# Vortrag

| | |
|---|---|
| Datum RR-Sitzung: | 9. September 2026 |
| Direktion: | Finanzdirektion |
| Geschäftsnummer: | 2023.KAIO.444 |
| Klassifizierung: | Nicht klassifiziert |

## Verordnung über die Informations- und Datensicherheit (IDSV)

### Inhaltsverzeichnis


**1. Zusammenfassung ..... 2**

**2. Ausgangslage ..... 2**
2.1 Bund ..... 2
2.2 Kanton Bern ..... 3
2.2.1 Gesetze ..... 3
2.2.2 Verordnungen und Weisungen ..... 4
2.3 Handlungsbedarf ..... 4

**3. Grundzüge der IDSV ..... 5**
3.1 Normenhierarchie und -architektur für die Informations- und Datensicherheit ..... 5
3.2 Schutzniveaus ..... 6
3.3 Inhaltsübersicht ..... 6
3.4 Sicherheitsorganisation des Kantons und der kantonalen Verwaltung ..... 7
3.5 Wirkungsziele ..... 8

**4. Erlassform ..... 9**

**5. Rechtsvergleich ..... 9**
5.1 Bund ..... 9
5.2 Kantone ..... 9

**6. Umsetzung und Evaluation des Vollzugs ..... 9**

**7. Erläuterung zu einzelnen Artikeln ..... 10**
7.1 Allgemeine Bestimmungen ..... 10
7.2 Grundsätze der Informations- und Datensicherheit ..... 11
7.3 Schutzmassnahmen kantonaler Behörden ..... 22
7.3.1 Sicherheitsverfahren bei ICT-Mitteln ..... 22
7.3.2 Management der Informations- und Datensicherheit ..... 26
7.3.3 Klassifizierung von Informationen ..... 30
7.3.4 Einstufung von ICT-Mitteln ..... 33
7.3.5 Zu prüfende Personen ..... 34
7.4 Sicherheitsorganisation ..... 35
7.5 Übergangs- und Schlussbestimmungen ..... 41

**8. Verhältnis zu den Richtlinien der Regierungspolitik und anderen wichtigen Planungen ..... 43**

**9. Auswirkungen auf Finanzen, Organisation, Personal, IT und Raum ..... 43**
9.1 Informationssicherheit ..... 43
9.2 Datensicherheit ..... 45

**10. Auswirkungen auf die Gemeinden und die anderen Träger öffentlicher Aufgaben ..... 45**
10.1 Informationssicherheit ..... 45
10.2 Datensicherheit ..... 46

**11. Auswirkungen auf die Volkswirtschaft ..... 46**

**12. Antrag ..... 46**

# 1. Zusammenfassung

Die Verordnung über die Informations- und Datensicherheit (IDSV)[1] enthält die Ausführungsbestimmungen zum Gesetz vom 12. Juni 2025 über die Informations- und Cybersicherheit (ICSG)[2] sowie diejenigen Ausführungsbestimmungen zum totalrevidierten kantonalen Datenschutzgesetz (KDSG), welche die Datensicherheit betreffen. Sie orientiert sich auch an der Verordnung vom 8. November 2023 über die Informationssicherheit in der Bundesverwaltung und der Armee (Informationssicherheitsverordnung, ISV)[3], allerdings an die Berner Verhältnisse angepasst und deshalb auf ein Minimum reduziert.

Die IDSV konkretisiert für alle Berner Behörden die Grundsätze und die Schutzmassnahmen für die Informations- und Datensicherheit nach dem ICSG und dem KDSG. Im Vergleich zu den anderen Behörden, insbesondere für die Einwohner-, Kirch- und Burgergemeinden, gelten für die kantonalen Behörden zusätzliche Regeln, damit der Bund deren Gleichwertigkeit anerkennt und ohne Einschränkungen auch weiterhin in sicherheitskritischen Bereichen mit dem Kanton Bern zusammenarbeitet.

Die IDSV ersetzt die Direktionsverordnung vom 3. Januar 2011 über Informationssicherheit und Datenschutz (ISDS DV)[4]. Zudem integriert sie sämtliche Bestimmungen über die Datensicherheit der heutigen Datenschutzverordnung vom 22. Oktober 2008 (DSV)[5], welche seit der Revision des KDSG Kantonale Datenschutzverordnung (KDSV) heisst.

Weil die Schutzmassnahmen sowohl für die Informations- als auch die Datensicherheit die gleichen sind, werden sie in der IDSV vereinheitlicht und zusammengefasst. Die IDSV wird mit dem ICSG auf den 1. November 2026 in Kraft gesetzt.

# 2. Ausgangslage

## 2.1 Bund

Mit der Inkraftsetzung des Bundesgesetzes vom 18. Dezember 2020 über die Informationssicherheit (Informationssicherheitsgesetz, ISG)[6] per 1. Januar 2024 sind die Kantone für den Fall, dass sie auf ICT-Mittel, Informationen oder Personendaten des Bundes zugreifen, verpflichtet, entweder direkt die Bestimmungen des Bundes umzusetzen oder aber eine mindestens gleichwertige Informationssicherheit zu gewährleisten (Art. 3 ISG).

Mit dem ISG hat der Bund ebenfalls die ISV per 1. Januar 2024 in Kraft gesetzt. Neben den Ausführungsbestimmungen u.a. zum Informationssicherheitsmanagement und den organisatorischen, technischen, physischen und personellen Schutzmassnahmen definiert die Verordnung auch die Sicherheitsorganisation sowie deren Zuständigkeiten und Kompetenzen (Art. 36 ff. ISV). Die ISV

[1] IDSV, BSG 152.091
[2] ICSG, BSG 152.09
[3] ISV, SR 128.1
[4] ISDS DV, BSG 152.040.2
[5] DSV, BSG 152.040.1
[6] ISG, SR 128

ist massgeblich für die Feststellung der Gleichwertigkeit der Informationssicherheit der Kantone durch den Bund nach Artikel 3 i.V.m. Artikel 86 ISG. Aus diesem Grund lehnt sich die IDSV an die ISV und stellt sicher, dass die Anforderungen des Bundes – stark an die Berner Verhältnisse angepasst und reduziert – durch den Kanton Bern erfüllt werden.

Im Weiteren hat der Bund die Verordnung vom 7. März 2025 über die Cybersicherheit (Cybersicherheitsverordnung, CSV)[7] per 1. April 2025 in Kraft gesetzt, welche insbesondere die Pflicht zur Meldung von Cybervorfällen durch die Betreiberinnen kritischer Infrastrukturen konkretisiert. Mit der IDSV sollen die Meldepflichten für die Berner Behörden gemäss ICSG, KDSG und CSV stark vereinfacht und mittels einer einzigen Meldeplattform vereinheitlicht werden.

## 2.2 Kanton Bern

### 2.2.1 Gesetze

Im Kanton Bern befinden sich die folgenden vier Gesetze bereits in Kraft, welche die Informations- und Datensicherheit sowie den Datenschutz in den Grundsätzen regeln:

a) Das Gesetz vom 10. März 2020 über die zentralen Personendatensammlungen des Kantons Bern (PDSG)[8], welches am 1. März 2021 in Kraft getreten ist.
b) Das Gesetz vom 7. März 2022 über die digitale Verwaltung des Kantons Bern (DVG)[9], welches am 1. März 2023 in Kraft getreten ist.
c) Das revidierte KDSG, welches seit dem 1. September 2026 in Kraft ist.
d) Das ICSG, vom Grossen Rat in zweiter Lesung am 12. Juni 2025 einstimmig beschlossen, welches mit der IDSV am 1. November 2026 in Kraft gesetzt wird.

Diese Gesetze bilden die vier Säulen für die Informations- und Datensicherheit sowie für den Datenschutz («Vier ISDS-Säulen»):

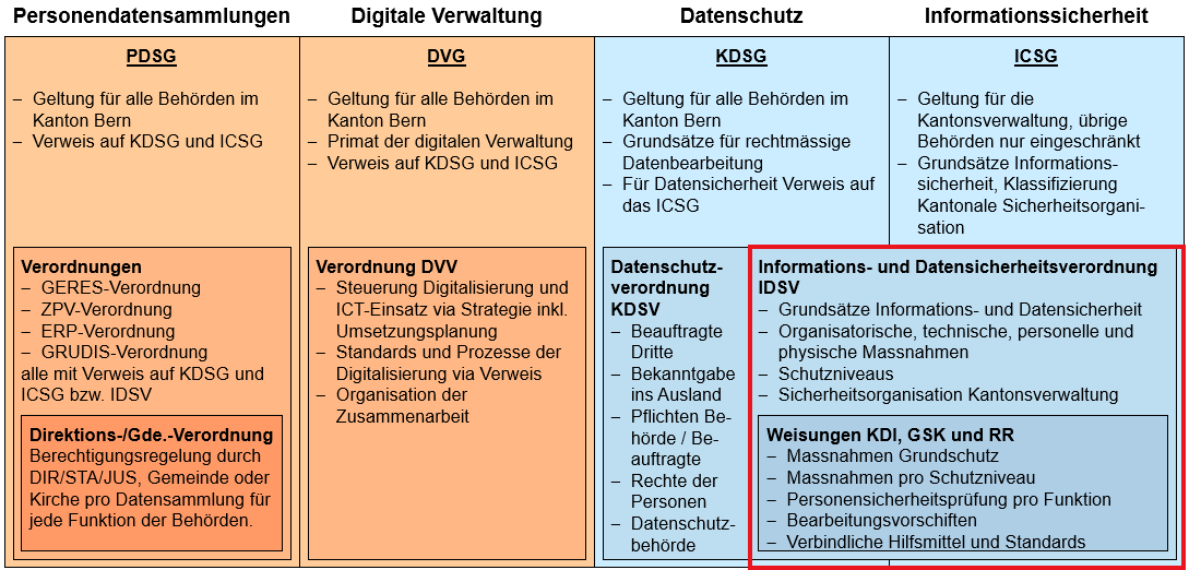



Abbildung 1: Die «Vier ISDS-Säulen» der Berner Gesetzgebung

[7] CSV, SR 128.51
[8] PDSG BSG 152.05
[9] DVG BSG 109.1

### 2.2.2 Verordnungen und Weisungen

Der Kanton Bern hat seit dem Erlass des KDSG im Jahr 1986 im Zuge der Digitalisierung der Verwaltungsführung vorab zum Schutz der Personendaten, später dann auch zum Schutz von für die Staatsführung kritischen Informationen, zahlreiche Verordnungen und Weisungen erlassen (beispielhafte Aufzählung):

a) Verordnungen

1. Datenschutzverordnung DSV;
2. Direktionsverordnung über Informationssicherheit und Datenschutz ISDS DV;
3. Verordnung vom 13. März 2013 über die Klassifizierung, die Veröffentlichung und die Archivierung von Dokumenten zu Regierungsratsgeschäften (Klassifizierungsverordnung, KRGV)[10];
4. Randdatenverordnung vom 20. November 2019 (RDV)[11];
5. Verordnung über die digitale Verwaltung vom 11. Januar 2023 (DVV)[12].

b) Weisungen und Richtlinien

1. Richtlinien des Regierungsrates vom 24. November 2021 über das Risikomanagement des Kantons Bern (RM-Richtlinien)[13];
2. Weisung des Regierungsrates vom 17. März 2021 über die Verwendung von Online-Übersetzungsprogrammen in der Kantonsverwaltung[14];
3. Weisung der Konferenz digitale Verwaltung und ICT (KDI)[15] über den Umgang mit User-IDs[16];
4. Weisung des Strategischen ICT-Ausschusses (SIA) vom 8. Dezember 2020 über die Standards der Informations- und Kommunikationstechnologie der Kantonsverwaltung (ICT-Standards BE)[17];
5. Weisung der KDI vom 27. Juni 2023 über den Umgang mit ICT in der Kantonsverwaltung für Endanwenderinnen und Endanwender[18];
6. Weisung des KAIO über die Netzwerksicherheit (Network Security Policy, NSP) vom 18. Dezember 2024[19];
7. Weisung des KAIO vom 4. März 2024 über das über das Identity- und Access-Management (IAM) sowie die Verzeichnisdienste (IAM-Weisung)[20];
8. Weisung des KAIO vom 9. Juli 2025 über den Grundschutz für die Informations- und Cybersicherheit (ICSGW)[21].

## 2.3 Handlungsbedarf

Es ist unschwer zu erkennen, dass den Regelungsinhalten, den Geltungsbereichen und insbesondere auch den Zuständigkeiten der verschiedenen Behörden für die Informations- und Datensicherheit eine einheitliche und nachvollziehbare Systematik fehlt. Dies ist vorab der Tatsache geschuldet, dass sich seit 1986 die ICT-Mittel und damit auch die Anforderungen an die Digitalisierung der Bevölkerung und der Verwaltung ständig, rasch und spontan verändert haben. Ebenso haben sich auch die Anforderungen an die Gesetzgebung verändert, welche mit der technischen Entwicklung nur noch mit Mühe schritthalten konnte, weil zu viele Fragen auf der langsamen Gesetzes- oder Verordnungsstufe geregelt werden müssen.

[10] KRGV BSG 152.17
[11] RDV BSG 153.011.5
[12] DVV BSG 109.111
[13] RRB 1382/2021
[14] Weisung Online-Übersetzungsprogramme auf Rahmenwerk DV und ICT (verwaltungsintern)
[15] Art. 18 DVV
[16] Weisung User-IDs auf Rahmenwerk DV und ICT
[17] Weisung ICT-Standards auf Rahmenwerk DV und ICT
[18] Weisung Enduser auf Rahmenwerk DV und ICT
[19] Weisung NSP BE auf Rahmenwerk DV und ICT
[20] Weisung IAM auf Rahmenwerk DV und ICT
[21] ICSGW

Mit den oben als «Vier ISDS-Säulen» bezeichneten Gesetzen hat sich der Kanton Bern nun aber strategische Vorgaben gegeben, die sowohl eine systematische als auch reaktionsfähige Neuordnung der Informations- und Datensicherheit sowie des Datenschutzes ermöglichen.

Bei der Erarbeitung der IDSV wurde deshalb überprüft, welche der vorgenannten Regelungen weiterhin Bestand haben, aufgehoben, delegiert oder übernommen werden sollen. Diese Überprüfung wird anschliessend auch auf der Stufe Weisung erfolgen. Die nachstehende Normenhierarchie ist dabei massgeblich.

# 3. Grundzüge der IDSV

## 3.1 Normenhierarchie und -architektur für die Informations- und Datensicherheit

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




Abbildung 2: Normenhierarchie der Informations- und Datensicherheit (IDS)

Während im Vortrag vom 16. August 2023 zum ICSG in Ziffer 4.2 die Normenhierarchie allein auf dem ICSG basierte, wird vorliegend nun auch das revidierte KDSG beigezogen. Der Grund liegt darin, dass die IDSV nicht nur die Grundlage für die Informations-, sondern auch für die Datensicherheit bildet. Informationen und Personendaten sind dann sicher, wenn die Integrität, Verfügbarkeit, Vertraulichkeit sowie Nachvollziehbarkeit ihrer Bearbeitung gewährleistet sind.

Die Informationssicherheit ist in Artikel 4 Absatz 1 Buchstabe a ICSG beschrieben, die Datensicherheit definiert der Artikel 10 Absatz 2 KDSG mittels Verweis auf das ICSG. Die Informations- und Datensicherheit sind Sachverhaltsvoraussetzungen, die erfüllt sein müssen, damit die Informationen und Personendaten ICSG- und KDSG-konform und damit rechtmässig bearbeitet werden.

## 3.2 Schutzniveaus

Die Sachverhaltsvoraussetzungen sind erfüllt, wenn die risikoangemessenen Schutzmassnahmen umgesetzt sind. Diese sind für die Informations- und Datensicherheit die gleichen und werden deshalb mit der IDSV durch sog. Schutzniveaus von 0 bis 3 generisch beschrieben. Die KDI regelt für die kantonalen und die Schutzobjekte des Bundes per Weisung die für Schutzniveau 0 und 1 erforderlichen Schutzmassnahmen der kantonalen Behörden, den sog. Grundschutz. Stellen die kantonalen Behörden Dritten Schutzobjekte zur Verfügung, sind die Schutzmassnahmen durch Weisung, Verfügung oder Vertrag zu bestimmen und den Dritten zu übertragen. Im Übrigen bestimmen die Sicherheitsverantwortlichen der für die Schutzobjekte verantwortlichen Behörden die Schutzmassnahmen, die erforderlich sind, um das Sicherheitsrisiko auf das von ihnen akzeptierte Mass zu reduzieren.

Damit wird die IDSV zur Schnittstelle zwischen dem ICSG und KDSG:

| **Informations- und Cybersicherheitsgesetz ICSG** | | **Informations- und Datensicherheits-verordnung IDSV** | **Datenschutzgesetz KDSG** |
|---|---|---|---|
| **Schutz der Interessen des Staates** | | **Massnahmen für die Informations- und Datensicherheit** | **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) |
| Personensicherheitsprüfung (PSP) nach ICSG durch anstellende Behörde | | Vollzugsvorschriften für ICSG und KDSG | Prüfung der Vertrauenswürdigkeit nach Personalgesetz durch anstellende Behörde |

Abbildung 3: Schutzobjekte, Einstufung, Schutzniveaus nach IDSV: «Interface» zwischen ICSG und KDSG

Wichtig ist die Unterscheidung der Schutzziele bzw. -objekte des ICSG und des KDSG:

- Das ICSG schützt öffentliche Interessen wie Entscheidungsfreiheit und Handlungsfähigkeit des Staates und die Erfüllung seiner Aufgaben.
- Das KDSG schützt private Interessen, nämlich Personen vor ungesetzlichen Eingriffen in ihre Persönlichkeit.

Beide Interessenslagen verfügen daher über eigene Einstufungen des Schutzbedarfs (s. erste, zweite und vierte Spalte der Abbildung 3), die über die Definition der vier Schutzniveaus in der IDSV synchronisiert werden (dritte Spalte). Die Schutzziele sind zwar verschieden, die Schutzmassnahmen jedoch die gleichen.

Von der Grösse des Schutzbedarfs einer Information, eines Personendatums oder eines ICT-Mittels hängt deren Einstufung und damit auch das Schutzniveau ab. Dieses beinhaltet das risikoangemessene Bündel von organisatorischen, technischen, physischen oder personellen Schutzmassnahmen.

