Auswertung Vernehmlassungsverfahren

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

Gesetz über die Informations- und Cybersicherheit (ICSG) (Extern)

Inhalt

1. Übersicht der Stellungnahmen

1.1 Politische Parteien

Stellungnahme	*Anzahl / GR-Sitze*	*Stellungnehmende*
Zustimmung, ggf. mit geringfügigen Anliegen	77	SVP, SP
Wesentliche Vorbehalte	18	Grüne, EDU
Bemerkungen zu einzelnen Bestimmungen	28	GLP, die Mitte
Ablehnung		
Keine Bemerkungen / Verzicht auf eine Stellungnahme		

1.2 Gemeinden

Stellungnahme	*Anzahl*	*Stellungnehmende*
Zustimmung, ggf. mit geringfügigen Anliegen	5	Steffisburg, Thun, Biel, Bern, Langenthal
Wesentliche Vorbehalte	-	-
Bemerkungen zu einzelnen Bestimmungen	1	Worb
Ablehnung	-	-
Keine Bemerkungen / Verzicht auf eine Stellungnahme	2	Ostermundigen, Zollikofen

1.3 Verbände und andere Organisationen

Stellungnahme	*Anzahl*	*Stellungnehmende*
Zustimmung, ggf. mit geringfügigen Anliegen	5	BSPV, Berner KMU, CJB, VBG
Wesentliche Vorbehalte	1	Büro GR
Bemerkungen zu einzelnen Bestimmungen	4	JL, FK, RSTA, DSA
Ablehnung		
Keine Bemerkungen / Verzicht auf eine Stellungnahme	4	Bedag, KGV, VG, CAF, Verwaltungsgericht

2. Allgemeine Bemerkungen

Nr.	Absender	Bemerkung/Forderung	Art der Berücksichtigung durch die Finanzdirektion
1.	BSPV	Dem BSPV als Personalverband ist die Informations- und Cybersicherheit sehr wichtig und begrüsst das Gesetz. Der Mehraufwand für die Sicherheit sollte für das Personal möglichst gering sein. Dies wird dann mehr bei der Umsetzung des Gesetzes zum Tragen kommen.	Kenntnisnahme.
2.	BSPV	Wir möchten aber weiterhin ein möglichst einfaches Arbeiten, ohne mehrmaliges Anmelden etc.	Kenntnisnahme. Das ist auch unser Ziel. In der Kantonsverwaltung wird es dadurch realisiert, dass gemäss den ICT-Standards alle Applikationen über die Funktion «single sign-on» verfügen müssen. Damit erfolgt die Anmeldung an der Applikation durch die Anmeldung am Arbeitsplatz.
3.	BSPV	Sollten für die Sicherheit private Geräte genutzt werden, sollte deren Einsatz pauschal entschädigt werden.	Kenntnisnahme. Das ist nicht Thema des ICSG, sondern der Personalgesetzgebung bzw. der Spesenregelung.
4.	Steffisburg	Wir haben vom Gesetzestext und dem dazugehörenden Vortrag Kenntnis genommen. Diesem stimmen wir im Grundsatz zu, zumal sich jede Gemeinde mit den Herausforderungen der Digitalisierung sowie der Informations- und Cybersicherheit auseinandersetzen muss.	Kenntnisnahme.

		Momentan überarbeitet Steffisburg die IT-Strategie. Themen rund um die Digitalisierung und die Cybersicherheit werden miteinbezogen. Wichtig und entscheidend wird schlussendlich sein, wie die Systeme von Bund, Kanton und Gemeinden untereinander interagieren.	
5.	CJB	**Prise de position du CJB** Après avoir pris connaissance du contenu de cette consultation, le CJB approuve la loi sur la sécurité de l'information et la cybersécurité sans remarque particulière sur son contenu.	Kenntnisnahme.
6.	CJB	A titre de commentaire général, le CJB relève que dans le rapport, il est mentionné que les autorités qui n'appartiennent pas à l'administration cantonale doivent se doter d'une organisation de sécurité adaptée à leurs tâches et à leurs risques. Le CJB relève que beaucoup d'institutions n'ont très certainement pas les ressources nécessaires quant à l'application de cette loi et que par conséquent, le soutien du canton s'avèrera nécessaire.	Kenntnisnahme. Grundsätzlich müssen sich alle Behörden die zur Erfüllung ihrer Aufgaben erforderlichen Mittel selbst besorgen. Weil das Gesetz aufgrund der finanziellen Rahmenbedingungen des Kantons ohne zusätzliche Ressourcen umgesetzt werden muss, sind Unterstützungsleistungen des Kantons für Behörden ausserhalb der Kantonsverwaltung nicht vorgesehen.
7.	RSTA	Die technische Entwicklung macht die entworfenen Regelungen notwendig. Wir nehmen zur Kenntnis, dass der Entwurf die klassifizierten Informationen reduziert. (...) Um den Anforderungen gerecht zu werden, und dabei den administrativen Aufwand in Grenzen zu halten, sollten die Verordnung nach dem Prinzip «so viel wie nötig, so wenig wie möglich» ausgestaltet sein.	Kenntnisnahme. Das ist auch unser Ziel.
8.	RSTA	Damit gehen wir davon aus, dass die Ausführungen im Vortrag über die Informationen, die bei den Gerichten oder Staatsanwaltschaften im Rahmen ihrer ordentlichen Verfahren bearbeitet werden, ebenso für unsere Verwaltungs- und Verwaltungsjustizverfahren gelten.	Das trifft für Verwaltungsjustizverfahren zu.
9.	Worb	Sie stellen in ihrem Vortrag an den Grossen Rat richtig fest, dass die Gemeinden nur beschränkt vom ICSG betroffen sind und sie frei sind, sich selber Informationssicherheitsregeln zu geben. Ob es für kleine und mittlere Gemeinden aber zielführend ist, das ICSG als integral anwendbar zu erklären, wagen wir zu bezweifeln.	Kenntnisnahme. Dies wird von den einzelnen Gemeinden in eigener Verantwortung zu beurteilen sein.
10.	Worb	Uns ist beispielsweise nicht klar, wie Gemeinden Personensicherheitsprüfungen vornehmen sollen, die über das Einholen von Straf- und Betreibungsregisterauszügen hinausgehen. Auch was die technischen Massnahmen betrifft, ist uns unklar, wie das beschriebene Sicherheitsverfahren in einer Gemeinde aussehen könnte.	Grundsätzlich können die Gemeinden beides, wenn sie es für angebracht halten, in der gleichen Weise tun wie kantonale Behörden, und dazu auf die Grundlagen der Kantonsverwaltung zurückgreifen.
11.	Worb	Der Gemeinderat hat keine Vorbehalte zum ICSG. Er erachtet es aber als nicht zielführend, das ICSG integral als für die Gemeinde verbindlich zu erklären. Er wird stattdessen den Verband Bernischer Gemeinden anfragen, ob er für Gemeinden nicht eine Handlungsempfehlung zum Thema Informations- und Cybersicherheit erarbeiten könnte.	Kenntnisnahme.

12.	Büro GR	Der Grosse Rat und seine Organe sind von der Vorlage, so wie sie sich gegenwärtig präsentiert, betroffen, weshalb das Büro erstaunt ist, dass es weder vorgängig konsultiert (wie z.B. Justizleitung, Finanzkontrolle oder Datenschutzaufsichtsstelle [zeitlich parallel zum Mitberichtsverfahren]) noch zumindest im Rahmen der nun laufenden Vernehmlassung direkt begrüsst worden ist. Dies umso mehr, als dass die vorgängig konsultierten Parlamentsdienste gewisse den Grossen Rat und seine Organe betreffende Punkte vorgebracht haben, welche allerdings nicht übernommen wurden, mit dem Hinweis der Finanzdirektion, das Büro könne sich im Vernehmlassungsverfahren äussern. Nebenbei sei erwähnt, dass seit dem 1. Februar 2023 eine vorgängige Konsultation des Büros vorgeschrieben und ein Einbezug schon vorher auch rechtlich ohne weiteres möglich gewesen wäre.[1]	Kenntnisnahme. Nach unserem Verständnis nimmt der Grosse Rat seine Aufgabe als Gesetzgeber im parlamentarischen Gesetzgebungsverfahren wahr, während das Vorverfahren in den Händen der Regierung liegt (Art. 88 Abs. 1 KV). Ein zu intensiver Einbezug parlamentarischer Organe in das Vorverfahren ist daher unter dem Gesichtspunkt der Gewaltenteilung u.E. problematisch. Jedenfalls im vorliegenden Fall erschien uns eine separate Konsultation des Büros vor dem Vernehmlassungsverfahren insbesondere deshalb nicht angezeigt, weil es nicht wesentlich anders betroffen ist als alle anderen Behörden. Was den von Ihnen erwähnten Art. 19 Bst. b VMV betrifft, wonach Erlassentwürfe im Mitberichtsverfahren dem Büro des Grossen Rates zur Stellungnahme vorzulegen sind, wenn der Grosse Rat oder seine Organe betroffen sind, ist darauf hinzuweisen, dass diese Bestimmung im Zeitpunkt des ersten Mitberichtsverfahrens zum ICSG, im Herbst 2022, noch nicht in Kraft war. Für zukünftige Mitberichtsverfahren, so auch für das zweite Mitberichtsverfahren zum ICSG, werden wir diese Bestimmung natürlich berücksichtigen und zusätzlich zu den Parlamentsdiensten auch das Büro zur Stellungnahme im Rahmen des Mitberichtsverfahrens einladen.
13.	Büro GR	Inhaltlich bittet das Büro, die Vorlage in verschiedener Hinsicht abzuändern, insbesondere in Bezug auf die Vorgaben des Bundes und den Geltungsbereich des ICSG – hier sind Korrekturen sowie Ausnahmen für den Grossen Rat und seine Organe nötig. Anpassungen sind auch bei der Personensicherheitsprüfung erforderlich. (...) Zusammenfassend sind der Grosse Rat und seine Organe vom Geltungsbereich dieses Gesetzes auszunehmen und ist auf die Vorgaben zur Klassifizierung von Grossratsunterlagen zu verzichten. Ferner sind die oberwähnten wichtigen Punkte zur Personensicherheitsprüfung im Gesetz selber zu normieren und ist auf Personensicherheitsprüfungen gegenüber Richterinnen und Richtern sowie dem/der (stv.) Generalstaatsanwalt/-anwältin zum Vornherein zu verzichten.	Vgl. unten zu den entsprechenden Anliegen.
14.	GLP	Die Grünliberale Partei Bern begrüsst die Einführung des Informations- und Cybersicherheitsgesetz (ICSC) und erachtet das Gesetz als ausgewogen. Der Ansatz, dass das neue ICSG das bestehende Bundesgesetz über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG), sowie die kantonalen Gesetzgebungen über die zentralen Personendatensammlungen (PDSG), die digitale Verwaltung (DVG) und die Revision des Datenschutzgesetzes (KDSG) nur punktuell ergänzt, ist sinnvoll. Damit werden neu auch die Staatsinteressen geschützt, wie dies bei den Personendaten heute bereits der Fall ist.	Kenntnisnahme.

[1] Artikel 19 Buchstabe b VMV; vgl. zudem Artikel 4 Absatz 3 Buchstabe a VMV (sowie Art. 21 alt-VMV).

		Wo liegen die Hebel? Aus dem Vortrag des Regierungsrats geht hervor, dass sich die Regierung bewusst ist, dass die Informationssicherheit zum Schutz von öffentlichen Interessen nur beschränkt eine technologische Herausforderung (Beschränkung der elektronischen Zugänge, etc.) und ein Dokumenten-Klassifizierungsproblem ist. Der wichtigste Schlüssel ist meistens trivial naheliegend und betrieblicher Natur: Sicherstellen, dass ehemalige Angestellte oder Beauftragte nach Beendigung des Vertragsverhältnisses ihren Schlüssel oder ihren Badge zurückzugeben sowie Zugänge zu Räumlichkeiten wo nötig einzuschränken. **Grundrechte** Wichtig und erkannt ist auch, dass bei der Beurteilung des Schutzbedarfs von Informationen politischer Natur besondere Zurückhaltung erforderlich ist. Die Klassifizierung darf nicht dazu dienen, bestimmte Sachverhalte der öffentlichen Debatte zu entziehen, wenn kein überwiegendes öffentliches Interesse dafür besteht. **Personensicherheitsprüfung (PSP)** Es ist sinnvoll, nur Personen, welche regelmässig mit als VERTRAULICH oder GEHEIM klassifizierten Informationen arbeiten, einer PSP zu unterziehen. Nachfolgend finden sie einige Anregungen zu konkreten Artikeln: (...)	
15.	GLP	Aus dem Vortrag des Regierungsrats geht hervor, dass sich die Regierung bewusst ist, dass die Informationssicherheit zum Schutz von öffentlichen Interessen nur beschränkt eine technologische Herausforderung (Beschränkung der elektronischen Zugänge, etc.) und ein Dokumenten-Klassifizierungsproblem ist. Der wichtigste Schlüssel ist meistens trivial naheliegend und betrieblicher Natur: Sicherstellen, dass ehemalige Angestellte oder Beauftragte nach Beendigung des Vertragsverhältnisses ihren Schlüssel oder ihren Badge zurückzugeben sowie Zugänge zu Räumlichkeiten wo nötig einzuschränken.	Kenntnisnahme. Das stimmt.
16.	Berner KMU	**Ausgangslage** Mit der Digitalisierung der Verwaltung wird die Informations- und Cybersicherheit immer wichtiger, um die zunehmenden Angriffe von Cyberkriminellen auf Verwaltungssysteme abzuwehren. Basierend auf dem von der Bundesversammlung am 18.12.2020 verabschiedete ISG (Inkrafttreten 01.04.2023) wurde im Kanton Bern festgestellt, dass die Kantonsverfassung heute in vielen Punkten die technischen, organisatorischen und rechtlichen Grundlagen fehlen. (heute nur ansatzweise und auf Normebene geregelt). Der Kanton Bern bewegt sich konsequent in Richtung E-Government und strebt das Primat der digitalen Verwaltungsführung an. Da alle kantonalen und kommunalen Behörden stark miteinander verbunden sind, kann die Informations- und Cybersicherheit nur mit einheitlichen, für alle Behörden geltenden Regeln gewährleistet werden. Zu diesem Zweck wird das ICSG erlassen. Das vorliegende Gesetz soll diese Lücken füllen. Es ergänzt: – Die Gesetzgebung über die zentralen Personendatensammlungen (PDSG) – Die digitale Verwaltung (DVG) – Die Revision des Datenschutzgesetzes (KDSG)	Kenntnisnahme.

