Kommission für Staatspolitik und Aussenbeziehungen
Commission des institutions politiques et des relations extérieures

5. November 2024

Informations- und Cybersicherheitsgesetz

Zusätzliche Informationen für die 1. Lesung

Inhalt

1. Gegenstand

Die Kommission für Staatspolitik und Aussenbeziehungen (SAK) hat das Informations- und Cybersicherheitsgesetz im Oktober 2024 für die erste Lesung in der Wintersession 2024 vorberaten. Im Anschluss hat sie die Finanzdirektion um Beantwortung zusätzlicher Fragen gebeten mit der Absicht, die Antworten dem Grossen Rat für die erste Lesung zur Verfügung zu stellen.

Gestützt auf Art. 16 des Kommissionsreglements hat die SAK das vorliegende Dokument mit Beschluss vom 11. November 2024 öffentlich zugänglich gemacht.

2. Fragen der SAK vom 25. Oktober 2024 und Antworten der Finanzdirektion

2.1 Stand der Arbeiten in den Kantonen

Frage: Aktualisierung der Informationen (siehe Vortrag Kap. 6.2) gemäss der im Namen der SAK durchgeführten Umfrage sowie seither erhaltenen neuen Informationen, insofern diese öffentlich gemacht werden dürfen.

Nachdem die SAK das ICSG am 16. Oktober 2023 erstmals beriet und die Finanzdirektion mit der Abklärung der Situation und der Absichten der anderen Kantone beauftragte, führte das Amt für Informatik und Organisation (KAIO) bei den Sicherheitsfachstellen der anderen Kantone sehr kurzfristig eine entsprechende Umfrage durch. Die Ergebnisse der Umfrage präsentierte die Finanzdirektion der SAK an der Sitzung vom 22. Oktober 2023, gestützt auf die bis dann eingegangenen Antworten von 11 Kantonen.

Nach dieser Sitzung gingen weitere Antworten ein, so dass sich das Meinungsbild der Kantone gestützt auf die Antworten von 17 Kantonen mit Stand Anfang 2024 wie folgt darstellt:

a) Acht Kantone planten den Erlass eines eigenen Informationssicherheitsgesetzes (AG, BE, FR) bzw. anderer kantonaler Gesetzgebung (AI, BL, NW, ZG, ZH).
b) Zwei Kantone hatten das gesetzgeberische Vorgehen noch nicht bestimmt (GE, SG).
c) Acht Kantone planten keine Anpassung der Gesetzgebung (NE, GR, JU, LU, SH, SO, UR, VS).
d) Vier Kantone wollten das ISG, soweit es für die Kantone gilt, direkt anwenden (NE, SH, UR, VS).

Wie an der Kommissionssitzung vom 22. Oktober 2023 in Aussicht gestellt, hat sich das KAIO im Herbst 2024 bilateral mit den Fachstellen anderer Kantone ausgetauscht, die angaben, gesetzgeberischen Handlungsbedarf zu erkennen. Diese Gespräche ergaben zusammengefasst folgende Erkenntnisse:

a) **Aargau:** Der Aargauer Gesetzesentwurf («InfoSIG») war von Mai bis Mitte August 2024 in der Vernehmlassung. Er sieht unter anderem auch dessen Geltung für die Gemeinden und für andere Träger öffentlicher Aufgaben vor, wenn diese klassifizierte Informationen des Kantons bearbeiten oder Zugang zu Informatikmitteln des Kantons haben. Das Gesetz soll aber nicht zum Tragen kommen, wenn die Gemeinden und die anderen Träger öffentlicher Aufgaben eine vergleichbare Informationssicherheit garantieren können. Dies ist der Fall, wenn der IKT-Minimalstandard des Bundes gewährleistet werden kann.

b) **Basel-Landschaft:** Der Kanton will seine Sicherheitsvorschriften vollständig überarbeiten, um das ISG umzusetzen. Eine eigene kantonale Gesetzgebung dazu ist zurzeit nicht geplant. Stattdessen werden zurzeit die Verordnungen zur Informatik und der Informationssicherheit sowie die internen Weisungen zur Informationssicherheit überarbeitet.

c) **St. Gallen:** Die Kantone der Ostschweiz haben sich auf der Stufe der Staatsschreiberinnen und Staatsschreiber über den Handlungsbedarf zur Umsetzung des ISG ausgetauscht und ein gemeinsames Schreiben vom 15. Oktober 2024 an das Staatssekretariat für Sicherheitspolitik des Bundes (SEPOS) verfasst. In diesem bitten sie um die Koordination der Umsetzung des ISG durch den Bund und um entsprechende Hilfestellungen, wie eine Wegleitung, sowie im Bereich der Rechtsetzung um einen Mustererlass z.B. in Anlehnung an das Berner ICSG.

d) **Zug:** Das gesetzgeberische Vorgehen zur Umsetzung des ISG ist im Herbst 2024 noch in juristischer Abklärung. Zur Diskussion stehen ein Gesetz oder eine Verordnung, welche der Regierungsrat gestützt auf seine verfassungsmässigen Zuständigkeiten erlassen könnte.

e) **Zürich:** Das ISG soll für die Kantonsverwaltung mit einer Weisung des Regierungsrates umgesetzt werden, der Allgemeinen Informationssicherheitsrichtlinie (AISR), die die Grundlage des kantonalen Informationssicherheitsmanagementsystems (ISMS) sein soll. Dazu läuft im Herbst 2024 das interne Mitberichtsverfahren. Die AISR beschränkt sich grundsätzlich auf die Kantonsverwaltung (Exekutive), beansprucht aber auch Geltung für alle anderen Behörden, die kantonale Systeme nutzen oder Informationen des Kantons bearbeiten.

2.2 Zusammenarbeit des Kantons bzw. der Kantone mit dem neuen SEPOS und der DVS

Welche Rolle spielt das SEPOS?

Die Aufgaben des SEPOS sind in Artikel 7 der Organisationsverordnung für das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (OV-VBS, SR 172.214.1) geregelt. Soweit im vorliegenden Zusammenhang interessierend, sorgt das SEPOS für die sichere Bearbeitung der Informationen, für die der Bund zuständig ist (Abs. 1 Bst. c), und führt die Fachstellen des Bundes für Informationssicherheit, für Personensicherheitsprüfungen und Betriebssicherheit (Abs. 2).

Die Zusammenarbeit des SEPOS mit den Kantonen regelt das Bundesgesetz über die Informationssicherheit (ISG, SR 232). Danach besteht eine Konferenz der Informationssicherheitsbeauftragten des Bundes, an der auch zwei Vertreterinnen oder Vertreter der Kantone teilnehmen (Art. 82 Abs. 1 ISG), und die namentlich den Informationsaustausch und die Koordination im Bereich der Informationssicherheit sicherstellt (Abs. 2). Die Konferenz berät geplante neue Vorgaben des Bundes, und die Vertretungen der Kantone sollen die Umsetzbarkeit solcher Vorgaben für die Kantone beurteilen. Zudem hat die Fachstelle des Bundes für Informationssicherheit im SEPOS die Aufgabe, die Kantone beim Vollzug des ISG zu beraten (Art. 83 Abs. 1 Bst. a ISG). Sie wird den Kantonen unter anderem Zugang zu den Ausbildungsgrundlagen und Vorgaben des Bundes geben.