## 3.3 Inhaltsübersicht

Das ICSG mit seinen 39 Artikeln wurde bewusst knapper gehalten als das ISG mit über 100 Artikeln. Das ICSG beschränkt sich auf die Grundsätze und grundrechtsrelevante Bestimmungen, wie z.B. die Personensicherheitsprüfung (PSP). Die IDSV muss demzufolge z.B. das Management der Informationssicherheit (ISM), die Einstufung der Schutzobjekte oder das Bestimmen der Funktionen, welche eine PSP voraussetzen, genauer regeln. Weiter sind in der IDSV die Zuständigkeiten

zum Erlass von Weisungen, Verfügungen, Verträgen und Vollzugshilfen zur Informations- und Datensicherheit durch die KDI und die anderen Sicherheitsorgane vorgesehen. Die IDSV hat mit ihren 44 Artikeln – trotz der Integration von Teilen der DSV – einen ebenfalls überschaubaren Umfang.

| **Informations- und Cybersicherheitsgesetz ICSG** | **Informations- und Datensicherheits-verordnung IDSV** | **Informations- und Datensicherheitsvor-gaben der KDI und anderer Sicherheitsorgane** |
|---|---|---|
| Strategische Wirkungsziele, Grundsätze und Grundrechtseingriffe:<br><br>1. Allgemeine Bestimmungen<br>2. Grundsätze<br>3. Organisatorische Massnahmen<br>4. Technische Massnahmen<br>5. Physische Massnahmen<br>6. Personelle Massnahmen<br>7. Standardisierung<br>8. Sicherheitsorganisation<br>9. Ausführungsbestimmungen<br>10. Schlussbestimmungen<br><br>Delegationen an RR betr.<br>– Klassifizierungen<br>– Technische Massnahmen<br>– Sicherheitsorganisation und –Behörden<br>– Übergangsfristen | Normen ohne Grundrechtsrelevanz und taktischer Natur:<br><br>1. Allgemeine Bestimmungen<br>2. Grundsätze der Informations- und Datensicherheit<br>3. Schutzmassnahmen kantonaler Behörden<br>3.1 Sicherheitsverfahren bei ICT-Mitteln<br>3.2 Management der Informations- und Datensicherheit<br>3.3 Klassifizierung von Informationen<br>3.4 Einstufung von ICT-Mitteln<br>3.5 Zu prüfende Personen<br>4. Sicherheitsorganisation<br>5. Übergangs- und Schlussbestimmungen<br><br>Delegationen an KDI und anderen Sicherheitsorgane. | Vollzugsnormen operativer Natur:<br><br>1. ISM-System<br>2. Klassifizierung und Bearbeitung von Informationen und Personendaten<br>3. Sicherheitsverfahren und –massnahmen<br>4. Physische Schutzmassnahmen<br>5. Prüfung von Identitäten von Personen und Systemen sowie Identitäts- und Berechtigungsmanagement (IAM)<br>6. Sicherheitsmassnahmen pro Schutzniveau<br>7. Verbindliche Hilfsmittel, z.B. zur Schutzbedarfsanalyse, zum ISDS-Konzept etc. |

Abbildung 4: Inhaltsübersicht ICSG, IDSV und IDS-Vorgaben der KDI und anderer Sicherheitsorgane

## 3.4 Sicherheitsorganisation des Kantons und der kantonalen Verwaltung

In Umsetzung des Artikels 31 ICSG sowie des Artikels 21 Absatz 2 Buchstabe a DVG wird mit der IDSV das folgende Konzept der kantonalen Sicherheitsorganisation umgesetzt:

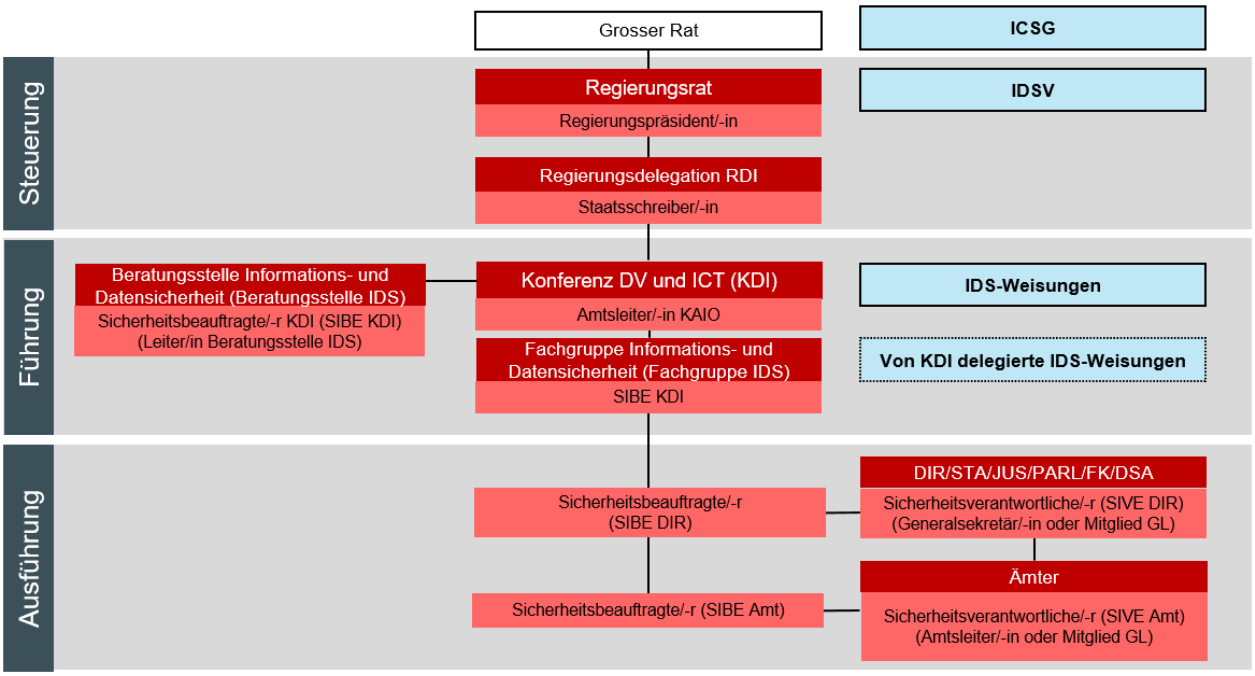



Abbildung 5: Sicherheitsorganisation der Kantonsverwaltung

Die Informations- und Datensicherheit wird mit dem Erlass der IDSV in die Verantwortung der obersten Führung gelegt. Die IDSV sieht aber auch den Erlass von IDS-Weisungen durch die KDI

vor, welche technische Ausführungsbestimmungen an die Fachgruppe Informations- und Datensicherheit weiterdelegieren kann. Die KDI kann durch die Regierungsdelegation digitale Verwaltung und ICT (RDI) mit Vertretungen anderer Behörden, so z.B. der Gemeinden, ergänzt werden (Art. 18 Abs. 1 Bst. d DVV).

Die Gewährleistungsverantwortung obliegt den Generalsekretärinnen und -sekretären der DIR/STA/JUS, den Vorsteherinnen und Vorstehern der Parlamentsdienste, der Finanzkontrolle (FK) sowie der kantonalen Datenschutzbehörde (DSB), welche als Sicherheitsverantwortliche (SIVE) für die Umsetzung der Vorschriften in ihrer Behörde zu sorgen haben. Sie können die Rolle an ein anderes, ihnen direkt unterstelltes Mitglied der obersten Führung delegieren.

Die Fachexpertise wird durch die Sicherheitsbeauftragten (SIBE) auf den Stufen KDI, DIR/STA/JUS/PARL/FK, der DSB sowie der Ämter wahrgenommen. Die Leiterin oder der Leiter der Beratungsstelle IDS bzw. des Fachbereichs Sicherheit des KAIO ist auch die oder der Sicherheitsbeauftragte der KDI. Sie oder er leitet auch die Fachgruppe IDS.

Die Rollenbeschriebe mit den Aufgaben, Kompetenzen und Verantwortungen sind durch die KDI zu erlassen.

Zu beachten ist, dass das Büro des Grossen Rates für die Informationssicherheit im parlamentarischen Bereich Ausführungsbestimmungen erlassen kann, die von der IDSV und von den gestützt darauf erlassenen Weisungen abweichen (Art. 34 ICSG). Es kann z.B. die Organisation und die Zuständigkeiten der Sicherheitsorgane für sich anders als in der IDSV vorgesehen regeln. Im Interesse der Einheitlichkeit der Sicherheitsvorschriften wird die KDI aber bemüht sein, Anliegen des Grossen Rates möglichst auch in ihren Weisungen zu berücksichtigen, so dass die Notwendigkeit für abweichende Regeln des Grossen Rates entfällt.

### 3.5 Wirkungsziele

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

a) Kantonsweites und auf jeder Ebene ein einheitliches Verständnis der Klassifizierungsstufen INTERN, VERTRAULICH und GEHEIM.
b) Weniger klassifizieren, besser schützen: Reduktion der klassifizierten Informationen dank klaren und einheitlichen Vorgaben zur Klassifizierung von Informationen und der Einstufung von ICT-Mitteln und Personendaten:

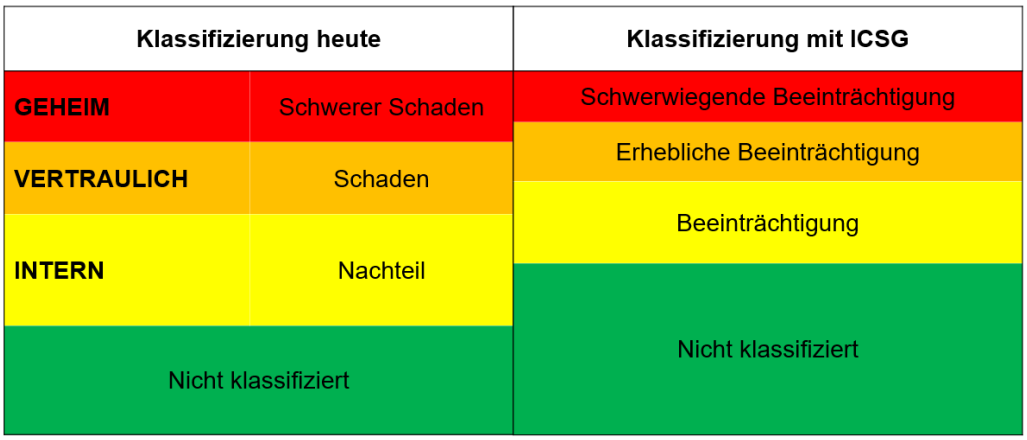



Abbildung 6: Reduktion der Klassifizierungen durch ICSG

c) Mit der risikoangemessenen Einstufung und infolgedessen der Reduktion besonders schutzbedürftiger Informationen, Personendaten und ICT-Mittel können Kosten für unnötige Schutzmassnahmen gespart werden: «Holz auf die Scheiterbeige, Gold in den Safe.».
d) Die IDSV schafft zusammen mit den Ausführungsweisungen- und Hilfsmitteln für die Berner Behörden konsistente und einheitliche Vorschriften über den Umgang mit eingestuften Schutzobjekten.
e) Die nötige Aufmerksamkeit für die Informations- und Datensicherheit des Personals und insbesondere der Führungskräfte wird sichergestellt («Awareness»).
f) Den Führungskräften werden Hilfsmittel zur Verfügung gestellt, um die für die Informations- und Datensicherheit relevanten Schwächen ihrer Organisation, ICT-Mittel und Mitarbeitenden zu erkennen.
g) Es wird eine Sicherheitsorganisation mit klaren Zuständigkeiten, Aufgaben und Kompetenzen geschaffen, welche mit dem DVG bereits heute in ihrer Struktur besteht.

## 4. Erlassform

Sowohl das ICSG als auch das KDSG delegieren dem Regierungsrat den Erlass der Ausführungsbestimmungen zur Informations- und Datensicherheit, weshalb die IDSV auf Verordnungsstufe erlassen wird.

## 5. Rechtsvergleich

### 5.1 Bund

Die IDSV orientiert sich auch an der ISV des Bundes, um damit die Gleichwertigkeit der Bundesregelungen zu gewährleisten und vom Bund weiterhin ohne Einschränkung als Partner mit aktueller und wirksamer Informations- und Datensicherheit anerkannt zu werden. Die IDSV ist aber absichtlich weniger umfangreich und komplex als die ISV, damit sie für alle kantonalen Staatsebenen verständlich und anwendbar bleibt.

### 5.2 Kantone

Ein Vergleich mit der Gesetzgebung der anderen Kantone (Stand Oktober 2025) zeigte, dass es kein Regelungsmodell gibt, an dem sich der Kanton Bern orientieren könnte. Noch kein Kanton verfügt aktuell über ein zum ICSG analoges Gesetz. Hingegen orientieren sich andere Kantone am Berner ICSG. So erarbeitete z.B. der Kanton Aargau ein Gesetz über die Informationssicherheit (InfoSiG), welches sich stark an der Struktur des ICSG orientiert.

Ebenso wenig besteht ein anderes Datenschutzgesetz, welches für die Datensicherheit auf die Schutzmassnahmen der Informationssicherheit verweist.

Mit diesem vereinfachten Konzept schafft der Kanton Bern neue, wirkungsorientierte und zukunftsfähige Grundlagen für seine Informations- und Datensicherheit.

## 6. Umsetzung und Evaluation des Vollzugs

Die IDSV wird zusammen mit dem ICSG per 1. November 2026 in Kraft gesetzt.

Die Evaluation des Vollzugs wird Gegenstand der im Rahmen der Umsetzung zu erarbeitenden kontinuierlichen Verbesserungsprozesse sein, die ein zentraler Bestandteil des in der IDSV vorgesehenen Informationssicherheits-Managementsystems (ISMS) sind.

# 7. Erläuterung zu einzelnen Artikeln

## 7.1 Allgemeine Bestimmungen

### Artikel 1 – Gegenstand

Grundlage dieser Verordnung sind sowohl das ICSG als auch das KDSG. Die IDSV regelt daher sowohl die Informations- als auch Datensicherheit.

### Artikel 2 – Geltungsbereich

Absatz 1: Die «kantonalen Behörden» werden in Artikel 3 Bst. h aufgezählt. Sie haben sowohl die Sicherheit der Schutzobjekte des Kantons als auch des Bundes nach den Regeln der IDSV zu gewährleisten. Ausgenommen sind die teilautonomen Organisationen nach Artikel 3 Absatz 1 der Verordnung vom 27. November 2002 über die Organisation und die Aufgaben der Bildungs- und Kulturdirektion (Organisationsverordnung BKD, OrV BKD][22], s. Erläuterung zu Art. 3 Bst. h IDSV).

Absatz 2: Die anderen Behörden im Kanton sind von der IDSV nur dann betroffen, wenn sie mit Schutzobjekten des Kantons oder des Bundes arbeiten. Diese Behörden sind z.B. die Einwohner-, Kirch- oder Burgergemeinden sowie anderen gemeinderechtlichen Körperschaften nach Kapitel 7 Kantonsverfassung (KV), die Landeskirchen nach Kapitel 8.1 KV sowie die anderen Träger öffentlicher Aufgaben nach Artikel 95 KV. Die Vorschriften der IDSV gelten also z.B. nicht für die mit BE-Login und AGOV erschlossenen kommunalen Applikationen und Informationen.

Der Geltungsbereich der IDSV kann grafisch wie folgt dargestellt werden:

| **Geltungsbereich** | **Schutzobjekte** | **Kantonale Behörden** | **Andere Behörden** |
|---|---|---|---|
| **Informationssicherheit** | Informationen / ICT-Mittel von Kanton oder Bund | IDSV<br>Alle Vorschriften | • IDSV Abschnitt 1 und 2<br>• Von Bund oder Kanton vorgegebene Schutzmassnahmen (Art. 22 IDSV)<br>• Weitergehende risikoangemessene Schutzmassnahmen<br>• Grundschutz BE empfohlen |
| | Informationen / ICT-Mittel anderer Behörden | IDSV<br>Alle Vorschriften | • IDSV gilt nicht<br>• Grundschutz BE empfohlen<br>• Weitergehende risikoangemessene Schutzmassnahmen in eigener Verantwortung |
| **Datensicherheit** | Personendaten | IDSV<br>Alle Vorschriften | • IDSV Abschnitt 1 und 2<br>• Risikoangemessene Schutzbedarfsanalyse bzw. ISDS-Konzept gemäss Empfehlungen der Datenschutzbehörde (Art. 8 IDSV)<br>• Grundschutz BE empfohlen |

Abbildung 7: Geltungsbereich IDSV

[22] OrV BKD, BSG 152.221.181

**Artikel 3 – Begriffe**

Keine Bemerkungen ausser zu Buchstabe h: Kantonale Behörden

Die kantonalen Schulen und Bildungsinstitutionen sind teilautonome Organisationseinheiten; ihre Organisation, Aufgaben und Befugnisse werden durch die Gesetzgebung bestimmt (Art. 3 Abs. 1 OrV BKD). Sie fallen deshalb wie die Hochschulen unter den Begriff der «anderen Träger öffentlicher Aufgaben» gemäss Artikel 95 Absatz 1 Bst. a KV. Damit gelten sie als «andere Behörden» im Sinne von Artikel 2 Absatz 2 IDSV.

## 7.2 Grundsätze der Informations- und Datensicherheit

**Artikel 4 – Führungsverantwortung**

Absatz 1:

Die oberste Führung einer Behörde, also z.B. auch einer selbstständigen Organisation oder Körperschaft mit öffentlich-rechtlichen Aufgaben, hat zur Sicherstellung der Informations- und Datensicherheit eine besondere Verantwortung (zur obersten Führung in der Kantonsverwaltung s. die Ausführungen zu Art. 19 Abs. 1 IDSV, Restrisiken und aktuelle Bedrohungen).

Buchstabe a: Sorgt für die Informations- und Datensicherheit

Die oberste Führung hat die Informations- und Datensicherheit in ihrem Bereich nach dem Stand der Technik zu gewährleisten, also zu organisieren und die Umsetzung sowie Überprüfung sicherzustellen. Sie muss in Allgemeinen Sicherheitsleitlinien oder durch ihre Risikoentscheide im Einzelfall Folgendes festlegen:

a) Mit den Sicherheitsleitlinien werden die Ziele für die Informations- und Datensicherheit vorgegeben, also der angestrebte Soll-Zustand. Sie setzen eine Kosten-Nutzen-Analyse voraus: Wie viel Sicherheit will bzw. muss die Behörde haben, und wie viel darf bzw. wird diese Sicherheit kosten?

b) Die oberste Führung hat auch zu bestimmen, wie die unterstellten Organisationen mit Risiken umgehen sollen, welche Risiken sie ohne Weiteres tragen dürfen und welche Risiken der Führung rapportiert werden müssen (Risikoakzeptanz). Auch wenn die meisten Risiken der Informations- und Datensicherheit auf der operativen Ebene (z.B. Amt oder unterstellte Einheit) behandelt und getragen werden können, haben ausgewählte Risiken eine strategische Bedeutung.

c) Es gibt immer wieder Personen, welche die Informations- und Datensicherheit nicht genug ernst nehmen und vorschriftswidrig oder unsorgfältig mit Informationen, Personendaten oder ICT-Mitteln umgehen. Oft haben solche Verstösse keine Konsequenzen für diese Personen. Die oberste Führung hat die Vorschriften konsequent durchzusetzen sowie nötigenfalls personal- und strafrechtlich zu sanktionieren.

Buchstabe b: Akzeptiert nachweisbar Restrisiken

Einen risikofreien Umgang mit Schutzobjekten gibt es in der Praxis nie. Weil eine hundertprozentige Sicherheit unmöglich, unpraktikabel oder viel zu teuer wäre, verbleiben auch nach dem Umsetzen von Schutzmassnahmen regelmässig sog. Restrisiken, die von der zuständigen Behörde bewusst und ausdrücklich akzeptiert werden müssen. Die «nachweisbare» Akzeptanz von Restrisi-

ken ist wichtig. Denn diese bestätigt einen durchlaufenen Risikoanalyse- und Entscheidungsprozess und damit einen bewussten Entscheid über die in Kauf genommenen Restrisiken. Damit nimmt die Behörde im Interesse ihrer Aufgabenerfüllung in Kauf, dass sich ein Restrisiko möglicherweise realisiert.

Die Zuständigkeit für dieses Risikoakzept richtet sich nach der Zuständigkeit für die jeweilige staatliche Aufgabe, im Bereich der kantonalen ICT-Mitteln nach Artikel 32 DVG. Danach ist das KAIO für das Akzept von Restrisiken im Bereich der ICT-Grundversorgung und seiner Konzernapplikationen verantwortlich. Die einzelnen Fachbehörden (Direktionen, Ämter, Justizbehörden, Grosser Rat oder Aufsichtsbehörden) sind für das Akzept von Restrisiken im Bereich ihrer jeweiligen Fach- und Konzernapplikationen verantwortlich. Alle Behörden sind zudem für das Akzept von Restrisiken verantwortlich, die sich aus der Art und Weise ergeben, wie sie ICT-Mittel nutzen, die ihnen von einer anderen Behörde zur Verfügung gestellt werden (z.B., wenn ein Amt zu schützende Informationen unverschlüsselt per E-Mail verschickt).

Absatz 2:

Die Vorgesetzten aller Stufen tragen auch im Bereich der Informations- und Datensicherheit die Verantwortung für die funktionsbezogene, praxisnahe Aus- und Fortbildung ihrer Mitarbeitenden oder Beauftragten sowie für die Überprüfung der Einhaltung der Vorschriften. Die Mitarbeitenden und Beauftragten sollen in der Lage sein, Gefahren und Bedrohungen selbst zu erkennen, korrekt zu reagieren und entsprechende Sicherheitsmeldungen zu erstatten. Die Behörden stellen die Schulung sicher, z.B. regelmässige Sensibilisierungs- und Awareness-Kampagnen oder Eintrittsschulungen.

Die Beratungsstelle IDS stellt in Zusammenarbeit mit der kantonalen Datenschutzbehörde den Behörden allgemeine Hilfsmittel (z.B. E-Learning BE-Secure) zur Verfügung und lanciert für die kantonalen Behörden zusätzlich Awareness-Kampagnen, z.B. Phishing-Simulationen. Das Absolvieren des heute schon bestehenden BE-Secure dauert maximal zwei Stunden, richtet sich an alle Mitarbeitenden und kann auch von Personen ausserhalb der Kantonalen Behörden genutzt werden. Die Awareness-Kampagnen werden weiterhin mit den bestehenden Ressourcen des Bereichs Sicherheit beim KAIO lanciert.

