizierungsregeln.

  Der Regierungsrat verzichtet darauf. Wie auf Bundesebene hält er es für sachgerecht, die Regeln für die Klassifizierung nicht im Detail auf Gesetzesstufe zu regeln, weil auf dieser Stufe den sehr unterschiedlichen Geschäftsfällen der Verwaltung nicht genügend Rechnung getragen werden kann. Dies soll vielmehr pro Organisationseinheit in einem Klassifizierungskatalog erfolgen.

Die detaillierte Stellungnahme der Finanzdirektion zu diesen und weiteren Anliegen kann der Vernehmlassungsauswertung entnommen werden. Sie wird nach der Überweisung der Vorlage an den Grossen Rat auf www.be.ch/icsg veröffentlicht.

15. Antrag

Der Regierungsrat beantragt dem Grossen Rat, das vorliegende Gesetz zu genehmigen.