Kanton Zug

Finanzdirektion

Beilage 1
FD FDS 4.5 / 19 / 163445

Gesetz über die Informationssicherheit (Informationssicherheitsgesetz, ISG)

Bericht und Antrag des Regierungsrates
vom Datum

Sehr geehrter Herr Präsident
Sehr geehrte Damen und Herren

Wir unterbreiten Ihnen eine Vorlage zum Gesetz über die Informationssicherheit (Informationssicherheitsgesetz, ISG) und erstatten Ihnen dazu nachstehen-den Bericht, den wir wie folgt gliedern:

1. In Kürze

Die grundlegenden Bestimmungen über Einschränkungen verfassungsmässiger Rechte müssen in einem Gesetz im formellen Sinn geregelt werden. Die kantonalen Organe dürfen besonders schützenswerte Personendaten sowie Persönlichkeitsprofile nur bearbeiten, wenn ein Gesetz dies ausdrücklich vorsieht. Im Informationssicherheitsgesetz des Bundes wurde mit einer zusätzlichen, per 1. April 2025 in Kraft getretenen Bestimmung über die Bearbeitung von Personendaten die notwendige Grundlage geschaffen. Das vorliegende Informationssicherheitsgesetz des Kantons Zug (ISG) bildet die gesetzliche Grundlage für die Bearbeitung der Personendaten. Die technischen und organisatorischen Vollzugsbestimmungen werden in einer Verordnung des Regierungsrates geregelt, um eine hohe Flexibilität bei notwendigen Anpassungen an sicherheitstechnische Rahmenbedingungen zu ermöglichen.

Die Informationssicherheit im Kanton Zug muss an die Herausforderungen der Informationsgesellschaft angepasst werden. Die Umsetzung bzw. Gewährleistung der Informationssicherheit steht im ISG im Vordergrund. Es gilt den Schutz von Informationen und die Sicherheit beim Einsatz von Informatikmitteln zu gewährleisten. Das ISG schafft für die kantonalen Organe einen einheitlichen formell-gesetzlichen Rahmen für die Steuerung und Umsetzung der Informationssicherheit im Zuständigkeitsbereich des Kantons. Der Missbrauch von Informationen und die Störung von Informationssystemen können wesentliche Interessen des Kantons und die Rechte von Personen beeinträchtigen.

Das ISG richtet sich primär an die kantonalen Organe. Private und die Wirtschaft sind vom Gesetz nur dann betroffen, wenn sie im Auftrag der kantonalen Organe sicherheitsempfindliche Tätigkeiten ausführen. Die Gemeinden sind für eine gleichwertige Informationssicherheit verantwortlich, wenn sie klassifizierte Informationen des Kantons und des Bundes bearbeiten oder auf seine Informatikmittel zugreifen. Für sie gelten die Bestimmungen des ISG, wenn keine gleichwertigen Grundlagen im Bereich der Informationssicherheit bestehen. Daher ist das ISG für die Gemeinden subsidiär anwendbar.

Die Regelung über die Personensicherheitsprüfungen (PSP) setzt eine gesetzliche Grundlage voraus, weil besonders schützenswerte Personendaten gemäss der Datenschutzgesetzgebung bearbeitet werden. Die Bestimmungen über die PSP bilden einen wesentlichen Bestandteil des vorliegenden ISG.

Im ISG werden ausschliesslich diejenigen Themen geregelt, welche auf einer formellen gesetzlichen Grundlage beruhen müssen. In der ISV werden die technisch organisatorischen Themen behandelt.

Die Fachstelle ist das Fachorgan für die Informationssicherheit und ist der Finanzdirektion zugeordnet; sie muss ihre Aufgaben fachlich unabhängig und selbständig erfüllen können.