Die Beratungsstelle IDS kann zudem die Führungspersonen mit den Daten über die Teilnahme der Mitarbeitenden an Schulungen sowie über deren Lernerfolg orientieren, damit die Führungspersonen ihre Pflichten hinsichtlich der Ausbildung und deren Überprüfung wahrnehmen können.

Absatz 3:

Die Vorgesetzten jeder Stufe sowie die Mitarbeitenden müssen bei der Arbeit mit Schutzobjekten die gesetzlichen Verhaltensvorschriften einhalten. Die Wahrnehmung dieser Verantwortung setzt aber voraus, dass die Mitarbeitenden entsprechend instruiert und ausgebildet werden sowie über die notwendigen Ressourcen verfügen. Mit Mitarbeitenden sind interne und externe Mitarbeitende gemeint, die der Weisungsbefugnis der Behörde unterstehen: «Interne» Mitarbeitende sind Angestellte der Behörde gemäss dem kantonalen oder kommunalen Personalrecht. «Externe» Mitarbeitende hingegen sind Personen, die mittels eines Personalverleihvertrages zur Mitarbeit verpflichtet sind.

Keine Mitarbeitende hingegen sind selbständige Privatpersonen oder Mitarbeitende von Unternehmen, die basierend auf einem privatrechtlichen Vertrag nach dem Obligationenrecht[23] für die Behörde beratend tätig sind oder für diese Dienst- oder Sachleistungen erbringen (wie Softwareentwicklung, Netzwerkausbau, Bau eines Serverraums, Übernahme der Projektleitung etc.). Solche

[23] OR, SR 220

Personen sind nach den Vorschriften von Artikel 17 als beauftragte Dritte zu steuern. Dies gilt ebenso für die Freiwilligen, welche sich z.B. in Kirchgemeinden engagieren.

Absatz 4:

Die oberste Führung bleibt in jedem Fall für die Gewährleistung der Informations- und Datensicherheit durch die ihnen unterstellten Einheiten sowie durch die beauftragten Dritten verantwortlich. Insbesondere bei der Beauftragung von privaten Leistungserbringern ist sie für die sorgfältige Auswahl, Instruktion, Überwachung und nötigenfalls auch für die Trennung oder Sanktionierung verantwortlich.

**Artikel 5 – Präventive Schutzmassnahmen**

Artikel 10 Absatz 1 KDSG verpflichtet die Datenbearbeitenden, für die nötige Datensicherheit zu sorgen; das aktuelle Datenschutzrecht regelt die Grundschutzanforderungen an die technischen, organisatorischen, physischen und personellen Schutzmassnahmen (Art. 4 ff. DSV). Diese Bestimmungen werden in die IDSV übertragen und auch im Lichte der Bundesgesetzgebung aktualisiert. Sie formulieren damit auf generell-abstrakter Ebene die Elemente des allgemeinen Schutzes von sowohl von Personendaten als auch von Informationen: Den Grundschutz.

Mit diesem Artikel werden neu für alle vier Elemente der Informations- und Datensicherheit die für jedes Schutzobjekt zu erreichende Wirkungsziele genannt, und zwar sowohl für den digitalen als auch analogen Umgang. Dabei bleibt die IDSV bei einer noch generischen Beschreibung, die konkreten Schutzmassnahmen werden von der KDI in der Weisung über den Grundschutz für die Informations- und Datensicherheit des Kantons Bern (Grundschutz BE) festgelegt. Müssen erhöhte Schutzanforderungen erfüllt werden, sind die weitergehenden Schutzmassnahmen im Informations- und Datenschutzkonzept (ISDS-Konzept) zu beschreiben. Die Schutzmassnahmen sind immer nach Massgabe desjenigen Risikos auszugestalten, welches das Schutzobjekt gefährdet; sie müssen also risikoangemessen sein.

Buchstabe a: Vertraulichkeit

Die Zugriffskontrolle ist eine fundamentale Aufgabe der Behörden zur Gewährleistung der Informations- und Datensicherheit. Es sollen nur Angehörige der Behörden und diese nur zur Erfüllung ihrer gesetzlichen Aufgaben Zugriff auf Informationen und Personendaten haben. Dabei ist auch der Umfang des Zugangs, die Zugangsberechtigung, festzulegen und zu kontrollieren.

Im Rahmen der Zugangskontrolle ist z.B. festzulegen, wer Zutritt zu den Räumlichkeiten und Anlagen hat, in denen die Daten bearbeitet werden. Mit «Anlagen» wird ausgedrückt, dass auch der Zugang zu mobilen Bearbeitungsanlagen zu unterbinden ist. Der Begriff ist sehr weit gefasst und umfasst von fest angelegten Rechenzentren mit Serveranlagen über Computer bis hin zu Mobiltelefonen oder Tablets jegliche Geräte zur Bearbeitung von Personendaten. Mögliche Massnahmen sind beispielsweise Vereinzelungsanlagen mit biometrischer Identitätskontrolle oder die sichere Identifikation bei der Anmeldung auf dem eigenen PC oder Laptop.

Die Behörden müssen im Rahmen der Benutzerkontrolle auch sicherstellen, dass nur berechtigte Personen auf Applikationen mit nicht öffentlichen Informationen oder mit Personendaten zugreifen können. Einfache Massnahmen sind beispielsweise die regelmässige Kontrolle und Überprüfung von Berechtigungen, die automatische Sperrung von Benutzerkonten, welche länger als ein Jahr nicht mehr verwendet wurden, oder aber der Einsatz von Software gegen Mal- oder Spyware.

Buchstabe b: Verfügbarkeit und Integrität

Die Datenträgerkontrolle soll die Verfügbarkeit und die Integrität der Informationen und Personendaten gewährleisten. Mögliche Massnahmen sind beispielsweise die Verschlüsselung oder differenzierte Zugriffsberechtigungen für Applikationen und Betriebssysteme. Die Behörden müssen zudem geeignete Massnahmen treffen, um die Daten bei der Bekanntgabe sowie beim Transport von Datenträgern zu schützen (Transportkontrolle). Auch hierzu dienen die sichere Identifikation der Personen oder die Verschlüsselung der Informationen oder Personendaten (Ziff. 1).

Die rasche Wiederherstellung der Verfügbarkeit der Personendaten und Informationen und des Zugangs zu ihnen nach einem Ausfall ist z.B. mit einem Backup-Konzept sicherzustellen, welches redundante Datenträger oder Rechenzentren vorsieht (Ziff. 2).

Die Stabilität bzw. die Belastbarkeit der eingesetzten ICT-Mittel soll dauerhaft gewährleistet werden (Ziff. 3). Es sollen alle Funktionen des digitalen Datenbearbeitungssystems zur Verfügung stehen (Verfügbarkeit), Fehlfunktionen gemeldet (Zuverlässigkeit) und gespeicherte Informationen und Personendaten nicht durch Fehlfunktionen des Systems beschädigt werden können (Informations- und Datenintegrität).

Schliesslich muss die Systemsicherheit gewährleistet sein (Ziff. 4): Die Betriebssysteme und Anwendungssoftware müssen stets auf dem aktuellen Sicherheitsstand gehalten und bekannte Schwachstellen geschlossen werden.

Buchstabe c: Nachvollziehbarkeit

Aus Kostengründen muss die lückenlose Nachvollziehbarkeit von Veränderungen der Informationen erst ab der Klassifizierung «INTERN» erfolgen. Bei Personendaten ist sie unabhängig von ihrem Schutzbedarf sicherzustellen.

Die Eingabekontrolle (Ziff. 1) verlangt, dass in digitalen Systemen nachträglich überprüft werden kann, welche Informationen oder Personendaten zu welcher Zeit und von welcher Person eingegeben oder verändert wurden. Als mögliche Massnahme kommt insbesondere die Protokollierung nach Artikel 6 hiernach in Betracht. Denkbar sind aber auch

a) das Einschränken der Berechtigungen auf sehr wenige Personen,
b) die Kontrolle des Zugangs zur Applikation durch physische Massnahmen,
c) eine enge zeitliche Eingrenzung der Verfügbarkeit der Applikation,
d) das Festhaltens des Zeitpunkts eines Zugriffs oder
e) die Kombination dieser verschiedenen Massnahmen.

Die Bekanntgabekontrolle (Ziff. 2) muss insbesondere ermöglichen, die Datenempfängerinnen und -empfänger zu identifizieren. Dabei kann es je nach Fall ausreichen, dass die empfangende Behörde feststeht, ohne dass die für sie handelnde Person identifizierbar sein muss. Bei Bedarf muss anhand von Aufzeichnungen feststellbar sein, mit welchen Mitteln welche Personendaten an wen bekanntgegeben wurden.

Die Massnahmen zur Erkennung und Beseitigung von Sicherheitsvorfällen (Ziff. 3) sind reaktiv und in entsprechenden Vorsorgeplänen vorzusehen.

**Artikel 6 – Protokollierung bei digitaler Bearbeitung von Personendaten**

Absatz 1:

Diese Protokollierungspflicht ist eine zusätzliche Massnahme zur Gewährleistung der Datensicherheit für den Fall, dass die präventiven Massnahmen nach Artikel 5 nicht ausreichen. Der Artikel konkretisiert also die Schutzmassnahmen zur Gewährleistung der Nachvollziehbarkeit bei der digitalen Bearbeitung von Personendaten. Der Hauptanwendungsfall sind sehr weitgehende Berechtigungen für Personen, die nicht von vornherein bloss auf diejenigen Daten eingeschränkt werden können, welche die jeweilige Person zur Erfüllung ihrer Aufgaben bearbeiten muss. Mit der «digitalen» Bearbeitung ist dasselbe gemeint wie im bisherigen Berner Recht (Art. 6 Abs. 1 DSV) und im Bundesrecht (Art. 4 Abs. 1 und 2 Verordnung vom 31. August 2022 über den Datenschutz [Datenschutzverordnung, DSV][24]) mit der «automatisierten» Bearbeitung, also die typischerweise ohne menschliches Zutun oder Überprüfung erfolgende Datenbearbeitung.

Die Protokollierung dient nicht vorab der Überwachung der Nutzerinnen und Nutzer, sondern hat folgende Zwecke:

a) Die Behörden können bei besonderen Risiken die Bearbeitung von Personendaten nachträglich überprüfen, mit dem Ziel, festzustellen, ob solche abhandengekommen, gelöscht, vernichtet, verändert oder offengelegt worden sind.
b) Darüber hinaus können sich aus der Protokollierung auch Hinweise ergeben, ob Personendaten zweck- und damit rechtskonform bearbeitet wurden.

Im Fall von Absatz 1 protokollieren die Behörden mindestens das Speichern, Verändern, Löschen und Vernichten der Daten. Indem sie die digitale Bearbeitung von Personendaten protokollieren, gewährleisten sie deren Nachvollziehbarkeit und kommen damit auch ihren Pflichten nach Artikel 5 Buchstabe c nach.

Absatz 2:

Wenn Behörden und beauftragte Dritte besonders schützenswerte Personendaten digital bearbeiten oder ein Profiling mit hohem Risiko durchführen, und dabei die präventiven Schutzmassnahmen nach Artikel 5 nicht genügen, protokollieren sie zusätzlich das Zugreifen auf die bzw. das Lesen sowie die Bekanntgabe der Personendaten. Beispielsweise haben Angehörige des Polizeikorps über ihr Mobiltelefon einen weitgehenden Zugriff auf polizeiliche Datenbanken, und dieser Zugriff lässt sich nicht von vornherein einschränken, weil nicht vorhersehbar ist, mit welchen Menschen die Polizistinnen und Polizisten im Rahmen ihrer Aufgaben in Kontakt geraten. In solchen Fällen ist es nötig, auch Lesezugriffe zu protokollieren, um damit allfällige nicht dienstlich gebotene Abfragen nachvollziehen und sanktionieren zu können.

Diese Vorschrift orientiert sich an Artikel 4 Absatz 2 der DSV des Bundes und sieht vor, dass der Lesezugriff und die Bekanntgabe nur protokolliert werden müssen, wenn die Schutzbedarfsanalyse zeigt, dass die präventiven Schutzmassnahmen nicht genügen. Damit werden auch die europarechtlichen Anforderungen an die Protokollierung gemäss Artikel 25 der Richtlinie (EU) 2016/680 bei der Strafverfolgung oder -vollstreckung erfüllt, da die Daten im Anwendungsbereich der Richtlinie in der Regel besonders schützenswert sind.

Das Protokoll sollte enthalten:

a) die Identität des bearbeitenden Systems oder der Person, welche über das System auf die Informationen oder Personendaten zugreift,
b) die Art der Bearbeitung,

[24] DSV, SR 235.11

c) das Datum und die Uhrzeit der Bearbeitung und
d) gegebenenfalls die Identität der Empfängerin oder des Empfängers der Personendaten.

Die Behörden sollten beim Verdacht auf Missbrauch der Informationen oder Personendaten diese Informationen rasch zu Handen der Strafverfolgungsbehörde sichern.

Absatz 3:

Die Protokolle sind mindestens während sechs Monaten aufzubewahren. Aus Ressourcengründen wird in Abweichung zum Bund darauf verzichtet, generell ein Jahr vorzuschreiben. Hingegen wird eine Mindestfrist definiert, die je nach Risikobeurteilung pro Applikation entsprechend zu verlängern ist. Sie sind so zu führen und aufzubewahren, dass ein Ereignis bis ein halbes Jahr danach nachvollzogen werden kann.

Bei Informationen der Klassifizierung «VERTRAULICH» und «GEHEIM» sowie bei besonders schützenswerten Personendaten und solchen, deren Bekanntwerden die betroffene Person an Leib und Leben gefährden könnte, ist ein längeres Vorhalten der Protokolle angezeigt. Ansonsten ist die Möglichkeit zum Nachweis eines Missbrauchs und damit einer realistischen Strafverfolgung und wirkungsvollen Abschreckung zu gering.

In den Fällen, wo eine besondere Gefahr besteht, dass bei Sicherheitsvorfällen auch das Protokoll selbst gestohlen, zerstört, gelöscht, manipuliert oder verschlüsselt werden könnte, muss es getrennt vom System, in dem die Personendaten bearbeitet werden, aufbewahrt werden. Dies ist z.B. bei Automaten der Fall, welche Rotlichter, Geschwindigkeiten und Abstände überwachen. Sie können vor Ort zerstört oder gestohlen werden, weshalb sie ihre Protokolle an einen anderen Ort senden müssen.

Die Protokolle dürfen ausschliesslich denjenigen Stellen zugänglich sein, denen die Überwachung der Datenschutzvorschriften oder andere gesetzliche Aufgaben obliegen. Sie dürfen nur für diese Zwecke verwendet werden. Das gilt bereits nach der allgemeinen Zweckbindungsbestimmung nach Artikel 6 KDSG und muss deshalb nicht ausdrücklich in der Verordnung festgehalten werden.

**Artikel 7 – Meldung von Sicherheitsvorfällen, Schwachstelle und Cyberangriffen**

Zum Schutz der Schweiz vor Cyberbedrohungen erstellt das Bundesamt für Cybersicherheit (BACS) technische Analysen zur Bewertung und Abwehr von Cybervorfällen und Cyberbedrohungen sowie zur Identifikation und Behebung von Schwachstellen (Art. 73a Abs. 1 ISG). Das Hauptmotiv für die Einführung auch einer kantonalen Meldepflicht ist die Frühwarnung und die bessere Übersicht zur Bedrohungslage (s. auch Botschaft zur Änderung des Informationssicherheitsgesetzes [Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen] zum ISG vom 2. Dezember 2022, Ziff. 4.1[25]). Die Meldepflicht ist also Teil der Vorsorgepflicht und Reaktionsfähigkeit nach Art. 7 Bst. a ICSG und somit Teil der präventiven Schutzmassnahmen nach Artikel 5 Buchstabe c Ziffer 3 IDSV, sowohl zum Schutz von Informationen als auch Personendaten.

Da Angreiferinnen und Angreifer oft ähnliche Vorgehensweisen und Angriffsmuster für mehrere kritische Infrastrukturen verschiedener Sektoren verwenden, kann die Meldepflicht wesentlich dazu beitragen, durch frühzeitiges Erkennen der Angriffsmethoden und entsprechende Warnungen die Informations- und Datensicherheit zu stärken. Durch die grössere Anzahl von Meldungen, die aufgrund der Meldepflicht eingehen, ist eine bessere Beurteilung der Bedrohungslage und damit eine bessere Abwehr möglich.

[25] BBl 2023 84

Für die Berner Behörden ergeben sich bei der Gefährdung oder Beeinträchtigung der Informations- oder Datensicherheit aus drei Gesetzen des Bundes und des Kantons unterschiedliche Meldepflichten mit verschiedenen Zwecken, Fristen und Meldeinhalten:

a) Artikel 26 ff. KDSG: Zum Schutz der betroffenen Personen und potenziellen weiteren Opfern, zur Erhöhung der Transparenz sowie zur Verbesserung der Datensicherheit; Frist: 72 Stunden nach Entdeckung der Verletzung der Datensicherheit (Art. 26 Abs. 1 KDSG);
b) Artikel 7 ICSG: Die Pflicht zur Vorsorge und Abwehr setzt für die Behörden Meldepflichten bei Sicherheitsvorfällen, Schwachstellen oder Cyberangriffen voraus;
c) Artikel 73b ff. ISG: Zum Schutz der betroffenen Behörden, Organisationen oder Personen und potenziell weiteren Opfern; Frist: 24 Stunden nach Entdeckung der Schwachstelle oder des Cyberangriffs (Art. 74e Abs. 1 ISG).

Für letztere bezeichnet der Bund zudem ausdrücklich in Artikel 74b ISG zahlreiche meldepflichtige Behörden und Organisationen, insbesondere in Absatz 1 Buchstabe b neben den Kantons- auch die «Gemeindebehörden». Gemäss Auskunft des BACS fallen darunter sämtliche öffentlich-rechtlichen Körperschaften nach kantonalem Recht, welche hoheitliche Aufgaben wahrnehmen. Dazu gehören auch die Einwohner-, Kirch- und Burgergemeinden und ihre selbständigen Träger öffentlicher Aufgaben.

Zwar statuiert Art. 74a Abs. 1 ISG nur für Cyberangriffe eine Meldepflicht. Aber als Teil der in Art. 7 Bst. a ICSG festgeschriebenen Pflicht zur Vorsorge und Reaktionsfähigkeit ist das Melden aller Sicherheitsvorfälle eine wichtige Voraussetzung für eine Schutzmassnahme, zu welcher die Berner Behörden mit Artikel 5 Buchstabe c Ziffer 3 IDSV angehalten sind: Die rasche Erkennung und Behebung der Folgen von Sicherheitsvorfällen.

Mit den drei verschiedenen gesetzlichen Grundlagen bestehen grundsätzlich auch drei verschiedene Empfänger der Meldungen: Die Berner Datenschutzbehörden, die kantonale Beratungsstelle IDS sowie das BACS. Mit der vorliegenden Bestimmung können die Meldepflichtigen gegenüber allen drei Behörden mit dem gleichen ICT-Mittel in einfacher Weise ihre gesetzliche Pflicht erfüllen.

Absatz 1:

Nicht jedes sicherheitsrelevante Ereignis muss gemeldet werden, sondern nur solche, die zu einer wesentlichen Gefährdung oder bereits zu einer konkreten Beeinträchtigung der Informations- und Datensicherheit geführt haben. Sicherheitsvorfälle, Schwachstellen oder Cyberangriffe sind also insbesondere in den folgenden Fällen zu melden:

a) Die Aufgabenerfüllung der Mitarbeitenden oder beauftragten Dritten wird beeinträchtigt:

   Spätestens, wenn die Verfügbarkeit von Informationen, Personendaten oder ICT-Mitteln leidet, ist auch die Aufgabenerfüllung beeinträchtigt. Dies kann aber auch der Fall sein, wenn erkannt wird, dass die Informationen oder Personendaten verfälscht worden sind und damit deren Integrität nicht mehr vorhanden ist.

b) Die Sicherheit von Schutzobjekten ab Schutzniveau 2 ist gefährdet, also von:

   1. Informationen mit der Klassifizierung VERTRAULICH oder GEHEIM.
   2. Personendaten, die besonders schützenswert sind, oder deren Bekanntgabe zu einer schweren Gefährdung für die Sicherheit der Person führen kann.
   3. ICT-Mittel mit der Einstufung «Hoher Schutz» und «Sehr hoher Schutz».