Darüber hinaus sieht Artikel 86 Absatz4 ISG vor, dass der Bundesrat festlegt, in welchen Fällen die Kantone die Leistungen der Fachstellen nach dem ISG für ihre eigene Informationssicherheit gebührenpflichtig in Anspruch nehmen können. In diesem Rahmen können die Kantone gestützt auf eine Leistungsvereinbarung mit dem VBS bei der Fachstelle Betriebssicherheit eine Sicherheitsüberprüfung ihrer Auftragnehmer in Auftrag geben (Art. 24 der Verordnung über das Betriebssicherheitsverfahren, VBSV, SR 128.41). Dabei geht es um die Frage, ob ein Unternehmen zur Ausführung eines sicherheitsempfindlichen Auftrags geeignet ist oder ob ein Sicherheitsrisiko besteht (Art. 55 ff. ISG). Ebenso können die Kantone gebührenpflichtig Leistungen der Fachstelle Personensicherheitsprüfung für ihre eigene Informationssicherheit in Anspruch nehmen, wenn sie dazu über eine ausreichende gesetzliche Grundlage für Prüfungen nach dieser Verordnung verfügen, zur Gewährleistung der Informationssicherheit ähnliche Beurteilungen wie der Bund vornehmen wollen, und mit dem VBS eine Leistungsvereinbarung abgeschlossen haben (Art. 35 der Verordnung über die Personensicherheitsprüfungen, VPSP, SR 128.31).

Welche Rolle (Nicht-Rolle) spielt die DVS?

Die Digitale Verwaltung Schweiz (DVS) ist eine gemeinsame Organisation des Bundes und der Kantone. Sie hat die Aufgabe, die digitale Transformation der Verwaltungen in der Schweiz zu fördern, namentlich durch die Entwicklung von Standards und als politische Plattform. Dazu fördert sie den Austausch und die Koordination bei Projekten auf Bundes- und interkantonaler Ebene im Bereich der digitalen Transformation der Verwaltung, gibt Empfehlungen ab, arbeitet mit Fachorganisationen zusammen, und sucht den Dialog mit der Wissenschaft, mit der Wirtschaft und mit der Zivilgesellschaft. Ihre Träger wollen sie zu einer politischen Plattform mit verbindlicher Standardsetzung weiterentwickeln (Ziff. 2 der öffentlich-rechtlichen Rahmenvereinbarung über die Digitale Verwaltung Schweiz, BBl 2021 3030).

Die Rahmenvereinbarung weist der DVS nicht ausdrücklich Aufgaben im Bereich der Informations- und Cybersicherheit zu. Zu ihren Aufgaben gehört jedoch die Förderung gemeinsamer rechtlicher und politischer Grundlagen und Rahmenbedingungen für die digitale Verwaltung, sowie die Stärkung von Vernetzung, Zusammenarbeit und Wissensaustausch innerhalb der öffentlichen Verwaltungen aller drei Staatsebenen (Ziff. 4.2 Bst. d und f der Rahmenvereinbarung). Daraus ergibt sich nach der Meinung der Finanzdirektion, dass es zu den Aufgaben der DVS gehört, die Schaffung von kantonalen Rechtsgrundlagen für die Informationssicherheit zu koordinieren und zu unterstützen. Denn die Sicherheit ist eine zentrale Rahmenbedingung der Digitalisierung, und die von der DVS zu fördernde Digitalisierungszusammenarbeit setzt voraus, dass die miteinander zusammenarbeitenden Gemeinwesen ihre Sicherheitsvorschriften und -massnahmen aufeinander abstimmen.

Mit Recht hat die SAK daher im Rahmen ihrer Beratungen des ICSG verlangt, dass die Finanzdirektion die DVS um die Koordination der Rechtsetzungstätigkeiten der Kantone und des Bundes im Bereich der Informations- und Cybersicherheit bittet. Diese Démarchen erwiesen sich jedoch leider als fruchtlos:

Auf zwei Anfragen vom 30. Oktober 2023 und 6. Dezember 2023 reagierte der Leiter der DVS (der Beauftragte von Bund und Kantonen für die digitale Verwaltung Schweiz) nicht. Nach einem weiteren Schreiben

der Finanzdirektorin vom 19. Januar 2024 an die DVS erfolgte am 30. Januar 2024 ein Treffen zwischen Vertretungen der Finanzdirektion und der DVS. Dessen Ergebnis fasste der Beauftragte mit Schreiben an die Finanzdirektion vom 9. Februar 2024 wie folgt zusammen: «Die Geschäftsstelle der DVS organisiert in Abstimmung mit den Aktivitäten des SEPOS zeitnah einen Roundtable mit Bundes- und Kantonsvertretungen, um Form und Interesse der Kantone an einer Koordination abzuklären. Gestützt darauf prüft die DVS die Einsetzung einer Arbeitsgruppe, eines Projekts oder eines anderen geeigneten Gefässes zur Koordination der Anforderungen und Stossrichtungen der Informationssicherheitsgesetzgebung bzw. der dazugehörigen Ausführungsbestimmungen.»

Diese Vereinbarung setzte die DVS aber nicht um. Am 7. Juni 2024 teilte die DVS dem KAIO mit, am 5. Juni 2024 habe die Konferenz der Informationssicherheitsbeauftragten mit drei Kantonsvertretungen stattgefunden, und das SEPOS sehe im September 2024 eine Konferenz vor, an der alle Kantone teilnehmen sollen. Die DVS sehe, dass bei der Abstimmung der Gesetzgebungstätigkeiten das SEPOS im Lead sei. Die DVS sei der Meinung, dass «die etablierten und geplanten Gefässe» die Erwartungen des Kantons Bern erfüllten. Die erwähnte Konferenz des SEPOS ist nun im November 2024 angesetzt.

Die Finanzdirektion konzentriert sich daher für die weiteren Arbeiten auf den direkten Austausch mit dem SEPOS und den Sicherheitsverantwortlichen anderer Kantone (s. oben).

2.3 Interpellation 050-2024 «Zusammenarbeit zwischen Kanton und Gemeinden bei Digitalisierung» (2024.RRGR.70)

Welches Fazit lässt sich aus der Vorstossantwort für das ICSG und dessen Umsetzung ziehen? Kann die erwähnte Studie dem Grossen Rat oder zumindest der SAK zugänglich gemacht werden?

Diese Frage beantwortet die Finanzdirektion in Abstimmung mit der Geschäftsstelle Digitale Verwaltung der Staatskanzlei.