2. Grundlagen der Informationssicherheit gemäss Bundesrecht

2.1. Bundesgesetzgebung als Grundlage des kantonalen ISG

Das Bundesgesetz über die Informationssicherheit (Informationssicherheitsgesetz, ISG-Bund) vom 18. Dezember 2020 (SR 128) ist am 1. Januar 2024 in Kraft getreten. Es soll Lücken des geltenden Rechts schliessen und für alle Behörden und Organisationen des Bundes (Art. 2 ISG-Bund) gelten. Für die Kantone gelten die Bestimmungen des ISG-Bund und dessen Ausführungsverordnungen nur dann, sofern sie klassifizierte Informationen des Bundes bearbeiten oder auf Informatikmittel des Bundes zugreifen (Art. 3 Abs. 1 ISG-Bund). Für Organisationen des öffentlichen und des privaten Rechts, die kritische Infrastrukturen betreiben, gelten die Bestimmungen über die Massnahmen des Bundes zum Schutz der Schweiz vor Cyberbedrohungen (Art. 2 Abs. 5 ISG-Bund). Das ISG-Bund regelt die Vorgaben und Massnahmen, um eine sichere Bearbeitung der Informationen, für die der Bund zuständig ist, und den sicheren Einsatz und Betrieb der Informatikmittel des Bundes zu gewährleisten.

Art. 3 Abs. 2 ISG-Bund enthält eine Ausnahme für die Kantone. Danach sind die Bestimmungen des ISG-Bund dann nicht auf die Kantone anwendbar, wenn diese über eine mindestens gleichwertige Informationssicherheit verfügen. In der Botschaft des Bundesrates zum ISG-Bund vom 22. Februar 2017 (BBl 2017 2953) wird dazu festgehalten (S. 2975): «Die Kantone sind für ihre Informationssicherheit selbst zuständig. Der Bundesrat will und kann aus verfassungsrechtlichen Gründen keine allgemeinen Vorschriften für die Kantone festlegen. Allerdings hat der Bund ein direktes Interesse daran, dass die Kantone und ihre untergeordneten Stellen einen gleichwertigen Schutz gewährleisten, wenn sie geschützte Informationen des Bundes bearbeiten oder auf seine Informatikmittel zugreifen.» Allerdings sollen «die Vorschriften des Bundes nur dann zur Anwendung kommen, wenn die Vorschriften und Massnahmen der Kantone den Sicherheitsanforderungen des Bundes nicht genügen (Subsidiarität). Die Kantone sollen zudem verpflichtet werden, die Wirksamkeit der getroffenen Schutzmassnahmen periodisch zu überprüfen und die zuständige Stelle des Bundes über die Ergebnisse zu informieren…».

Massgebend ist damit das in der Botschaft des Bundesrates erwähnte Subsidiaritätsprinzip: Danach gelten die Bestimmungen des ISG-Bund und dessen Ausführungsverordnungen für die Kantone nur dann, wenn ihre Gesetzgebung keinen gleichwertigen Schutz gewährleistet. Voraussetzungen für das Vorliegen einer Gleichwertigkeit:

1. Die kantonalen Vorschriften und Massnahmen zur Informationssicherheit müssen die gleichen Schutzwirkungen erzielen, wie die Sicherheitsanforderungen des Bundes in Bezug auf klassifizierte Informationen und Informatikmittel.
2. Die Informationssicherheit im Kanton muss auch die Informationen des Bundes und dessen Informatikmittel miteinbeziehen.
3. Die Kantone müssen die Wirksamkeit der getroffenen Schutzmassnahmen periodisch prüfen und die zuständige Stelle des Bundes über die Ergebnisse orientieren.

2.2. Sicherheitsanforderungen des Bundes

Die Informationen und die Informatikmittel des Bundes müssen mittels organisatorischen, personellen, technischen und physischen Sicherheitsmassnahmen geschützt werden. Das ISG-Bund enthält hierzu unter dem 2. Kapitel (Allgemeine Massnahmen) Grundsätze und Vorgaben, wie diese Sicherheitsmassnahmen auszugestalten sind. Zentral ist dabei Art. 6 Abs. 2 ISG-Bund, wonach die Informationen ihrem Schutzbedarf entsprechend:

1. nur Berechtigten zugänglich sind (Vertraulichkeit);
2. verfügbar sind, wenn sie benötigt werden (Verfügbarkeit);
3. nicht unberechtigt oder unbeabsichtigt verändert werden (Integrität);
4. nachvollziehbar bearbeitet werden (Nachvollziehbarkeit).