Die Folgen der Verletzung ihrer Sicherheit können derart schwer wiegen, dass allein deren Gefährdung eine Meldung erfordert, analog zu Art. 74d Bst. a ISG, Gefährdung der Funktionsfähigkeit kritischer Infrastruktur. Die Gefahr muss eine unmittelbare, aber nicht unausweichliche sein, analog den Gefährdungsdelikten nach dem Schweizerischen Strafgesetzbuch vom 21. Dezember 1937 (StGB)[26].

c) Sie könnten eine hohe politische Bedeutung haben:

Ein weiterer meldepflichtiger Sachverhalt ist die Möglichkeit, dass Sicherheitsvorfälle, Schwachstellen oder Cyberangriffe hohe politische Bedeutung haben könnten, ohne dass die vorstehenden beiden Kriterien erfüllt sind. Die hohe politische Bedeutung eines Vorfalls hängt einerseits von den betroffenen Schutzobjekten oder Behörden ab. Andererseits aber sind auch die Umstände des Vorfalls massgeblich. Die politische Bedeutung kann sich verändern und wird von der Beratungsstelle IDS zusammen mit der oder dem SIVE beurteilt.

Beispiele meldepflichtiger Sicherheitsvorfälle sind:

- Ein Mitarbeiter versendet einen grossen Datenbestand, welcher vertrauliche Informationen enthält (Schutzniveau 2) fälschlicherweise an eine externe Drittperson, anstatt an seine Vorgesetzte.
- Die Berechtigungen für den Zugriff auf eine Personalverwaltungsapplikation wurden falsch gesetzt: Anstatt nur diejenigen der Personalabteilung haben alle Mitarbeitenden der Verwaltung die Personaldossiers einsehen können.
- Eine Schwachstelle ist in einer breit verwendeten Geschäftsverwaltungssoftware entdeckt worden.

Absatz 2:

Das ISG und das KDSG sehen verschiedene Meldefristen vor, was in diesem Absatz verdeutlicht wird.

Absatz 3:

Sofern sie Artikel 27 KDSG dazu verpflichtet, hat die Behörde der durch die Verletzung der Datensicherheit betroffenen Person in einfacher Sprache mindestens die genannten Angaben mitzuteilen.

Die Meldung von Verletzungen der Informations- und Datensicherheit muss zudem die folgenden Angaben enthalten, soweit beurteilbar und vorhanden (s. auch Art. 15 CSV):

a) Datum und Uhrzeit der Feststellung des Sicherheitsvorfalls, der Schwachstelle oder des Cyberangriffes,
b) Datum und Uhrzeit des Sicherheitsvorfalls oder des Cyberangriffs,
c) Beschreibung der Beeinträchtigung der Verfügbarkeit, Integrität, Vertraulichkeit oder Nachvollziehbarkeit der Informationen oder ICT-Mittel,
d) Ausmass der Beeinträchtigung der Funktionsfähigkeit der Behörde,
e) Getroffene und geplante Massnahmen zur Wiederherstellung und künftigen Sicherstellung der Informationssicherheit.

Sind zum Zeitpunkt der Meldung nicht alle erforderlichen Informationen bekannt, ist sie zu ergänzen, sobald neue Erkenntnisse vorliegen.

[26] StGB SR 311.0

Absatz 4:

Damit das Meldewesen funktioniert, muss es einfach, einheitlich und niederschwellig ausgestaltet werden. Den Meldepflichtigen wird daher von der Beratungsstelle IDS im Internet unter www.be.ch/isds eine kantonale Meldeplattform zur Verfügung gestellt, womit gegenüber den drei Empfängern alle Meldepflichten erfüllt werden.

Die Behörden müssen für einen reibungslosen Ablauf ihr Meldewesen organisieren. Aufgaben, Kompetenzen und Verantwortlichkeiten sowie die Prozesse sind vorsorglich intern und insbesondere auch gegenüber ihren beauftragten Dritten festzulegen. Dafür sollte jede Behörde eine einzige interne Meldestelle bestimmen. Bei einer kantonalen Direktion oder einer Stadt ist das sinnvollerweise eine Stelle pro Amt, bei einer grossen Gemeinde pro Abteilung oder bei einer kleinen Behörde z.B. die geschäftsführende Person. Die interne Meldestelle erstattet dann Meldung über die kantonale Plattform.

Die Behörden sollten insbesondere vorsorglich und auch gegenüber ihren beauftragten Dritten Folgendes festlegen:

a) welcher einzigen internen Meldestelle Sicherheitsvorfälle, Schwachstellen oder Cyberangriffe zu melden sind,
b) auf welchem Weg die Meldung an die interne Meldestelle erfolgt,
c) wie Sicherheitsvorfälle, Schwachstellen und Cyberangriffe zu bewältigen sind, und
d) wer Sofortmassnahmen anordnen kann.

Da die Meldepflicht nach Artikel 74b Absatz 1 ISG auch verschiedene Anbieter von ICT-Mitteln trifft, haben diese ebenfalls und selbständig via Plattform nach Absatz 4 sowie der auftraggebenden Behörde gemäss Vertrag zu melden. Eine Meldung des gleichen Vorfalls durch die einzige Meldestelle der auftraggebenden Behörde wird dabei in Kauf genommen.

**Artikel 8 – Schutzbedarfsanalyse und ISDS-Konzept anderer Behörden**

Alle Behörden des Kantons Bern müssen die Risiken für die von ihnen verwendeten Personendaten mit einer Risikoanalyse nach Artikel 18 KDSG beurteilen und nötigenfalls besondere Risiken mit Schutzmassnahmen gemäss der Datenschutzfolgeabschätzung nach Artikel 19 KDSG eingrenzen, damit das erforderliche Mass an Datensicherheit gewährleistet ist. Zum Schutz von Informationen ist der inhaltlich gleiche Prozess zu durchlaufen, nur dass hier die Schritte Schutzbedarfsanalyse und ISDS-Konzept heissen. Der Einfachheit und Klarheit halber werden die beiden Begriffspaare für die kantonalen Behörden mit den Artikeln 13 und 16 IDSV mit «Schutzbedarfsanalyse» und «ISDS-Konzept» vereinheitlicht.

Dieser Artikel stellt klar, dass die anderen Behörden nach Artikel 2 Absatz 2 IDSV sich in ihren Risiken für die Personendaten von den kantonalen Behörden unterscheiden. So bearbeiten z.B. fast alle gemeinderechtlichen Körperschaften deutlich weniger Personendaten als die kantonalen Behörden, welche z.B. via die Gemeinderegistersysteme-Plattform (GERES) auf die Personendaten der rund 1.1 Mio. im Kanton gemeldeten Personen zugreifen können. Zudem verfügen die gemeinderechtlichen Körperschaften tendenziell über weniger Fachwissen und Ressourcen für die Datensicherheit als die kantonalen Behörden.

Aus diesen Gründen verlangt die IDSV zwar auch von den anderen Behörden als Grundlagen für die Vorabkontrolle (Art. 9 IDSV) eine Schutzbedarfsanalyse und nötigenfalls ein ISDS-Konzept, welche die Erfüllung der datenschutzrechtlichen Pflichten dokumentiert. Die kantonale Datenschutzbehörde wird hierfür aber den Risiken der anderen Behörden angepasste Empfehlungen und Vorlagen publizieren (Art. 9 Abs. 4 IDSV).

**Artikel 9 - Vorabkontrolle**

Artikel 3 Absatz 1 Buchstabe b ICSG i.V.m. Artikel 10 Absatz 2 KDSG führen dazu, dass die Schutzmassnahmen für die Informations- sowie an die Datensicherheit die gleichen sind. Dies wird mit den Schutzniveaus gemäss Anhang 1 IDSV verdeutlicht.

Die Vorabkontrolle nach Artikel 20 KDSG ist ein Instrument der Datenschutzbehörden zur Prüfung, ob die Bearbeitung von Personendaten mittels eines ein ICT-Mittels die Datensicherheit nach Artikel 10 KDSG bzw. nach ICSG und IDSV gewährleistet und damit auch dem Datenschutzrecht entspricht. Es ist also eine Sachverhaltsfrage, die vor der Bestätigung des rechtmässigen Datenschutzes zu klären ist. Die Prüfung muss naturgemäss vor der Datenbearbeitung bzw. Inbetriebnahme des ICT-Mittels stattfinden.

Darüber hinaus prüft die Datenschutzbehörde aber auch weitere rechtliche Voraussetzungen zur rechtmässigen Bearbeitung von Personendaten. Die wichtigsten sind:

1. Die Personendatenbearbeitung ist gesetzlich vorgesehen oder dient zur Erfüllung einer gesetzlichen Aufgabe (Art. 4 Abs. 1 KDSG);
2. Bei besonders schützenswerten Personendaten muss deren Bearbeitung in einem Gesetz vorgesehen oder für die Erfüllung einer gesetzlichen Aufgabe unentbehrlich sein, oder es muss die Zustimmung der betroffenen Person vorliegen (Art. 4 Abs. 2 KDSG);
3. In beiden Fällen müssen zudem die Personendaten und die Art der Bearbeitung für die Erfüllung der gesetzlichen Aufgabe geeignet und erforderlich sowie für die betroffene Person zumutbar sein (Verhältnismässig, Art. 7 KDSG).

Da ein wesentlicher Teil der Vorabkontrolle die Prüfung der Datensicherheit ist, wird die Vorabkontrolle bzw. werden die Kriterien für deren Notwendigkeit in der IDSV geregelt.

Absatz 1:

Ist die Behörde verpflichtet, der Datenschutzbehörde eine Bearbeitung zur Vorabkontrolle zu unterbreiten, muss sie der Datenschutzbehörde auch wesentliche Änderungen dieser Bearbeitung zur Vorabkontrolle unterbreiten (Art. 20 Abs. 2 KDSG). Änderungen sind der Datenschutzbehörde unter denselben Voraussetzungen zur Vorabkontrolle vorzulegen wie bisher (s. noch Art. 7 Abs. 3 DSV).

Das ist einerseits der Fall, wenn Mittel und Zweck der Datenbearbeitung erheblich ändern. Die Zweckbindung ist im Datenschutzrecht ein zentrales Element (Art. 6 KDSG). Die Mittel der Datenbearbeitung bestimmen in der Regel die Schwere des Eingriffs. Ändern die Mittel der Datenbearbeitung erheblich, ist deshalb ebenfalls eine Vorabkontrolle notwendig. Bleiben die Mittel die gleichen, ändert aber der Zweck der Datenbearbeitung, so muss dieser noch immer über eine genügende gesetzliche Grundlage verfügen (Art. 6 Abs. 2 Bst. b KDSG), was in einer erneuten Vorabkontrolle zu überprüfen ist.

Eine Änderung ist andererseits dann wesentlich, wenn sie für sich allein die Voraussetzungen für eine Vorabkontrolle erfüllt. Dies ist zum Beispiel der Fall, wenn die Ordnungsbussenzentrale mit einem vernetzten System zur Geschwindigkeits- und Rotlichtüberwachung erweitert wird. Systemänderungen dieser Art sollen Anlass einer Vorabkontrolle sein.

Absatz 2:

Wie bisher liegt grundsätzlich keine wesentliche Änderung im Sinne der Bestimmung vor, wenn sich der Umfang der Datenbearbeitung beschränkt vergrössert, weil davon auszugehen ist, dass

sich dadurch die Schwere des Eingriffs in die Persönlichkeitsrechte nicht ändert. Die Grenze jedoch bildet Absatz 3 Buchstabe b.

Absatz 3:

Nach Artikel 20 KDSG muss die Behörde der Datenschutzbehörde eine Datenbearbeitung dann zur Vorabkontrolle vorlegen, wenn ein hohes Risiko für die betroffene Person besteht. Grundsätzlich ist das Risiko im Einzelfall zu beurteilen. In den beiden in diesem Absatz genannten Fällen ist aber davon auszugehen, dass kein hohes Risiko für die betroffene Person besteht und auf eine Vorabkontrolle verzichtet werden kann.

Im Sinne des bisherigen Artikel 9 Absatz 1 Buchstabe a DSV soll auch zukünftig keine Vorabkontrollpflicht bestehen, wenn eine Zertifizierung entsprechend den Voraussetzungen des Bundesgesetzes vom 25. September 2020 über den Datenschutz (Datenschutzgesetz, DSG)[27] vorliegt. Die Bestimmung ist aber anzupassen: Der Ausnahmetatbestand wird mit der Revision der KDSV an den Wortlaut des revidierten DSG angepasst. Demnach können Systeme, Produkte oder neu auch Dienstleistungen zertifiziert werden. Neu gilt die Ausnahme auch nicht mehr nur für Gemeinden und andere gemeinderechtliche Körperschaften. Es ist zudem davon auszugehen, dass das Risiko für die betroffene Person in jedem Fall gering ist, wenn ICT-Mittel nach Artikel 13 DSG zertifiziert sind.

Absatz 4: Keine Bemerkungen.

**Artikel 10 – Betrieb von ICT-Mitteln**

Absatz 1:

Die Behörden sind für die Informations- und Datensicherheit bei ihrer Arbeit eingesetzten ICT-Mittel verantwortlich. Deren Nutzung ist daher zu überwachen, ihre Sicherheit regelmässig zu überprüfen. Die Häufigkeit der Überprüfung bestimmt sich anhand der Risikobeurteilung pro Applikation. Die Überwachung ist eine rein sicherheitstechnische Angelegenheit und darf allein das sicherheitsrelevante Verhalten der Mitarbeitenden betreffen.

Die Behörden können für diese Aufgaben unabhängige und qualifizierte Dritte beauftragen. Solche können beispielsweise private Sicherheitsdienstleister sein, sog. Managed-Security-Service-Provider (MSSP), oder die Betreiberin eines sog. Bug-Bounty-Programms (s. Art. 40 IDSV). Dabei haben die Behörden darauf zu achten, dass die Beauftragten nicht in direkter Konkurrenz zu den kontrollierten Leistungserbringerinnen oder -erbringern stehen, so dass deren Geschäftsgeheimnisse nicht Konkurrenten in die Hände fallen. Zudem müssen die Beauftragten fachlich qualifiziert sein sowie als Hilfspersonen der Behörden auf das Amtsgeheimnis und dessen Strafbewehrung nach Artikel 320 StGB hingewiesen werden.

Absatz 2: Keine Bemerkungen.

**Artikel 11 – Restriktive Berechtigungen**

Absatz 1: Diese Bestimmung betont einen zentralen Grundsatz der Informations- und Datensicherheit. Die Mitarbeitenden und Beauftragten 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 oder Personendaten eines anderen Bereichs bearbeiten kann. Es kommt vor, dass ehemalige Mitarbeitende oder Beauftragte

[27] DSG, SR 235.1

nach Beendigung des Arbeitsverhältnisses, des Auftrags oder einer besonderen Aufgabe nicht aufgefordert werden, ihren Schlüssel oder Badge zurückzugeben, oder dass ihre Benutzerkonten nicht gesperrt werden. Solche unzulässigen Berechtigungen können in der Folge benutzt werden, gegen die Interessen der Behörden zu handeln. Wenn eine Anstellung, ein Vertrag oder eine Aufgabe beendet ist, müssen die entsprechenden Berechtigungen entzogen werden.

Absatz 2: Besteht Grund zur Annahme, dass eine Gefährdung der Informations- oder Datensicherheit vorliegt, müssen die Berechtigungen sofort gesperrt oder entzogen werden. Beide Schutzmassnahmen sollen insbesondere dazu beitragen, das Risiko einer Innentat zu reduzieren.

Absatz 3: Die jährliche Überprüfung des KAIO der rund 10'000 GERES-Berechtigungen der kantonalen und übrigen Behörden zeigt beispielshaft und deutlich, dass trotz klaren Personalanstellungs- und -trennungsprozessen immer wieder nicht mehr benötigte Berechtigungen noch lange Zeit bestehen bleiben. Daher sind diese periodisch und je nach Schutzbedarf der ICT-Mittel zu überprüfen.

**Artikel 12 – Zusammenarbeit zwischen den Behörden**

Absatz 1: Keine Bemerkungen.

Absatz 2 erlaubt den zuständigen Stellen, zur Erfüllung ihrer Aufgaben und zum eigenen Schutz untereinander Personendaten bekanntzugeben. Die Datenbekanntgabe hat jedoch allein dem gesetzlichen Zweck der Informations- und Datensicherheit zu dienen. Dies ist etwa der Fall bei der Weitergabe von Informationen darüber, wer von Sicherheitsvorfällen wie betroffen ist und bereits kontaktiert oder informiert wurde.

## 7.3 Schutzmassnahmen kantonaler Behörden

### 7.3.1 Sicherheitsverfahren bei ICT-Mitteln

Dieser Abschnitt stützt sich sowohl auf Artikel 11 ff. ICSG (Schutzbedarfsanalyse und ISDS-Konzept) als auch auf Artikel 18 ff. KDSG (Risikoanalyse und Datenschutzfolgeabschätzung). Zwar gelten die Bestimmungen nur für die kantonalen Behörden. Die anderen Behörden bleiben nach Artikel 18 bis 20 KDSG zur Risikoanalyse und Datenschutzfolgeabschätzung verpflichtet. Dabei wenden sie die Schutzbedarfsanalyse und das ISDS-Konzept ihren Risiken angemessen und unter Berücksichtigung der Empfehlungen (Art. 8 IDSV) oder Vorgaben (Art. 9 Abs. 4 IDSV) ihrer Datenschutzbehörde an.

**Artikel 13 – Schutzbedarfsanalyse**

Absatz 1: Die Beurteilung der Risiken durch die kantonalen Behörden ist eine unverzichtbare Grundlage für ein wirksames Risikomanagement und damit einer zweckmässigen und wirtschaftlichen Informations- und Datensicherheit. Die kantonalen Behörden haben den Schutzbedarf von ICT-Mitteln inklusive der damit bearbeiteten Informationen und Personendaten zu erheben.

Absatz 2: Werden ICT-Mittel ohne Schutzbedarfsanalyse in Betrieb genommen, nehmen die Verantwortlichen bewusst in Kauf, dass die Sicherheit von Informationen oder Personendaten verletzt wird. Dies kann einer vorsätzlichen Verletzung des Amtsgeheimnisses oder der Persönlichkeit der betroffenen Personen gleichkommen, was nicht nur straf- und zivilrechtliche, sondern auch dienstrechtliche Konsequenzen haben kann. Bei vorabkontrollpflichtigen ICT-Mitteln kann dies zudem dazu führen, dass die Datenschutzbehörde gestützt auf Artikel 48 KDSG mittels Verfügung die Anpassung oder die Ausserbetriebsetzung der ICT-Mittel anordnet.

**Artikel 14 – Grundschutz**

Der von der KDI beschlossene Grundschutz BE ist von den kantonalen Behörden für alle Schutzobjekte zu gewährleisten.

Die anderen Behörden stellen die Informations- und Datensicherheit mit den präventiven, risikoangemessenen Schutzmassnahmen nach Artikel 5 und 6 IDSV sicher; der Grundschutz BE wird hierfür empfohlen. Sofern sie Schutzobjekte des Kantons oder des Bundes einsetzen, haben sie die Schutzmassnahmen gemäss der spezifischen Weisung, Verfügung oder Vertrag umzusetzen (Art. 22 IDSV).

Der Grundschutz BE ist eine Vollzugsrichtlinie zur Entlastung der verpflichteten Behörden: Mit dessen nachweislichen Umsetzung erfüllen die Behörde und Mitarbeitenden ihren gesetzlichen (Mindest-)Pflichten. Die Behörden sowie beauftragte Dritte, die ICT-Leistungen für die kantonalen Behörden erbringen, müssen die Erfüllung der Grundschutzanforderungen z.H. den Aufsichtsbehörden bzw. den Auftraggebern nachweisen können.

