

Gesetz über die Informations- und Cybersicherheit (ICSG)

vom [Datum]

Erlass(e) dieser Veröffentlichung:

Neu: ????.???

Geändert: 551.1

Aufgehoben: –

Der Grosse Rat des Kantons Bern,

gestützt auf Artikel 18 Absatz 3 und Artikel 37 der Kantonsverfassung (KV)
vom 6. Juni 1993

beschliesst:

I.

1 Allgemeine Bestimmungen

Art. 1 Zweck

¹ Dieses Gesetz gewährleistet die sichere Bearbeitung von Informationen und den sicheren Einsatz von ICT-Mitteln durch Behörden.

² Es schützt die folgenden öffentlichen Interessen:

- a* die Entscheidungs- und Handlungsfähigkeit der Behörden,
- b* die öffentliche Ordnung und Sicherheit,
- c* die Erfüllung der gesetzlichen und vertraglichen Verpflichtungen der Behörden zum Schutz von Informationen.

Art. 2 Geltungsbereich

¹ Dieses Gesetz gilt für die kantonalen Behörden und die Gemeinden im Sinne der Kantonsverfassung (Kapitel 5 und 7), unter Vorbehalt von Absatz 2.

² Für Gemeinden und für andere Träger öffentlicher Aufgaben gelten nur die Bestimmungen

- a über klassifizierte Informationen, soweit klassifizierte Informationen des Kantons oder des Bundes bearbeitet werden, und
- b über die Sicherheit beim Einsatz von ICT-Mitteln, soweit auf ICT-Mittel des Kantons oder des Bundes zugegriffen wird.

Art. 3 *Verhältnis zu anderen Gesetzen*

¹ Die Bestimmungen über die Information auf Anfrage (Art. 27 bis 31a) des Gesetzes über die Information und die Medienförderung vom 2. November 1993 (IMG)¹ gehen diesem Gesetz vor.

² Für Informationen, deren Schutz gleichzeitig in anderen Gesetzen des Kantons oder Bundes geregelt ist, und für die Sicherheit von Personendaten gemäss Artikel 2 Absatz 1 des Datenschutzgesetzes vom 19. Februar 1986 (KDSG)² findet dieses Gesetz ergänzend Anwendung.

Art. 4 *Begriffe*

¹ In diesem Gesetz bedeuten:

- a Informationen: Angaben über Sachverhalte, welche die öffentlichen Interessen gemäss Artikel 1 Absatz 2 betreffen,
- b Informationssicherheit: Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit von Informationen,
- c Cybersicherheit: Informationssicherheit bei der Übertragung von Informationen über Netzwerke,
- d ICT-Mittel: Güter und Dienstleistungen der Informations- und Telekommunikationstechnik (ICT), einschliesslich Hardware und Software.

2 Grundsätze

Art. 5 *Pflichten der Behörden zur Informations- und Cybersicherheit*

¹ Die Behörden sorgen dafür, dass

- a der Schutzbedarf der Informationen in ihrem Verantwortungsbereich beurteilt wird,
- b die Informationen gemäss Buchstabe a ihrem Schutzbedarf entsprechend
 1. nur Berechtigten zugänglich sind (Vertraulichkeit),
 2. verfügbar sind, wenn sie benötigt werden (Verfügbarkeit),
 3. nicht unberechtigt oder unbeabsichtigt verändert werden (Integrität),
 4. nachvollziehbar und zurechenbar bearbeitet werden (Nachvollziehbarkeit),

¹) BSG [107.1](#)

²) BSG [152.04](#)

c ihre ICT-Mittel vor Missbrauch, Fehlern und Störungen geschützt werden.

² Sie stellen das Risikomanagement sicher, indem sie

- a die Risiken für die Informationssicherheit laufend beurteilen,
- b die erforderlichen Massnahmen treffen, um die Risiken zu vermeiden oder auf ein tragbares Mass zu reduzieren, und
- c Risiken, die getragen werden sollen, nachweislich akzeptieren.

³ Sie tragen den Grundsätzen der Zweckmässigkeit, der Wirtschaftlichkeit und der Benutzerfreundlichkeit Rechnung.

Art. 6 *Beauftragte Dritte*

¹ Beauftragen die Behörden Dritte, so sorgen sie dafür, dass die Anforderungen und Massnahmen nach diesem Gesetz

- a den Dritten vertraglich überbunden werden,
- b die Nichteinhaltung sanktioniert wird und
- c die Umsetzung angemessen überprüft wird.

Art. 7 *Reaktionsfähigkeit und Vorsorge*

¹ Die Behörden stellen sicher, dass Verletzungen der Informationssicherheit rasch erkannt, deren Ursachen behoben und die Auswirkungen minimiert werden.