		Zu den wesentlichen Neuerungen gehören Regeln für die oberste Führung zur Prävention, für die Klassifizierung von Informationen (anhand Risikobeurteilungsmatrix) und ICT-Mittel sowie für die Personensicherheitsprüfung (Übernahme der Regelung des Polizeigesetzes). Auch Massnahmen zur physischen und insbesondere personellen Sicherheit sind zu ergreifen, da der Mensch das grösste Risiko für die Informations- und Cybersicherheit darstellt. Das gegenüber dem ISG auf Bundesebene deutlich kürzere und übersichtlichere ICSG ist die gesetzliche Grundlage und damit die Voraussetzung für die einheitliche, umfassende, effektive und effiziente Informations- und Cybersicherheit im Kanton Bern. Es soll zusammen mit der dazugehörenden Verordnung im Verlauf des Jahres 2024 in Kraft gesetzt werden. **Stellungnahme** Im ICSG basiert auf dem ISG des Bundes, ist jedoch viel kürzer und übersichtlicher gestaltet, was zu begrüssen ist. Ebenfalls positiv ist, dass die Thematik gesamtheitlich betrachtet und Lücken im vorhandenen Regelwerk schliesst. (...) Es ist grundsätzlich unbestritten, dass die Cybersicherheit angesichts der rasch fortschreitenden Digitalisierung zunehmend an Bedeutung gewinnt. Sowohl für Behörden als auch für Unternehmen und Privatpersonen kann der Verlust, der Diebstahl, die unberechtigte Preisgabe oder der Missbrauch von Informationen schwerwiegende Folgen haben (in den Medien ist fast täglich von heiklen Leaks zu lesen). Besonders schützenswert ist dabei die so genannte kritische Infrastruktur. Aus diesem Grund ist das vorliegende Gesetz im Interesse Aller und kann unterstützt werden. Auch Behörden, die nicht Teil der kantonalen Verwaltung sind, müssen eine den Risiken angemessene Sicherheitsorganisation haben, was ebenfalls begrüssenswert ist. Das Gesetz entspricht den Richtlinien der Regierungspolitik 2023 bis 2026. Diese priorisieren für den Kanton Bern die digitale Transformation. Die finanziellen Auswirkungen sind im Rahmen des Budgets bewerkstelligbar – ebenso werden keine zusätzlichen Personalressourcen gesprochen.	
17.	Berner KMU	Im Papier sind sehr viele Detailelemente aufgeführt und es bestehen diverse Abhängigkeiten zu anderen Gesetzen, was rasch zu Komplexität führt. Es wird daher empfohlen, bei der Stellungnahme nicht im Detail auf diese Punkte einzugehen und diese auf übergeordneter Ebene abzugeben.	Kenntnisnahme. Uns ist nicht klar, worauf hier Bezug genommen wird und was genau das Anliegen der Stellungnehmenden ist.
18.	Berner KMU	Aus Sicht von Berner KMU sind folgende Punkte kritisch zu würdigen: – Mit der fortschreitenden Digitalisierung verfolgt die öffentliche Hand einerseits eine zukunftsgerichtete Stossrichtung, erhöht dabei aber gleichzeitig die Anfälligkeit für Cyberangriffe. Es stellt sich die Frage, inwieweit die Abwicklung heikler Prozesse auch «analog» (Redundanz) sichergestellt werden muss.	Kenntnisnahme. Dies ist gerade das Ziel des Gesetzes. Nach ihm müssen die Behörden Risiken für die Informationssicherheit analysieren und adressieren. Dazu gehört auch das Risiko des Verlusts der Verfügbarkeit von Informationen. Die Behörden müssen also mit einem «Business Continuity Management» (BCM) die Handlungsbereitschaft der Verwaltung auch im Krisen- oder Störungsfall sicherstellen. Dazu kann die Vorbereitung paralleler Papierprozesse gehören, oder Backups bzw. redundante Systeme, oder das Risiko kann (z.B. aus Kostengründen) bewusst akzeptiert werden.

19.	Berner KMU	– Die Klassifizierungskriterien (nicht klassifiziert / intern / vertraulich / geheim) sind nie «schwarz/weiss» - es stellt sich die Frage, wer diese Klassifizierungen final erteilen resp. unter welchen Voraussetzungen bspw. als geheim klassifizierte Dokumente weitergeben kann. Dies wird der Regierungsrat auf Verordnungsebene klären und muss dann nochmals kritisch beurteilt werden.	Kenntnisnahme. Es stimmt, dass diese Regeln auf Verordnungsebene konkretisiert werden müssen. Letztendlich hängt es aber von der Beurteilung und vom gesunden Menschenverstand der Personen ab, die Dokumente erstellen, sie angemessen zu klassifizieren.
20.	Berner KMU	– Die Hürden für die «Beauftragung Dritter» werden auf den ersten Blick stark erhöht. Dritte müssen sicherstellen, dass das Gesetz eingehalten wird. Es besteht die Gefahr, dass aufgrund der zunehmenden Komplexität nur noch Grosskonzerne Aufträge der öffentlichen Hand erhalten und KMU de facto wegfallen, da hier häufig Limitationen vorhanden sind.	Kenntnisnahme. Das ist tatsächlich ein Risiko. Die Anforderungen an Unternehmen, die sicherheitsrelevante Dienstleistungen für Dritte erbringen, steigen ständig an. Das ist aber nicht nur ein Phänomen der Verwaltung, sondern auch der Privatwirtschaft, und reflektiert letztendlich die allgemeine Zunahme der Komplexität des Wirtschaftslebens und der Informationssicherheitsbedrohungen aufgrund der Digitalisierung. Für KMU kann es auch ein Marktvorteil sein, wenn sie sich gezielt so aufstellen, dass sie diesen Anforderungen genügen, z.B. durch Kooperationen mit anderen Unternehmen.
21.	Berner KMU	Das Stichwort resp. Bemerkung «Überwachungsstaat» hat eine gewisse Berechtigung.	Kenntnisnahme. Es wird jedoch nicht dargelegt, und ist für uns auch nicht ersichtlich, welche Bestimmung des Gesetzes konkret mit einem «Überwachungsstaat» in Verbindung gebracht werden könnte.
22.	SVP	Die SVP Kanton Bern begrüsst die vorgesehene Gesetzeseinführung, welche die Informations- und Cybersicherheit verstärken und im Umgang mit Informationen sensibilisieren soll. **Grundsatz** Die digitale Verwaltungsführung ist Teil unserer Zukunft, kann nicht aufgehalten und soll nicht verhindert werden. Die Voraussetzung hierfür ist aber, dass die Sicherheit der verwendeten Informationen jederzeit gewährleistet ist. Die SVP Kanton Bern begrüsst es, dass hierfür nicht nur das Augenmerk auf die ICT-Mittel gelegt wird, sondern auch auf die physische und personelle Sicherheit. **Organisatorische Massnahmen** Die Klassifizierung und die detaillierte Beschreibung der Informationen in die Stufen ‘intern’, ‘vertraulich’ und ‘geheim’ wird als richtig und wichtig erachtet. Die entsprechende Zugänglichkeit der Daten soll durch das Gesetz gewährleistet werden. **Personelle Massnahmen** Die Anwenderin oder der Anwender der Daten stellt nach wie vor das grösste Risiko für die Datensicherheit	Kenntnisnahme.

		dar. Mit der Möglichkeit der Personensicherheitsprüfung, der restriktiven Berechtigungen und entsprechenden Schulungen kann dies verbessert und das Risiko minimiert werden. Die SVP Kanton Bern begrüsst, dass für den Gegenstand der Überprüfung die Kann-Formulierung gewählt wurde und die Informationsquellen gemäss der Sicherheitsstufe gewählt werden können.	
23.	SVP	**Allgemeine Bemerkungen** Die ausgearbeitete Gesetzeseinführung als Ergänzung und Lückenschliessung der bisherigen Grundlagen wird von der SVP Kanton Bern generell begrüsst. Die Ausformulierung des Gesetzes ist aber relativ offen formuliert und soll im Detail in der Verordnung geregelt werden. Die Begründung, dass auf die schnelllebige Entwicklung im ICT-Bereich mit einer Verordnung rascher reagiert werden kann, ist nachvollziehbar. Allerdings wären eine detailliertere Ausführung und die Bekanntgabe der Verordnung bereits zum jetzigen Zeitpunkt wünschenswert.	Kenntnisnahme. Die Verordnung liegt leider noch nicht vor, weil sie parallel zu den anderen technischen Ausführungsbestimmungen im Rahmen des kantonalen Projekts IS@BE noch erarbeitet wird.
24.	Die Mitte	**1. Grundsätzliches** Die Mitte Kanton Bern begrüsst, dass die Gesetzgebung über die Informations- und Cybersicherheit (ICSG) vereinheitlicht und mit der Gesetzgebung des Bundes abgestimmt wird. Wichtig erscheint uns, dass die Strategie der digitalen Verwaltung konsequent weiterverfolgt wird. Gleichzeitig soll die neue Gesetzgebung indes nicht in einer ausufernden Bürokratie münden (Kontrolle der Kontrolle).	Kenntnisnahme.
25.	Thun	Wir stehen der Gesetzesvorlage positiv gegenüber. Im Hinblick auf das angestrebte Primat der digitalen Verwaltung ist es wichtig, dass dem Schutz bzw. der Klassifizierung von Informationen und Personendaten die notwendige Beachtung geschenkt wird. Deren Sicherheit ist nicht zuletzt eine Voraussetzung dafür, dass die Bevölkerung und die Wirtschaft überhaupt bereit sind, den Behörden ihre Personendaten und vertraulichen Informationen anzuvertrauen. Wir begrüssen deshalb, dass mit dem Gesetz die technischen, organisatorischen und rechtlichen Grundlagen geschaffen werden für eine ganzheitliche Regelung der Informations- und Cybersicherheit.	Kenntnisnahme.
26.	DSA	Vorweg nehmen wir mit Befriedigung zur Kenntnis, dass die überwiegende Mehrzahl unserer Anträge und Hinweise im ersten Mitberichtsverfahren berücksichtigt und umgesetzt wurden, und danken Ihnen dafür.	Kenntnisnahme.
27.	DSA	Auf Hinweis der Direktion für Inneres und Justiz haben wir zusammen mit dessen Rechtsamt und dem KAIO die Frage des Geltungsbereichs des ICSG und dessen Abstimmung mit dem Geltungsbereich des revidierten Datenschutzgesetzes (KDSG) vertieft geprüft. Ein erster Entwurf für das revidierte KDSG hatte vorgesehen, zum Thema Datensicherheit pauschal auf die Gesetzgebung über die Informations- und Cybersicherheit zu verweisen; gemäss Vorentwurf für das ICSG soll dieses aber für Gemeinden und «andere» Träger öffentlicher Aufgaben (d.h. weder Parlament, Regierungsrat/Verwaltung noch Gerichte) – welche ebenfalls dem KDSG unterstehen – nur sehr beschränkt anwendbar sein. Die Prüfung hat ergeben, dass der Geltungsbereich des ICSG keiner Anpassung bedarf, sondern dass es angezeigt ist, im KDSG die Grundsätze der Art. 5 bis 7 ICSG für alle dem KDSG unterstellten Behörden als sinngemäss anwendbar zu erklären.	Kenntnisnahme. Das halten wir für sinnvoll, weil die dort beschriebenen Grundsätze und Methoden auch für den Datenschutz fundamental sind.