Der Geltungsbereich des Grundschutzes BE kann wie folgt grafisch dargestellt werden:

| **Geltungsbereich** | **Schutzobjekte** | **Kantonale Behörden** | **Andere Behörden** |
|---|---|---|---|
| **Informationssicherheit** | Informationen / ICT-Mittel von Kanton oder Bund | Grundschutz BE | • Vom Bund oder Kanton vorgegebene Schutzmassnahmen (Art. 22 IDSV)<br>• Grundschutz BE empfohlen<br>• Weitergehende risikoangemessene Schutzmassnahmen |
| | Informationen / ICT-Mittel anderer Behörden | Grundschutz BE | • Grundschutz BE empfohlen<br>• Weitergehende risikoangemessene Schutzmassnahmen in eigener Verantwortung |
| **Datensicherheit** | Personendaten | Grundschutz BE | • Grundschutz BE empfohlen<br>• Risikoangemessene, präventive Schutzmassnahmen (Art. 5 IDSV)<br>• Risikoangemessene Schutzbedarfsanalyse bzw. ISDS-Konzept gemäss Empfehlungen der Datenschutzbehörde (Art. 8 IDSV) |

Abbildung 8: Geltungsbereich Grundschutz BE

Der Grundschutz BE richtet sich als Weisung der KDI nur an die sich im Geltungsbereich befindenden kantonalen Behörden, nicht aber an die beauftragten Dritten. Die kantonalen Behörden müssen diese daher mit der Vereinbarung der AGB ISDS BE die Pflicht zur Umsetzung des Grundschutzes BE auferlegen.

Sofern dies infolge der Marktstellung des beauftragten Dritten nur teilweise umsetzbar ist oder dieser den Grundschutz BE durch andere Sicherheitsmassnahmen gewährleisten kann, kann von den AGB ISDS BE abgewichen werden. Die entsprechenden Risiken sind in der Schutzbedarfsanalyse sowie im ISDS-Konzept auszuweisen. Dabei kann beispielsweise ein Grundschutznachweis des beauftragten Dritten in der Form einer Selbstdeklaration zum Zeitpunkt seiner Offerte verlangt werden, worin die Gewährleistung des Grundschutzes BE trotz der Abweichungen zu belegen ist. Die Risiken sind durch geeignete Massnahmen auf ein akzeptiertes Mass zu senken.

**Artikel 15 – Einstufen in Schutzniveaus**

Absätze 1:

Wertsachen sind nach Massgabe ihres Wertes und ihrer Gefährdung zu schützen, nach der Maxime: «Holz auf die Scheiterbeige, Gold in den Safe.».

Dieses einfache Prinzip ist in der Praxis nicht immer einfach umsetzbar, erfordert es doch vorab einmal ein Inventar, worin das Gold vom Holz unterschieden wird. In einem weiteren Schritt ist zu bestimmen, wie stark die Wand des Safe sein muss. Pro Wertsache bzw. Schutzobjekt ist also aufgrund des Schutzbedarfs das Schutzniveau zu bestimmen.

Dieses Prinzip ist für die drei Schutzobjekte Informationen, Personendaten und ICT-Mittel in Anhang 1 zu dieser Verordnung beschrieben. Welche konkreten Schutzmassnahmen für Schutzniveau 0 und 1 durch die kantonalen Behörden zu ergreifen sind, hat die KDI in ihrer Weisung Grundschutz BE zu beschreiben. Mit dessen Umsetzung können die Behörden darauf vertrauen, dass ihre Informations- und Datensicherheit den gesetzlichen Vorschriften entspricht. Sobald also die Führungsverantwortlichen zusammen mit ihren Sicherheitsfachleuten jeder Stufe die Risikoanalyse gemacht, anhand der Weisung der KDI Schutzmassnahmen bestimmt und über die akzeptierten Restrisiken entschieden haben, müssen sie nur noch für die Umsetzung der definierten Schutzmassnahmen sorgen. Mit diesem Vorgehen sind alle Verantwortlichen ihren gesetzlichen Pflichten nachgekommen.

Absatz 2: Keine Bemerkung.

**Artikel 16 – ISDS-Konzept**

Absatz 1:

Ergibt die Schutzbedarfsanalyse, dass ein ICT-Mittel über den Grundschutz BE hinausgehende Anforderungen erfüllen muss, so werden diese erhöhten Sicherheitsanforderungen in einem ISDS-Konzept beschrieben. Nicht oder teilweise erfüllte Grundschutzanforderungen müssen ebenfalls im ISDS-Konzept als Risiken ausgewiesen und deren Vermeidung, Verminderung oder Akzeptanz beschrieben werden.

Seit dem Bestehen der ISDS DV verwendet der Kanton Bern für das Dokument, welches die über den Grundschutz hinausgehenden Schutzmassnahmen beschreibt, den Begriff «Informationssicherheits- und Datenschutzkonzept», kurz ISDS-Konzept. Die ISDS DV unterscheidet noch nicht zwischen der Informations- und der Datensicherheit. Hingegen geht schon sie davon aus, dass nicht nur die Informations- und Datensicherheit, sondern auch die Folgen für den Datenschutz und die erforderlichen Schutzmassnahmen aufgezeigt werden müssen. Artikel 19 KDSG verwendet neu hierfür den Begriff «Datenschutzfolgeabschätzung». Sie ist demnach Teil des ISDS-Konzepts, bei dessen Nennung auch immer die Datenschutzfolgeabschätzung zu verstehen ist.

Ein ISDS-Konzept hat demzufolge mindestens folgenden Inhalt aufzuweisen:

a) die Risiken, welche infolge nicht oder teilweise erfüllten Grundschutzanforderungen bestehen,
b) die besonderen, über den Grundschutz hinausgehenden Schutzmassnahmen,
c) die verbleibenden Restrisiken,
d) die Datenschutzfolgeabschätzung, also die Bewertung der Risiken für die betroffenen Personen (Art. 19 Bst. b KDSG).

Absatz 2: Keine Bemerkungen.

Absatz 3: Das ISDS-Konzept ist ein zentrales Sicherheitsinstrument. Es kann insbesondere bei der Abklärung von Verletzungen der Informations- und Datensicherheit von Bedeutung sein. Denn das ISDS-Konzept führt aus, wie die Behörde die Risiken für die betroffenen Personen bewertet und welche Massnahmen sie getroffen oder bewusst weggelassen hat (Risikoakzept). Das ISDS-Konzept ist deshalb nach Beendigung der Informations- oder Datenbearbeitung, bei ICT-Mitteln also ab deren Ausserbetriebnahme, mindestens zwei Jahre aufzubewahren. Die Aufbewahrungsfrist von zwei Jahren orientiert sich an der Regelung des Bundes (vgl. Art. 14 DSV).

**Artikel 17 – Beauftragte Dritte**

Absatz 1:

Als beauftragte Dritte gelten nach Artikel 6 ICSG bzw. Artikel 12 KDSG alle juristischen und natürlichen Personen des öffentlichen und privaten Rechts, die mittels Vertrag von einer Behörde zur Erfüllung ihrer gesetzlichen Aufgabe beigezogen wurden. Freiwillige sind ebenso beauftragte Dritte, jedoch ohne Entgelt.

Für die Kantonsverwaltung sind das zurzeit insbesondere die Bedag Informatik AG, die Swisscom AG oder die SPIE Schweiz AG. Die Einwohner-, Kirch- und Burgergemeinden werden gemäss der Umfrage der Datenschutzbehörde vom 30. Januar bis 15. März 2026 überwiegend von der Talus AG sowie der Dialog Verwaltungsdata AG unterstützt. Die genannten Unternehmen wurden daher auch in die Erarbeitung der IDSV einbezogen.

Absatz 2:

Mehrere Vorfälle bei beauftragten Dritten des Bundes haben gezeigt (z.B. der Sicherheitsvorfall bei der Xplain AG), dass diese den gleichen Sicherheitsstandard wie die Behörden selbst einhalten müssen, wenn sie Informationen oder Personendaten bearbeiten oder ICT-Leistungen erbringen. Deshalb sollten die Verträge mit Dritten klare Anforderungen an die Sicherheit und deren Überprüfung stellen. Die Verträge sollten die Pflicht beinhalten, den Schutz der Informationen, Personendaten und ICT-Mittel gemäss den kantonalen Vorschriften zu gewährleisten und sicherheitsrelevante Ereignisse zu melden. In den Verträgen sollten ebenfalls die Nachweise der Umsetzung der Sicherheitsvorgaben vorgeschrieben und insbesondere ein Audit- und Kontrollrecht der Behörde vorgesehen werden.

Hierfür erlässt die KDI mit dem Grundschutz BE auch die Allgemeinen Geschäftsbedingungen über die Informations- und Datensicherheit (AGB ISDS BE). Diese werden im Internet unter www.be.ch/agb veröffentlicht. Die Zentrale Koordinationsstelle Beschaffung (ZKB) stellt den Behörden zudem unter www.be.ch/beschaffungen seit 2015 ICT-Musterverträge zur Verfügung.

Es ist entscheidend, dass die Behörden bei der Beschaffung von Leistungen Dritter die Sicherheitsanforderungen zum Gegenstand der Ausschreibung oder Offertanfrage machen.

**Artikel 18 – Bestätigung der Informations- und Datensicherheit**

Die oberste Führung bzw. die SIVE DIR haben zu entscheiden, ob sie noch zusätzlichen Aufwand betreiben wollen, um auch diese Risiken zu reduzieren, oder ob sie bereits auf ein akzeptiertes Mass reduziert worden sind.

### 7.3.2 Management der Informations- und Datensicherheit

**Artikel 19 – Restrisiken und aktuelle Bedrohungen**

Absatz 1:

Diese Bestimmung konkretisiert die Verantwortung der Sicherheitsverantwortlichen (SIVE) für die Informations- und Datensicherheit. Sie haben zu entscheiden, ob und welche bedeutsamen Restrisiken zu akzeptieren sind.

Die Zuständigkeit für das Risikoakzept richtet sich nach der jeweiligen staatlichen Aufgabe, im Bereich der kantonalen ICT-Mittel nach dem Stufenmodell gemäss Artikel 32 DVG. Demnach ist das KAIO für das Akzept von Restrisiken im Bereich der ICT-Grundversorgung und seiner Konzernapplikationen verantwortlich. Die einzelnen Fachbehörden (Direktionen, Ämter, Justizbehörden, Grosser Rat, Aufsichtsbehörden) sind es für Restrisiken im Bereich ihrer jeweiligen Fach- und Konzernapplikationen. Alle Behörden sind zudem für das Akzept von Restrisiken verantwortlich, die sich aus der Art und Weise ergeben, in der sie ICT-Mittel nutzen, die ihnen von einer anderen Behörde zur Verfügung gestellt werden (z.B., wenn ein Amt schutzbedürftige Informationen unverschlüsselt per E-Mail verschickt).

Wie im Fall der Einführung von M365 sollen jedoch Restrisiken mit besonders grossem Umfang oder von besonderer politischer Bedeutung von der zuständigen politischen Führung beurteilt und akzeptiert werden können, oder bei Risiken im Verantwortungsbereich der DIR/STA auch vom Regierungsrat als oberster Führungsbehörde der Kantonsverwaltung. In welchen Fällen dies geschehen soll, liegt im fachlichen und politischen Ermessen der jeweiligen Behörden.

Die SIVE der DIR/STA/PARL/JUS können solche Risiken demnach ihren Vorgesetzten zum Akzeptieren wie folgt vorlegen:

a) Durch die oder den SIVE DIR oder Amt: Der Direktorin oder dem Direktor der betreffenden Direktion beziehungsweise der Staatsschreiberin oder dem Staatsschreiber,
b) Durch die oder den SIVE DIR des Grossen Rates: Dem Büro des Grossen Rates,
c) Durch die oder den SIVE DIR der Gerichtsbehörden und der Staatsanwaltschaft: Dem hierfür von ihnen bestimmten Organ.

Absatz 2: Keine Bemerkungen.

**Artikel 20 – Informationssicherheits-Managementsystem**

Absatz 1:

Ein Informationssicherheits-Managementsystem (ISMS) umfasst Verfahren und Regeln, die aufzeigen, wie die Informations- und Datensicherheit in einem System organisiert ist und macht sichtbar, welche Aufgaben, Kompetenzen und Verantwortlichkeiten entsprechenden Funktionen zugeordnet wurden. Während die KDI den Aufbau, den Betrieb, die Überprüfung und die kontinuierliche Verbesserung des kantonalen ISMS zu gewährleisten hat, obliegt der eigentliche Betrieb des ISMS der Beratungsstelle IDS unter Mitwirkung der SIBE der kantonalen Behörden. Gemäss Artikel 41 Absatz 1 muss das kantonale ISMS bis spätestens zwei Jahre nach Inkrafttreten der IDSV aufgebaut sein. Es wird von der Beratungsstelle IDS betrieben und orientiert sich an den Anforderungen des ISO/IEC 27001-Standards.

Ein ISMS bezweckt, die Informations- und Datensicherheit in der Behörde zu führen und zu verbessern. Dafür werden konkrete Ziele benötigt, anhand derer auch der Regierungsrat beurteilen

kann, ob es die gewünschte Wirkung erbringt. Diese Zielsetzung und die Messung deren Erfüllung ist Aufgabe der KDI. Sie legt die Ziele für das ISMS fest, prüft jährlich, ob diese erreicht werden und erhebt die dafür nötigen Kennzahlen.

Absatz 2: Um eine gewisse Objektivität und Vergleichbarkeit bei der Bewertung der Umsetzung und Wirksamkeit des ISMS sicherzustellen, wird eine periodische Überprüfung durch eine von der Behörde unabhängigen oder einer vorgesetzten Stelle verlangt. Diese unabhängige ISMS-Überprüfung sorgt für die kontinuierliche Verbesserung der Sicherheit und schafft gleichzeitig Vertrauen für die Partner der Behörde. Die für das ISMS verantwortliche KDI entscheidet, wie sie mit den Befunden der Überprüfung umgehen und welche Schutzmassnahmen sie umsetzen will. Der kontinuierliche Verbesserungsprozess ist für die Gewährleistung der Sicherheit zentral. Diesem wird mit solchen Überprüfungen Rechnung getragen. Die Periodizität von drei Jahren richtet sich zwar nach dem offiziellen Zertifizierungszyklus der ISO-Norm (ISO/IEC 27001), der Umfang der vorgeschriebenen Überprüfung ist jedoch weniger ambitiös als im ISO-Standard: Verlangt wird nicht zwangsläufig ein formelles Audit im Sinne der ISO-Norm. Je nach Auftrag können das gesamte ISMS oder nur bestimmte Teile davon überprüft werden. Die KDI entscheidet über die Wahl einer unabhängigen Prüfstelle. Solche Prüfungen können durch die Finanzkontrolle, die kantonale Datenschutzbehörde oder durch Dritte durchgeführt werden.

**Artikel 21 – Inventar der Schutzobjekte**

Absatz 1:

Das hier geregelte Inventar enthält eine Auflistung sämtlicher Schutzobjekte (Art. 3 Bst. b IDSV), also der Informationen, Personendaten und ICT-Mittel zu einem bestimmten Zeitpunkt. Für die Erfassungsarbeiten sind allenfalls bestehende Konzernapplikationen zu verwenden.

Bereits heute besteht für die Kantonsverwaltung das sog. IT-Servicemanagement-System (ITSMS), wo sämtliche Applikationen erfasst und u.a. auch eingestuft sind; so zum Beispiel auch die Applikation der BVD BExpert (Link auf das ITSMS, Zugriff nur für Mitarbeitende mit ICT-Rollen der Kantonsverwaltung). Diese Applikation wurde im ITSMS dem Grundschutz bzw. dem Schutzniveau 0 zugeordnet. Die ICT-Mittel sind alle nach Artikel 33 IDSV einzustufen.

Demgegenüber bildet das Inventar der Sammlungen von Personendaten – in fast allen Fällen ICT-Mittel – die Grundlage für die Meldung von Datensammlungen zuhanden des Registers nach Artikel 21 KDSG. Das Inventar enthält auch die Personendatensammlungen, die nach Artikel 21 Abs. 4 KDSG von der Meldepflicht ausgenommen sind, da sich Auskunftsgesuche nach Artikel 29 KDSG auch auf nicht registrierte Datensammlungen erstrecken.

Absatz 2: Keine Bemerkungen

Absatz 3:

Die KDI regelt, welche Angaben im Inventar zu führen sind, wie beispielsweise:

a) Der Schutzbedarf der Schutzobjekte.
b) Die für die Schutzobjekte verantwortliche kantonale Behörde und die bei ihr dafür zuständige Person oder Funktion.
c) Die Beteiligung von beauftragten Dritten.
   Die Übersicht über vertragliche Bindungen zu Dritten, beispielsweise zu Informatiklieferanten, dient einerseits dem funktionierenden Lieferantenmanagement und ermöglicht es, eventuelle

Abhängigkeiten von Lieferanten frühzeitig zu erkennen inkl. Beurteilung der Gefahr von Klumpenrisiken. Sie ermöglicht andererseits die Identifizierung von Risiken, die über diese Lieferanten Auswirkungen auf die Behörde haben können.

d) Die Zuordnung zum Schutzniveau.
e) Die Umsetzung der Schutzmassnahmen gemäss Schutzniveau.
   Sie muss nicht zwingend im Inventar selbst dokumentiert werden. Es muss aber zumindest festgehalten werden, wo die Sicherheitsdokumentation zu finden ist und wer dafür zuständig ist,
f) Die periodischen Kontrollen und Audits.
g) Das Datum der letzten Aktualisierung des Inventars.

**Artikel 22 – Schutzmassnahmen bei Nutzung von Schutzobjekten durch Dritte**

Absatz 1: Damit werden diejenigen Fälle geregelt, in denen kantonale Schutzobjekte von Dritten zu deren eigenen rechtmässigen Zwecken verwendet werden (in Abgrenzung zur vertraglich zu regelnden Sicherheit bei Auftragsdatenbearbeitungen zu Zwecken der kantonalen Behörden). Die kantonale Behörde entscheidet je nachdem über die geeignete Regelungsform (Weisung, Verfügung, öffentlich-rechtlicher oder privatrechtlicher Vertrag). Allfällige öffentlich-rechtliche Verträge stützen sich, sofern dafür keine fachgesetzliche Grundlage besteht, auf Art. 25 DVG. Sie können z.B. als Nutzungsbestimmungen kantonaler ICT-Mittel ausgestaltet werden, deren Akzept eine Voraussetzung der Nutzung ist. Die Regelung kann, soweit risikoangemessen, auch Vorschriften zur Kontrolle der Umsetzung der Massnahmen sowie Sanktionen bei der Unterlassung beinhalten, z.B. Sperrung des Zugangs oder Konventionalstrafen.

Absatz 2: Weil der Kanton mit dem ICSG eine dem ISG gleichwertige Informationssicherheit beim Umgang mit Schutzobjekten des Bundes gewährleisten will, ist es erforderlich, auch den Bundesbehörden die Möglichkeit zu geben, entsprechende Vorschriften für ihre Schutzobjekte zu erlassen, soweit sich diese Regelungskompetenz nicht bereits aus dem Bundesrecht ergibt. Der Kanton kann dies den Bundesbehörden jedoch nicht vorschreiben. Verzichten sie auf schutzobjektspezifische Vorschriften, kann sich aus Artikel 3 ISG für Dritte, welche Schutzobjekte des Bundes einsetzen, die Pflicht ergeben, direkt das ISG und seine Ausführungsbestimmungen umzusetzen. In diesem Sinne hat Absatz 2 rein deklaratorischen Charakter.

**Artikel 23 – Ausnahmen von den Vorschriften**

Die Bestimmung konkretisiert das Prinzip, dass sich Schutzmassnahmen an der jeweiligen Risikosituation orientieren, und dass die oder der für das jeweilige Schutzobjekt verantwortliche SIVE darüber entscheidet, welche Risiken akzeptiert werden. Auch dort, wo bestimmte Schutzmassnahmen durch Erlass oder Weisung vorgeschrieben sind (z.B. im Grundschutz BE), kann die risikoverantwortliche Führungsperson im Einzelfall davon abweichen, wenn sie zum - dokumentierten und begründeten - Schluss gelangt, dass die Kosten der Schutzmassnahme oder ihre anderen Nachteile für die behördliche Aufgabenerfüllung die mit der Massnahme bezweckte Risikoreduktion im Einzelfall überwiegen und das Restrisiko akzeptiert wird.

Solche Ausnahmen von Sicherheitsvorschriften sind zu befristen, um eine regelmässige Überprüfung zu erzwingen, und samt Begründung in einer von der Beratungsstelle IDS zur Verfügung gestellten Konzernapplikation zu dokumentieren.

Die Kompetenz zur Genehmigung der Ausnahme liegt grundsätzlich bei der oder dem SIBE KDI, weil sich Ausnahmen auf Schutzobjekte mehrerer Behörden auswirken können. Als Beispiel: Entscheidet eine Behörde, eine Zugriffsschutzmassnahme für ihre Fachapplikation zu lockern, kann dies das Risiko erhöhen, dass Angriffe über das kantonale Netzwerk auf andere Behörden einfacher werden. Dies setzt eine Risikobeurteilung auf übergeordneter Ebene voraus. Soweit sich eine

Massnahme aber tatsächlich nur auf die Schutzobjekte einer Behörde auswirkt, kann die oder der SIBE KDI den Entscheid der oder dem risikoverantwortlichen SIVE überlassen.