Die Interpellation 050-2024 warf Fragen zur Zusammenarbeit zwischen Kanton und Gemeinden bei der Digitalisierung auf. In seiner Antwort vom 4. September 2024 bestätigte der Regierungsrat, dass Handlungsbedarf zur Verbesserung der Zusammenarbeit besteht und informierte darüber, dass der Kanton zusammen mit dem Verband Bernischer Gemeinden (VBG) eine Studie in Auftrag gab, die entsprechenden Lösungsansätze erarbeiten soll. Die ersten Studienergebnisse liegen jetzt vor. Die seitens des Kantons federführende Staatskanzlei wird nun einen würdigenden Bericht zuhanden des Regierungsrates erstellen und das weitere Vorgehen durch den Regierungsrat beschliessen lassen. Sobald diese Arbeiten abgeschlossen sind, können die Studie und der würdigende Bericht der SAK zugestellt werden.

Die Interpellation betrifft nicht Fragen der Informations- und Cybersicherheit. Daher geht auch die Studie nicht besonders auf dieses Thema ein. Wir gehen jedoch davon aus, dass die organisatorischen und rechtlichen Grundlagen und Strukturen, die gegebenenfalls zur Vertiefung der Zusammenarbeit zwischen Kanton und Gemeinden bei der Digitalisierung zu erarbeiten sein werden, sich auch dazu eignen werden, die Zusammenarbeit im eng mit der Digitalisierung verbundenen Bereich der Informations- und Cybersicherheit zu organisieren und zu verbessern, soweit dafür Bedarf besteht. Die Staatskanzlei und die Finanzdirektion werden diesem Aspekt bei den weiteren Arbeiten Rechnung tragen.

2.4 Geltungsbereich des Gesetzes für die Gemeinden bzw. Auswirkungen des Gesetzes auf die Gemeinden

In Bezug auf den Geltungsbereich und die Auswirkungen des Gesetzes auf die Gemeinden bestehen für die Kommission gewisse Ungereimtheiten und Widersprüche.

Gemäss Art. 2 gilt das Gesetz für die Gemeinden nur unter Vorbehalt:

Art. 2
Geltungsbereich

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

[2] Für andere Träger öffentlicher Aufgaben und Gemeinden gelten nur die Bestimmungen über

a klassifizierte Informationen, soweit klassifizierte Informationen des Kantons oder des Bundes bearbeitet werden,

b die Sicherheit beim Einsatz von ICT-Mitteln, soweit auf ICT-Mittel des Kantons oder des Bundes zugegriffen wird.

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

Gleichzeitig finden sich im Vortrag aber insbesondere folgende Aussagen:
- *Ziff. 2.2, S. 4: «Weil im Kanton Bern aber alle kantonalen und kommunalen Behörden via ICT-Mittel miteinander vernetzt sind, kann die Informations- und Cybersicherheit nur mit einheitlichen, für alle Behörden geltenden Regeln gewährleistet werden. Zu diesem Zweck wird das ICSG erlassen.»*
- *Ziff. 3.2.1, S. 7: «Dem Kanton Bern fehlt eine effektive und effiziente Sicherheitsorganisation.»*
- *Ziff. 8.4.1, S. 21: Das Gesetz legt im Grundsatz fest, welche Aufgaben die auftraggebenden Behörden erfüllen müssen, um ihre Verantwortung in Bezug auf die Sicherheit wahrzunehmen (vgl. Art. 5, Pflichten der Behörden). Der Regierungsrat muss diese Aufgaben in einem standardisierten Sicherheitsverfahren für alle Behörden näher umschreiben. […] Die wichtigsten Verfahrensetappen müssen auf Verordnungsebene für alle Behörden, nicht nur diejenigen der Kantonsverwaltung, vereinheitlicht werden.*

Im Gesamtkontext ergibt sich daher nach Ansicht der SAK eine regelrechte Pflicht der Gemeinden, sich eine den kantonalen Anforderungen entsprechende umfassende Sicherheitsorganisation zu geben, und zwar eben nicht nur in Bezug auf Informationen und Systeme des Kantons oder des Bundes. Diesbezüglich ist auch auf die Ausführungen zu Art. 29 zu verweisen, welcher gemäss Vortrag auch für die Gemeinden gilt. Im Rahmen der Kommissionssitzung führte die Finanzdirektion jedoch aus, dass diese Bestimmung nicht für die Gemeinden gelte.

Die SAK rechnet jedenfalls damit, dass das ICSG für die Gemeinden weitgehende Auswirkungen haben wird, die gerade kleinere Gemeinden vor grosse Herausforderungen stellen wird, insbesondere im finanziellen Bereich.

Die SAK hätte daher gerne folgende Punkte geklärt: Welche Bestimmungen genau gelten für die Gemeinden?
Der **Geltungsbereich des ICSG** basiert auf dem folgenden Grundsatz: Das Gesetz verpflichtet die Gemeinden und die anderen Träger öffentlicher Aufgaben (TöA) nur in dem Umfang, wie dies zur Wahrung der Sicherheitsinteressen des Bundes und des Kantons nötig ist – mit anderen Worten, nur soweit, wie dies zum Schutz von Informationen oder ICT-Systemen des Bundes oder des Kantons nötig ist. Dies entspricht dem Regelungsansatz von Artikel 3 ISG, der die Kantone auch nur in dem Umfang verpflichtet, wie Informationen oder Systeme des Bundes betroffen sind. Und es reflektiert die Organisationsautonomie der

Gemeinden und TöA: Weil es im ICSG «nur» um die Sicherheitsinteressen der Behörden geht, nicht der Bevölkerung (s. dazu nachstehend), ist es nicht nötig, dass der Kanton den Gemeinden und TöA vorschreibt, wie sie ihre eigenen Sicherheitsinteressen zu schützen haben. Jedoch ist es aus der Sicht des Kantons empfehlenswert, dass die Gemeinden und TöA das ICSG für sich ebenfalls anwenden, ggf. mit Anpassungen, die ihre Risikolage reflektieren, so wie dies der Kanton mit dem ISG tut.

Zu beachten ist zudem, dass das ICSG wie das ISG seinen Geltungsbereich gleich doppelt einschränkt: Es gilt nur im Bereich der Zusammenarbeit mit den höheren Staatsebenen, und auch dort nur in Bezug auf die Regeln über klassifizierte Informationen und die Sicherheit von ICT-Mitteln.

In Bezug auf die **geplante Totalrevision des Datenschutzgesetzes (KDSG)** ist zum Vorstehenden aber ein wichtiger Vorbehalt anzubringen. Das ICSG regelt wie gesagt nur die Sicherheit von Informationen, deren Schutz zur Wahrung öffentlicher Interessen geboten ist, also nicht den ebenso wichtigen Schutz von Personendaten, d.h. Informationen, deren Schutz zur Wahrung der Privatsphäre von Privaten geboten ist. Dies ist ein Thema des Datenschutzrechts. Die Methoden zum Schutz beider Kategorien von Informationen sind aber dieselben, soweit es um die Schutzziele der Sicherheit (Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit) geht.