28.	Grüne	Die GRÜNEN begrüssen die Einführung eines neuen Gesetzes zur Regelung der Aufgaben, Verfahren und Kompetenzen im Bereich Cybersicherheit im Kanton Bern. Auch auf nationaler Ebene haben sich die GRÜNEN für eine starke Behörde in diesem Bereich engagiert und haben sogar die Frage in den Raum gestellt, ob es nicht ein eigenes Bundesamt oder Staatssekretariat zu diesem Thema bräuchte (Vorstoss 21.4389 / Interpellation Gerhard Andrey). Aus Sicht der GRÜNEN ist es zentral, dass seitens der Politik Sicherheit im digitalen Raum ernst genommen wird und die Behörden Datensicherheit als hohe Priorität ansehen. Nur so kann den grossen demokratiepolitischen Risiken, welche Cyberangriffe mit sich bringen, angemessen begegnet werden.	Kenntnisnahme.
29.	Grüne	Zu den Bestimmungen im vorliegenden Gesetzesentwurf äussern sich die GRÜNEN wie folgt: – Allgemein: Entgegen den im Bericht gemachten Aussagen (10. Finanzielle Auswirkungen; 11. Personelle und organisatorische Auswirkungen) sind wir nicht überzeugt, dass dieses Gesetz mit den bestehenden bzw. geplanten, für die ICT und die Digitalisierung vorgesehenen Finanzmittel umsetzbar ist. Einerseits ist es richtig, dass mit dem ICSG keine grundsätzlich neue staatliche Aufgabe eingeführt wird. Andererseits sind wir der Meinung, dass die Anforderungen durch das ICSG viel höher sind als durch die bestehenden Regulierungen. Die GRÜNEN fordern deshalb, dass genügend (Personal-) Ressourcen, für die im neuen Gesetz ausdifferenzierten Aufgaben zur Verfügung gestellt werden. Die Inventarisierung von Informationen und die Abklärung des Schutzbedarfs gemäss Art. 5, aber auch technische Verfahren, Vorsorge und der Umgang mit tatsächlichen Vorfällen, erfordert sicher teilweise zusätzliche Ressourcen, ansonsten ist eine seriöse Umsetzung des vorliegenden Gesetzes nicht vorstellbar. Dies umso mehr, als dass höhere Sensibilität, bessere Übersicht und Inventarisierung zwingend auch dazu führen sollte, dass mehr Vorfälle gemeldet werden, die heute gar nicht entdeckt werden.	Kenntnisnahme. Der Regierungsrat hat mehrmals darauf hingewiesen, dass sich aus der Digitalisierung durchaus Mehr- bzw. Zusatzaufgaben ergeben, wozu auch mehr Cybersicherheitsaufwand gehört. Er will dies aber dadurch ermöglichen, dass er dafür die Effizienzgewinne einsetzt, welche die Digitalisierung ermöglicht (s. namentlich den Bericht des Regierungsrates zur Motion 100-2021 FDP (Reinhard, Thun) «Informatikoffensive des Kantons Bern – Konsequenzen für den Stellenplan»). Damit verfolgt er einen Mittelweg zwischen der seiner Meinung nach nicht realistischen Forderung, mit ICT-Vorhaben primär Einsparungen zu realisieren, und der seiner Meinung nach finanzpolitisch ebenfalls nicht realistischen Forderung, für die Digitalisierung in wesentlichem Umfang Zusatzausgaben zu tätigen.
30.	FK	Wir danken Ihnen für die Gelegenheit zur Stellungnahme. Wir haben uns bereits anlässlich des Mitberichtsverfahrens ausführlich zu dieser Vorlage geäussert und verweisen für unsere nicht berücksichtigten Anträge auf unsere Stellungnahme vom 3. November 2022.	Kenntnisnahme.
31.	Langenthal	Wir danken Ihnen für die anerbotene Gelegenheit zur Teilnahme und können Ihnen mitteilen, dass die Stadt Langenthal die geplante Vorlage und insbesondere das Interesse an einem einheitlichen Sicherheitsraum zustimmend zu Kenntnis nimmt. (...) Gerne nimmt die Stadt Langenthal auch an der Vernehmlassung der Verordnung zum Gesetz teil und betont die Wichtigkeit des weiteren Einbezugs der Gemeinden für eine erfolgreiche Umsetzung.	Kenntnisnahme.
32.	Langenthal	Im Bereich der Informationssicherheit hat die Stadt Langenthal bereits erste Massnahmen ergriffen. Aufgrund der in diesem Rahmen gemachten Erfahrungen, wäre es aus unserer Sicht sehr begrüssenswert, wenn der Kanton, im Sinne der Wirtschaftlichkeit und Zweckmässigkeit, generische Grundlagen und Basisdienstleistungen zur Verfügung stellen könnte. Damit würde verhindert, dass die Gemeinden diese aufwändig eigenständig erarbeiten müssen.	Kenntnisnahme. Es ist vorgesehen, alle für die Umsetzung des ICSG erarbeiteten Grundlagen öffentlich und damit auch den Gemeinden zur Verfügung zu stellen.

33.	Langenthal	Überdies bleibt anzumerken, dass im Rahmen der Erarbeitung von Gesetzen in Zusammenhang mit der fortschreitenden Digitalisierung auch die Einhaltung der Löschungspflicht gemäss der geltenden Datenschutzgesetzgebung und insbesondere die technische Umsetzung (mit Blick auf Backups) geprüft werden sollte.	Kenntnisnahme. Die Löschung nicht mehr benötigter Daten ist auch ein Gebot des Datenschutzes und wird Thema der Ausführungsbestimmungen sein.
34.	Biel / Bienne	Afin de maîtriser les coûts, le texte de loi propose aux communes et autres organisations chargées de tâches publiques d'« arrêter des mesures de sécurité ciblées et adaptées aux risques et en créant des synergies avec d'autres communes et avec l'administration cantonale ».	Kenntnisnahme.
35.	Biel / Bienne	Concernant les coûts générés par la sécurité de l'information, le Canton indique qu'ils pourront être réduits ou optimisés grâce, notamment, aux synergies avec d'autres communes et avec l'administration cantonale. Le Conseil municipal est intéressé de connaître les synergies déjà en place et les possibilités pour les communes d'utiliser des outils de l'administration cantonale.	Kenntnisnahme. Voir le point 32 ci-dessus.
36.	EDU	Grundsätzlich beurteilt die EDU Kanton Bern das Gesetz über die Informations- und Cybersicherheit in der vorliegenden Form kritisch. Ohne wichtige Anpassungen dürfte es einen zu grossen administrativen und damit auch finanziellen Mehraufwand auslösen, was in keinem Verhältnis zu einem allfälligen Zusatznutzen steht. Die EDU Kanton Bern bittet den Regierungsrat, transparenter darzulegen, welche Vorgaben tatsächlich aufgrund von Bundesrecht in einem kantonalen Gesetz umgesetzt werden müssen.	Kenntnisnahme. Dies ergibt sich aus Art. 3 ISG: «[1] Für die Kantone gelten nur die Bestimmungen: a. über klassifizierte Informationen, soweit sie klassifizierte Informationen des Bundes bearbeiten; und b. über die Sicherheit beim Einsatz von Informatikmitteln, soweit sie auf Informatikmittel des Bundes zugreifen. [2] Diese Bestimmungen gelten nicht, wenn die Kantone eine mindestens gleichwertige Informationssicherheit gewährleisten.» Wegen des Abs. 2 ist es im Interesse des Kantons Bern, ein inhaltlich gleichwertiges eigenes Gesetz zu erlassen, weil er sonst im Umfang des Abs. 1 das deutlich bürokratischere und kompliziertere ISG des Bundes umsetzen müsste.
37.	EDU	Zudem sollen wichtigen Bestimmungen zwingend auf Gesetzesstufe geregelt werden. Die EDU Kanton Bern teilt im Übrigen die Einschätzung des Regierungsrates, dass das grösste Sicherheitsrisiko beim Endnutzer und dessen Umgang mit sensiblen Daten liegt. Allenfalls könnte im Gesetz die Sensibilisierung der Mitarbeitenden besser aufgegriffen werden.	Nicht umgesetzt. Mangels eines konkreten Formulierungsvorschlags und einer Begründung verzichten wir auf eine entsprechende Anpassung des Gesetzes. In diesem wollen wir nicht einzelne Sicherheitsmassnahmen nennen. Die Sensibilisierung der Mitarbeitenden gehört aber sicher zu den risikoangemessenen Massnahmen, welche die verantwortlichen Behörden ergreifen müssen.
38.	SP	Die SP begrüsst das Gesetz über die Informations- und Cybersicherheit. Die Informations- und Cybersicherheit ist ein sehr wichtiger Aspekt für den Kanton Bern. Mit der zunehmenden Digitalisierung muss die Kantonsverwaltung besser geschützt werden vor Angriffen auf die Verwaltungssysteme. Die SP Kanton Bern begrüsst somit, dass hier eine Lücke geschlossen wird. Der SP Kanton Bern ist dabei wichtig, dass	Kenntnisnahme.

		der Datenschutz effizient und qualitativ hochwertig ist. Gleichzeitig darf er aber nicht dazu dienen, bestimmte Sachverhalte der öffentlichen Debatte zu entziehen. Für die SP Kanton Bern ist deshalb entscheidend, dass in jedem Fall das Öffentlichkeitsprinzip gewahrt bleibt.	
39.	Bern	Die Stadt Bern begrüsst die Einführung eines Gesetzes über die Informations- und Cybersicherheit auf Kantonsebene. Der vorgeschlagene Entwurf ist aus seiner Sicht eine sinnvolle Ergänzung zu den bereits heute bestehenden gesetzlichen Regelungen über die zentralen Personendatensammlungen (PDSG), die digitale Verwaltung (DVG) sowie die Revision des Datenschutzgesetzes (KDSG). Das ICSG schafft die Grundlage für ein gesamtes Regelwerk zur Steuerung und Führung der Informations- und Cybersicherheit des Kantons Bern. Für die Gemeinden und andere autonome Träger öffentlicher Aufgaben gilt das ICSG nur, soweit sie klassifizierte Informationen des Kantons oder des Bundes bearbeiten oder ihre ICT-Mittel nutzen. Im Interesse konsequenter Anschlussfähigkeit und Interoperabilität sind die städtischen Strategien, Konzepte und Erlasse mit der kantonalen Rechtssetzung weitgehend harmonisiert. Dies betrifft namentlich die Digitalstrategie Stadt Bern 2030, die Strategie Sourcing und Cloud Computing 2022, das Klassifizierungskonzept 2023 (inkl. Weisungen) und die Cyberstrategie 2024 (in Arbeit).	Kenntnisnahme.
40.	VBG	Zum Inhalt des Gesetzes hat der VBG keine Bemerkungen. Dass eine rechtliche Grundlage für die Informations- und Cybersicherheit geschaffen wird, ist unbestritten. Auch sind die vorgeschlagenen materiellen Regelungen nachvollziehbar.	Kenntnisnahme.

3. Bemerkungen zum ICSG

Art. 1

Nr.	Absender	Bemerkung/Forderung	Art der Berücksichtigung
41.	GLP	Wir stellen in Frage, ob es den Buchstaben Art. 1 Abs. 2 lit. c braucht. Die Erfüllung einer gesetzlichen Pflicht scheint uns kein alleinstehendes öffentliches Interesse zu sein. Auf Nachfrage wurden wir informiert, dass es bei Art. 1 Abs. 2 lit. c um das Verhältnis mit Dritten geht, sofern sie kantonale Ressourcen benutzen. Auch in Zusammenhang mit Dritten scheint uns dies wenig verständlich formuliert und nicht in die Aufzählung der öffentlichen Interessen passend. Viel eher sollte in Abs. 1 ergänzt werden, dass es nicht nur für Behörden, sondern auch für genannte Dritte Geltung hat – sofern dies gewünscht ist.	Nicht umgesetzt. Die Regelung entspricht der des ISG. Der Bundesrat begründet sie wie folgt: «[Damit] wird der Bereich Compliance, d. h. die Einhaltung der gesetzlichen und vertraglichen Verpflichtungen der Bundesbehörden zum Schutz von Informationen erfasst, die nicht unter die Buchstaben a–d fallen. Die Bundesbehörden bearbeiten zur Erfüllung ihrer gesetzlichen Aufgaben sehr viele Informationen, die sie aufgrund verschiedenster gesetzlicher Bestimmungen schützen müssen (DSG, RVOG, ParlG, NBG, BÖB, FHG usw.) oder die sie von Dritten nur unter der Bedingung der Gewährleistung eines angemes-

			senen Schutzes erhalten. Berufs-, Geschäfts- und Fabrikationsgeheimnisse oder die Wahrung der Vertraulichkeit und Integrität von Personendaten stellen zwar keine unmittelbaren Eigeninteressen des Bundes dar. Der Bund ist aber entweder gesetzlich oder durch Vereinbarung verpflichtet, diese Informationen zu schützen. Wenn bekannt wird, dass die Bundesbehörden ihre Verpflichtungen zum Schutz dieser Informationen nicht einhalten, kann ihre Vertrauenswürdigkeit erheblich darunter leiden und der Bund zur Verantwortung gezogen werden. Buchstabe e stellt somit ein Auffangbecken für alle Informationen dar, welche die Bundesbehörden bearbeiten und schützen, aber nicht unbedingt klassifizieren müssen. Er schützt überdies das Interesse der Bundesbehörden an der Aufrechterhaltung ihrer hohen Vertrauenswürdigkeit» (BBl 2017 3011 f.)
42.	DSA	Einen Änderungsantrag haben wir dennoch anzubringen: In unserem Mitbericht vom 08.11.2022 hatten wir beantragt, Art. 1 Abs. 1 ICSG sei wie folgt (oder sinngemäss) zu ändern: «Dieses Gesetz sollgewährleistet … gewährleisten». Erst die Umsetzung des Gesetzes kann nämlich die Informationssicherheit gewährleisten, nicht das Gesetz selbst. Deshalb ist die gleiche Formulierung zu wählen wie im Informationssicherheitsgesetz des Bundes (ISG). Obwohl in der Auswertung des Mitberichtsverfahrens zuhanden des Regierungsrates steht, dass jener Antrag umgesetzt wurde, enthält der Vernehmlassungsentwurf immer noch den früheren Wortlaut, was zweifellos nur ein Versehen darstellt. Wir bitten deshalb darum, dies in der Endversion zu korrigieren.	Umgesetzt.

Art. 2

Nr.	Absender	Bemerkung/Forderung	Art der Berücksichtigung
43.	Langenthal	Gleichzeitig möchten wir Sie darauf aufmerksam machen, dass insbesondere die Umsetzung von Art. 2 Abs. 2 eine grosse operative Herausforderung darstellt: Die Trennung der Informationen des Kantons oder des Bundes von denjenigen der Stadt Langenthal dürfte mit einigem Aufwand verbunden sein. Ohne die Trennung führt Art. 2 indes dazu, dass die Bestimmungen ohne Ausnahmen auch für die Gemeinden und andere Träger öffentlicher Aufgaben gelten.	Kenntnisnahme. Es wird meistens nicht möglich bzw. sinnvoll sein, Informationen des Kantons bzw. des Bundes einerseits und solche der Gemeinden strikt voneinander zu trennen. Es stimmt, dass dies zur Folge hat, dass das ICSG damit in der Praxis möglicherweise auch auf Gemeindeinformationen Anwendung findet. S. Ziff. 45 unten.
44.	EDU	*Zu einzelnen Artikeln:* Art. 2 und Art. 8 (Geltungsbereich und Klassifizierung) – Der Grosse Rat und seine Organe sind von dem Klassifizierungssystem auszunehmen. Für den Grossen Rat hat sich die Unterscheidung zwischen zugänglichen und nicht-zugänglichen Informationen bewährt; ohne Ausnahmeregelung befürchten wir, dass die bisher einfache Handhabung, welche dem Milizsystem entspricht, unnötigerweise verloren geht.	S. Ziff. 46 unten.