² Sie stellen sicher, dass

- a Vorsorgeplanungen erstellt werden für schwerwiegende Verletzungen der Informationssicherheit, welche die Erfüllung von Aufgaben des Kantons mit grosser Wichtigkeit für die Bevölkerung gefährden können,
- b die Vorsorgeplanungen umgesetzt und regelmässig aktualisiert werden.

3 Organisatorische Massnahmen

Art. 8 *Klassifizierung*

¹ Die Behörden klassifizieren Informationen, wenn ihre Kenntnisnahme durch Unberechtigte die öffentlichen Interessen gemäss Artikel 1 Absatz 2 Buchstabe a und b beeinträchtigt.

² Die Klassifizierung erfolgt in den folgenden Stufen:

- a "INTERN", wenn die öffentlichen Interessen beeinträchtigt werden können,
- b "VERTRAULICH", wenn die öffentlichen Interessen erheblich beeinträchtigt werden können,

c "GEHEIM", wenn die öffentlichen Interessen schwerwiegend beeinträchtigt werden können.

³ Die Klassifizierung ist die Ausnahme. Sie ist auf die erforderliche Mindeststufe zu beschränken und möglichst zeitlich zu begrenzen.

⁴ Der Regierungsrat regelt die Klassifizierung und Entklassifizierung durch Verordnung.

Art. 9 *Zugang zu klassifizierten Informationen*

¹ Zugang zu klassifizierten Informationen erhalten nur Personen, die Gewähr dafür bieten, dass sie die öffentlichen Interessen gemäss Artikel 1 Absatz 2 nicht beeinträchtigen und die Informationen zur Erfüllung einer gesetzlichen oder vertraglichen Aufgabe benötigen.

² Der Zugang zu klassifiziertem Archivgut richtet sich nach den Bestimmungen der Archivierungsgesetzgebung.

Art. 10 *Zugang in besonderen Verfahren*

¹ Der Zugang zu klassifizierten Informationen des Grossen Rats und der Parlamentsdienste sowie der Gerichtsbehörden und der Staatsanwaltschaft richtet sich unter Vorbehalt von Absatz 2 nach den Bestimmungen der Spezialgesetzgebung.

² Vor dem Entscheid, den Zugang zu einer klassifizierten Information gemäss Absatz 1 zu ermöglichen, hört das zuständige parlamentarische Organ, das zuständige Gericht oder die zuständige Staatsanwaltschaft die klassifizierende Stelle an.

4 Technische Massnahmen

Art. 11 *Sicherheitsverfahren*

¹ Der Regierungsrat oder das von ihm bestimmte Organ der Kantonsverwaltung legt ein Verfahren zur Gewährleistung der Informationssicherheit beim Einsatz von ICT-Mitteln fest (Sicherheitsverfahren).

² Das Sicherheitsverfahren umfasst insbesondere

- a die Beurteilung des Schutzbedarfs der Informationen vor dem Einsatz von ICT-Mitteln,
- b die Bestimmung der sich aus dem Schutzbedarf ergebenden Sicherheitsstufe und der angemessenen Sicherheitsmassnahmen,
- c die Umsetzung der Sicherheitsmassnahmen und die Überprüfung der Umsetzung,

- d* die Zuständigkeit für die Sicherheitsfreigabe von ICT-Mitteln und für die Akzeptanz verbleibender Risiken,
- e* das Vorgehen bei Veränderung der Risiken.

³ Für die ICT-Mittel gilt die Sicherheitsstufe

- a* «sehr hoher Schutz», wenn die Interessen gemäss Artikel 1 Absatz 2 schwerwiegend beeinträchtigt werden können,
- b* «hoher Schutz», wenn die Interessen gemäss Artikel 1 Absatz 2 erheblich beeinträchtigt werden können,
- c* «Grundsatzschutz» in den anderen Fällen.

⁴ Für die Durchführung des Sicherheitsverfahrens ist die Behörde zuständig, welche die ICT-Mittel zur Erfüllung ihrer gesetzlichen Aufgabe einsetzt oder anderen Behörden zur Verfügung stellt.

⁵ Der Regierungsrat kann durch Verordnung die Schutzmassnahmen regeln, die für ICT-Mittel, Informationen und Personendaten zu ergreifen sind, abhängig von

- a* der Sicherheitsstufe von ICT-Mitteln,
- b* der Klassifizierung von Informationen, und
- c* der Schutzwürdigkeit von Personendaten nach Massgabe der Datenschutzgesetzgebung.

Art. 12 *Sicherheit beim Betrieb*

¹ Die Behörden gewährleisten in ihrem Verantwortungsbereich die Sicherheit der ICT-Mittel, die sie für sich selbst oder im Auftrag einer anderen Behörde betreiben.