Zudem müssen die Informatikmittel, welche zur Erfüllung von gesetzlichen Aufgaben eingesetzt werden, vor Missbrauch und Störung geschützt werden (Art. 6 Abs. 3 ISG-Bund). Damit ein gleichwertiger Schutz innerhalb eines Kantons vorliegt (und somit die Ausnahme nach Art. 3 Abs. 2 ISG-Bund geltend gemacht werden kann), müssen deshalb neben den spezifischen Anforderungen zum Schutz von klassifizierten Informationen und von Informatikmitteln des Bundes auch die übrigen Bestimmungen des ISG-Bund vom kantonalen Recht erfasst werden.

Es handelt sich dabei einerseits um die allgemeinen Grundsätze zur Informationssicherheit (Art. 6 bis Art. 10 ISG-Bund). Andererseits müssen die kantonalen Vorschriften auch Regeln enthalten, welche den Zugang zu klassifizierten Informationen (Art. 14 ISG-Bund) sowie die Sicherheit von Informatikmitteln beim Einsatz (Art. 16 ISG-Bund) und beim Betrieb (Art. 19 ISG-Bund) gewährleisten. Hierzu gehören zum einen die in den Art. 20 und Art. 21 ISG-Bund geregelten personellen Massnahmen, welche nicht nur den Zugang zu Informationen und Informatikmitteln des Bundes definieren, sondern den Geltungsbereich auch auf die Räumlichkeiten und auf «andere Infrastrukturen» des Bundes erweitern. Zudem wird in Art. 22 und Art. 23 ISG-Bund auch der physische Schutz von Informationen und Informatikmitteln eingeschlossen (Schutz vor Missbrauch und Störung).

Die Bearbeitung von Informationen und der Zugriff auf Informatikmittel müssen soweit als nötig eingeschränkt werden. Eine solche Einschränkung gilt speziell für sog. «sicherheitsempfindliche Tätigkeiten», welche in Art. 5 Bst. b. ISG-Bund definiert sind. Als solche gelten die Bearbeitung von «vertraulich» oder «geheim» klassifizierten Informationen und die Verwaltung, der Betrieb, die Wartung und die Überprüfung von Informatikmitteln der Sicherheitsstufen «hoher Schutz» oder «sehr hoher Schutz».

Für solche sicherheitsempfindliche Tätigkeiten sieht das ISG-Bund besondere Vorschriften vor, namentlich die Personensicherheitsprüfung (Art. 27 bis Art. 48 ISG-Bund) sowie das Betriebssicherheitsverfahren (Art. 49 bis Art. 73 ISG-Bund). Diese Bestimmungen sind für die Gleichwertigkeit der kantonalen Vorschriften ebenfalls mitzuberücksichtigen, damit ein umfassender Schutz der Informationssicherheit gewährleistet werden kann.

Gemäss Art. 86 ISG-Bund sorgen die Kantone für die periodische Überprüfung der Umsetzung und Wirksamkeit der Informationssicherheit nach Art. 3 ISG-Bund.
Aus Art. 86 ISG-Bund ergeben sich die folgenden Pflichten für die Kantone:

1. Durchführung einer periodischen Prüfung der Umsetzung und Wirksamkeit der Informationssicherheit (Abs. 1)

2. Information der Fachstelle des Bundes für Informationssicherheit über die Ergebnisse der Prüfung (Abs. 2)
3. Bezeichnung einer Dienststelle als Ansprechpartnerin für die verpflichteten Behörden des Bundes.