45.	VBG	Umfassender Klärungsbedarf besteht jedoch bezüglich der Anwendung des Gesetzes auf bzw. durch die Gemeinden. Das ICSG soll einerseits nur beschränkt auf die Gemeinden angewendet werden (Art. 2 Abs. 2). Andererseits ist es so, dass dann, wenn das ICSG für die Gemeinden doch zur Anwendung kommt, die Vorgaben des ICSG im Grundsatz voll gelten. Dabei darf aber nicht übersehen werden, dass Fälle, in denen das ICSG tatsächlich zur Anwendung kommt, nicht selten sind und in Zukunft voraussichtlich massiv zunehmen werden. Mit anderen Worten: Ob es sachlich gerechtfertigt war, nach anfänglich anderer Gesetzeskonzeption die kommunale Ebene grundsätzlich aus dem Geltungsbereich auszuschliessen, ist fraglich. In wesentlichen Zusammenhängen erfolgt nun eine Ausdehnung auf die Gemeinden auf andere Weise. Realistischerweise ist davon auszugehen, dass die Gemeinden beispielsweise bezüglich der «Sicherheit beim Einsatz von ICT-Mitteln» (Art. 2 Abs. 2 Bst. b) generell die Anforderungen zu erfüllen haben werden, welche der Kanton an sich selbst stellt. Eine Gemeinde kann nicht zwei verschiedene ICT-Infrastrukturen betreiben – eine, welche den Zugriff auf kantonale oder Bundesmittel erlaubt, und eine andere. Inhaltlich ist es nicht falsch, dass auch auf kommunaler Ebene der Informations- und Cybersicherheit angemessene Beachtung geschenkt wird. Die Gemeinden benötigen jedoch eine entsprechende Unterstützung und Richtschnur, wenn der Kanton verlangt, dass sie in wesentlichen Bereichen dann doch die kantonalen Standards erfüllen müssen. Der VBG fordert deshalb, dass im Rahmen der Verordnung detailliert geregelt wird, was insbesondere die Pflicht zur Klassifizierung und zur Sicherheit beim Einsatz von ICT-Mitteln bedeutet und welche Anforderungen hier im Einzelnen von den Gemeinden zu erfüllen sind. Ebenso hat die Verordnung die Anforderungen an die Sicherheitsorganisation der Gemeinden (Art. 21) detailliert zu beschreiben. In die Erarbeitung der entsprechenden Verordnungsregelungen kommunale Vertretungen eng einzubeziehen, damit die Bedürfnisse der Gemeinden realistisch einfliessen können.	Kenntnisnahme. Wir teilen die Einschätzung, dass es in der Praxis oft am einfachsten sein wird, das ICSG auf alle ICT-Systeme der Gemeinden anzuwenden. Formell betrifft diese Pflicht aber nur kantonale bzw. Bundesinformationen. Daher und aus Ressourcengründen wird es dem Kanton nicht möglich sein, die Gemeinden bei der Anwendung des ICSG umfassend zu unterstützen. Die Verordnung wird Fragen der Klassifizierung näher regeln, und wir ziehen gerne auch eine Vertretung der Gemeinden zur Erarbeitung bei. Eine detaillierte Regelung der Sicherheitsorganisation der Gemeinden ist aber mit Rücksicht auf die Organisationsautonomie der Gemeinden nicht vorgesehen.
46.	Büro GR	Weiter bittet das Büro, den **Grossen Rat und seine Organe** sowohl in **Artikel 2 ICSG** als auch in **Artikel 8 ICSG** wie folgt **vom Geltungsbereich auszunehmen** (vgl. nachfolgend Unterstrichenes [Tabelle im Vortrag auf S. 8 erwähnt selber zum integralen Geltungsbereich einzig die Kantonsver-waltung]): **Art. 2 ICSG** *Geltungsbereich* [1]Dieses Gesetz gilt für die kantonalen Behörden, mit Ausnahme des Grossen Rates und seiner Organe, 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. [3]Die Informations- und Cybersicherheit für den Grossen Rat und seine Organe richtet sich nach der Grossratsgesetzgebung. *(Kommentar: GRG/GO regelt diese Bereiche damit selber und abschliessend, weshalb es nicht zu einer ergänzenden Anwendung des ICSG nach Art. 3 Abs. 2 E-ICSG kommen kann)*	Nicht umgesetzt. Das Büro beantragt hier die Ausnahme des Grossen Rates vom Geltungsbereich des ICSG sowohl insgesamt (Art. 2) wie auch spezifisch in Bezug auf die Klassifizierung (Art. 8). Dieser Antrag ist so nicht sinnvoll: Wenn der Grosse Rat in Art. 2 insgesamt vom Geltungsbereich des ICSG ausgeschlossen würde, gälte dies auch für Art. 8, weshalb eine weitere Ausnahmenorm dort keinen Sinn ergeben würde. Daher verstehen wir den Antrag zu Art. 8 als Eventualantrag. Wir gehen hier auf den Antrag zu Art. 2 ein, und weiter unten (Ziff. 53) auf den Antrag zu Art. 8. Der Antrag zu Art. 2 (vollständige Ausnahme des Grossen Rates von der Anwendung des ICSG) wird in der Vernehmlassung nicht begründet, ist aus unserer Sicht aber aus folgenden Gründen nicht umzusetzen: Der Grosse Rat sollte als Gesetzgeber auch eine Vorbildfunktion wahrnehmen. Es wäre u.E. politisch schwer vermittelbar, wenn der Grosse Rat sich selbst als einzige Behörde

			im Kanton von der Pflicht entbindet, eine professionelle Informationssicherheit sicherzustellen, die er gleichzeitig allen anderen Behörden auferlegt. Daran ändert u.E. auch die Tatsache nichts, dass der Grosse Rat ein Milizparlament ist. – Denn erstens wird er von professionellen Parlamentsdiensten unterstützt, welche die Umsetzung des ICSG sicherstellen können und müssen. – Zweitens hat der Grosse Rat viel Spielraum, das ICSG im Sinne seiner bisherigen Praxis umzusetzen, da fast alle Massnahmen auf der Risikobeurteilung der verantwortlichen Behörde beruhen. – Drittens setzt die Mitnutzung der kantonalen ICT-Grundversorgung durch den Grossen Rat voraus, dass der Grosse Rat auch die für die ganze Kantonsverwaltung geltenden Sicherheitsvorschriften einhält, denn sonst stellen die von den Mitgliedern und Angestellten des Grossen Rates genutzten PCs ein Sicherheitsrisiko für die ganze Kantonsverwaltung bzw. ein Einfallstor für Angreifer dar. – Und viertens kann es für die zu schützenden öffentlichen Interessen (Art. 2 ICSG) keinen Unterschied machen, ob die zu schützenden Informationen vom Grossen Rat oder von einer anderen Behörde bearbeitet werden, denn dies ändert nichts an den Risiken, die sich als Folge eines unsicheren Umgangs mit Informationen verwirklichen können. Daher ist der Grosse Rat ja wie alle Behörden auch dem Amtsgeheimnis und dem Datenschutzgesetz unterstellt. Aus diesen Gründen halten wir daran fest, dass aus unserer Sicht der Grosse Rat wie alle anderen Behörden dem ICSG unterstellt sein sollte, wie dies übrigens auch auf Bundesebene für die Bundesversammlung der Fall ist.
Art. 4			
Nr.	Absender	Bemerkung/Forderung	Art der Berücksichtigung
47.	GLP	Im Gesetz ist oft die Rede von «Bearbeitung». Die Definition, was unter Bearbeitung zu verstehen ist, bleibt dabei aus. Insbesondere im Hinblick darauf, dass das Gesetz in der Verwaltung von einem breiten Publikum verstanden werden soll, ist eine diesbezügliche Definition wünschenswert. Dabei ist dringend zu empfehlen, die «Bearbeitung» breit zu definieren, etwa analog des Art. 3 lit. e DSG. (siehe dazu auch Kommentar zu Art. 14).	Umgesetzt durch Anpassung des Vortrags. Es trifft zu, dass der Begriff der «Bearbeitung» im ICSG die gleiche breite Bedeutung hat wie im DSG bzw. KDSG: «Das Bearbeiten von Personendaten umfasst jeden Umgang mit

			Personendaten, wie das Beschaffen, Aufbewahren, Verändern, Verknüpfen, Bekanntgeben oder Vernichten» (Art. 2 Abs. 4 KDSG). Weil das ISG aber auf die Definition des Begriffs verzichtet, halten wir es im ICSG gleich. Wir erläutern den Begriff jedoch im Vortrag (Ziff. 2.3).

Art. 5

Nr.	Absender	Bemerkung/Forderung	Art der Berücksichtigung
48.	Die Mitte	**2. Bemerkungen zu den einzelnen Bestimmungen** ***Art. 5:*** *Pflichten der Behörden zur Informations- und Cybersicherheit* *Abs. 2: Bst. d (neu einzufügen): Verdachtsfälle abklären und entsprechende Massnahmen einleiten.* Begründung: Der Umgang mit Verdachtsfällen darf nicht vernachlässigt werden und soll ebenfalls ins Gesetz aufgenommen werden. Den Mitarbeitenden soll klar sein, wie sie mit Unregelmässigkeiten umgehen müssen und wo sie solche deponieren können.	Nicht umgesetzt. Das Anliegen ist natürlich berechtigt. U.E. ergibt sich dies jedoch bereits aus Abs. 2 Bst. a und b («a die Risiken für die Informationssicherheit laufend beurteilen, b die erforderlichen Massnahmen treffen, um die Risiken zu vermeiden (...)»). Zu diesen erforderlichen Massnahmen gehört auch ein angemessenes Meldeverfahren für Probleme im Sicherheitsbereich. Es scheint uns methodisch nicht stufengerecht, alle denkbaren Massnahmen hier auf Gesetzesstufe zu nennen. Neben der Meldung von Problemen gehören dazu noch sehr viele andere Massnahmen. In dieser Bestimmung geht es nur um die Grundmechanik des Risikomanagements. Die Festlegung der (Mindest-)Massnahmen ist dann Sache des Regierungsrates auf Verordnungsebene, bzw. der zuständigen Behörden im Einzelfall.

Art. 8

Nr.	Absender	Bemerkung/Forderung	Art der Berücksichtigung
49.	JL	**Klassifizierung** Im Grundsatz unterstützen wir die Regelung zur Klassifizierung in Art. 8 ICSG. Das Verhältnis zum KDSG sollte jedoch konkretisiert werden. Wie der Vortrag richtig ausführt, bearbeiten die Gerichtsbehörden und die Staatsanwaltschaft eine grosse Zahl besonders schützenswerter Personendaten. Wir begrüssen, dass deren Bearbeitung keine Klassifizierung begründet (Vortrag, S. 15), sprechen uns aber klar dafür aus, dies im Gesetz festzulegen.	Nicht umgesetzt. Unserer Meinung nach ergibt es sich klar genug aus dem Gesetz, dass die Klassifizierung eine Frage der auf dem Spiel stehenden öffentlichen Interessen ist, und nicht eine Frage des Datenschutzes. Daher, und weil das ISG sich dazu auch nicht äussert, verzichten wir auf eine solche Klarstellung im Gesetz.
50.	JL	Aus der Abbildung 8 im Vortrag ergibt sich eine Gleichsetzung der besonders schützenswerten Personendaten mit der Klassifizierungsstufe «Vertraulich» und der Sicherheitsstufe «Hoher Schutz». Ein Grossteil der durch die Gerichtsbehörden und die Staatsanwaltschaft bearbeiteten Informationen wäre folglich diesen	Kenntnisnahme. Der vermeintliche Widerspruch besteht nicht: Die Klassifizierung von Informationen zum Schutz öffentlicher Interessen,