Daher sieht der Entwurf für die KDSG-Totalrevision vor, dass die *Grundsätze* des ICSG auch für die Sicherheit von Personendaten – sog. Datensicherheit – sinngemäss gelten sollen. Und daher bereiten die Finanzdirektion und die Direktion für Inneres und Justiz eine gemeinsame Ausführungsverordnung für beide neuen Gesetze vor, nämlich die Informations- und Datensicherheitsverordnung (IDSV). Diese (und ihre Ausführungsbestimmungen) werden die Methoden für die Sicherheit staatlicher Informationen und Personendaten einheitlich regeln. Und weil das KDSG vollumfänglich (und nicht wie das ICSG eingeschränkt) auch für die Gemeinden und TöA gilt bzw. weiterhin gelten soll, werden auch die gemeinsamen Ausführungsbestimmungen beider Gesetze auch für die Gemeinden und TöA vollumfänglich gelten, soweit es um die Datensicherheit geht. Das ist nicht neu: Schon heute schreibt die Datenschutzverordnung (DSV, BSG 152.040.1) in Artikel 4 bis 9 allen Behörden, auch den Gemeinden und TöA, vor, mit welchen Massnahmen sie die Datensicherheit sicherzustellen haben. Diese Regelungsthemen werden in die IDSV übernommen und dem aktuellen Stand der Technik angepasst. Der Grosse Rat wird aber später bei der Beratung der Totalrevision des KDSG entscheiden können, ob er sich diesem Lösungsansatz anschliesst.

Damit muss die Frage, inwiefern das ICSG und seine Ausführungsbestimmungen für die Gemeinden und TöA gelten, für die Zeit vor und nach der geplanten KDSG-Totalrevision (rKDSG) separat beantwortet werden:

ICSG Abschnitt	Nur ICSG	ICSG und rKDSG	Bemerkungen
1 Allgemeine Bestimmungen	✓ **Gilt**	✓ **Gilt**	Enthält keine Verpflichtungen.
2 Grundsätze	✗ **Gilt nicht**	✓ **Gilt (PD)**	Die Grundsätze des ICSG sollen nach dem rKDSG auch für Personendaten sinngemäss gelten.
3 Organisatorische Massnahmen	○ **Gilt teils**	○ **Gilt teils**	Es gelten nur die Regeln über den Umgang mit klassifizierten Informationen der höheren Staatsebenen.
4 Technische Massnahmen	○ **Gilt teils**	○ **Gilt teils**	*Nur ICSG:* Es gelten die von der höheren Staatebene vorgeschriebenen Regeln über den Umgang mit deren ICT-Mitteln, ggf. das Sicherheitsverfahren für die Bearbeitung klassifizierter Informationen des Bundes oder Kantons (s. u.) *Mit rKDSG:* Die gemeinsamen Ausführungsbestimmungen zu ICSG und rKDSG können das Sicherheitsverfahren für die Bearbeitung von Personendaten zur Anwendung gelangen lassen.
5 Physische Massnahmen	✗ **Gilt nicht**	✗ **Gilt nicht**	–
6.1 Auswahl, Instruktion und Berechtigung	○ **Gilt teils**	○ **Gilt teils**	*Nur ICSG:* Es gelten nur die von der höheren Staatebene vorgeschriebenen Regeln über den Umgang mit deren ICT-Mitteln. *Mit rKDSG:* Die gemeinsamen Ausführungsbestimmungen zu ICSG und KDSG können dies Grundsätze für die Bearbeitung von Personendaten zur Anwendung gelangen lassen.
6.2 Personensicherheitsprüfung	✗ **Gilt nicht**	✗ **Gilt nicht**	Wenn die Gemeinden eine PSP durchführen wollen, müssen sie dies durch Reglement selbst regeln, z.B. durch Verweis auf das ICSG.
7 Sicherheitsorganisation	✗ **Gilt nicht**	✗ **Gilt nicht**	Art. 29 bezieht sich nur auf die kantonalen Behörden, die dem Gesetz voll unterstehen, aber nicht zur Verwaltung gehören (z.B. Justiz).
8 Ausführungsbestimmungen	○ **Gilt teils**	○ **Gilt teils**	*Nur ICSG:* Es gelten nur die Ausführungsbestimmungen über den Umgang mit ICT-Mitteln und klassifizierten Informationen der höheren Staatsebenen. *Mit rKDSG:* Zudem gelten die gemeinsamen Ausführungsbestimmungen zu ICSG und rKDSG in Bezug auf die Sicherheit von Personendaten.

Vor diesem Hintergrund sind die oben von der SAK angeführten Stellen des Vortrags potenziell missverständlich und hier zu erläutern bzw. zu präzisieren:

1. Die oben zitierte Stelle in Ziff. 2.2, S. 4 des Vortrags ist zutreffend, weil sie die Notwendigkeit reflektiert, im Bereich der staatsebenenübergreifenden Zusammenarbeit einheitliche Regeln anzuwenden, wie das ICSG es vorsieht.

2. In Ziff. 3.2.1, S. 7 des Vortrags ist mit «Kanton Bern» die Gebietskörperschaft mit ihrer Kantonsverwaltung gemeint, nicht alle Behörden im Kantonsgebiet, obwohl die Aussage wohl auch auf viele Gemeinden und TöA zutreffen würde.

3. Wenn allerdings in Ziff. 8.4.1, S. 21 des Vortrags davon die Rede ist, das Sicherheitsverfahren müsse «für alle Behörden, nicht nur diejenigen der Kantonsverwaltung» vereinheitlicht werden, so ist das jedenfalls aus der Perspektive des ICSG nur beschränkt zutreffend: Weil die Gemeinden und TöA nach Massgabe von Art. 2 dem ICSG nur insoweit unterstellt sind, wie sie mit Systemen oder Informationen des Bundes und des Kantons arbeiten, können auch die Vorschriften über das Sicherheitsverfahren für Gemeinden und TöA nur in diesem Umfang Geltung beanspruchen. Das heisst, dass ein Sicherheitsverfahren nach kantonalen Vorgaben für Systeme von Gemeinden nur dann erforderlich ist, wenn die Gemeinden klassifizierte Informationen des Kantons in solchen eigenen Systemen bearbeiten wollen, was wohl selten der Fall sein dürfte.
   Aber wie oben erwähnt, soll das revidierte KDSG die kantonalen Sicherheitsvorschriften auch für die Bearbeitung von Personendaten durch Gemeinden gelten lassen. Wenn der Grosse Rat dieser Absicht im Rahmen der Revision des KDSG folgt, kann dies zur Folge haben, dass die Gemeinden auch für die Systeme, mit denen sie besonders schützenswerte Personendaten bearbeiten wollen, ein Sicherheitsverfahren durchführen müssen. In welchen Fällen dies verhältnismässig ist, wird im Rahmen der Erarbeitung der Ausführungsbestimmungen auch im Austausch mit Vertretungen der Gemeinden zu bestimmen sein.