**Artikel 24 – Unterstützung bei Sicherheitsvorfällen**

Der Grosse Rat und die SAK haben dem ICSG in Kenntnis des möglichen Mehraufwands für die anderen Behörden, insbesondere die Gemeinden, zugestimmt. Sie haben der Kantonsverwaltung aber die Auflage gemacht, Ausbildungsmöglichkeiten anzubieten (Art. 19 Abs. 2 ICSG). Diese haben grundsätzlich gegen Entgelt zu erfolgen. Die direkte Beratung und Unterstützung der übrigen Behörden im Ereignisfall ist aufgrund dieses Artikels ausgeschlossen.

Die Beratungsstelle IDS bietet daher aus Ressourcengründen nur den kantonalen Behörden ihre direkte Unterstützung an. Sollten ihre eigenen Ressourcen hierfür nicht ausreichen, so wird sie dazu die Leistungen aus den verschiedene Rahmenverträgen beanspruchen. Dies setzt jedoch voraus, dass die um Unterstützung ersuchte kantonale Behörde hierfür die Kostengutsprache erteilt hat.

Die betroffene kantonale Behörde gelangt bei einem Sicherheitsvorfall gemäss dem bereits heute definierten sog. Major-Security-Incident-Prozess (Link auf Adonis, nur kantonsinterner Zugriff), der für solche direktionsübergreifende Sicherheitsvorfälle vorgesehen ist und die heutige Rolle IT-SIBE (zukünftig SIBE KDI) als führende Funktion bezeichnet.

Auch die anderen Behörden können zu günstigen Konditionen bei qualifizierten Dienstleistern Einzelverträge auf eigene Kosten abrufen können. Die Informationen dazu sind auf der Internetseite der Zentralen Beschaffungsstelle ICT des KAIO (www.be.ch/zbsict) verfügbar.

**Artikel 25 – Kontrollen und Audits**

Mit Kontrollen und Audits können die Behörden feststellen, ob die Sicherheitsvorschriften eingehalten werden, ob die ergriffenen Schutzmassnahmen wirken und welche Korrekturmassnahmen erforderlich sind. Daher schreibt Artikel 5 Absatz 1 Buchstabe d ICSG vor, dass die Informationssicherheit regelmässig überprüft wird. Mit dem Verweis von Artikel 10 Absatz 2 KDSG auf das ICSG gilt das ebenso für die Personendaten.

Dieser Artikel verlangt deshalb, dass die kantonalen Behörden jährlich festlegen, welche risikobasierten Kontrollen und Audits sie im nächsten Jahr durchführen werden und aus welchem Grund. Der Auditplan und die dafür nötigen Ressourcen werden durch die SIVE DIR der betreffenden Behörde genehmigt. Daraus ergibt sich nicht eine Pflicht, eine bestimmte Anzahl Kontrollen und Audits jährlich durchzuführen; dieser Entscheid obliegt den SIVE DIR auf der Basis ihrer Risikobeurteilung.

Da auch die Finanzkontrolle und die Datenschutzbehörde die Informations- und Datensicherheit periodisch überprüfen, sollen sich die SIVE DIR mit der Beratungsstelle IDS absprechen. Denn diese erhebt in Zusammenarbeit mit der kantonalen Datenschutzbehörde sowie der Finanzkontrolle den Kontroll- und Auditbedarf, tauscht sich jährlich mit ihnen aus und kennt deren Auditplanung. Zudem kann auch die Beratungsstelle IDS selbst Audits durchführen. So wird gewährleistet, dass die Audits risikobasiert, effektiv und effizient stattfinden. Die auditierten Behörden und ihre Beauftragten sollen damit vor unkoordinierten, wiederholten Kontrollen gleichen Inhalts geschützt werden.

**Artikel 26 – Berichterstattung**

Absätze 1 bis 3:

Um eine nachhaltige Verbesserung der Informations- und Datensicherheit bewirken zu können, sind eine kontinuierliche kritische Überprüfung ihrer Wirksamkeit sowie eine stete Anpassung der Schutzmassnahmen notwendig. Dazu wird ein jährlicher Bericht über den Zustand der Informations- und Datensicherheit vorgeschrieben, welcher von der KDI, für die Steuerung der Sicherheit zuständig, beurteilt wird. Die SIVE DIR liefern zusammen mit ihren SIBE die nötigen Angaben der oder dem SIBE KDI. Die oder der SIBE KDI legt den Bericht der KDI vor.

Der Bericht umfasst insbesondere:

a) den Stand und die Wirksamkeit des ISMS der kantonalen Behörden,
b) den Stand der Umsetzung der Schutzmassnahmen,
c) die Übernahme besonders bedeutsamer Restrisiken durch die SIVE DIR oder den Regierungsrat,
d) die durchgeführten Sensibilisierungsmassnahmen,
e) die Erkenntnisse aus Sicherheitsvorfällen und Sicherheitslücken,
f) die Erkenntnisse aus den Kontrollen und Audits, und
g) die getroffenen und beantragten Verbesserungsmassnahmen.

Absatz 4:

Der Bericht beinhaltet sicherheitsempfindliche und daher als VERTRAULICH zu klassifizierende Informationen. Es muss eindeutig und ohne abweichende Risikobeurteilung auf Stufe Verordnung klargestellt werden, dass der Bericht von der KDI nur einem kleinen, klar definierten Kreis von Adressatinnen und Adressaten bekanntgegeben werden darf. Es sind dies höchstens:

a) der Regierungsrat,
b) die SIVE DIR im Umfang ihrer Betroffenheit,
c) die kantonale Datenschutzbehörde,
d) die Finanzkontrolle,
e) die Fachstelle des Bundes für Informationssicherheit nach Artikel 83 ISG.

### 7.3.3 Klassifizierung von Informationen

Die Klassifizierung ist zwingend, sofern die entsprechenden Kriterien nach den Artikeln 27 ff. IDSV erfüllt sind. Das «Need-to-know-Prinzip» nach Artikel 9 Absatz 1 Buchstabe b ICSG ist einzuhalten. Wie in Ziffer 3.5, Wirkungsziele, oben beschrieben, sollen das ICSG und die IDSV aber auch dazu führen, dass künftig weniger und nur noch nach klaren Kriterien klassifiziert wird. Die Beschränkung soll sowohl in der Menge als auch in der Zeit erfolgen.

Personendaten nach dem KDSG oder Geschäfts-, Fabrikations- oder Berufsgeheimnisse werden grundsätzlich nicht klassifiziert, es sei denn, dass einzelne Informationen zum Schutz des öffentlichen Interesses nach Artikel 1 Absatz 2 Buchstaben a und b ICSG 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 ICSG nicht klassifiziert werden müssen. Hingegen können die besonderen Massnahmen, die zum Schutz solcher Informationen getroffen werden, klassifiziert werden (zum Beispiel ein ISDS-Konzept; s. dazu auch den Vortrag zum ICSG vom 16. August 2023 zu Art. 8 Abs. 1). Ebenso schützt die Einstufung der ICT-Mittel nach Artikel 33 IDSV die Personendaten.

**Artikel 27 – Klassifizierungskataloge**

Absatz 1: Die SIVE DIR sind die obersten Führungspersonen, die in ihrem Zuständigkeitsbereich am besten beurteilen können, für welche Arten von Informationen regelmässig ein Schutzinteresse besteht. Mit Absatz 1 werden sie beauftragt, in einem Klassifizierungskatalog diese Informationen für ihren Zuständigkeitsbereich möglichst umfassend aufzuführen. Dazu gehört auch die voraussichtliche Dauer der Klassifizierung. Da diese zu klassifizierenden Informationen bei der Aufgabenerfüllung regelmässig bearbeitet werden, kann grösstenteils im Voraus festgelegt werden, bis wann sie auf welcher Stufe klassifiziert sein sollen. Die IDSV gibt keine minimale oder maximale Frist vor.

Absatz 2: Mit dieser Überprüfung soll sichergestellt werden, dass bei der Erstellung der Klassifizierungskataloge die gesetzlichen Kriterien für die Klassifizierung der kantonalen Behörden nach vergleichbaren Massstäben angewendet werden. Der abschliessende Entscheid bleibt bei den SIVE DIR.

Absatz 3: Bestimmte Arten von Informationen werden in allen oder den meisten Behörden bearbeitet (z.B. Informationen über Informatikmittel, Regierungsratsgeschäfte oder Sicherheitszonen nach Art. 18 ICSG), und ihre Klassifizierung ist daher verwaltungsweit einheitlich zu regeln. Diesen allgemeinen Klassifizierungskatalog wird der SIBE KDI zusammen mit den SIBE DIR erarbeiten und der KDI zum Beschluss vorlegen. Darin ist festzulegen, wie die Informationen zu klassifizieren sind und wie lang die Klassifizierung dauern soll.

Die Beratungsstelle IDS wird Vorlagen für Klassifizierungskataloge erarbeiten.

**Artikel 28 – Klassifizierende und Ausführungsweisungen**

Absatz 1 und 2:

Die Klassifizierungskataloge sind für die Mitarbeitenden verbindlich. Sie müssen die darin enthaltenen Informationen entsprechend klassifizieren, indem sie den Klassifizierungsvermerk anbringen. Die Klassifizierungskataloge enthalten aber keine abschliessenden Aufzählungen. Die Mitarbeitenden können daher in die Situation geraten, dass sie zwar eine Information als schutzwürdig beurteilen, diese im Katalog aber nicht finden. Ihnen obliegt in diesem Fall die Pflicht, die fragliche Angabe entweder im Klassifizierungskatalog neu aufnehmen zu lassen oder direkt anhand der Klassifizierungskriterien nach den Artikeln 29 ff. IDSV zu klassifizieren. Die gleiche Pflicht trifft die Organe der auftraggebenden Behörden, wenn sie Dritte mit der Bearbeitung schutzwürdiger Informationen oder Personendaten betrauen.

Um sicherzustellen, dass die mit einem Schutzobjekt befassten Personen dessen Schutzwürdigkeit rasch erkennen und entsprechend behandeln, ist auf Unterlagen und anderen Informationsträgern mit klassifizierten Informationen ein Klassifizierungsvermerk in Grossbuchstaben anzubringen: «INTERN», «VERTRAULICH» oder «GEHEIM»; beim mündlichen Austausch von Informationen ist die allfällige Klassifizierung zu erwähnen.

Absatz 3:

Bisher lag der Erlass von Bearbeitungsvorschriften in der Verantwortung der STA, welche u.a. auch Artikel 8 KRGV, Bearbeitungsvorschriften, vorbereitet hat. Neu soll diese Kompetenz bei der KDI liegen, wo die STA ebenfalls vertreten ist. Der oder die SIBE KDI wird bei der Vorbereitung der Bearbeitungsvorschriften die insbesondere STA einbeziehen. Diese Lösung lehnt sich an die einheitlichen Bearbeitungsvorschriften des Bundes an, welche nicht nur den Umgang mit klassifizierten Informationen beschreibt, sondern auch deren Kennzeichnung mit dem Klassifikationsvermerk,

auch im Falle der Entklassifizierung. Das integrale Regeln dieser Aufgaben durch zwei verschiedene Behörden würde die Umsetzung durch die Mitarbeitenden und damit die Wirkung der Klassifizierung eindeutig erschweren, was wiederum der Anerkennung der Gleichwertigkeit durch den Bund abträglich wäre.

**Artikel 29 – Klassifizierung «INTERN»**

Die Klassifizierungsregeln orientieren sich generell an den öffentlichen Interessen nach Artikel 1 Absatz 2 Buchstaben a und b ICSG und im Konkreten an denjenigen des Bundes, jedoch übertragen auf die Aufgaben und die Risikolage des Kantons.

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, die Beeinträchtigung der öffentlichen Interessen muss vielmehr spürbar sein. Wenn es um sicherheitsrelevante Informationen im Sinne der öffentlichen Ordnung und Sicherheit geht (Art. 1 Abs. 2 Bst. b ICSG), 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.

In diesem Zusammenhang ist daran zu erinnern, dass die Klassifizierung nicht entscheidend ist für die Frage, ob Informationen im Rahmen des Öffentlichkeitsprinzips auf Anfrage herausgegeben werden müssen oder nicht (Art. 27 ff. des Gesetzes vom 2. November 1993 über die Information und die Medienförderung [IMG][28]). Denn das IMG geht dem ICSG vor (Art. 3 Abs. 1 ICSG). Auch bei klassifizierten Unterlagen ist daher eine Interessenabwägung nach Art. 27 ff. IMG erforderlich. Die Klassifizierung dient aber immerhin als Indiz dafür, dass wesentliche öffentliche Interessen gegen eine Bekanntgabe sprechen.

**Artikel 30 – Klassifizierung «VERTRAULICH»**

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

**Artikel 31 – Klassifizierung «GEHEIM»**

Als «GEHEIM» werden die seltenen Informationen klassifiziert, deren Bekanntwerden zu einem besonders grossen, katastrophalen Schaden für Behörden oder Personen führen kann. Grundsätzlich soll diese Klassifizierung nur in Ausnahmefällen vorgenommen werden. Denn einerseits gibt es wenige Informationen, deren Bekanntwerden ein derartiges Schadensausmass verursachen können. Und andererseits führt die Bearbeitung solcher Informationen zu aufwändigen Schutzmassnahmen.

Nach den aktuellen Bearbeitungsvorschriften des Bundes im Anhang seiner Verordnung über den Schutz von Informationen des Bundes (Informationsschutzverordnung, ISchV)[29] dürfen solche Informationen nur auf besonders geschützten ICT-Mitteln bearbeitet werden, die Datenträger sind zu nummerieren und zu registrieren, die elektronische Übermittlung muss mit starker Verschlüsselung und nachverfolgbar erfolgen, die mündliche Übermittlung darf nur in abhörsicheren Bereichen erfolgen, die physische Übergabe darf nur persönlich oder nur mit Spezialkurier gegen Quittung erfolgen etc..

[28] IMG, BSG 107.1
[29] ISchV, SR 510.411

**Artikel 32 – Entklassifizierung und Entfallen der Klassifizierung**

Absatz 1 und 2:

Das erklärte Ziel des ICSG und der IDSV ist, die Menge der klassifizierten Informationen deutlich zu reduzieren (s. Ziff. 3.5). Hierfür sind diejenigen kantonalen Behörden verantwortlich, welche die Informationen zu schützen und zu klassifizieren haben. Ihnen bzw. ihren Mitarbeitenden obliegt es, sowohl ihren Klassifizierungskatalog als auch klassifizierte Informationen auf ihren Schutzbedarf zu überprüfen und die Klassifizierung bei Wegfall ihrer Voraussetzungen anzupassen oder die Informationen gänzlich zu entklassifizieren (s. auch Art. 28 Abs. 1 IDSV).

Damit ist keine Verpflichtung zur ständigen oder regelmässigen Überprüfung der Klassifizierung verbunden, sondern dies ist nur nötig, wenn dafür ein besonderer Anlass besteht, wie etwa beim Abschluss eines Geschäfts oder bei einem Zugangsbegehren zu behördlichen Informationen (Gesuche bzw. formlose Anfragen um Zugang zu Informationen nach Art. 27 ff. IMG). Hierfür ist ausschliesslich diejenige Behörde zuständig, welche den Schutzbedarf der Information beurteilt und gestützt darauf die Klassifizierung vorgenommen hat.

Befristete Klassifizierungen (z.B. «VERTRAULICH bis 1.1.2030») fallen mit dem Ablauf der Frist dahin, ohne dass eine Aktualisierung des Klassifizierungsvermerks oder ein weiteres Handeln der Behörde nötig wäre.

Absatz 3:

Wie bereits Artikel 9 Absatz 2 ICSG festhält, richtet sich der Zugang zu klassifiziertem Archivgut nach den Bestimmungen der Archivierungsgesetzgebung. Dabei sind insbesondere die ordentlichen und besonderen Schutzfristen zu beachten (siehe Art. 17 und Art. 18 des Archivierungsgesetztes vom 31. März 2009 [ArchG][30]). Der Gesetzgeber hat mit den archivrechtlichen Schutzfristen dem im Laufe der Zeit schwindenden Interessen an der Geheimhaltung Rechnung getragen und im Sinn einer vorweggenommen Interessenabwägung festgelegt, dass entsprechende Geheimhaltungsinteressen nach Ablauf der Schutzfrist das Einsichtsinteresse nicht mehr überwiegen (Vortrag des Regierungsrates an den Grossen Rat zum Gesetz über die Archivierung, in Tagblatt des Grossen Rates 2009, Beilage Nr. 14, S. 5).

Während laufender Schutzfrist ist eine allfällige Klassifizierung als Element der Interessenabwägung nach Artikel 27 ff. IMG zu berücksichtigen (Erläuterungen im Vortrag vom 16. August 2023 zu Art. 3 ICSG), die aufgrund der Verweisung in Artikel 16 Absatz 1 ArchG nach IMG vorzunehmen ist. Ist eine Schutzfrist abgelaufen, hat dies aus archivrechtlicher Sicht zur Folge, dass allfällige Geheimhaltungsinteressen einer Einsichtnahme nicht mehr entgegenstehen.

Artikel 32 IDSV übersetzt diese Grundsätze auf die Klassifizierung und stellt klar, dass diese mit Ablauf der archivrechtlichen Schutzfristen automatisch entfällt, wodurch die Informationen frei zugänglich werden.

### 7.3.4 Einstufung von ICT-Mitteln

**Artikel 33 – «Grundschutz», «Hoher Schutz» und «Sehr hoher Schutz»**

Absatz 1:

[30] ArchG, BSG 108.1

Massgebend für die Einstufung sind die öffentlichen Interessen des Kantons nach Artikel 1 Absatz 2 Buchstaben a bis c ICSG. Die materiellen Kriterien zur Einstufung von Informationen und Personendaten gelten grundsätzlich auch für die Einstufung von ICT-Mitteln. Im Gegensatz zu den Einstufungskriterien für klassifizierte Informationen ist im Rahmen der Einstufung der ICT-Mittel auch auf finanzielle Kriterien abzustellen. Eine Verletzung der Verfügbarkeit oder Integrität von Informationen, die mit ICT-Mitteln bearbeitet werden, ist einfacher quantifizierbar als beispielsweise eine Verletzung der Vertraulichkeit eines Dokumentes mit klassifizierten Informationen.

Buchstabe b Ziffer 4:

Artikel 30 Absatz 1 Buchstabe d IDSV schützt vor allem die öffentlichen Interessen nach Artikel 1 Absatz 2 Buchstabe b ICSG, also die öffentliche Ordnung und Sicherheit. Demgegenüber schützt Artikel 33 Absatz 1 Buchstabe b Ziffer 4 IDSV z.B. die Personendaten eines verdeckten Ermittlers oder von Kindern, deren vom getrennten Ehepartner eine Entführung droht, also vor allem die individuellen Interessen von Personen.

Absatz 2:

Die Behörden haben auch bei jeder Veränderung eines ICT-Mittels zu prüfen, ob sich dessen Schutzbedarf verändert hat. Ist dies der Fall, ist die Schutzbedarfsanalyse und allenfalls das ISDS-Konzept anzupassen. Aber auch mit einer neuen oder wiederkehrenden Bedrohung kann eine bereits vorliegende Schutzbedarfsanalyse ganz oder teilweise in Frage gestellt werden, was dann wiederum zu einer Anpassung des ISDS-Konzepts führen kann.

Aus diesen Gründen sind die eingestuften ICT-Mittel spätestens nach zwei Jahren wieder einem Sicherheitsverfahren zu unterziehen. Im Gegensatz zum Bund verzichtet der Regierungsrat aber darauf, dem Grundschutz zugeordnete ICT-Mittel zwingend periodisch dem Sicherheitsverfahren zu unterziehen; das hier vorhandene Risiko rechtfertigt den Aufwand nicht, der allein bei den Hunderten, mit dem Grundschutz versehenen Fachapplikationen erforderlich wäre. Die Kantonsverwaltung verfügt insgesamt über mehr als 1’400 Applikationen. Davon weisen rund 700 oder 50% die Schutzniveaus 0 und 1, wurden also dem Grundschutz zugeordnet (ITSMS, Stand Juli 2026).