2.3. Klassifizierte Informationen des Bundes

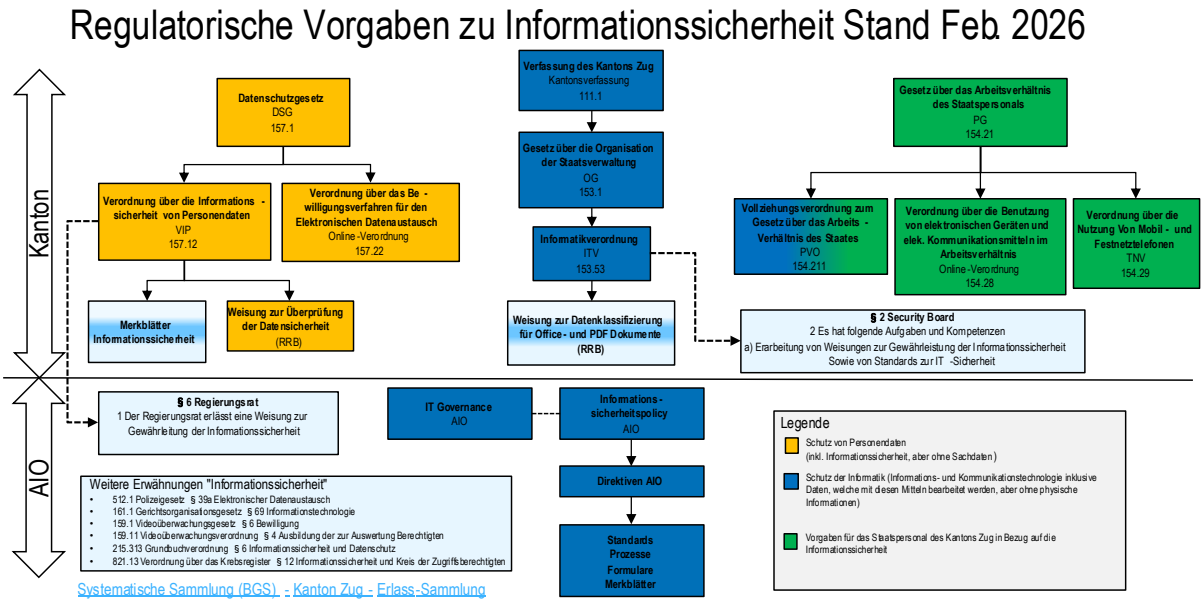
Das ISG-Bund selbst enthält keine Definition für den Begriff «Informationen». In der Botschaft des Bundesrates zum ISG-Bund finden sich jedoch im Zusammenhang mit der Kommentierung der einzelnen Bestimmungen Hinweise, welche Informationen zu klassifizieren sind. Es handelt sich dabei grundsätzlich um Informationen, die für die innere und äussere Sicherheit, die internationalen Beziehungen oder die wirtschaftspolitischen Interessen der Schweiz besonders wichtig sind. Ein erhöhter Schutzbedarf ergibt sich aber auch für Informationen, welche sowohl Geschäfts- und Fabrikationsgeheimnisse als auch Personendaten umfassen. Gemäss ISG-Bund gelten Informationen als «klassifizierte Informationen», wenn sie die Kriterien von Art. 13 ISG-Bund erfüllen (Art. 11 Abs. 1 ISG-Bund). Die Einordnung erfolgt anhand des Grades der Beeinträchtigung der in Art. 1 Abs. 2 Bst. a – d ISG-Bund aufgeführten öffentlichen Interessen.

2.4. Informatikmittel des Bundes

Informatikmittel sind nach Art. 5 Bst. a. ISG-Bund «Mittel der Informations- und Kommunikationstechnik, namentlich Anwendungen, Informationssysteme und Datensammlungen sowie Einrichtungen, Produkte und Dienste, die zur elektronischen Verarbeitung von Informationen dienen». Für diese Informatikmittel sieht Art. 17 ISG-Bund drei Sicherheitsstufen vor, wobei die Sicherheitsstufe «Grundschutz» für sämtliche Informatikmittel gilt, sofern diese nicht höher (Stufe «hoher Schutz» und Stufe «sehr hoher Schutz») eingestuft werden müssen.

Ein weiterer Bezug zu den Kantonen ergibt sich aus Art. 29 Abs. 1 Bst. b. ISG-Bund. Danach werden Angestellte der Kantone, die sicherheitsempfindliche Tätigkeiten des Bundes ausüben, durch den Bund auf deren Sicherheit hin überprüft. Hierfür müssen die Kantone festlegen, welche Stellen für die Einleitung einer Personensicherheitsprüfung (einleitende Stelle) sowie für den Entscheid über die Ausübung der sicherheitsempfindlichen Tätigkeit (entscheidende Stelle) zuständig sind (Art. 31 Abs. 1 ISG-Bund). Die Kosten für die Durchführung der Personensicherheitsprüfung trägt der Bund (Art. 36 Abs. 3 ISG-Bund).