		Stufen gleichzusetzen. Dies steht in einem gewissen Widerspruch dazu, dass eine Klassifizierung nach Art. 8 Abs. 3 ICSG nur in Ausnahmefällen Anwendung findet. Die praktischen Auswirkungen der Gleichsetzung von schützenswerten Personendaten, Informationen und ICT-Mitteln sind unseres Erachtens noch zu wenig greifbar. Der Vorlage lässt sich lediglich entnehmen, dass der Regierungsrat auf dieser Basis einheitliche Schutzstufen und -massnahmen definieren kann (Art. 11 Abs. 5 ICSG; Vortrag, S. 20).	wie im ICSG vorgesehen, soll tatsächlich die Ausnahme sein, und auch in der Justiz werden wohl kaum je Akten aus diesen Gründen zu klassifizieren sein (auch vor dem Hintergrund des Grundsatzes der Justizöffentlichkeit). Der erhöhte Schutzbedarf der Justizakten ergibt sich vielmehr aus dem Privatinteresse der an Justizverfahren Beteiligten am Schutz ihrer Privatsphäre und ihrer Geheimnisse. Aus diesen Gründen, und nicht wegen einer Klassifizierung, werden wohl tatsächlich die meisten Justizakten einer hohen Schutzstufe zuzuordnen sein.
51.	Grüne	Art. 8 Klassifizierung: Die Klassifizierung von Dokumenten ausserhalb von Regierungsratsgeschäften wird in diesem Gesetz neu eingeführt. Angesichts der Bedeutung einer Klassifizierung für die Zugänglichkeit zu einer Information und damit auch für die Wahrung demokratischer Rechte, sind Kriterien für und Handhabung der Klassifizierung, auch welche Verwaltungsbereiche alle betroffen sind, ziemlich spärlich umschrieben. Die GRÜNEN fordern, dass dieser Bereich ausgebaut wird und klare Kriterien angelehnt an nationale Regelungen eingeführt werden. Dabei ist insbesondere auch darauf zu achten, dass möglichst wenige Dokumente klassifiziert werden sollen. Es wäre auch hilfreich, wenn der Gesetzgeber den Verordnungsentwurf kennen würde, bevor über das Gesetz entschieden wird.	Nicht umgesetzt. Wie auf Bundesebene halten wir es für sachgerecht, die Regeln für die Klassifizierung nicht im Detail auf Gesetzesstufe zu regeln, weil auf dieser Stufe den sehr unterschiedlichen Geschäftsfällen der Verwaltung nicht genügend Rechnung getragen werden kann. Dies soll vielmehr pro Organisationseinheit in einem Klassifizierungskatalog erfolgen (s. Ziff. 54 unten).
52.	EDU	Art. 2 und Art. 8 (Geltungsbereich und Klassifizierung) – Der Grosse Rat und seine Organe sind von dem Klassifizierungssystem auszunehmen. Für den Grossen Rat hat sich die Unterscheidung zwischen zugänglichen und nicht-zugänglichen Informationen bewährt; ohne Ausnahmeregelung befürchten wir, dass die bisher einfache Handhabung, welche dem Milizsystem entspricht, unnötigerweise verloren geht.	S. Ziff. 53 unten.
53.	Büro GR	**Art. 8 ICSG** Klassifizierung [1]Die Behörden nach Artikel 2 ICSG klassifizieren … (bis Absatz 4 weiter wie bisher) [5]Die Informations- und Cybersicherheit für den Grossen Rat und seine Organe richtet sich nach der Grossratsgesetzgebung. Begründung: Nach Artikel 2 E-ICSG würden die Vorgaben des ICSG, namentlich die Pflicht zur Einführung eines förmlichen Klassifizierungssystems (gemäss den Vorgaben von Art. 8 E-ICSG) auch für den Grossen Rat gelten (da Art. 72 ff. vom 5. Titel KV [Art. 66 – 100 KV] miterfasst ist). Details würden sich zudem aus einer regierungsrätlichen Verordnung ergeben (vgl. Art. 8 Abs. 4 E-ICSG). Ein solches Regime (mit drei Klassifizierungsstufen und der Annahme, eine Klassifizierung solle die Ausnahme sein) passt in keiner Art und Weise auf **Informationen und Unterlagen des Grossen Rates**: Für den Grossen Rat ist einzig zwischen **zugänglichen** und **nicht-zugänglichen** Informationen und Unterlagen zu unterscheiden, was sich seit Jahren bewährt hat und was im Besonderen miliztauglich ist.[2] Der Gesetzgeber hat damit die erforderliche Interessenabwägung (Art. 17 Abs. 3 KV) bereits vorgenommen (und eben bei den nicht-zugänglichen	Nicht umgesetzt. Wie oben erwähnt (Ziff. 7) verstehen wir diesen Antrag als Eventualantrag zu dem Antrag betreffend Art. 2, weil er als kumulativer Antrag keinen Sinn ergäbe. Die hier vorgebrachte Begründung rechtfertigt die Ausnahme des Grossen Rates von den Klassifizierungsvorschriften u.E. nicht: Art. 8 ICSG zwingt den Grossen Rat in keiner Weise, seine bisherige Praxis der Unterscheidung zwischen öffentlichen und nicht öffentlichen Unterlagen aufzugeben. Denn alle öffentlichen Unterlagen sind nicht klassifiziert, und alle nicht öffentlichen Unterlagen sind (neu) klassifiziert. Neu ist nur,

[2] Nach Grossratsgesetzgebung gilt als Regel, dass Sitzungen/Sitzungsberatungen und Unterlagen der Ratsorgane *nicht-öffentlich/vertraulich/geheim* sind (Terminologie ist uneinheitlich, gemeint ist immer dasselbe [Nichtzugänglichkeit] vgl. Art. 12 GRG i.V. mit Art. 4 IG, Erläuterungen im Vortrag zu Art. 12 GRG, Art. 48 Abs. 4 GO, Richtlinie Grosser Rat S. 21; vgl. auch Kommissionsreglemente mit abgestuften Vorgaben für den Geheimnisschutz wie z.B. zu Einschränkung Adressatenkreis/Örtlichkeit/Verfügbarkeit etc.]). Sitzungen/Beratungen und Unterlagen des Plenums sind hingegen i.d.R. *öffentlich* zugänglich (Art. 11 GRG). Die Grossratsgesetzgebung erlaubt dabei gewisses Zugänglichmachen (z.B. Unterlagen zu Erlassen nach dem Inkrafttreten, vgl. Art. 48 Abs. 1 GO).

		Informationen der Ratsorgane das öffentliche Interesse an deren Schutz höher gewichtet als andere Interessen [insb. damit die freie Meinungs- und Willensbildung sowie die Kompromissfindung gewährleistet bleibt), weshalb sich eine **Einzelfallprüfung und Detailklassifizierungen erübrigen**.[3]	dass der Grosse Rat innerhalb der Kategorie der nicht öffentlichen Unterlagen festlegen muss, welche Unterlagen INTERN, VERTRAULICH oder (was wohl nie der Fall sein dürfte) GEHEIM sind. Dazu kann und muss er sich selbst Regeln geben, damit diese Klassifizierung einheitlich erfolgt (s. nachstehend). Dies überfordert den Grossen Rat bzw. die Parlamentsdienste u.E. nicht. Gegen die hier beantragte Ausnahme spricht aber vor allem, dass die meisten Sicherheitsmassnahmen an der Schutzstufe der Informationen ansetzen werden, welche u.a. von der Klassifizierung abhängt. Ohne Klassifizierung ist ein sachgerechtes und gezieltes Festlegen und Umsetzen von Sicherheitsmassnahmen daher nicht möglich. Zudem geht der vorgeschlagene Verweis auf die Grossratsgesetzgebung ins Leere, weil diese heute u.W. keine bzw. nur ansatzweise Informationssicherheitsvorschriften enthält, und nicht beantragt wird, mit welchen Sicherheitsvorschriften sie zu ergänzen wäre.
54.	Büro GR	Zudem würde die Zuteilung beim Nichtzugänglichem als «intern», «vertraulich» oder «geheim» in der Praxis in den Ratsorganen mitunter lange Diskussionen auslösen, weil darüber in guten Treuen unterschiedliche Auffassungen bestehen können, je nachdem, ob man ein öffentliches Interesse als nur «beeinträchtigt», «erheblich beeinträchtigt» oder «schwerwiegend beeinträchtigt» auffassen könnte. Diese Unterscheidung brächte keinen Mehrwert, denn alle solche Unterlagen blieben nicht zugänglich. **Für den Grossen Rat und seine Organe ist und bleibt es relevant, ob eine Information oder Unterlage öffentlich zugänglich ist oder nicht**. Dieses duale System hat sich bewährt, ist einfach handhabbar und miliztauglich und erreicht das mit einem förmlichen Klassifizierungssystem anvisierte Ziel auch, dass nämlich die Behörden festlegen, welche Informationen vor Kenntnisnahme durch Unberechtigte zu schützen sind und welche nicht. Ein Wechsel hin zu einem viel aufwändigeren Klassifizierungssystem, noch dazu ohne ersichtlichen Mehrwert, ist deshalb nicht nötig.	Kenntnisnahme. Diese Bedenken sind nachvollziehbar. Um solche langen Diskussionen zu vermeiden, werden die Ausführungsbestimmungen vorsehen, dass jede Behörde für die Dokumente in ihrem Aufgabenbereich einen Klassifizierungskatalog erlässt, der die einheitliche Klassifizierung regelt (wie im Bundesrecht: Art. 17 Absatz 2 des Vernehmlassungsentwurfs zur Informationssicherheitsverordnung, ISV). Der Grosse Rat oder seine Organe können daher in einem solchen Katalog schematisch festlegen, dass z.B. Kommissionsprotokolle immer als VERTRAULICH klassifiziert werden. S. dazu auch unten Ziff. 56. Diese Absicht wird im Vortrag vermerkt.
55.	Büro GR	In diesem Zusammenhang sei noch erwähnt, dass selbst ein ausgeklügeltes Klassifizierungssystem, wie es mit der vorliegenden Vorlage vorgeschlagen und bereits ähnlich im Bund praktiziert wird, nicht vor Indiskretionen schützt, wie die in letzter Zeit in aller Munde stehenden Leaks bei der Bundesverwaltung gezeigt haben.	Kenntnisnahme. Das stimmt, jedoch erleichtert eine formelle Klassifizierung das Entdecken und Sanktionieren von Indiskretionen. Denn wenn Dokumente unübersehbar als «VERTRAULICH» gekennzeichnet sind, kann sich niemand in einem Strafverfahren wegen Amtsgeheimnisverletzung damit herausreden, sie

[3] Es kommt auch nicht zu einem «Entzug von Informationen für die öffentlich stattzufindende politische Debatte» (vgl. Vortrag zum ICSG, S. 16 unten), weil Letztere im Ratsplenum und damit im öffentlich ohne Weiteres zugänglichen Bereich erfolgt. Das unterscheidet im Übrigen sehr wesentlich grossrätliche von regierungsrätlichen Unterlagen (Regierungssitzungen sind nicht-öffentlich; weshalb die Nachvollziehbarkeit staatlichen Handelns anderweitig zu gewährleisten ist, z.B. mit bloss ausnahmsweisem Klassifizieren).

			oder er habe nicht gewusst, dass ein Dokument nicht öffentlich sei. Und wenn VERTRAULICHE Dokumente in den ICT-Systemen des Kantons bzw. des Grossen Rates besonders gekennzeichnet werden müssen, können automatische Systeme z.B. Alarm schlagen, wenn solche Dokumente in grosser Zahl heruntergeladen oder an Dritte weitergemailt werden. Ohne Klassifizierung sind solche und andere technische Sicherheitsmassnahmen nicht möglich.
56.	Büro GR	Wäre sodann die Einführung eines förmlichen Klassifizierungssystems für den Grossen Rat und seine Organe zwingend, was es aber nicht ist, müsste ein solches den beiden vorerwähnten Kriterien entsprechen, und wären die entsprechenden Bestimmungen grossrats- und nicht regierungs-seitig festzulegen (d.h. durch GRG/GO, sicher nicht mittels regierungsrätlicher Verordnung, also nicht gemäss Art. 8 Abs. 4 E-ICSG bzw. Art. 22 Abs. 1 E-ICSG usw.).	Umgesetzt. Wie bereits erwähnt (Ziff. 57 oben), werden die Ausführungsbestimmungen vorsehen, dass jede Behörde für die Dokumente in ihrem Aufgabenbereich einen Klassifizierungskatalog erlässt, der die die einheitliche Klassifizierung regelt. Es wird also in der Hand des Grossen Rates bzw. seiner Organe bleiben, wie die parlamentarischen Dokumente konkret klassifiziert werden.

Art. 9

Nr.	Absender	Bemerkung/Forderung	Art der Berücksichtigung
57.	Büro GR	In diesem Zusammenhang wären auch noch die **Artikel 9 und 10 E-ICSG** anzupassen, welche beide den Zugang zu klassifizierten Informationen regeln: Dass ein Parlaments- oder Gerichtsorgan zuerst das Regierungsrats- bzw. Verwaltungsorgan anzuhören hätte, wollte es klassifizierende Informationen von Regierungsrat/Verwaltung zugänglich machen, ist sachgerecht – und entspricht, soweit den Grossen Rat betreffend, bereits den Vorgaben der Grossratsgesetzgebung und der langjährigen Praxis.[4] Allerdings müsste dies auch im umgekehrten Fall gelten (d.h. wenn Regierung/Verwaltung eine klassifizierte Information des Parlaments oder der Gerichte zugänglich machen wollte). Für den Fall, dass an der Klassifizierung für Grossratsunterlagen festgehalten wird, ist das ICSG somit zwingend um diese zweite Konstellation zu ergänzen, am passendsten mit Einbettung in Artikel 9 und zwar als Absatz 2 (bisheriger Abs. 2 würde zu Abs. 3). **Art. 9 ICSG** *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] Vor dem Entscheid, Zugang zu einer klassifizierten Information zu ermöglichen, hört das zuständige Gericht, die zuständige Staatsanwaltschaft, das zuständige parlamentarische Organ oder die zuständige Stelle von Regierung und Verwaltung die klassifizierende Stelle an.	Umgesetzt in Art. 10 Abs. 2, der nun lautet: «Vor dem Entscheid, den Zugang zu einer klassifizierten Information gemäss Absatz 1 zu ermöglichen, hört die zuständige parlamentarische, Justiz- oder Verwaltungsbehörde die klassifizierende Stelle an.»

[4] So verlangt Artikel 55 Absatz 1 GRG bereits, dass Kommissionen der betroffenen Behörde Gelegenheit zur Stellungnahme einzuräumen haben, wenn sie zu neuen Erkenntnissen gelangen oder Mängel in der Geschäftsführung oder in der Führung des Finanzhaushalts feststellen. Im Rahmen solcher Stellungnahmen hat die betroffene Behörde, in der Regel eine Direktion oder der Regierungsrat, somit schon heute die Möglichkeit, sich auch zur Verwendung von allenfalls heiklen Aussagen zu äussern. Artikel 55 Absatz 2 GRG regelt zudem, dass ein solcher Bericht nur veröffentlicht werden darf, wenn keine schützenswerten Interessen entgegenstehen.