5 Physische Massnahmen

Art. 13 *Grundsatz*

¹ Die Behörden sorgen in ihrem Verantwortungsbereich für einen angemessenen physischen Schutz der Informationen und der ICT-Mittel.

Art. 14 *Sicherheitszonen*

¹ Die Behörden können Räumlichkeiten oder Bereiche als Sicherheitszonen bezeichnen, in denen

- a* Informationen der Klassifizierung «GEHEIM» regelmässig bearbeitet werden oder
- b* ICT-Mittel der höchsten Sicherheitsstufe betrieben werden.

² Sie können in Sicherheitszonen

- a das Mitführen bestimmter Gegenstände, insbesondere von Aufnahmege-
räten, verbieten,
- b sicherheitsempfindliche Bereiche mit Aufnahmegegeräten überwachen,
- c Taschen- und Personenkontrollen durchführen,
- d unangemeldet Raumkontrollen durchführen, auch in Abwesenheit der
Angestellten,
- e störende Fernmeldeanlagen gemäss Artikel 34 Absatz 1ter des eidgenös-
sischen Fernmeldegesetzes vom 30. April 1997 (FMG)¹⁾ betreiben.

6 Personelle Massnahmen

6.1 Auswahl, Instruktion und Berechtigung

Art. 15 *Voraussetzungen für den Zugang zu Informationen und ICT-Mit- teln*

¹ Die Behörden sorgen dafür, dass Personen, die Zugang zu ihren Informatio-
nen, ICT-Mitteln, Räumlichkeiten und anderen Infrastrukturen haben,

- a sorgfältig ausgewählt werden,
- b risikogerecht identifiziert werden,
- c funktionsgerecht aus- und weitergebildet werden,
- d gegebenenfalls zur Geheimhaltung und besonderer Sorgfalt verpflichtet
werden.

Art. 16 *Restriktive Berechtigungen*

¹ Die Behörden sorgen dafür, dass den Personen gemäss Artikel 15 nur die In-
formationen, ICT-Mittel, Räumlichkeiten und andere Infrastrukturen zur Verfü-
gung stehen, die sie zur Erfüllung ihrer gesetzlichen oder vertraglichen Aufga-
ben benötigen.

6.2 Personensicherheitsprüfung

Art. 17 *Voraussetzungen und Zweck*

¹ Die Personensicherheitsprüfung dient zur Beurteilung, ob ein Risiko für die In-
formationssicherheit bestehen könnte, wenn eine Person im Rahmen ihrer
Funktion oder eines Auftrags Zugang zu sicherheitsrelevanten Informationen
hat.

² Folgende Personen können einer Personensicherheitsprüfung unterzogen
werden, sofern sie dieser zustimmen:

¹⁾ SR [784.10](#)

- a Angestellte der Behörden vor dem Abschluss des Arbeitsverhältnisses oder während seiner Dauer: durch die Anstellungsbehörde.
- b Personen, die als Mitglied einer Behörde gewählt werden sollen: durch die Wahlbehörde oder die Behörde, die den Antrag zur Wahl stellt.
- c Private, die im Rahmen der ihnen übertragenen Aufgaben oder Leistungen zum direkten Zugriff, zur selbstständigen Bearbeitung oder zur Einsichtnahme in die von Behörden bearbeiteten Informationen berechtigt sind: durch die auftraggebende Behörde.

³ Die Personensicherheitsprüfung kann durchgeführt werden, wenn die mit ihrer Tätigkeit verbundenen Sicherheitsrisiken die Personensicherheitsprüfung rechtfertigen, namentlich wenn die geprüfte Person

- a häufig oder in grossem Umfang Zugang zu klassifizierten Informationen oder besonders schützenswerten Personendaten hat,
- b weitreichenden Einblick in wichtige politische oder sicherheitsrelevante Geschäfte hat und darauf Einfluss nehmen kann, oder
- c regelmässig oder unbegleitet Zugang zu sicherheitsrelevanten Anlagen oder Räumlichkeiten oder zu Sicherheitszonen gemäss Artikel 14 hat.

⁴ Die geprüfte Person ist verpflichtet, an der Personensicherheitsprüfung mitzuwirken.

⁵ Bei Personen, die klassifizierte Informationen des Bundes bearbeiten oder auf ICT-Mittel des Bundes zugreifen, bleiben die Bestimmungen der Bundesgesetzgebung über die Informationssicherheit vorbehalten.

Art. 18 *Gegenstand*

¹ Bei der Personensicherheitsprüfung werden die für die Beurteilung nach Artikel 17 Absatz 1 benötigten Daten über die Lebensführung der geprüften Person erhoben, insbesondere über ihre allfällige Straffälligkeit und finanzielle Lage.