Welche «impliziten» Pflichten ergeben sich aus dem Gesetz für die Gemeinden (entsprechend dem Grundsatz «Eine Kette ist nur so stark wie ihr schwächstes Glied»)?

Dieser Grundsatz gilt für die Zusammenarbeit der Gemeinden mit dem Bund und dem Kanton, also dann, wenn die Gemeinden Systeme des Bundes oder des Kantons nutzen oder deren Informationen bearbeiten. In diesem Fall ist es wichtig, dass alle Beteiligten dasselbe Sicherheitsniveau gewährleisten, d.h., die gemäss dem ICSG erlassenen Sicherheitsvorschriften bzw. die von der höheren Staatsebene vorgegebenen Nutzungsbestimmungen anwenden. Im Rahmen der oben erwähnten Revision des KDSG ist zudem vorgesehen, die kantonalen Sicherheitsvorschriften auch für die Bearbeitung von Personendaten anzuwenden, denn für die Bürgerinnen und Bürger, deren Privatsphäre es zu schützen gilt, macht es keinen Unterschied, ob ihre Personendaten von einer Gemeinde oder vom Kanton bearbeitet werden.

Wie werden die anderen Behörden, also nicht nur Gemeinden, im Aufbau und der Befähigung zur Sicherheitsorganisation unterstützt, zu welchen Bedingungen können sie beim Kanton Supportleistungen beziehen und welcher Ressourcenbedarf wäre dafür beim Kanton nötig (siehe auch unten «Kosten/Ressourcen»)? FAQs reichen für die Gemeinden nämlich nicht aus. Sie benötigen konkrete Vorlagen und konkreten Support.

Das KAIO unterstützt die kantonalen und kommunalen Behörden bei der Umsetzung des ICSG wie folgt:

1. Erstens wird es die im Rahmen des Projekts IS@BE erstellten **Vorlagen, Hilfsmittel und Schulungsunterlagen** im Internet allen Behörden zur Verfügung stellen. Dazu gehören beispielsweise Vorlagen und Muster für Sicherheitsdokumente. Der Kanton bietet aber auch niederschwellige Aus- und Weiterbildungsangebote für Mitarbeitende und ICT-Fachleute an, etwa in der Form von Webinaren (Videokonferenzen mit der Möglichkeit, Fragen zu stellen und die Aufzeichnung später als Video anzusehen), oder web-basierte Trainings (interaktive Trainingssequenzen mit Übungen und Tests).

2. Zweitens unterstützt das KAIO die kantonalen und kommunalen Behörden im Rahmen seiner Kapazitäten mit **Beratung** zum zweckmässigen Vorgehen im Bereich der Informationssicherheit. Ein möglicher Ansatz dafür ist, den Sicherheitsverantwortlichen der Gemeinden einen niederschwelligen Zugang zu

den Sicherheitsfachleuten des Kantons zu vermitteln, um einfache Fragen und Anliegen rasch beantworten zu können.

3. Weil jedoch die personellen Kapazitäten des Kantons für eine eingehende Beratung oder Unterstützung der kantonalen und kommunalen Behörden nicht ausreichen, ermöglicht das KAIO drittens allen Behörden und Trägern öffentlicher Aufgaben im Kanton den **Abruf von Sicherheitsdienstleistungen bei externen Leistungserbringern.** Einen entsprechenden Rahmenvertrag zu Gunsten aller Behörden hat das KAIO bereits 2023 öffentlich ausgeschrieben. Er umfasst folgende Leistungen:
   a) *ICT-Sicherheits-Spezialist/-in Junior, Senior, Senior Expert:* Beratung und Unterstützung von Führungspersonen und Mitarbeitenden bei der Erarbeitung von ISDS-Unterlagen auf der Basis von bestehenden Vorlagen (ISDS-Konzepte, Risikoanalysen, etc.) und bei der Umsetzung der daraus folgenden Massnahmen. Wahrnehmung der HERMES-Rolle als ISDS-Verantwortliche/-r. Mithilfe bei der Erarbeitung der Informationssicherheitsvorgaben auf allen Ebenen. Überprüfung der Einhaltung von Sicherheitsvorgaben. Förderung des Informationssicherheits- und Datenschutzbewusstseins innerhalb der Organisationseinheiten.
   b) *ICT-Sicherheits-Beauftragte/-r Senior:* Unterstützung und Beratung bei konzeptionellen Aufgaben im Bereich ISMS. Mithilfe bei der Erarbeitung der Informationssicherheits-Vorgaben auf allen Ebenen. Abklärungen im Bereich komplexer Sicherheitsfragen. Überprüfung der Einhaltung von Sicherheitsvorgaben.
   c) *IT-Security Awareness:* Für die Sensibilisierung der Mitarbeitenden setzt der Rahmenvertragspartner ein Tool ein, welches bereits standardisierte Inhalte (Kampagnen, e-Learnings) enthält. Zudem verfügt er über ein Vorgehenskonzept und ist in der Lage, Auswertungen vorzunehmen. Er bietet die Rollen Projektleiter(in) / Awareness-Berater(in) und Integrationsspezialist(in), Social Engineering an.
   d) *IT-Security-Audit:* Das Audit umfasst eine Sicherheits- und Risiko-Analyse anhand vorhandener Schwachstellen und Sicherheitslücken, Prozessen oder organisatorischen Massnahmen in einer Organisation, und das Erarbeiten von Massnahmenvorschlägen. Der Rahmenvertragspartner bietet die Rollen Auditleiter/-in und Audit-Prüfungsmitglied an.
   e) *IT-Penetration-Testing:* Ein IT-Penetration-Test prüft, z.B. im Rahmen eines IT-Security-Audits, die Sicherheit möglichst aller Systembestandteile und Anwendungen eines Netzwerks oder Softwaresystems mit Mitteln und Methoden, die tauglich sind, um unautorisiert in das System einzudringen (Penetration). Der Anbieter verfügt über ein standardisiertes Verfahren (z.B. OSSTMM) für die Durchführung von IT-Penetration-Tests.

   Mit dieser gebündelten Ausschreibung für den ganzen Kanton können die Berner Behörden von besseren Konditionen profitieren, als sie erhalten würden, wenn sie die Leistungen einzeln beschaffen würden. Die Konditionen unterstehen der vertraglichen Geheimhaltungspflicht und werden interessierten Behörden auf Anfrage bekannt gegeben. Dieses Angebot und weitere zentrale Beschaffungsangebote des Kantons sind zurzeit im Intranet des Kantons beschrieben, auf das die Gemeinden und die Mitglieder des Grossen Rates mit dem kantonalen Arbeitsplatz Zugang haben. Ab Dezember 2024 werden diese Angebote im Internet veröffentlicht (www.be.ch/beschaffungen > Zentrale Beschaffungsstellen (ZBS) > ZBS ICT).