		[3] Der Zugang zu klassifiziertem Archivgut richtet sich nach den Bestimmungen der Archivierungsgesetzgebung	

Art. 10

Nr.	Absender	Bemerkung/Forderung	Art der Berücksichtigung
58.	JL	**Zugang zu klassifizierten Informationen in Verfahren** In Art. 10 ICSG wird richtigerweise festgelegt, dass sich der Zugang zu klassifizierten Informationen in Verfahren der Gerichtsbehörden und der Staatsanwaltschaft nach der Spezialgesetzgebung bzw. den Verfahrensgesetzen richtet. Die Bestimmung lehnt sich an die entsprechende Regelung auf Bundesebene an (Art. 15 ISG). Ein Unterschied zur Bundesgesetzgebung besteht in Absatz 2: Das ICSG schreibt in solchen Fällen zwingend eine Anhörung der klassifizierenden Stelle vor. Im Bundesrecht ist dieser Einbezug in einer Kann-Vorschrift geregelt und damit optional. Für uns ist nicht nachvollziehbar, weshalb der Kanton hier eine weitergehende Regelung trifft. Eine zwingende Anhörung der klassifizierenden Stelle sorgt für Aufwände, die sich nicht in jedem Fall rechtfertigen. Die Bestimmung ist der Bundesregelung anzugleichen.	Nicht umgesetzt. Dieser Abweichung vom ISG liegt eine andere politische Würdigung zu Grunde. Aus unserer Sicht ist kein Grund denkbar, wieso die drei Staatsgewalten (vgl. Ziff. 57 oben) sich nicht in jedem Fall zumindest gegenseitig anhören müssen, wenn sie beabsichtigen, klassifizierte Informationen einer anderen Staatsgewalt der Öffentlichkeit bzw. Dritten zugänglich zu machen. An der Muss-Bestimmung wird daher festgehalten.
59.	Büro GR	Artikel 10 E-ICSG wäre dementsprechend auch noch wie folgt zu ändern (vgl. nachfolgend Unterstrichenes/Durchgestrichenes): **Art. 10 ICSG** *Zugang in besonderen Verfahren* 1 Der Zugang zu klassifizierten Informationen des Grossen Rates und der Parlamentsdienste sowie der Gerichtsbehörden und der Staatsanwaltschaft richtet sich <u>im Übrigen</u> ~~unter Vorbehalt von Absatz 2~~ nach den Bestimmungen der Spezialgesetzgebung.	Das Anliegen wurde anders aufgegriffen (s. Ziff. 61 oben).

Art.14

Nr.	Absender	Bemerkung/Forderung	Art der Berücksichtigung
60.	GLP	Was ist mit den Räumlichkeiten, in denen Informationen archiviert/aufbewahrt werden?	Auch solche Räume können zu Sicherheitszonen erklärt werden, weil das Aufbewahren von Informationen auch eine Bearbeitung der Informationen ist.
61.	Grüne	Art. 14 Sicherheitszonen: Die Einrichtung von Sicherheitszonen am Arbeitsplatz stellt einen grossen Eingriff in die Arbeitsrechte der Verwaltung dar. Die GRÜNEN beantragen, dass diese nur in wenigen und ausreichend begründeten Einzelfällen errichtet werden, zumindest wenn Überwachung durch Aufnahmegeräte, Taschen- und Personenkontrollen oder unangemeldete Raumkontrollen durchgeführt werden.	Kenntnisnahme. Das ist auch unsere Meinung. Soweit damit eine entsprechende Anpassung des Gesetzestexts beantragt werden soll, verzichten wir aber darauf, weil das ISG (Art. 23) keine entsprechende Bestimmung kennt. Schon wegen den Kosten für die Einrichtung von Sicherheitszonen ist davon auszugehen, dass die Behörden von dieser Möglichkeit nur zurückhaltend Gebrauch machen werden. Jedoch wird im Vortrag ergänzt, dass in Bezug auf die vorgesehenen Taschen- und Personenkontrollen kein Eingriff in das

			staatliche Gewaltmonopol der Kantonspolizei erfolgt. Sollte die Anwendung von Zwang notwendig sein, ist daher zwingend die Kantonspolizei beizuziehen. Die Bestimmung stellt mit anderen Worten keine Rechtsgrundlage für die Anwendung von Zwang z.B. durch private Sicherheitsorgane oder Behördenmitarbeitende dar.
62.	Büro GR	Weitere Bestimmungen sind für eine Anwendung für den Grossen Rat, seine Organe und die Parlamentsdienste untauglich. Exemplarisch sei auf die Bestimmung zur Sicherheitszone in Artikel 14 E-ICSG hingewiesen. Es wäre davon auszugehen, dass Büros der Mitarbeitenden der Parlaments-dienste einer Sicherheitszone zuzurechnen wären. In diesen Büros dürfte in deren Abwesenheit die sogenannte «Clean-Desk-Policy» überprüft werden (vgl. Art. 14 Abs. 2 Bst. d E-ICSG). Bei den Mitgliedern des Grossen Rates hingegen, die alle solche Unterlagen auch benützten, sei es daheim oder unterwegs, digital oder mittels ausgedruckten Unterlagen, gäbe es solche Kontrollen realistischerweise und weil sie keine «Angestellten» sind nicht, was die Grenzen der Überprüfbarkeit aufzeigt. Insbesondere aber bestehen für die Unterlagen der Ratsorgane seit Langem schon griffige Vorgaben zu deren Schutz, die sich in der Praxis auch bewährt haben (Art. 43 GRG und Kommissionsreglemente).	Kenntnisnahme. Die Annahme, dass Parlamentsbüros quasi automatisch einer Sicherheitszone «zuzuordnen» wären, geht fehl. Die Einrichtung einer Sicherheitszone ist ein bewusster und ausnahmsweiser (s. vorstehend) Entscheid einer zuständigen Behörde, mit dieser Massnahme einem sehr hohen Sicherheitsrisiko zu begegnen. Wir denken dabei an einzelne Räumlichkeiten der Polizei (v.a. im Bereich Nachrichtendienst / Staatsschutz / organisierte Kriminalität) sowie allenfalls des Strafvollzugs oder der Justiz, aber kaum des Grossen Rats. Nur wenn dieser es für nötig hält, kann er – muss aber nicht – eine solche Sicherheitszone einrichten. Dies könnte allenfalls punktuell zum Schutz der Informationen einer parlamentarischen Untersuchungskommission (PUK) ein Thema werden, aber kaum im Arbeitsalltag des Parlaments.

Art.17

Nr.	Absender	Bemerkung/Forderung	Art der Berücksichtigung
63.	JL	**Personensicherheitsprüfung** Die überarbeiteten Regelungen zur Personensicherheitsprüfung beurteilen wir grundsätzlich positiv. Wir stellen indes fest, dass an der Personensicherheitsprüfung für zu wählende Behördenmitglieder nach Art. 17 Abs. 2 Bst. b ICSG festgehalten wird. Diese Bestimmung erscheint mit Blick auf die Unabhängigkeit der Justiz heikel: Während die obersten Vertreter/innen der beiden anderen Staatsgewalten keiner entsprechenden Prüfung unterzogen werden, ist eine solche für die Angehörigen der Justiz vorgesehen. Die Problematik wird dadurch akzentuiert, dass der Behörde bei der Durchführung der Personensicherheitsprüfung ein grosses Ermessen zukommt. Dies könnte einer politischen Einflussnahme Vorschub leisten: Es wäre beispielsweise denkbar, dass die Justizkommission des Grossen Rates bei einzelnen Anwärterinnen oder Anwärtern für ein Richteramt eine Personensicherheitsprüfung durchführt, während sie bei anderen darauf verzichtet. Aus diesen Überlegungen lehnen wir die Personensicherheitsprüfung bei zu wählenden Behördenmitgliedern ab, dies auch in Anlehnung an die entsprechende Bestimmung im Bundesrecht (vgl. Art. 29 Abs. 4 Bst. c und d ISG).	Nicht umgesetzt. Aus unserer Sicht ist es sachlich angebracht, dass die Wahlbehörde auch bei Richterinnen oder Staatsanwälten zumindest die Möglichkeit hat, eine Personensicherheitsprüfung durchzuführen, wenn sie das will. Denn diese Behördenmitglieder üben staatliche Macht in einer Weise aus, welche sich auf die Rechtsunterworfenen sehr einschneidend auswirken kann, und sie haben Zugang zu vielen sehr schützenswerten Informationen über die Rechtsunterworfenen. Daher haben diese ein legitimes Interesse daran, darauf vertrauen zu können, dass die Personen, die über sie urteilen, vertrauenswürdige und integre Menschen sind. Im Übrigen führt die Justizkommission gemäss der Vernehmlassung des Büros gemäss des Büros des Grossen Rates schon heute *de facto* Personensicherheitsprüfungen durch,

			indem sie die Straf- und Betreibungsregisterauszüge der Kandidierenden einholt (Ziff. 72 unten). Insoweit kodifiziert die vorgesehene Bestimmung bloss die heutige Praxis. Endlich ist eine Wahl ein politischer Akt. Wenn die Wahlbehörde frei entscheiden kann, eine Person aus welchen Gründen auch immer in ein Amt zu wählen oder auch nicht, kann es ihr auch nicht verwehrt sein, die Vertrauenswürdigkeit der Kandidierenden mehr oder weniger genau abzuklären.
64.	Die Mitte	***Art. 17****: Voraussetzungen und Zweck* *Abs. 2 Folgende Personen sollen einer Personensicherheitsprüfung unterzogen werden*. Begründung: Die Freiwilligkeit ist gemäss Abs. 4 nicht gegeben. Wir unterstützen eine einheitliche und zuverlässige Überprüfung der Personen, die Zugang zu geheimen und vertraulichen Informationen haben.	Kenntnisnahme. Aus der Stellungnahme geht nicht hervor, ob und welche Änderung des ICSG die Stellungnehmenden vorschlagen. Daher können wir gestützt auf diese Bemerkung nichts unternehmen.
65.	Die Mitte	*Art. 17 Abs. 2 Bst. d (neu): Die Personensicherheitsprüfung soll periodisch erneuert werden*. Begründung: Eine Personensicherheitsprüfung ist stets eine Momentaufnahme und kann nicht „lebenslänglich“ gelten.	Nicht umgesetzt. Das ist an sich fachlich sinnvoll, und im Bund auch so vorgesehen. Mit Blick auf das politische Ziel, möglichst wenig Mehraufwand zu generieren, haben wir im Entwurf jedoch bewusst darauf verzichtet und dies der Risikobeurteilung der einzelnen Behörde zu überlassen: Wenn sie frei ist, abhängig von ihrer Risikobeurteilung eine PSP überhaupt durchzuführen oder auch nicht, muss das auch für die Erneuerung der PSP gelten.
66.	GLP	Es liegt in der Verantwortung der einzelnen Behörden, gestützt auf ihre Risikobeurteilung (Art. 5 Abs. 4) festzulegen, welche Personen sie wie oft einer PSP unterziehen wollen. Wir würden eine einheitliche Handhabung begrüssen. Insbesondere führt es zu ungleicher Handhabung im Kanton und zu Ineffizienzen, wenn alle Einheiten diesbezügliche Vorgaben erarbeiten müssen.	Kenntnisnahme.
67.	Grüne	Art. 17 – 19 Personensicherheitsprüfung: Eine Personensicherheitsprüfung ist eine datenschutz- und arbeitsrechtlich höchst delikate Massnahme und sollte nur in Bereichen angewendet werden, wo Personen mit sehr grossen Sicherheitsrisiken umgehen müssen. Im Informationssicherheitsgesetzes ISG des Bundes ist die Personensicherheitsprüfung, auch für «Angestellte eines Kantons, die eine sicherheitsempfindliche Tätigkeit ausüben» geregelt. Es erschliesst sich den GRÜNEN nicht, wieso der Kanton hier eine eigene, weitergehende Regelung einführen soll.	Kenntnisnahme. Tatsächlich ist die vorgeschlagene Regelung weniger weitergehend als die des Bundes. Dieser sieht eine noch eingehendere Prüfung durch eine dafür eingerichtete Fachstelle vor.
68.		– Die GRÜNEN lehnen insbesondere die Ausweitung der Personensicherheits-prüfung auf Personen ab, die als Mitglied einer Behörde gewählt werden sollen, also namentlich Richter*innen.	S. Ziff. 68 oben.
69.		– Ebenso sind die GRÜNEN der Meinung, dass eine richtige Personensicherheitsprüfung mit all den möglichen Massnahmen gemäss Art. 18 nicht sinnvoll durch die «eigene» Behörde durchgeführt werden	Nicht umgesetzt.