² Die Daten können erhoben werden

- a aus dem Strafregister,
- b aus den Registern der Betreibungs- und Konkursbehörden,
- c aus den Datenbearbeitungssystemen der Kantonspolizei gemäss Artikel 143 des Polizeigesetzes vom 10. Februar 2019 (PolG)¹⁾,
- d aus den Datenbearbeitungssystemen des Bundes oder der Kantone, soweit die Kantonspolizei gemäss Artikel 147 PolG zum direkten Zugriff berechtigt ist,

¹⁾ BSG 551.1

- e durch die Befragung der geprüften Person,
- f durch die Befragung von Drittpersonen, wenn die geprüfte Person zustimmt.

Art. 19 *Rechtsschutz und Folgen*

¹ Die prüfende Behörde teilt der geprüften Person das Ergebnis der Personensicherheitsprüfung mit, wenn diese ergibt, dass ein Risiko gemäss Artikel 17 Absatz 1 besteht.

² Die geprüfte Person kann innert zehn Tagen Einsicht in die Prüfungsunterlagen nehmen und die Berichtigung falscher Daten verlangen.

³ Stimmt die zu prüfende Person der Prüfung nicht zu oder ergeben sich aus der Prüfung Erkenntnisse, die einem Arbeitsverhältnis oder einem Auftrag entgegenstehen,

- a kann auf den Abschluss eines Arbeitsvertrags oder auf die Beauftragung verzichtet werden,
- b kann von einer bereits erfolgten mündlichen oder schriftlichen Zusage zurückgetreten werden,
- c können bei bestehendem Arbeitsverhältnis personalrechtliche Massnahmen ergriffen werden.

7 Sicherheitsorganisation

Art. 20 *Sicherheitsorganisation der kantonalen Behörden gemäss Artikel 2 Absatz 1*

¹ Der Regierungsrat regelt durch Verordnung die Organisation und die Aufgaben

- a der für gesamtkantonale Sicherheitsbelange zuständigen Organe,
- b der Sicherheitsorgane der kantonalen Verwaltung.

² Er kann diese Aufgaben Organen gemäss Artikel 21 Absatz 2 Buchstabe b des Gesetzes vom 7. März 2022 über die digitale Verwaltung (DVG)¹⁾ übertragen.

³ Die Einwohnergemeinden und gemischten Gemeinden sind in diesen Organen angemessen vertreten, soweit sie betroffen sind.

¹⁾ BSG [109.1](#)

Art. 21 *Sicherheitsorganisation der Gemeinden und der anderen Träger öffentlicher Aufgaben gemäss Artikel 2 Absatz 2*

¹ Die nicht der kantonalen Verwaltung angehörenden Behörden geben sich eine ihren Aufgaben und den damit verbundenen Sicherheitsrisiken angemessene Sicherheitsorganisation.

² Sie bezeichnen eine Person, die für die Informationssicherheit verantwortlich ist und über angemessene Kompetenzen und Ressourcen sowie eine angemessene Ausbildung verfügt.

8 Ausführungsbestimmungen

Art. 22

¹ Der Regierungsrat erlässt die Ausführungsbestimmungen durch Verordnung.

² Er kann den Erlass technischer und organisatorischer Ausführungsbestimmungen wie Standards, Sicherheitsanforderungen und Prozesse an die Finanzdirektion, ein Amt oder ein Fachorgan der Kantonsverwaltung delegieren. Er kann die Finanzdirektion dazu zum Erlass von Direktionsverordnungen ermächtigen.

³ Er bestimmt die Übergangsfristen, innerhalb derer die von diesem Gesetz und seinen Ausführungsbestimmungen vorgesehenen Massnahmen erstmals ergriffen werden müssen.

9 Schlussbestimmungen

Art. 23 *Änderung anderer Erlasse*

¹ Das Polizeigesetz vom 10. Februar 2019 (PolG)²⁾ wird geändert.

Art. 24 *Inkrafttreten*

¹ Der Regierungsrat bestimmt den Zeitpunkt des Inkrafttretens.

II.

Der Erlass [551.1](#) Polizeigesetz vom 10.02.2019 (PolG) (Stand 01.01.2023) wird wie folgt geändert:

²⁾ BSG [551.1](#)

Art. 17 Abs. 4 (aufgehoben)

⁴ Aufgehoben.

Art. 149 Abs. 4 (aufgehoben)

⁴ Aufgehoben.

Titel nach Art. 159

10.2.3 (aufgehoben)

Art. 160

Aufgehoben.

Art. 161

Aufgehoben.

Art. 162

Aufgehoben.

III.

Keine Aufhebungen.

IV.

[Abschlussklausel]

[Ort], [Datum]

[Behörde]

[Funktion 1]

[NAME 1]

[Funktion 2]

[NAME 2]