### 7.3.5 Zu prüfende Personen

Die Prüfung der Personensicherheit ist infolge ihres Eingriffs in die Persönlichkeitsrechte der Betroffenen bereits auf Stufe Gesetz in den Artikeln 19 ff. ICSG ausführlich geregelt. Aus diesem Grund wird auch auf die entsprechenden Stellen im Vortrag zum ICSG, Ziff. 8.6.2, verwiesen. In der IDSV werden nur noch die nachstehenden Aspekte des Vollzugs geregelt.

**Artikel 34**

Nach Artikel 23 ICSG soll der Entscheid, ob und wie welche Person geprüft wird, nicht Sache der individuellen Risikobeurteilung der verantwortlichen Behörde sein, sondern sich aus einer Liste ergeben, welche die zu prüfenden Funktionen aufführt.

Absatz 1: Der Regierungsrat soll bestimmen, für welche von ihm ernannten Personen welche Personensicherheitsprüfung (PSP) nötig ist, getreu dem Grundsatz, wonach die Informations- und Datensicherheit Chefsache ist. Die Finanzdirektion wird den Beschluss nach Konsultation der KDI sowie der Konferenz der Generalsekretärinnen und -sekretäre (GSK) vorbereiten. Die KDI ist das Fachorgan der Verwaltung für die Informations- und Datensicherheitsrisiken, die GSK dasjenige der obersten Verwaltungsführung; beide Kompetenzen sind massgebend für die Erstellung der Liste mit den obersten Führungsfunktionen, die eine PSP voraussetzen.

Absatz 2: Analoge Überlegungen liegen auch dem Entscheid zu Grunde, dass die GSK bestimmen soll, welche subalternen Führungs- und Mitarbeiterfunktionen eine PSP zu bestehen haben. Die KDI als oberstes ICT-Organ soll dabei mitbestimmen, welche ICT-Funktionen dazugehören.

Absatz 3: Bei Funktionen, deren Verantwortung und Risiken eine PSP voraussetzen, handelt es sich um Schlüsselpositionen, welche deshalb zum Ziel von Cyber- oder anderen Angriffen werden könnten. Damit sind nicht nur die betroffenen Personen, sondern auch wichtige Interessen des Kantons Bern potenziell gefährdet. Aus diesem Grund ist die Liste nicht öffentlich.

## 7.4 Sicherheitsorganisation

Mit der DVV hat der Regierungsrat Organe eingerichtet, welche die Steuerung und Führung der Digitalisierung und der ICT sowohl teilweise kantonsweit - einschliesslich der Belange der Gemeinden und der autonomen Träger öffentlicher Aufgaben - als auch innerhalb der Kantonsverwaltung sicherstellen. Weil sich Informations- und Datensicherheitsfragen primär im Zusammenhang mit ICT-Systemen und Digitalisierungsvorhaben stellen, ermächtigt Artikel 31 Absatz 2 ICSG den Regierungsrat, die gesamtkantonalen Sicherheitsbelange sowie die Sicherheitsorgane der kantonalen Verwaltung den Organen gemäss DVG und DVV zu übertragen, statt für die Informations- und Datensicherheit eine separate Organisation aufzubauen, wie es z.B. der Bund tat. Dies vereinfacht es, die Sicherheit als integralen Teil der Digitalisierung der öffentlichen Verwaltung zu berücksichtigen. Auf die Schaffung neuer, teurer Fachgremien kann deshalb verzichtet werden.

Die anderen Behörden – insbesondere die Einwohner-, Kirch- und Burgergemeinden – haben eine eigene, den Verhältnissen und Risiken angepasste Sicherheitsorganisation vorzusehen. Sie haben mindestens eine für die Informations- und Datensicherheit zuständige und hinreichend ausgebildete Person zu bezeichnen und diese mit angemessenen Kompetenzen und Ressourcen auszustatten (Art. 32 ICSG).

Die Sicherheitsorganisation besteht aus den nachfolgenden Organen (vgl. auch die Grafik in Ziff. 3.4).

**Artikel 35 – Konferenz digitale Verwaltung und ICT**

Absatz 1:

Auf gesamtstaatlicher Ebene steuern und führen die KDI sowie ihre Fachgruppe Informations- und Datensicherheit (Fachgruppe IDS) die Informationssicherheitstätigkeiten der Verwaltung. Sie erlassen namentlich Sicherheitsgrundlagen wie Weisungen oder Vollzugshilfen.

Die KDI erlässt insbesondere auch zu den nachfolgenden Bereichen konkretisierende Weisungen:

a) Grundschutz BE,
b) Ziele für das ISMS,
c) Management der Informations- und Datensicherheit,
d) Schutzniveaus und -massnahmen für Schutzobjekte,
e) Einstufung von Schutzobjekten durch kantonale Behörden,
f) Umgang mit eingestuften Schutzobjekten,
g) Technische Massnahmen,
h) Physische Massnahmen,
i) Prüfung der Identitäten von Personen und Systemen,
j) Identitäts- und Berechtigungsmanagement-Systems (Identity- and Access- Management-System, IAM-System).

Unterstützt wird die KDI dabei von der oder dem SIBE KDI, die oder der auch die Beratungsstelle IDS und den Fachbereich Sicherheit im KAIO leitet. Sie oder er ist neu Mitglied der KDI (s. dazu die indirekte Änderung von Artikel 18 Abs. 1 DVV).

Absatz 2:

Die KDI führt in Zusammenarbeit mit der kantonalen Datenschutzbehörde eine periodisch aktualisierte Liste der neuen Technologien nach Artikel 18 Absatz 2 KDSG, die für die damit bearbeiteten Personendaten hohen Risiken verursachen und deshalb nach Artikel 20 Absatz 1 Buchstabe b KDSG eine Vorabkontrolle nötig machen können. Diese Liste fand sich bisher in der DSV. In der Praxis zeigte sich allerdings, dass die Liste aufgrund der technischen Entwicklung rasch veraltet und z.B. neue, risikoreiche Technologien nicht aufführt. Dieses Vollzugshilfsmittel wird daher neu auf Verwaltungsebene geführt.

Absatz 3: Keine Bemerkungen.

Absatz 4:

Es ist vorgesehen, z.B. die technischen Anhänge der Weisung über den Grundschutz BE an die Fachgruppe IDS zu delegieren (Art. 31 Abs. 2 ICSG).

**Artikel 36 – Sicherheitsverantwortliche**

Absatz 1:

Auf der obersten Organisationsebene der kantonalen Behörden (in den DIR/STA/JUS, im Grossen Rat und in den Aufsichtsbehörden, hier zusammengefasst «Stufe Direktion») trägt die oberste Führungsperson, die nicht vom Volk gewählt wird, als Sicherheitsverantwortliche/-r der Stufe Direktion (SIVE DIR) die Verantwortung für die Informations- und Datensicherheit. Dies sind die Generalsekretärinnen und Generalsekretäre, die Staatsschreiberin oder der Staatsschreiber sowie die Vorsteherinnen und Vorsteher der Aufsichtsbehörden. Zudem übernimmt die Vorsteherin oder der Vorsteher des KAIO die Aufgaben der oder des SIVE DIR für die ICT-Grundversorgung und die Konzernapplikationen des KAIO, weil das KAIO in der ICT-Organisation der Kantonsverwaltung einer Direktion gleichgestellt ist.

Behörden, welche nicht der kantonalen Verwaltung angehören, geben sich gemäss Art. 32 ICSG eine angemessene Sicherheitsorganisation. Die Gerichtsbehörden und die Staatsanwaltschaft zählen zu Letzteren. Weil die SIVE DIR Aufgaben der gesamtkantonalen Sicherheitsorganisation wahrnehmen, u.a. als Ansprechpartner der oder des SIBE KDI, und weil die Justiz gemäss DVG die kantonale ICT nutzt, ist es zur Umsetzung von Artikel 31 ICSG nötig, festzuhalten, dass die Justiz diese Rolle mit einer Führungsperson besetzt, welche in der Lage ist, die damit verbundene Verantwortung zu tragen. Im Übrigen gibt sich die Justiz eine eigene Sicherheitsorganisation.

Absatz 2:

In den Ämtern der DIR/STA tragen die Amtsvorsteherinnen und -vorsteher die Verantwortung für die Informations- und Datensicherheit in ihrem Amt als Sicherheitsverantwortliche/-r der Stufe Amt (SIVE Amt). Für die Justizbehörden und die Staatsanwaltschaft ist es aufgrund der Selbstorganisation der Justiz an der Justizverwaltungsleitung, zu entscheiden, ob z.B. für die Staatsanwaltschaft oder einzelne Gerichte ebenfalls SIVE Amt bestimmt werden. Die Abgrenzung der Verantwortung zwischen den SIVE DIR und SIVE Amt ergibt sich aus der hierarchischen Unterstellung der Ämter unter die Direktion, womit die Sicherheitsverantwortung ein Teil der Dienstaufsicht der Direktion ist.

Der SIVE DIR ist demnach für die Sicherheit der Ämter mitverantwortlich, zusammen mit den SIVE Amt. Ausgenommen ist das KAIO, dessen Leitung die Rolle SIVE DIR hat.

Absatz 3:

Die in Absatz 1 und 2 erwähnten Führungspersonen können die Sicherheitsverantwortung und die damit verbundenen Aufgaben und Kompetenzen einer ihnen direkt unterstellten Funktion übertragen. Dies kann z.B. sinnvoll sein, wenn die betreffende Person über ein besonderes Fachwissen im Bereich der Informationssicherheit oder der ICT verfügt.

Absatz 4:

Den SIVE kommt generell die Gewährleistung der Informations- und Datensicherheit in ihrem Verantwortungsbereich zu. Dies ist Teil ihrer obersten Führungsaufgabe und kann nur im beschriebenen Umfang delegiert werden. Ihnen obliegen sowohl Sicherheits- als auch Führungsaufgaben:

Buchstabe a:

Die SIVE treffen alle Entscheide, welche die Informations- und Datensicherheit in ihrem Zuständigkeitsbereich massgeblich beeinflussen, insbesondere betreffend Organisation, Prozesse, Risikoakzeptanz und Sicherheitsziele.

a) Sie veranlassen die erforderlichen Schutzmassnahmen insbesondere zur Schulung und Sensibilisierung.
b) Sie genehmigen auf Antrag ihrer SIBE sowie in Absprache mit der Beratungsstelle IDS den jährlichen Kontroll- und Auditplan (Art. 25 Abs. 1 IDSV).
c) Sie stellen den Aufbau, den Betrieb, die Überprüfung und die kontinuierliche Verbesserung des ISMS in ihrem Zuständigkeitsbereich sicher.

Buchstabe b:

Da hohe Kader wie die SIVE in der Regel über kein spezifisches Fachwissen über die Informations- und Datensicherheit verfügen, werden ihnen Sicherheitsbeauftragte (SIBE) zur Seite gestellt. Deren Auswahl, Führung und Ausstattung mit den nötigen Ressourcen obliegt den SIVE. Bei der Auswahl ist sicherzustellen, dass die SIBE die nötigen Qualifikationen erfüllen, analog zu den Behörden nach Artikel 32 Absatz 2 ICSG.

**Artikel 37 – Sicherheitsbeauftragte**

Die oder der SIBE stellt als Fachperson die operativen Sicherheitsaufgaben der jeweiligen Behörde sicher und unterstützt die oder den SIVE. Die SIBE gewährleisten die Expertise über die Informations- und Datensicherheit ihrer Organisationseinheit. Insbesondere auf Stufe SIBE DIR erfordert diese Aufgabe die folgenden Qualifikationen:

a) Eidg. Berufsbildungs- oder Hochschuldiplom in der Informations- und Datensicherheit,
b) Berufserfahrung in der Informations- und Datensicherheit, im Datenschutz oder im Risikomanagement, und
c) Berufserfahrung in der Umsetzung oder Begleitung von ICT- oder Informations- und Datensicherheitsprojekten.

Das Fachwissen kann auch bei externen Fachpersonen beschafft werden. Das KAIO stellt der Kantonsverwaltung hierfür schon heute Rahmenverträge zur Verfügung, woraus Informations- und Datensicherheitsleistungen abgerufen werden können (www.be.ch/zbsict).

Um Interessenkonflikte zu vermeiden, sollten die SIBE wenn möglich nicht den ICT-Verantwortlichen unterstellt sein oder ICT-Betriebsaufgaben wahrnehmen.
Absatz 1:

Die KDI als Steuerungsorgan der Informations- und Datensicherheit verfügt ebenfalls über eine oder einen SIBE. Weil die personellen Ressourcen des Kantons es nicht erlauben, zwei parallele kantonale Kompetenzzentren für Informationssicherheit aufzubauen, übernimmt die Leitung des Fachbereichs Sicherheit bzw. der Beratungsstelle IDS des KAIO auch die Rolle der oder des SIBE KDI. Dabei wird in Kauf genommen, dass sie oder er dem SIVE KAIO untersteht. Denn erstens würde diese Funktion auch bei einer anderen organisatorischen Ansiedlung einer oder einem SIVE DIR unterstehen. Und zweitens nimmt die Funktion des SIBE KDI keine Aufsichtsaufgaben wahr, bei denen ein Interessenkonflikt zur Ansiedlung der Rolle im KAIO entstehen könnte, sondern nur beratende und koordinierende Aufgaben. Die Aufsicht über die Informations- und Datensicherheit ist Sache der DSB und gegebenenfalls der Finanzkontrolle als verwaltungsunabhängige fachkundige Aufsichtsbehörden.

Absatz 2:

Buchstabe a:

Es ist möglich und teils wohl auch sinnvoll, dass dieselbe Person die Rolle der oder des SIBE für die Direktion und/oder für mehrere der Ämter der Direktion wahrnimmt. In grösseren Ämtern oder solchen mit hohen Sicherheitsrisiken ist die Einsetzung separater SIBE der Stufe Amt dagegen angezeigt.

Die KDI wird insbesondere die Aufgaben der SIBE DIR und SIBE Amt voneinander abzugrenzen haben. Es ist nicht sinnvoll, dass beide Personen dasselbe tun, weil dies zu Doppelspurigkeiten und Friktionen führen würde. Bestimmte Aufgaben werden sinnvollerweise auf Stufe Amt wahrzunehmen und auf Stufe Direktion zu überprüfen sein, andere Aufgaben werden dagegen nur auf Stufe Direktion wahrzunehmen sein, allenfalls unterstützt von den SIBE Amt. Es ist möglich, dass dies aufgrund der unterschiedlichen Aufbau- und ICT-Organisation der Organisationseinheiten der Stufe Direktion nicht überall einheitlich ausgestaltet werden kann.

Buchstabe b: Diese Formulierung trägt dem Anliegen Rechnung, dass dieselbe Person die SIBE-Rolle für mehrere Organisationseinheiten wahrnehmen können soll. Diese Lösung setzt die Zustimmung aller beteiligter Organisationseinheiten voraus.

Absatz 3:

Zu den Aufgaben der SIBE gehört namentlich:

a) Sie erarbeiten Entscheidgrundlagen zuhanden der oder des SIVE und beantragen ihr oder ihm den Beschluss von Schutzmassnahmen.
b) Sie sind die zentrale Anlaufstelle ihrer Organisationseinheit für Fragen zur Informations- und Datensicherheit und beraten und unterstützen die zuständigen Personen und Stellen bei der Erfüllung ihrer Aufgaben und Pflichten.
c) Sie sorgen für die Umsetzung der Vorschriften über die Informations- und Datensicherheit und die Anwendung des Sicherheitsverfahrens für ICT-Mittel.
d) Sie beaufsichtigen das Inventar der Schutzobjekte und das Verzeichnis der Ausnahmebewilligungen.
e) Sie beaufsichtigen die Planung und Durchführung der Schulungs- und Sensibilisierungsmassnahmen.

f) Sie koordinieren die Bewältigung von Sicherheitsvorfällen und Behandlung von Schwachstellen in ihrer Verwaltungseinheit sowie bei beauftragten Dritten.
g) Sie erstellen den jährlichen Kontroll- und Auditplan und unterbreiten ihn der oder dem SIVE zur Genehmigung.
h) Sie überprüfen periodisch das Vorhandensein und die Sicherheit von ICT-Mitteln der Einstufung «Hoher Schutz» oder «Sehr hoher Schutz» in ihrem Zuständigkeitsbereich.
i) Sie können im Auftrag der oder des SIVE den Umgang mit Informationen und Personendaten an offenen, geteilten oder nicht abschliessbaren Arbeitsplätzen und in den ICT-Mitteln der Verwaltungseinheit kontrollieren oder kontrollieren lassen.
j) Die SIBE DIR erstatten der oder dem SIVE DIR jährlich über die Umsetzung und die Wirksamkeit der Informationssicherheit Bericht.
k) Die SIBE DIR koordinieren das Risikomanagement im ISMS ihrer Organisationseinheit.
l) Die SIBE DIR erheben die Kennzahlen ihrer Organisationseinheiten und sorgen für die ISMS-Berichterstattung gemäss den Vorgaben der Fachgruppe IDS.
m) Die SIBE DIR führen fachlich die SIBE Amt in ihrem Zuständigkeitsbereich.

Absatz 4: Keine Bemerkungen.

**Artikel 38 – Fachgruppe Informations- und Datensicherheit**

Die Fachgruppe Informations- und Datensicherheit (IDS) besteht bereits heute als Fachgruppe Informationssicherheit (IS). Hier werden ihre Mitglieder und Aufgaben konkretisiert. Zur Stellung und den Aufgaben von Fachgruppen allgemein siehe Artikel 19 DVV.

Die Fachgruppe IDS sorgt insbesondere für die direktionsübergreifende Koordination der Informationssicherheit und erlässt die Vorgaben zur ISMS-Berichterstattung.

**Artikel 39 – Beratungsstelle Informations- und Datensicherheit**

Absatz 1:

Die Beratungsstelle IDS entspricht dem heutigen Fachbereich Sicherheit des KAIO, in dem mehrere Sicherheitsberaterinnen und -berater zur Unterstützung von ICT-Vorhaben der Kantonsverwaltung tätig sind. Neu hinzu kommen werden insbesondere die Aufgaben und Kompetenzen im Zusammenhang mit dem Aufbau, dem Betrieb und der Koordination des kantonalen ISMS. Die Beratungsstelle IDS hat keine Aufsichts- oder Kontrollfunktion, weil die Sicherheitsverantwortung bei den SIVE bzw. bei der Führung liegt, und die verwaltungsunabhängige Aufsicht über die Einhaltung der IDS-Vorschriften eine Aufgabe der Datenschutzbehörde sowie der Finanzkontrolle ist.

Die Beratungsstelle IDS hat namentlich folgende Aufgaben:

a) Sie entwirft zu Handen der KDI die Informationssicherheitsstrategie und -ziele sowie die Ausführungsvorschriften für die Informations- und Datensicherheit.
b) Sie führt ein aktuelles Verzeichnis der massgebenden Vorschriften zur Informations- und Datensicherheit.
c) Sie kann bei sicherheitsrelevanten Vorhaben der Organisationseinheiten Informationen verlangen, dazu Stellung nehmen und den SIVE Änderungen beantragen.
d) Sie wirkt bei der Ausbildung der Organe der Sicherheitsorganisation mit.
e) Sie stellt die von der KDI als verbindlich erklärten Vorlagen und Hilfsmittel bereit.
f) Sie berät und unterstützt die SIVE und SIBE.
g) Sie vertritt den Kanton in Fachorganisationen der Informationssicherheit und ist Ansprechpartnerin des Bundes in Fragen der Informationssicherheit (Art. 86 Abs. 3 ISG).

h) Sie kann in Zusammenarbeit mit der Kantonspolizei für den Kanton mit dem Bund eine Leistungsvereinbarung über die erweiterte Personensicherheitsprüfung abschliessen (Art. 35 der Verordnung des Bundes vom 8. November 2023 über die Personensicherheitsprüfungen, VPSP[31]).
i) In Zusammenarbeit mit der Fachgruppe IDS baut, betreibt und koordiniert sie das ISMS und sorgt für dessen Überprüfung und Wirksamkeit.

Diese Angebote stehen grundsätzlich nur den kantonalen Behörden zur Verfügung. Für die anderen Behörden soll die Beratungsstelle IDS lediglich Aus- und Weiterbildungen gegen Entgelt zur Verfügung stellen (Art. 19 Abs. 2 ICSG). Daher haben sich KAIO und DSB auf die folgende Aufgabenteilung verständigt:

a) Die kantonale Datenschutzbehörde wird im Rahmen ihrer Beratung der kommunalen Behörden Vorlagen und Hilfsmittel spezifisch für diese erarbeiten und sich dabei mit der Beratungsstelle IDS abzustimmen.
b) Die Beratungsstelle IDS richtet ihre Vorlagen und Hilfsmitteln hauptsächlich auf die kantonalen und solche Behörden aus, welche den Schutz eigener, klassifizierter Informationen gewährleisten wollen.