		kann. Es ist datenschutz-rechtlich problematisch, wenn direkte Vorgesetzte oder Teammitglieder etwa Drittpersonen über die Lebenssituation einer Mitarbeiter*in befragen. Wenn es eine eigene kantonale Personensicherheitsprüfung braucht, dann ist wie beim Bund eine dafür spezialisierte Fachstellen einzusetzen.	Es gibt tatsächlich Argumente der Professionalität und der Einheitlichkeit, die für die Einrichtung einer PSP-Fachstelle sprechen würden. Weil das ICSG aber aufgrund der finanziellen Rahmenbedingungen des Kantons mit den bestehenden Ressourcen umgesetzt werden muss, verzichten wir darauf. Zu beachten ist auch, dass die allfällige Registerabfrage durch die Kantonspolizei und damit durch Fachpersonal erfolgt, und dass auch bei der Einrichtung einer Fachstelle die Vorgesetzten über das Ergebnis der Prüfung und damit über ein allfälliges risikoreiches Vorleben der geprüften Person informiert würden.
70.		– Die Frist von 10 Tagen, innert derer sich eine geprüfte Person melden kann, um Falschinformationen zu berichtigen, scheint uns zu kurz	Nicht umgesetzt. Die Stellungnahme führt nicht aus, welche Frist angemessener wäre, und wieso. Daher passen wir die Vorlage nicht an.
71.	EDU	Art. 17 – 19 (Personensicherheitsprüfung) – Die EDU Kanton Bern lehnt eine Personensicherheitsprüfung für Bewerberinnen und Bewerber für Richterstellen ab. Dies erscheint uns als unverhältnismässig was Aufwand und Mehrwert anbelangt. Ein aktueller Auszug aus dem Betreibungs- und Strafregister wird bereits verlangt. Zudem ist es aus unserer Sicht systemfremd, wenn nur Vertreterinnen und Vertreter der judikativen Gewalt einer Personensicherheitsprüfung unterzogen werden, jedoch nicht Mitglieder des Regierungsrates oder des Grossen Rates.	S. Ziff. 68 oben. Der hier massgebliche Unterschied zwischen Richterwahlen einerseits und Regierungs- oder Grossratswahlen andererseits ist, dass letztere Volkswahlen sind. Vgl. dazu Ziff. 72 unten.
72.	Büro GR	Hinsichtlich der **Personensicherheitsprüfung** (Art. 17 ff. E-ICSG) ist **vom Einbezug von Richterinnen und Richtern und dem/der (stv.) Generalstaatsanwalt/-anwältin zum Vornherein abzusehen**[5] und ist diese Ausnahme wie im Bund im Gesetz selbst festzuhalten: – Bereits heute haben bei Richterwahlen die Kandidierende einen aktuellen Auszug aus dem Straf-und dem Betreibungsregister vorzulegen.[6] Dies ist sachgerecht und ausreichend, weshalb auf eine förmliche Personensicherheitsprüfung verzichtet werden kann und die Richterinnen und Richter sowie der/die (stv.) Generalstaatsanwalt/-anwältin vom Geltungsbereich dieser Bestimmungen auszunehmen sind. Für eine Befragung der Kandidierenden sowie sogar von Drittpersonen, wie sie bei einer Personensicherheitsprüfung möglich sein sollen (vgl. Art. 18 Abs. 2 Bst. e und f E-ICSG), wären Ratsorgane als Milizbehörden wie die im Vortrag konkret vorgeschlagene Justizkommission – oder evtl. das Büro in anderen Fällen – ohnehin nicht geeignet. Zudem spielen bei Richterwahlen politische Überlegungen ebenfalls noch eine gewisse Rolle: Richterwahlen werden von der Justizkommission bzw. dessen Wahlausschuss (Ausschuss IV) vorbereitet. Der Ausschuss IV besteht aus je einem Mitglied der im Grossen Rat vertretenen Fraktionen (aktuell acht Grossrätinnen und Grossräten). Er schreibt die Stellen aus, holt die gemäss Gesetz vorgegebenen Stellungnahmen ein und führt basierend auf den Bewerbungsunterlagen	Nicht umgesetzt. S. Ziff. 68 oben. Dem dort Gesagten ist hier Folgendes hinzuzufügen: Aus dieser Stellungnahme ergibt sich, dass die Justizkommission schon heute (und ohne gesetzliche Grundlage) Personensicherheitsprüfungen vornimmt, indem sie sich die Straf- und Betreibungsregisterauszüge der Kandidierenden vorlegen lässt. Das heisst, dass sich mit der Einführung des ICSG an der Praxis der Justizkommission nichts Grundsätzliches ändern muss bzw. wird, denn auch eine PSP gemäss ICSG wird sich im Normalfall auf die Prüfung der Registereinträge beschränken (Art. 18 Abs. 2 Bst. a und b). Nur wenn diese Einträge oder andere Umstände vermuten lassen, dass mit der geprüften Person Risiken verbunden sein könnten, die sich aus den Registerauszügen nicht ergeben, wird die Wahlbehörde im eigenen Ermessen – sie muss dies nicht –

[5] Quantitativ ginge es um rund 140 hauptamtliche und rund 490 nebenamtliche Behördenmitglieder.
[6] Vgl. https://www.gr.be.ch/de/start/grosser-rat/organisation/kommissionen/juko_justizkommission/richterwahlen.html

			und den eingeholten Stellungnahmen die Gespräche durch (vgl. auch Auszug JuKo-Reglement betr. Richterwahlen[7]).	weitere Informationsquellen gemäss Art. 18 Abs. 2 Bst. c bis f erschliessen wollen. Damit führt das ICSG nicht eine neue Pflicht bzw. Aufgabe ein, sondern sie schafft die bisher fehlende Rechtsgrundlage für die bestehende Praxis der Justizkommission.
73.		–	Müsste der Ausschuss IV neu weitergehende Prüfungen durchführen, müsste wohl sogar das geltende Wahlsystem und dessen Ablauf vorher grundsätzlich überdacht werden und wären aufgrund der sehr offen gehaltenen Regelungen im ICSG wohl auch Anpassungen der Grossratsgesetzgebung und des Gesetzes über die Organisation der Gerichtsbehörden und der Staatsanwaltschaft (GSOG) nötig. Geklärt werden müsste insbesondere die Frage, wer zu welchem Zeitpunkt eine solche weitergehende Prüfung und welche genau vornehmen müsste.	Aus der Stellungnahme ergibt sich nicht konkret, welche Anpassung der Grossratsgesetzgebung erforderlich sein könnte. Weil nach dem oben Gesagten bereits bisher PSP bei Richterwahlen durchgeführt wurden, ohne dass dies in der Grossratsgesetzgebung geregelt war, erschliesst sich uns nicht, welcher Anpassungsbedarf konkret bestehen könnte. Gerne nehmen wir aber im 2. Mitberichtsverfahren entsprechende Vorschläge entgegen.
74.	Büro GR	–	Nebst diesen Gründen ist in staatspolitischer Hinsicht nicht einzusehen, weshalb nur Richterinnen und Richter – diesfalls nicht auch die Vertreterinnen und Vertreter der beiden anderen obersten Staatsgewalten (Regierungs- und Grossratsmitglieder) – sich u.U. einer Personensicherheitsprüfung unterziehen müssten. Wenn das Argument wie gemäss Finanzdirektion ist, bei Richterinnen und Richtern bestünde aufgrund der Macht, welche sie ausübten, mehr noch als bei Angestellten ein öffentliches Interesse daran, dass sie integer und nicht erpressbar seien, würde das auch für die Regierungsmitglieder gelten. Dass sich Regierungsmitglieder keiner Personensicherheitsprüfung zu unterziehen haben, wird im Vortrag damit begründet, sie seien vom Volk gewählt, weshalb keine solche Prüfung möglich sei. Wenn indes eine Überprüfung gewollt wäre, könnte diese schon vor der Wahl erfolgen. Auch bei Richterinnen und Richtern geht es deshalb vielmehr um eine staatspolitische Frage, ob bei ihnen eine Personensicherheitsprüfung zu erfolgen hat. Nach Auffassung des Büros kann es nicht sein, dass nur Angehörige einer der drei obersten Staatsgewalten personensicherheitsüberprüft werden. Der Bund sieht das gleich: Weder bei Mitgliedern der Bundesversammlung und des Bundesrates noch bei Richterinnen und Richter und dem Bundesanwalt erfolgt eine Personensicherheitsprüfung (Art. 29 Abs. 4 ISG); in der Logik des Vortrags der Finanzdirektion wären hingegen im Bund sowohl die Bundesräte wie auch die Richterinnen und Richter personensicherheitsmässig zu überprüfen, da mit dem Parlament eine Wahlbehörde vorläge.	Es trifft zu, dass im Umstand, dass bei Richterwahlen eine PSP erfolgen kann, bei Regierungs- oder Grossratswahlen aber nicht, eine Ungleichbehandlung liegt. Diese ist jedoch sachlich gerechtfertigt: Regierungs- oder Grossratswahlen sind Volkswahlen, während Mitglieder der Justizbehörden vom Grossen Rat gewählt werden. Das Volk als solches ist nun aber nicht in der Lage, eine PSP durchzuführen, anders als eine Kommission oder ein Ausschuss des Grossen Rates.
75.	Büro GR		Zudem sind die Bestimmungen zur Personensicherheitsprüfung auch in weiteren Belangen zu überarbeiten und zu ergänzen. So soll es gemäss Vortrag nicht nur im Belieben der einzelnen Behörden sein zu entscheiden, ob sie für die in Frage kommenden Personen eine Prüfung vorsehen wollen, sondern auch, in welcher Prüfintensität und zu welchem Zeitpunkt dies erfolgen würde. Diese Fragen sind allerdings wie im Bund – nicht nur der Transparenz halber, sondern auch ihrer Wichtigkeit wegen (Art. 69 Abs. 4 KV)[8] – vom Gesetzgeber selber zu beantworten, weshalb dies **im Gesetz festzuschreiben** ist (vgl. z.B. Art. 29 und 31	Nicht umgesetzt. Das ICSG übernimmt im Wesentlichen die Regelung der PSP im Polizeigesetz (Art. 160 ff. PolG), das der Grosse Rat erst 2019 total revidiert und dabei erstmals die PSP geregelt hat. Im PolG hat sich der Gesetzgeber bewusst für eine schlanke, wenig bürokratische Regelung der PSP entschieden. In der

[7] Vgl. file:///C:/Users/mb5j/Downloads/auszug-reglement-justizkommission-2020-10-21-de.pdf bzw. www.gr.be.ch – Der Grosse Rat – Organisation – Kommissionen – Justizkommission – Richterwahlen – Rechtliche Grundlagen

[8] Aus Rechtsgleichheitsgründen ist zudem zu gewährleisten, dass die übrigen Magistratspersonen (Beauftragter für Datenschutz, Vorsteher Finanzkontrolle, Staatsschreiber, Generalsekretär des Grossen Rates [vgl. Art. 38 PG]) gleichbehandelt werden (z.B. entweder alle oder keiner überprüft, und im Fall einer Überprüfung: in gleicher Intensität und von gleicher Stelle).

		ISG-Bund: Normierung, wer zu prüfen ist[9] und wer genau die prüfende Stelle ist / Art. 30 ISG-Bund: Prüfintensität mit dann jeweils einheitlicher Prüfungstiefe [Grundsicherheitsprüfung oder erweiterte Prüfung] / Art. 33 ISG-Bund: Zeitpunkt [in aller Regel *vor* An-stellung etc.]). Auch die Rechtsfolge des Prüfergebnisses (im Bund Empfehlung) sowie die Rechte und Pflichten geprüfter Personen sowie der Rechtsweg[10] sind im Gesetz selber zu regeln, einschliesslich der Information an die überprüfte Person, was die Überprüfung ergeben hat (nicht nur bei negativem Ergebnis, vgl. insb. Art. 32, 40, 41, 44 1 ISG-Bund; nur nebenbei noch bemerkt: die Absätze 2 und 4 von Art. 17 E-ICSG sind widersprüchlich, Absatz 4 ist wie im Bund auf die Mitwirkung bei der Sachverhalts-Feststellung einzuschränken). Ferner ist zu prüfen, ob Personensicherheitsprüfungen – um eine gleiche und damit faire sowie auch professionelle Praxis zu gewährleisten – nicht wie im Bund durch eine zentrale Fachstelle durchzuführen sind, wenn solche schon wie geplant breit eingeführt werden sollen.	Praxis sind uns bzw. der Kantonspolizei keine praktischen Probleme bekannt, die sich aus diesem Rechtsetzungsansatz ergeben haben. Indem wir diese für die Polizei bereits geltende Regelung auf die ganze Verwaltung ausdehnen, respektieren wir den gesetzgeberischen Entscheid des Grossen Rates von 2019.

Art. 20

Nr.	Absender	Bemerkung/Forderung	Art der Berücksichtigung
76.	JL	**Geltungsbereich** Die Regelung des Geltungsbereichs hat gegenüber der Mitberichtsfassung eine massgebliche Änderung erfahren, welche nicht zu überzeugen vermag. Aus der aktuellen Fassung der Vorlage geht nicht mehr klar hervor, ob das Gesetz für die Gerichtsbehörden und die Staatsanwaltschaft uneingeschränkte Geltung erlangt. Das liegt weniger an der Formulierung von Art. 2 ICSG als vielmehr an den Änderungen in Art. 20 f. ICSG. Die Mitberichtsfassung sah die vollumfängliche Geltung des Gesetzes für alle kantonalen Behörden vor. Für Gemeinden und andere Träger öffentlicher Aufgaben nach Art. 95 KV wurde der Geltungsbereich eingeschränkt. Bei der Sicherheitsorganisation erfolgte des Weiteren eine Differenzierung nach dem Kriterium der Zugehörigkeit zur kantonalen Verwaltung. Für die Gerichtsbehörden und die Staatsanwaltschaft hätte dies bedeutet, dass das Gesetz für sie vollumfänglich anwendbar ist, sie sich aber eine eigene Sicherheitsorganisation geben. Dies erschien uns sachgerecht. Diese Differenzierung nach kantonalen Behörden und Behörden, welche der kantonalen Verwaltung angehören, geht in der neuen Fassung verloren. Zwar stellen Art. 20 und 21 ICSG nach wie vor auf die Zugehörigkeit zur kantonalen Verwaltung ab. Die Titel der beiden Bestimmungen verweisen jedoch auf die Regelung zum Geltungsbereich. Dies führt zu unauflösbaren Widersprüchen. Obschon die Gerichtsbehörden und die Staatsanwaltschaft als kantonale Behörden dem Geltungsbereich voll unterstehen (vgl. Vortrag, S. 12), werden sie in der Vorlage auch zu den anderen Träger öffentlicher Aufgaben gezählt, für welche das Gesetz nach Art. 2 Abs. 2 ICSG nur eingeschränkt gilt (vgl. Vortrag, S. 26). Diesen Widerspruch gilt es aufzulösen. Nach Auffassung der Justizleitung muss sich der Geltungsbereich eindeutig aus Art. 2 ICSG ergeben. Die Sicherheitsorganisation nach Art. 20 und 21 ICSG sollte sich hingegen nach der Zugehörigkeit zur kantonalen Verwaltung richten und nicht am Geltungsbereich des Gesetzes anknüpfen.	Umgesetzt. Der Titel von Art. 20 ICSG lautet nun «Sicherheitsorganisation des Kantons und der kantonalen Verwaltung», der von Art. 21 «Sicherheitsorganisation der anderen Behörden».

[9] Im Bund nebst Richtern z.B. ebenfalls *nicht* Bundeskanzler und kantonale Magistratspersonen, die vom Volk oder vom kantonalen Parlament gewählt werden.
[10] Das Prüfergebnis dürfte wie im Bund eine Verfügung oder dergleichen (Realakt) sein (vgl. Art. 29a BV, Art. 49 VRPG). Wenn nicht, müsste der Vortrag eingehend begründen, weshalb dieses nicht justiziabel sein soll.