   Wenn sich in der Umsetzung zeigt, dass der Umfang der Leistungen oder die Kapazität der Rahmenvertragspartner nicht ausreicht, um die Nachfrage zu decken, ist das KAIO gerne bereit, in Zusammenarbeit z.B. mit Vertretungen des Verbandes Bernischer Gemeinden und grösserer TöA zusammen eine ergänzende öffentliche Ausschreibung zu konzipieren und durchzuführen.

4. Und viertens beabsichtigt das KAIO, mit Unterstützung der Rahmenvertragspartner der oben erwähnten Leistungen eine **Aus- oder Weiterbildung für die Sicherheitsverantwortlichen und Mitarbeitenden der Gemeinden** zu konzipieren und durchzuführen, um den Auftrag zu erfüllen, der nach dem Willen der SAK in Artikel 19 Absatz 2 ICSG verankert werden soll. Der Inhalt und Umfang dieser Aus- oder

Weiterbildung wird ebenfalls in Zusammenarbeit mit den Vertretungen interessierter Gemeinden und TöA sowie dem VBG und/oder dem Verband Bernisches Gemeindekader erarbeitet.

2.5 Kosten/Ressourcen

Gemäss Vortrag hat die Umsetzung des Gesetzes kostenneutral zu erfolgen (Ziff. 10 und 11). Die SAK bezweifelt nach wie vor, dass dies möglich ist. Die Aussage «Dem Kanton Bern fehlt eine effektive und effiziente Sicherheitsorganisation.» deutet in diese Richtung. Alleine das Personal mit den nötigen Kompetenzen für die Umsetzung der Sicherheitsorganisation in der kantonalen Verwaltung wird zu Mehrkosten führen (siehe Vorgaben betr. Kompetenzen im Verordnungsentwurf Art. 38 Abs. 4). Die Finanzdirektion räumte zudem selber in den Fragen und Antworten ein, das sich Effizienzgewinne aus der Digitalisierung nicht beziffern lassen.

Die SAK hätte daher gerne Ausführungen dazu, wo die Finanzdirektion realistischerweise zusätzlichen Ressourcenbedarf ausmacht.

Es steht ausser Frage, dass die öffentliche Verwaltung für Informations- und Cybersicherheit in der Zukunft mehr Geld und Personal einsetzen muss als bisher. Dieser Mehraufwand ist aber nicht eine Folge des ICSG als solchem. Denn das Gesetz bzw. seine Ausführungsbestimmungen beschreiben lediglich, was heute den «state of the art» der Informationssicherheit ausmacht. Es gibt daher nur wieder, was die Behörden daher grundsätzlich heute schon unternehmen müssen bzw. müssten, um ihre Informationen vor dem Zugriff durch Unbefugte zu schützen, und um ihre Systeme bzw. ihre Fähigkeit zur Aufgabenerfüllung vor Cyberangriffen zu schützen.

Stattdessen ergibt sich der Mehraufwand aus den stark zunehmenden Sicherheitsrisiken, die es unabhängig vom ICSG gibt. Diese Risiken sind zum einen eine Folge der zunehmenden Verwundbarkeit der Wirtschaft, Gesellschaft und öffentlichen Verwaltung der Schweiz hinsichtlich der Cyberrisiken. Wegen der Digitalisierung aller Lebensbereiche ist es heute viel eher als noch vor einigen Jahren möglich, dass Cyberangriffe auf kritische Infrastrukturen das öffentliche Leben und das Wirtschaftsleben in der Schweiz weitgehend lahmlegen können, oder dass durch den Diebstahl grosser Datenbestände viele Menschen in ihrer Privatsphäre oder als Folge von Identitätsdiebstahl an ihrem Vermögen geschädigt werden. Darüber hinaus sind die zunehmenden Sicherheitsrisiken aber auch eine Folge einer Zunahme geopolitischer Spannungen und kriegerischer Auseinandersetzungen, die immer mehr auch im Cyberraum stattfinden und die Schweiz direkt betreffen. So schreibt Bundesrätin Amherd im Vorwort des Sicherheitsberichts 2024 des Nachrichtendienstes des Bundes (NDB): «Russland und andere staatliche Akteure führen (...) einen hybriden Konflikt mit den westlichen Staaten, der uns etwa in Form von Spionage, Proliferation und Beeinflussungsaktivitäten direkt trifft.»

Um diesen steigenden Risiken gerecht zu werden, ist es nötig, dass die Behörden im Kanton Bern in den nächsten Jahren konkret in den folgenden Bereichen mehr unternehmen, wenn sie das nicht schon getan haben:

1. Die **Umsetzung von Sicherheitsmassnahmen.** Dazu gehören beispielsweise
   a) ein wirksamer Zugriffsschutz schützenswerter Informationen (z.B. durch Verschlüsselung) in jedem Stadium ihrer Bearbeitung,
   b) die Einführung und Pflege eines Systems zur Verwaltung der zum Zugriff auf schützenswerte Informationen berechtigten Personen und ihrer Berechtigungen («Identity and Access Management»), das namentlich sicherstellt, dass jede Person jederzeit nicht über mehr als die benötigten Berechtigungen verfügt,
   c) eine sichere Authentifizierung der Benutzenden bei ihrer Anmeldung an ICT-Systemen, die es möglichst ausschliesst, dass Unbefugte sich als Berechtigte ausgeben können, z.B. durch eine Zwei-

Faktor-Authentifizierungsmethode, die neben einem Passwort ein weiteres Zugangselement wie einen Code aus einer Smartphone-App voraussetzt, und
d) die regelmässige Überprüfung der Vertrauenswürdigkeit von Personen mit Zugang zu schützenswerten Informationen mit einer Personensicherheitsprüfung.

2. Die Massnahmen, die es ermöglichen, die **Sicherheitsmassnahmen risikogerecht auszugestalten,** wie etwa:
   a) der Aufbau und die Pflege eines Risikomanagements, mit dem die Führung Sicherheitsrisiken regelmässig identifiziert, bewertet, und entweder durch Massnahmen vermeidet oder reduziert, oder aber akzeptiert, und
   b) die Klassifizierung aller Informationen und ICT-Mittel auf ihren Schutzbedarf hin, damit die Sicherheitsmassnahmen in Abhängigkeit vom Schutzbedarf ausgestaltet werden können, und überschiessende bzw. zu aufwändige Sicherheitsmassnahmen vermieden werden können.