Absätze 2 und 3: Keine Bemerkungen.

**Artikel 40 – Belohnung für das Erkennen und Melden von Schwachstellen**

Absätze 1 und 2:

Hier wird das sog. Bug-Bounty-Programm beschrieben, ein Angebot von Unternehmen oder Behörden, das Sicherheitsspezialistinnen und -spezialisten (sog. Bug-Hunter) dafür belohnt, dass sie Schwachstellen (sog. Bugs) in ICT-Mitteln finden und den dafür Verantwortlichen melden. Der typische Ablauf gestaltet sich wie folgt:

1. Die kantonale Behörde bestimmt das zu untersuchende ICT-Mittel, den Umfang (sog. Scope), und die zu beachtenden Regeln, z.B. keine DoS-Angriffe oder keinen Zugriff auf Kundendaten.
2. Die Teilnehmenden suchen gezielt nach Schwachstellen innerhalb dieses Scopes und der Regeln.
3. Gefundene Schwachstellen werden über eine Bug-Bounty-Plattform eingereicht.
4. Die Behörde bewertet den Hinweis, bestätigt die Schwachstelle, behebt sie und zahlt gegebenenfalls eine Belohnung, sog. Bounty, entsprechend dem Sicherheitsrisiko und den Regeln aus.

Bug-Bounty-Programme sind heute «State of the Art» zur vorbeugenden Schwachstellenerkennung und -behebung. Verschiedene Schweizer Behörden und Unternehmen betreiben sie, z.B. die Schweizerische Post AG, Abraxas Informatik AG, das Bundesamt für Cybersicherheit (BACS) oder die Kantone St. Gallen, Zürich, Thurgau und Aargau. Es ist vorgesehen, dafür die Dienste eines professionellen Bug-Bounty-Plattformanbieters in Anspruch zu nehmen.

Absatz 3:

Im Rahmen des entsprechenden Webauftritts wird die Beratungsstelle IDS die Regeln des Programms konkretisieren und u.a. regeln, dass an Angestellte und Beauftragte des Kantons keine Belohnung ausgezahlt wird, weil das Abgeben von Hinweisen auf Schwachstellen zu deren Pflichten gehört. Der Höchstbetrag des Kantons Bern entspricht damit ungefähr demjenigen der Post, welche EUR 10'000 für Hinweise auf die schwerwiegendsten Schwachstellen vorsieht.

[31] VPSP, SR 128.31

Absatz 4:

Mit dem Ausschluss des Rechtsanspruchs werden Beschwerden über die Ausrichtung einer Belohnung bzw. deren Umfang ausgeschlossen. Dies rechtfertigt sich, weil es um geringe Beträge geht, die Frage des Anspruchs auf eine Belohnung nur mit hohem Sicherheitsfachwissen beurteilbar und daher schwer justiziabel ist, und weil erfahrungsgemäss die meisten Hinweise aus dem Ausland stammen, was die Abwicklung von Beschwerdeverfahren noch mehr verkomplizieren würde.

## 7.5 Übergangs- und Schlussbestimmungen

### Artikel 41 - Übergangsbestimmungen

Absatz 1: Das ISMS ist seit dem 1. Januar 2025 mit den entsprechenden Prozessen in Betrieb. Offen ist noch das IS-Risikomanagement, die Arbeiten dazu laufen seit der Einführung des ISMS. Die Verwaltungseinheiten haben die rund 1'400 Applikationen darin erfasst. Angesichts dieses weit fortgeschrittenen Umsetzungsstands sind die insgesamt zwei Jahre angepasst.

Absatz 2: Die im ITSMS inventarisierten kantonalen Applikationen weisen schon heute ihre Einstufung und damit das Schutzniveau aus. Das Inventar der Schutzobjekte liegt also bereits vor. Der Klassifizierungskatalog ist ein einfaches, effizientes Hilfsmittel für die Mitarbeitenden. Zudem ist es ein sehr wichtiges Steuerungsinstrument der Führung für das verwaltungsweit einheitliche und insbesondere auch sparsame Klassifizieren. Das KAIO wird hierfür ein Muster erstellen. Vor diesem Hintergrund ist die Jahresfrist verhältnismässig.

Absatz 3: Die kantonalen Behörden und ihre Mitarbeitende haben zu prüfen, wo es sinnvoll ist, diese nachträgliche Klassifizierung und das Anbringen des Klassifizierungsvermerks über das ICT-Mittel zu erzwingen.

Absatz 4:

Buchstabe a: Die Schutzbedarfsanalysen sowie die ISDS-Konzepte wurden zwar in den letzten Jahren immer konsequenter erstellt. Jedoch bestehen solche noch nicht für sämtliche ICT-Mittel der kantonalen Verwaltung, dies obwohl die Pflicht zum Erstellen dieser Dokumente mit der ISDS DV seit dem 1. April 2011 besteht. Ebenso werden sie von der per 1. Januar 2025 in Kraft gesetzten ICSGW verlangt. Vor diesem Hintergrund sind die Fristen von einem Jahr für die Schutzbedarfsanalyse und zwei Jahren für das ISDS-Konzept verhältnismässig.

Buchstabe b: Gemäss Artikel 8 IDSV haben auch die anderen und insbesondere kommunalen Behörden und Körperschaften für ihre Personendatensammlungen Schutzbedarfsanalysen und ISDS-Konzepte in risikoangemessener Form zu erstellen. Obwohl diese Pflicht bereits heute besteht, sie jedoch von den kommunalen Datenschutzaufsichtsstellen unterschiedlich überprüft worden ist, muss mit einem grösserer Nachholbedarf gerechnet werden. Sowohl zur Entlastung der Verpflichteten als auch der kantonalen Datenschutzbehörde werden hierfür zwei bzw. drei Jahre vorgesehen.

Absatz 5: Es sind jedoch nicht allein die Schutzbedarfsanalysen und die ISDS-Konzepte, welche die tatsächliche Schutzwirkung erzeugen. Vielmehr sind es die Ersteller und Betreiber von ICT-Mitteln, die vertragskonforme, sichere Leistungen zu erbringen haben. Daher sind bestehende Verträge bei der nächsten Änderung an die Vorschriften der IDSV anzupassen, ebenso bestehende ICT-Mittel. Der Termin vom 1. Oktober 2030 stimmt mit der Übergangsbestimmung nach Artikel 16 KDSV, laufende Verträge mit beauftragten Dritten, überein, wonach die Verträge innert Frist an den Vertragsinhalt nach Artikel 1 KDSV anzupassen sind.

Absatz 6: Es liegt nicht im Interesse der Gemeinden, wenn bei der kommunalen Aufsichtsstelle eingereichte Vorabkontrollen an die kantonale Datenschutzbehörde übergehen und sich diese neu in die Geschäfte einarbeiten muss. Dies würde zu unerwünschten Verzögerungen bei der Umsetzung von kommunalen Digitalisierungsvorhaben führen, was mit der Übergangsbestimmung verhindert werden soll.

Absatz 7: Für die Klassifizierung von Regierungsratsgeschäften besteht seit 2013 mit der Verordnung über die Klassifizierung, die Veröffentlichung und die Archivierung von Dokumenten zu Regierungsratsgeschäften (Klassifizierungsverordnung, KRGV) eine spezifische Regelung. Die KRGV bleibt für die Regierungsratsgeschäfte und deren Dokumente als lex specialis auch mit der IDSV anwendbar, wird aber im Nachgang an die Verabschiedung der neuen Gesetzgebung über die Informations- und Datensicherheit überprüft und angepasst.

**Artikel 42 – Änderung von Erlassen**

Buchstabe a: Verordnung über die digitale Verwaltung (DVV)

Artikel 9 - Identifikationsverfahren

Absatz 2: Dieser Absatz wird gestrichen. Es handelt sich der Sache nach um Sicherheitsvorschriften, nämlich um Massnahmen zur risikoangemessenen Authentifizierung von Nutzerinnen und Nutzern digitaler Leistungen. Damit gehören sie thematisch in die IDSV, weshalb sie aus der DVV entfernt werden. Aufgrund des hohen Detaillierungsgrades der Regelung wird sie aber nicht unverändert in die IDSV übernommen, sondern auf Weisungsebene aufgegriffen und dort voraussichtlich aktualisiert, indem auf die vom kantonalen Anmeldedienst BE-Login umgesetzten Qualitätsniveaus der Authentifizierung (AGOVaq) des nationalen Anmeldediensts AGOV Bezug genommen wird, statt auf den bisher referenzierten relativ abstrakten eCH-Standard. Mit der Verschiebung in das kantonale Sicherheitsregelwerk wird auch klargestellt, dass die SIVE wie in Bezug auf andere Sicherheitsmassnahmen Ausnahmen bewilligen können, wenn sie das sich daraus ergebende Risiko ausdrücklich akzeptieren.

Artikel 18 - Konferenz digitale Verwaltung und ICT (KDI)

Absatz 1:

- Buchstabe c wird mit den Parlamentsdiensten ergänzt.
- Buchstabe e wird neu eingefügt, so dass die oder der SIBE KDI auch Mitglied der KDI ist.

Absatz 2: Im Buchstabe c die Kompetenz der KDI zum dem Erlass von Weisungen über die Informations- und Datensicherheit ergänzt.

Artikel 19 - Fachgruppen

Absatz 2: Der Buchstabe d wird auf Antrag der Parlamentsdienste gestrichen.

Buchstabe b: Verordnung über die Ausgleichskasse des Kantons Bern und ihre Zweigstellen (AKBV)[32]

Artikel 6 - Kantonale Steuerverwaltung

[32] AKBV, BSG 841.111

Absatz 3: Bei der Protokollierung von Datenzugriffen gelten nicht mehr die Vorschriften der DSV, sondern diejenigen der IDSV.

Buchstabe c: Verordnung über die Datenbearbeitung im Asyl-, Flüchtlings- und Ausländerbereich (DAFAV)[33]

Artikel 9

Absatz 1 (Version in Kraft bis zum 31. August 2026): «Technische und organisatorische Massnahmen» nach der DSV wird mit «Sicherheitsmassnahmen» nach IDSV ersetzt, ebenso «Datenschutzaufsichtsstelle» mit «Datenschutzbehörde».

**Artikel 43 - Aufhebung eines Erlasses**

Direktionsverordnung über Informationssicherheit und Datenschutz (ISDS DV)

Die ISDS DV wird aufgehoben, weil ihre Inhalte nun Gegenstand der IDSV sind.

**Artikel 44 – Inkrafttreten**

Die KDSV trat mit dem KDSG bereits am 1. September 2026 in Kraft, wogegen die IDSV mit dem ICSG erst per 1. November 2026 in Kraft gesetzt wird. Die unterschiedliche Inkraftsetzung der Erlasse folgt aus dem Ansetzen eines zweiten Mitberichtes zur IDSV, nachdem diese auch zwecks besserer Verständlichkeit grundlegend überarbeitet wurde. Für die Übergangsfrist erklärt Art. 18 KDSV die Art. 4 bis 9 DSV für anwendbar (Technische und organisatorische Massnahmen sowie Vorabkontrolle), welche sodann per 1. November 2026 insbesondere von den Artikeln 5 bis 10 IDSV abgelöst werden.

## 8. Verhältnis zu den Richtlinien der Regierungspolitik und anderen wichtigen Planungen

Die IDSV entspricht den Richtlinien der Regierungspolitik 2023 bis 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.

Sie entspricht auch der vom Regierungsrat am 11. Juni 2026 beschlossenen Strategie Digitale Verwaltung und ICT 2026 bis 2030, welche die Informationssicherheit als strategischen Grundsatz in Ziffer 6.5 verankert.

## 9. Auswirkungen auf Finanzen, Organisation, Personal, IT und Raum

### 9.1 Informationssicherheit

Betreffend die finanziellen Auswirkungen können an dieser Stelle vorab die Angaben zum ICSG wiederholt werden (Ziff. 10 und 11 des Vortrags zum ICSG):

[33] DAFAV, BSG 861.112

Die Schutzmassnahmen für die Informationssicherheit werden grundsätzlich mit den bestehenden bzw. geplanten, für die ICT und die Digitalisierung vorgesehenen Finanzmitteln umzusetzen sein. Dies aus folgenden Gründen:

a) Bereits mit Artikel 17 des bisherigen KDSG sind die Behörden zur Gewährleistung der Datensicherheit verpflichtet. Das ICSG führt damit keine neue staatliche Aufgabe ein, sondern konkretisiert lediglich eine bereits bestehende Aufgabe.

b) 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:

    1. 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.).

    2. 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.

    3. Wenn Behörden ein angemessenes Risikomanagement betreiben (Art. 5 Abs. 2 ICSG), können sie ihre Schutzmassnahmen gezielt auf die risikoreichen Aspekte ihrer Tätigkeit ausrichten und Risiken in weniger sensiblen Tätigkeitsbereichen bewusst in Kauf nehmen (Art. 12 Abs. 1 Bst. d ICSG). Wenn sie nur so viele Informationen wie nötig klassifizieren (Art. 8 Abs. 3 ICSG), reduzieren sie damit den Umfang der Systeme mit erhöhter Sicherheitsstufe (Art. 12 Abs. 1 Bst. b ICSG) und die damit verbundenen Kosten.

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.

Die Kosten allfälliger Bug-Bounty-Programme werden, wenn solche Programme gestartet werden sollen, beim KAIO budgetiert (ca. CHF 40’000 p.a. für die Plattform, ca. CHF 60’000 p.a. für die Belohnungen). Die tatsächlichen Kosten hängen vom Umfang der Meldungen ab. Der Personalaufwand von ca. 0.25 FTE wird KAIO-intern kompensiert.

Die Schulung der Mitarbeitenden mittels BE-Secure wird wie bisher vom KAIO angeboten und wird nicht mehr als zwei Stunden beanspruchen. Auch die Awareness-Kampagnen werden wie bis anhin vom KAIO verwaltungsweit lanciert und finanziert.

Die Rolle des SIBE KDI wird vom Leiter der Beratungsstelle IDS beim KAIO wahrgenommen, welche wiederum dem heutigen Fachbereich Sicherheit des KAIO entspricht. Ein weiterer Stellenausbau ist nicht geplant.

Bereits heute verfügen die DIR/STA/JUS über die Rolle des oder der SIVE, welche sich jedoch in der Hierarchie, in der Ausbildung und in den Stellenprozenten sehr stark unterscheiden. Hier wird die oberste Führung eine Überprüfung und nötigenfalls Anpassungen vornehmen müssen.

Ein Audit kostet ca. CHF 20'000. Externe Fachleute für solche Audits können beim KAIO schon heute aus den bestehenden Rahmenverträgen abgerufen werden. Die Zahl der Audits ist durch die Koordination zwischen den DIR/STA/JUS sowie mit der Finanzkontrolle und der Datenschutzbehörde auf ein risikobasiertes, erforderliches Mass zu reduzieren.

Die zentrale Meldeplattform wird vom KAIO aufgebaut und betrieben. Es rechnet mit einem Aufwand von ca. CHF 5'000 pro Jahr.

Zusammenfassend ist eine verlässliche Prognose insbesondere des personellen Ressourcenbedarfs für die neu umzusetzenden Instrumente (ISMS, Inventar der Schutzobjekte, Audits) aktuell nicht möglich. Es kann daher nicht ausgeschlossen werden, dass im Rahmen der künftigen Planungsprozesse von den Direktionen und der Staatskanzlei zusätzlicher Ressourcenbedarf angemeldet wird.

### 9.2 Datensicherheit

Mit der Revision des KDSG und der Aufnahme des digitalen Bearbeitens von Personendaten bzw. dem Profiling mit hohem Risiko nach Artikel 2 Buchstabe h KDSG werden die Anforderungen an die Datensicherheit erhöht.

Hierfür schreibt Artikel 6 Absatz 2 IDSV für besonders schützenswerte Personendaten neben dem bisherigen Aufzeichnen des Speicherns, Veränderns, Löschens und Vernichtens zusätzlich auch das Aufzeichnen des Lesens und des Bekanntgebens von Personendaten vor, sofern die präventiven Massnahmen die Datensicherheit nicht gewährleisten können.

Die die Protokollierungspflicht besteht bereits seit dem Erlass von Artikel 5 Absatz 1 Buchstabe h DSV BE im Jahr 2008. Die mit der IDSV nun ausdrücklich definierten Verfahren zur Gewährleistung der Datensicherheit werden aber dazu führen, dass bis heute ohne Protokollierung und damit an sich rechtswidrig betriebene ICT-Mittel entdeckt und sicherer gemacht werden, was zu Kosten führen wird, die bereits bei der Inbetriebnahme der ICT-Mittel hätten aufgewendet werden müssen.

## 10. Auswirkungen auf die Gemeinden und die anderen Träger öffentlicher Aufgaben

### 10.1 Informationssicherheit

Das ICSG gilt für die Gemeinden und die anderen Träger öffentlicher Aufgaben 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 selbst 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 Schutzmassnahmen ergreifen und Synergien mit anderen Gemeinden sowie mit der Kantonsverwaltung realisieren.

### 10.2 Datensicherheit

Da die IDSV sowohl Informations- als auch Datensicherheit regelt, gilt sie aufgrund des KDSG für alle Behörden, welche Personendaten bearbeiten (s. Art. 2 Abs. 2 Bst. c IDSV). Die Datensicherheit ist jedoch nicht nur für die kantonalen, sondern auch für die anderen Behörden nichts Neues, wie nachstehend dargestellt wird. Damit konkretisiert die IDSV bloss bereits bestehende Aufgaben und schafft grundsätzlich keine neuen. Dass die Erfüllung dieser Aufgaben tendenziell immer aufwändiger wird, ist nicht eine Folge der Gesetzgebung, sondern der zunehmenden Digitalisierung der öffentlichen Verwaltung und den damit stark zunehmenden Cyberrisiken.

Artikel 17 KDSG verlangt seit dem Erlass des KDSG im Jahr 1986, dass die Datensicherheit gewährleistet ist. Diese Vorschrift wurde mit den Artikeln 4 und 5 DSV (technische und organisatorische Massnahmen) konkretisiert. Als Artikel 5 und 6 wurden diese Bestimmungen in aktualisierter Form in die IDSV integriert. Auch die Pflicht zur Vorabkontrolle bei der Datenbearbeitung durch ICT-Mittel schreibt Artikel 17a KDSG von 1986 schon lange vor.

Eine weitere Konkretisierung erfolgte im Jahr 2011 mit der ISDS DV, insbesondere was das Sicherheitsverfahren bei ICT-Mitteln und die Sicherheitsorganisation betrifft, allerdings hier nur für die Kantonsverwaltung.

Mit der IDSV gelten die Grundsätze der Informations- und Datensicherheit sowie der Führung gemäss Artikel 4 IDSV für sämtliche Behörden des Kantons Bern, also auch für die Einwohner-, Kirch- und Burgergemeinden. Hingegen gelten die Artikel 13 ff. IDSV nur für die kantonalen Behörden. Keine Geltung für die anderen Behörden haben insbesondere die Vorschriften zum ISMS, zum Inventar der Schutzobjekte, zur Kontrolle und zu den Audits oder der Klassifizierung von Informationen.

## 11. Auswirkungen auf die Volkswirtschaft

Bereits die Beurteilung des ICSG 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.

Auch der aktive Einbezug von Fachleuten der Bedag Informatik AG, der Swisscom AG sowie der SPIE Schweiz AG in die Erarbeitung der IDSV hat an diesem Ergebnis nichts geändert.

Die parallel zum Erlass dieser Verordnung gestarteten Arbeiten für den Grundschutz BE bestätigten dieses Ergebnis. Neben den drei vorgenannten Unternehmen wurden zusätzlich die beiden grössten Outsourcing-Partner der Berner Einwohnergemeinden, die Dialog Verwaltungsdata AG sowie die Talus AG, zur Konsultation der konkreten Sicherheitsmassnahmen einbezogen. Keine der beiden befürchtete Mehrkosten oder andere negative Auswirkungen auf ihre Tätigkeit. Denn schon heute orientieren sich auch diese Unternehmen an den Sicherheitsstandards nach ISO-27001.

## 12. Antrag

Die Finanzdirektion beantragt dem Regierungsrat, die vorliegende Verordnung zu erlassen.

Beilage
– Erlassentwurf