Art.22

Nr.	Absender	Bemerkung/Forderung	Art der Berücksichtigung
77.	EDU	Art. 22 (Ausführungsbestimmungen) - Ausführungsbestimmungen, die den Grossen Rates, seine Organe und die Parlamentsdienste betreffen, sollen vom Büro des Grossen Rates erlassen werden.	S. Ziff. 85 unten.
78.	Büro GR	Schliesslich wäre ohnehin **nicht klar, welche Behörde genau die Kompetenz hätte, solche Sicherheitszonen und dergleichen zu bezeichnen. Soweit jedenfalls Unterlagen des Grossen Rates, von Ratsorganen oder der Parlamentsdienste hinsichtlich der Ratsarbeit betroffen sind, darf diese Befugnis zum Vornherein nur einem Ratsorgan (z.B. Büro) eingeräumt werden** und nicht dem Regierungsrat, der Finanzdirektion, einem Amt oder einem blossen «Fachorgan» der Kantonsverwaltung (vgl. Art. 22 E-ICSG).[11] Aus diesen Gründen ist auch Artikel 22 E-ICSG wie folgt zu ändern (gilt hinsichtlich aller Ausführungsbestimmungen, z.B. auch betr. allfälliger Ent-/Klassifizierung [Art. 8 Abs. 4 E-ICSG, Sicherheitsverfahren [Art. 11 E-ICSG], Sicherheitsorganisation [Art. 20 E-ICSG], Personensicherheitsüberprüfungen [Art. 17 E-ICSG i.V. mit Art. 22 Abs. 1 ICSG] etc.): **Art. 22 ICSG** *Ausführungsbestimmungen* [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 Kantons-verwaltung 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. [4] Ausführungsbestimmungen hinsichtlich des Grossen Rates, seiner Organe und der Parlamentsdienste erlässt das Büro des Grossen Rates. (Kommentar: so wie das auch im Bund der Fall ist)	Anders umgesetzt. Im neuen Art. 23 werden sinngemäss die Bestimmungen von Art. 84 Abs. 2 und 3 ISG übernommen, die lauten: «[2] Zuständigkeiten, die das vorliegende Gesetz den verpflichteten Behörden zuweist, werden für die Bundesversammlung durch die Verwaltungsdelegation der Bundesversammlung wahrgenommen. [3] Die Ausführungsbestimmungen des Bundesrats gelten für die verpflichteten Behörden sinngemäss, sofern diese keine eigenen Ausführungsbestimmungen erlassen.» Damit hat der Grosse Rat bzw. sein Büro die Möglichkeit, bei Bedarf – und in eigener Verantwortung – von den für die Verwaltung geltenden Ausführungsbestimmungen abzuweichen. Dabei wird er aber beachten müssen, dass dies zur Folge haben kann, dass dadurch die Möglichkeit der Nutzung der ICT-Grundversorgung der Kantonsverwaltung durch den Grossen Rat eingeschränkt wird. Dies, weil die ICT-Grundversorgung auf die gesamtkantonalen Sicherheitsvorschriften ausgerichtet ist. An der Delegation der Kompetenz des Erlasses von technischen Vorschriften an Fachorgane der Verwaltung – die schon im geltenden Recht vorgesehen ist, siehe etwa Art. 38 KDSG, Art. 34 DVG – wird festgehalten, weil der Streichungsantrag nicht begründet wird.

[11] Die Parlamentsdienste sind unabhängig und arbeiten nach Weisungen des Grossen Rates, nicht des Regierungsrates oder untergeordneter Verwaltungsbehörden (Art. 91 GRG).

4. Bemerkungen zum Vortrag zum ICSG

Zum Vortrag im Allgemeinen

Nr.	Absender	Bemerkung/Forderung	Art der Berücksichtigung
79.	JL	Der Vortrag sollte näher erläutern, was dies konkret für Behörden bedeuten kann, welche entsprechende Informationen bearbeiten und ICT-Mittel einsetzen.	

Vortrag zu Ziff.1

Nr.	Absender	Bemerkung/Forderung	Art der Berücksichtigung
80.	Büro GR	Vorab ist in den **Ziffern 1, 3.1 und 6.1 des Vortrags die Ausgangslage**, was die bundesrechtlichen Vorgaben angeht, **korrekt darzustellen**, wie die Parlamentsdienste schon zurückgemeldet hatten. Sowohl der Grosse Rat **als Gesetzgeber als auch die Öffentlichkeit haben Anspruch auf eine korrekte und transparente Wiedergabe der Bundesvorgaben, welche auch darüber informiert, welchen Handlungsspielraum der Kanton hat**. So wie der Vortrag jetzt lautet, wird der Eindruck erweckt, Bundesrecht (ISG) verpflichte die Kantone zu einer Vorlage wie der vorliegenden, was nicht der Fall ist. Denn gemäss Artikel 3 ISG (Bund[12]) gelten für die Kantone die ISG-Bestimmungen a) über klassifizierte Informationen (vgl. Art. 11 – 15 ISG), aber nur soweit Kantone klassifizierte Informationen des Bundes bearbeiten und b) über die Sicherheit beim Einsatz von Informatikmitteln (vgl. Art. 16 – 19 ISG), wiederum nur, soweit Kantone auf Informatikmittel des Bundes zugreifen.[13] Bundesrecht verpflichtet die Kantone insbesondere nicht dazu, zu allen ISG-Bereichen gleichwertige Bestimmungen zu erlassen, ja nicht einmal dazu, Bestimmungen zu den Bereichen «Klassifizierung Informationen» und «Sicherheit Einsatz Informatikmittel» zu erlassen, so-lange keine Informationen des Bundes oder Informatikmittel des Bundes Gegenstand sind. Bundesrecht zwingt den Kanton somit auch nicht dazu, Informationen des Grossen Rates oder seiner Organe förmlich zu klassifizieren, wie das schon bisher nicht der Fall ist (vgl. dementsprechend auch den eingeschränkten sachlichen Geltungsbereich von Art. 1 der bernischen KRGV [Klassifizierungsvorgaben sind beschränkt auf Regierungsratsgeschäftsdokumente]). **Ziff. 1 des Vortrags ist deshalb wie folgt zu ändern:** Zweitletzter und letzter Satz des ersten Abschnitts («Zudem …[bis] … in Kraft») ersetzen mit: «Zudem schreibt das neue Bundesgesetz vom 18. Dezember 2020 über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG) den Kantonen im Falle einer Bearbeitung klassifizierter Informationen des Bundes oder eines Zugriffs auf Informatikmittel des Bundes eine gleichwertige Gesetzgebung vor. Das ISG tritt am 1. April 2023 in Kraft.»	Konziser umgesetzt: « ... bei der Bearbeitung von Bundesinformationen oder der Nutzung von ICT-Systemen des Bundes ...»

[12] Vgl. BBl 2020 9975 (https://www.fedlex.admin.ch/eli/fga/2020/2696/de).
[13] Die betreffenden Bundes-Bestimmungen gelten für die Kantone im Übrigen dann nicht, wenn die Kantone für diese Belange (klassifizierte Informationen des Bundes/Informatikmittel Bund) selber eine mindestens gleichwertige Informationssicherheit gewährleisten (Art. 3 Abs. 1 und 2 ISG).

Vortrag zu Ziff. 3.1.

Nr.	Absender	Bemerkung/Forderung	Art der Berücksichtigung
81.	Büro GR	**und Ziff. 3.1. des Vortrags ist wie folgt zu ändern:** Sätze 3 und 4 («Daher verpflichtet …[bis] … effizienter macht») ersetzen mit: *«Soweit Kantone klassifizierte Informationen des Bundes bearbeiten oder auf Informatikmittel des Bundes zugreifen, gelten für den Kanton die entsprechenden ISG-Bestimmungen des Bundes, es sei denn, Kantone gewährleisten diesbezüglich eine mindestens gleichwertige Informationssicherheit (Art. 3 ISG). Mit dem vorliegenden ICSG wird der letzte Weg gewählt und werden die Vorschriften des Bundes, soweit sie greifen, auf die Berner Verhältnisse zugeschnitten, was sie effektiver und effizienter macht. Wo der Kanton keine klassifizierten Informationen des Bundes bearbeitet oder nicht auf Informatikmittel des Bundes zugreift, ist von Bundesrechts wegen nichts vorzukehren. Der Kanton ist diesbezüglich frei, Regeln aufzustellen und wenn ja, welche genau. Bundesrecht zwingt beispiels-weise nicht dazu, dass Kantonsparlamente ein förmliches Klassifizierungssystem einführen.»*	Anders umgesetzt. Ziff. 3.1 des Vortrags wurde wie folgt ergänzt: «Für die Verwaltungsbereiche, in denen keine Bundesinformationen bearbeitet und keine Bundessysteme genutzt werden, ist der Kanton grundsätzlich frei, ob und wie er die Informationssicherheit regelt. Es wäre aber nicht praktikabel, dafür separate, inhaltlich unterschiedliche Sicherheitsvorschriften zu erlassen. Daher gilt das ICSG für alle Behörden einheitlich (zum Vorbehalt für den Grossen Rat siehe unten zu Art. 24).» Zur Frage der Klassifizierung s. oben zu Art. 8.

Vortrag zu Ziff. 6.1.

Nr.	Absender	Bemerkung/Forderung	Art der Berücksichtigung
82.	Büro GR	**und Ziff. 6.1 des Vortrags ist wie folgt zu ändern:** Sätze 3 und 4 («Daher verpflichtet .. [bis] … (vgl. Ziff. 4.3. oben)») ersetzen mit**:** *«Soweit Kantone klassifizierte Informationen des Bundes bearbeiten oder auf Informatikmittel des Bundes zugreifen, gelten für den Kanton die entsprechenden ISG-Bestimmungen des Bundes, es sei denn, Kantone gewährleisten diesbezüglich eine mindestens gleichwertige Informationssicherheit (Art. 3 ISG). Mit dem vorliegenden ICSG wird der letzte Weg gewählt, auch weil die Übernahme des ISG dem Kanton Bern infolge dessen grossen Umfangs und Tiefe nicht gerecht würde (vgl. Ziff. 4.3 oben). Wo im Übrigen der Kanton keine klassifizierten Informationen des Bundes bearbeitet oder nicht auf Informatikmittel des Bundes zugreift, ist von Bundesrechts wegen nichts vorzukehren. Der Kanton ist diesbezüglich frei, Regeln aufzustellen und wenn ja, welche genau. Bundesrecht zwingt beispiels-weise nicht dazu, dass Kantonsparlamente ein förmliches Klassifizierungssystem einführen.»*	Anders umgesetzt. Diese Vortragsstelle ist weitgehend redundant zu der oben diskutierten Ziff. 3.1 des Vortrags. Um Wiederholungen zu vermeiden, wird Ziff. 6.1 durch folgenden Text ersetzt: «Das Parlament hat am 18. Dezember 2020 das ISG verabschiedet, welches am 1. April 2023 in Kraft treten wird (s. Ziff. 3.1 oben).»

5. Keine Bemerkungen / Verzicht auf eine Stellungnahme

Nr.	Absender	Stellungnahme
83.	Bedag	Dieses Gesetz füllt in der Tat einige Lücken. Aus Sicht Bedag ist es nur zu begrüssen. Da die Bedag mit einer Ausnahme (Klassifizierung) nicht direkt betroffen ist, verzichten wir auf eine Eingabe im Vernehmlassungsverfahren.
84.	Ostermundigen	Wir können Ihnen mitteilen, dass seitens Gemeinde Ostermundigen kein Einwand gegen dieses Gesetz angebracht wird.
85.	Zollikofen	Der Gemeinderat Zollikofen verzichtet auf eine Stellungnahme.
86.	VG	Wir danken Ihnen für die Gelegenheit, im Vernehmlassungsverfahren zum Gesetz über die Informations- und Cybersicherheit (ICSG) Stellung nehmen zu können. Gerne teilen wir Ihnen mit, dass wir auf Bemerkungen zur Vorlage verzichten.
87.	CAF	Le CAF a pris connaissance du projet de loi et n'a pas de commentaires particuliers à formuler quant à la population francophone, au bilinguisme ou au respect des langues officielles.
88.	KGV	Nous constatons que le sujet est d'actualité, mais aussi particulièrement technique. Nous pouvons admettre que la sécurité en matière d'informatique appelle une attention accrue et, sous cet angle, n'avons pas de remarques particulières.

6. Verzeichnis der Teilnehmerinnen und Teilnehmer des Vernehmlassungsverfahrens

Die folgenden Organisationen und Personen haben eine Vernehmlassung eingereicht oder erklärt, dass sie auf Bemerkungen bzw. eine Stellungnahme verzichten.

6.1 Verwaltungsexterne Teilnehmende

1.	Bedag	Bedag Informatik AG
2.	Bern	Gemeinde Stadt Bern
3.	Berner KMU	Dachorganisation der kleinen und mittleren Unternehmen im Kanton Bern
4.	Biel	Gemeinde Stadt Biel / Ville de Bienne
5.	BSPV	Bernischer Staatspersonalverband

6.	CAF	Conseil des affaires francophones de l’arrondissemnet de Biel/Bienne
7.	CJB	Conseil du Jura bernois
8.	DSA	Datenschutzaufsichtsstelle
9.	Die Mitte	Die Mitte Partei Kanton Bern
10.	EDU	Eidgenössische-Demokratie Union
11.	FK	Finanzkontrolle des Kantons Bern
12.	GLP	Grünliberale Partei Kanton Bern
13.	Büro GR	Büro des Grossen Rates
14.	Grüne	GRÜNE Kanton Bern
15.	JL	Justizleitung des Kanton Bern
16.	KGV	Kirchgemeindeverband des Kantons Bern
17.	Langenthal	Gemeinde Langenthal
18.	Ostermundigen	Gemeinde Ostermundigen
19.	RSTA	Geschäftsstelle der Regierungsstatthalterämter des Kantons Bern
20.	SP	Sozialdemokratische Partei des Kanton Bern
21.	Steffisburg	Gemeinde Steffisburg
22.	SVP	Schweizerische Volkspartei des Kantons Bern
23.	Thun	Gemeinde Stadt Thun
24.	VG	Verwaltungsgericht des Kantons Bern
25.	Worb	Gemeinde Worb
26.	Zollikofen	Gemeinde Zollikofen