3. Die regelmässige **Überprüfung der Umsetzung der Sicherheitsmassnahmen** durch alle Beteiligten, wie die externen Dienstleistungserbringer (Auftragsdatenbearbeiter), die Partnerorganisationen mit Zugriff auf schützenswerte eigene Informationen, und die eigenen Mitarbeitenden. Dies erfolgt beispielsweise durch
   a) das Einverlangen und Auswerten einer Berichterstattung über die Umsetzung der Massnahmen,
   b) Audits der Sicherheitsdokumentation und der ICT-Systeme,
   c) die Auswertung der Meldungen allfälliger Sicherheitsvorfälle und Gegenmassnahmen, und
   d) die Überprüfung der Wirksamkeit der Sicherheitsmassnahmen, etwa durch simulierte Angriffe auf die eigene Organisation und die eigenen Systeme, um Schwachstellen ausfindig zu machen («Penetration Testing»).

4. Eine Organisation, die eine **stetige Verbesserung des Sicherheitsniveaus und der Sicherheitskultur** der jeweiligen Behörde ermöglicht, wie namentlich
   a) ein Informationssicherheitsmanagementsystem (ISMS), bestehend aus den Prozessen, mit denen eine Behörde ihre Sicherheitsanforderungen und -ziele festlegt, daraus Massnahmen ableitet, diese umsetzt und die Umsetzung kontrolliert, was als «Plan, Do, Check, Act»-Zyklus ständig wiederholt wird und somit zu einer stetigen Verbesserung führt,
   b) ein Verfahren zur einfachen und raschen Meldung, Nachverfolgung und Auswertung von Sicherheitsvorfällen, sowie
   c) die funktionsangemessene Aus- und Weiterbildung der eigenen Mitarbeitenden in Sicherheitsbelangen, sowie ihre regelmässige Sensibilisierung z.B. durch Übungen, mit denen überprüft wird, ob die Mitarbeitenden auf simulierte Angriffe (z.B. Phishing-E-Mails) angemessen reagieren.

Dafür benötigen die Behörden angemessene Ressourcen. Das gilt grundsätzlich auch für Gemeinden und TöA. Die Festlegung und Umsetzung von Massnahmen muss aber immer in einer den jeweiligen Risiken angemessenen Art und Weise erfolgen. Es ist daher möglich, dass die Gemeinden nach einer Risikobeurteilung zum Schluss gelangen, dass auf ihrer Stufe viele dieser Massnahmen nicht oder nur eingeschränkt nötig sind. Ausserdem zeigt die Erfahrung, dass Sicherheitsmassnahmen wirksamer und besser umsetzbar sind, wenn sie in kleinen Schritten im Sinne einer stetigen Verbesserung erfolgen, statt dass versucht wird, mit einem Grossprojekt die Sicherheitsmaturität einer Organisation auf einen Schlag stark zu verbessern. Dies erlaubt auch die zeitliche Staffelung und den sukzessiven Aufbau von zusätzlichen Sicherheitsressourcen.

Die finanziellen Rahmenbedingungen des Kantons verbieten es, den bei ihm anfallenden Mehraufwand durch eine Erhöhung der Ausgaben bzw. der Stellenplafonds der Verwaltung zu decken. Der Regierungsrat will den Mehraufwand in der Kantonsverwaltung daher im Rahmen der heutigen bzw. geplanten ICT-Budgets und Stellenbestände auffangen. Dazu verfolgt er drei Ansätze:

1. Er will die **Effizienzgewinne der Digitalisierung** für Investitionen in die Sicherheit nutzen. Dies setzt voraus, dass die Behörden den Auftrag des Gesetzes über die digitale Verwaltung zur Digitalisierung ihrer Abläufe konsequent umsetzen. Je mehr Geschäftsprozesse digital und damit – etwa dank künstlicher Intelligenz – ganz oder teilweise automatisch abgewickelt werden können, desto mehr personelle Ressourcen für die Sachbearbeitung werden frei und können unter anderem für Sicherheitsfachleute eingesetzt werden.

2. Er will die **Zusammenarbeit bei der Digitalisierung** stärken. Gerade, weil die ICT und ihre Sicherheit immer teurer wird, ist es essenziell, dass die Behörden im Kanton so viele Lösungen wie möglich gemeinsam nutzen – über alle Staatsebenen hinweg, mit den Gemeinden und allen anderen Akteuren im öffentlichen Sektor. Denn so müssen die Behörden die Kosten für die Entwicklung einer Lösung und für ihre Sicherheit nur einmal bezahlen statt vielfach. Auch dafür ist die Umsetzung des Zusammenarbeitsauftrags des DVG wichtig.

3. Und das **ICSG selbst** ist ein wichtiger Faktor zur Eindämmung steigender Sicherheitskosten. Denn es vermittelt den kantonalen Behörden ein einheitliches Sicherheitsrahmenwerk, mit einheitlichen Standards und Vorlagen. Das heisst z.B., dass die einzelnen Behörden keinen grossen Aufwand betreiben müssen, nur um zu entscheiden, welche Grundschutzmassnahmen sie ergreifen und wie sie sie umsetzen müssen. Sondern sie können sich auf das Identifizieren und Adressieren ihrer spezifischen Risiken konzentrieren.

2.6 Personensicherheitsprüfungen (PSP)

Hierzu hätte die SAK gerne zusätzliche Ausführungen, wie das im aktuellen Entwurf des Regierungsrates vorgesehene System genau funktionieren soll. Also ohne einheitliche Form oder Prüfstelle, keine Differenzierung von Prüfstufen, keine Periodizität und keine Regelung für Aufbewahrung/Vernichtung der erhobenen Daten. Dabei sollen die mündlichen Ausführungen der Finanzdirektion im Rahmen der Kommissionssitzung aufgegriffen werden, also etwa, dass sich Personensicherheitsprüfungen in den allermeisten Fällen auf das Einholen von Straf- und Betreibungsregisterauszügen beschränken dürften und dass es bei den Personensicherheitsprüfungen generell nur um wenige Funktionen gehe.

Vor dem Hintergrund, dass die SAK die Rückweisung der PSP-Bestimmungen an den Regierungsrat einstimmig beschlossen hat, beantragt die Finanzdirektion dem Regierungsrat, sich diesem Antrag anzuschliessen. Ein neuer Regelungsvorschlag soll dann in der 2. Lesung beraten werden. Daher halten wir unsere Ausführungen zu dem nun wohl dem Untergang geweihten Regelungsvorschlag des Regierungsrates kurz.

Nach der von der SAK zur Rückweisung beantragten Konzeption des Regierungsrates soll das bereits heute im Polizeigesetz vorgesehene Verfahren der Personensicherheitsprüfung auf alle kantonalen Behörden ausgedehnt werden. Das heisst, jede Behörde entscheidet selbst, wen sie prüft. Allerdings bedeutet das nicht, dass zukünftig jede Mitarbeiterin und jeder Mitarbeiter gewissermassen nach Gutdünken der Vorgesetzten durchleuchtet werden kann. Denn Artikel 22 ICSG schränkt die PSP auf Personen ein, die «häufig oder in grossem Umfang» bzw. «weitreichenden Einblick» in VERTRAULICHE oder GEHEIME Informationen haben. Daraus folgt, dass sich der Kreis der Geprüften in der Verwaltung wohl auf wenige hundert Personen beschränken dürfte. Dabei dürfte es sich primär um Führungspersonen und Mitarbeitende in den Generalsekretariaten und in den Ämtern mit sicherheitsrelevanten Aufgaben handeln (wie KAPO, BSM, AJV, KAIO) sowie ICT-Fachpersonen, die über erweiterte Berechtigungen verfügen, mit denen sie auf schützenswerte Informationen zugreifen können. Dazu gehört etwa das Supportpersonal des KAIO, oder die Service Manager von Applikationen wie BE-GEVER oder GERES, mit denen schützenswerte Informationen bearbeitet werden.

Auch entscheidet jede Behörde selbst, wann bzw. wie oft sie die Prüfung durchführt, und welche der vom Gesetz vorgesehenen Informationen sie im Rahmen der Prüfung durchführt. Dies legt die Behörde aber nicht willkürlich fest, sondern als Ergebnis der individuellen Beurteilung der Risiken für die von ihr zu schützenden Sicherheitsinteressen. Ebenso wie sie z.B. beurteilen muss, welche physischen oder organisatorischen Massnahmen zum Schutz ihrer Informationen zu ergreifen sind, muss sie beurteilen, welche der von ihr angestellten oder gewählten Personen ein massgebliches Risiko für die mit dem ICSG zu schützenden öffentlichen Interessen darstellen würden, wenn sie sich z.B. als korrupt oder erpressbar herausstellen würden. Wir gehen davon aus, dass im Regelfall eine Prüfung der Straf- und Betreibungsregister ausreichend ist, denn in den meisten Fällen finden ernsthafte Charakterfehler, die den Behörden zur Kenntnis gelangen, in diesen Registern Niederschlag. Bei den wohl sehr wenigen Funktionen mit sehr hohem Risikopotenzial dagegen kann es dagegen verhältnismässig sein, auch Informationen aus Polizeidatenbanken einzuhalten oder bisherige Kontaktpersonen der Geprüften zu befragen.

Im Gegensatz zum stark formalisierten und verrechtlichen Regelung des Bundes beschränken sich auch die Verfahrensvorschriften auf ein Minimum. Ebenso fehlen jedenfalls auf Gesetzesebene Regeln über die Aufbewahrung der Unterlagen. Diese wären auf Verordnungsebene aufzustellen, in Nachachtung des datenschutzrechtlichen Prinzips, wonach Personendaten nur so lange aufbewahrt werden dürfen, wie sie benötigt werden.

Dieser Regelungsansatz hat im Vergleich zur sehr ausführlichen Regelung des Bundes sicher den Nachteil, dass die PSP in den verschiedenen Behörden unterschiedlich angewendet werden kann und dass für die Geprüften weniger gut vorhersehbar ist, ob und wie sie geprüft werden. Aus der Sicht der Finanzdirektion hat diese Lösung aber den massgeblichen Vorteil, dass sie sich in der KAPO bewährt hat und dass sie von jeder Behörde selbst durchgeführt werden kann, ohne dass wie im Bund eine grosse Anzahl von PSP-Fachleuten angestellt werden muss.

Zudem soll auf die Gemeinden eingegangen werden («schwächstes Glied in der Kette», siehe auch oben).

Nach der Konzeption des ICSG gilt es für die Gemeinden nur stark eingeschränkt, nämlich in dem Umfang, wie Sicherheitsinteressen des Kantons oder des Bundes betroffen sind (s. oben Ziff. 2.4). Vor diesem Hintergrund wäre es denkbar gewesen, auch die Bestimmungen über die PSP für die Gemeinden gelten zu lassen, soweit Gemeindepersonal klassifizierte Informationen des Kantons oder des Bundes bearbeitet. Das ICSG sieht das aus folgenden Gründen nicht vor:

a) Die Belastung der Gemeinden durch das ICSG soll auf das zum Schutz der Sicherheitsinteressen des Kantons und des Bundes nötige Minimum beschränkt werden.
b) Es dürfte eher die Ausnahme als die Regel sein, dass Gemeinden klassifizierte Informationen der höheren Staatsebenen bearbeiten.
c) Für die sicherheitsverantwortlichen Stellen des Kantons wäre es schwer zu überblicken und zu kontrollieren, welche Personen auf Gemeindeebene einer PSP unterzogen werden müssten, bzw. ob das sachgerecht erfolgt ist.
d) Auf Gemeindeebene werden Geschäfte häufiger als auf kantonaler Ebene von vom Volk gewählten Behördenmitgliedern (Gemeinderats-, Parlaments- oder Kommissionsmitgliedern) bearbeitet, und für solche Personen sehen weder das ISG noch das ICSG eine PSP vor.

Aus diesen Gründen ist es aus der Sicht der Finanzdirektion unter Risikogesichtspunkten vertretbar, die Gemeinden vom Geltungsbereich der PSP-Bestimmungen auszunehmen. Wenn es aber aus der Sicht der SAK ein Mehrwert wäre, den Gemeinden und den anderen TöA optional die Anwendung der PSP-Bestimmungen zum Schutz ihrer eigenen Sicherheitsinteressen zu ermöglichen, würde sich die Finanzdirektion entsprechenden Anträgen nicht grundsätzlich widersetzen.

Weiter möchte die SAK Ausführungen zur Haltung der Finanzdirektion zum Expertenurteil, dass die Bestimmungen noch der «Schärfung» bedürfen.

Nach unserer Erinnerung – die Kommissionsprotokolle liegen im Zeitpunkt der Beantwortung dieser Fragen noch nicht vor – äusserte sich der von der SAK angehörte Experte sinngemäss wie folgt: Die PSP sei im ICSG seiner Meinung nach zu vage geregelt. Es bleibe unklar, wann welche Informationen eingeholt würden. Der Bund regle das klarer mit Prüfstufen. Das sollte auch im ICSG stehen.

Der Experte legte aber nach unserer Erinnerung nicht dar, aus welchen z.B. rechtlichen oder politischen Gründen er eine solche Präzisierung für sinnvoll hielt. Daher können wir seine Einschätzung nicht näher beurteilen. Wir können daher hier nur auf unsere vorstehende Beurteilung verweisen, wonach wir es für sinnvoll halten, den Entscheid über den Umfang der PSP abhängig von der jeweiligen Risikobeurteilung der verantwortlichen Behörde in deren Ermessen zu stellen. Ausserdem geben wir zu bedenken, dass die vom Regierungsrat vorgeschlagenen PSP-Regeln in Abstimmung mit dem kantonalen Datenschutzbeauftragten erarbeitet wurden, was darauf hinweist, dass sie jedenfalls aus grundrechtlicher Sicht unbedenklich sind.