3. Grundlagen im Kanton Zug



3.1. Übersicht

3.2. Verhältnis zum Öffentlichkeitsprinzip der Verwaltung

Das Gesetz über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz vom 20. Februar 2014; BGS 158.1) fördert die Transparenz über die Tätigkeit der kantonalen Organe und regelt den Zugang zu den amtlichen Dokumenten. Es berechtigt grundsätzlich jede Person, ohne besonderen Nachweis von Interessen amtliche Dokumente einzusehen und von den Verwaltungseinheiten Auskünfte über den Inhalt amtlicher Dokumente zu erhalten. Ausnahmen vom Öffentlichkeitsprinzip sind möglich; sie werden im Gesetz abschliessend aufgezählt.

Gemäss dem Vorbehalt von Spezialbestimmungen (§5 Öffentlichkeitsgesetz) können gestützt auf Bestimmungen anderer Gesetze und - demnach gemäss dem ISG - bestimmte Informationen als geheim bezeichnet oder vom Öffentlichkeitsgesetz abweichende Voraussetzungen für den Zugang zu bestimmten Informationen vorgesehen werden. Wird der Zugang zu einem Dokument zum Schutz von überwiegenden öffentlichen oder privaten Interessen ausnahmsweise eingeschränkt, aufgeschoben oder verweigert, muss das entsprechende Dokument aufgrund seinem tatsächlichen Schutzbedarf geschützt und darf nicht zur Einsicht freigegeben werden. Im ISG werden die dazu notwendigen gesetzlichen Grundlagen zur Einschränkung der Informationsansprüche gemäss dem Öffentlichkeitsgesetz geschaffen.

3.3. Datenschutzgesetzgebung

Das Datenschutzgesetz vom 28. September 2000 (DSG; BGS 157.1) regelt für private Personen den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden. Das DSG legt unter anderem fest, dass Personendaten durch die kantonalen Organe nur rechtmässig, verhältnismässig, zweckmässig und für die betroffenen Personen

möglichst transparent bearbeitet werden dürfen. Das DSG gilt im Verhältnis zum ISG als Spezialgesetzgebung. Die Datenschutzgesetzgebung setzt aber auch Anforderungen an den praktischen Schutz der Vertraulichkeit, Verfügbarkeit und Integrität der Daten selbst fest. So verlangt § 7 DSG, dass Personendaten durch angemessene technische und organisatorische Massnahmen vor Verlust, Fälschung, Entwendung, Kenntnisnahme, Kopieren und Bearbeiten durch Unbefugte zu sichern sind.

Beim Datenschutz geht es um den Schutz der Privatsphäre und der Persönlichkeit eines jeden Menschen im Bereich der Bearbeitung seiner Daten. Im Unterschied zum Datenschutz befasst sich die Informationssicherheit mit dem Schutz von Informationen unabhängig davon, ob diese einen Personenbezug aufweisen oder nicht. In Bezug auf die Informationssicherheit bedeutet dies, dass das Datenschutzgesetz somit ausschliesslich auf den Schutz und die Sicherheit von Personendaten natürlicher Personen ausgerichtet ist. Nicht in dieser (datenschutzrechtlich begründeten) Informationssicherheit eingeschlossen sind Personendaten von juristischen Personen, Geschäfts- und Fabrikationsgeheimnisse oder generell alle übrigen Sachdaten, welche keinen Personenbezug aufweisen, jedoch trotzdem unter den Begriff «Informationen» fallen und im Sinne des ISG klassifiziert werden.

3.4. Verordnung über die Informationssicherheit von Personendaten

Im § 4 der Verordnung über die Informationssicherheit von Personendaten vom 16. Januar 2007 (VIP; BGS 157.12) werden die Sicherheitsmassnahmen im Hinblick auf die Anforderungen an den Schutz von Personendaten festgelegt. Die Vorschriften des ISG sollen auf die Bearbeitung von Personendaten als ergänzendes Recht angewendet werden. Personendaten gelten im Sinne des ISG als Informationen, welche die kantonalen Organe hinsichtlich Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit schützen müssen.

Die VIP regelt das Verfahren und die Verantwortlichkeiten zur Gewährleistung der Sicherheit von Personendaten, die mit elektronischen Hilfsmitteln oder auf andere Weise bearbeitet werden. Sie bezweckt namentlich den Schutz von Personendaten gegen:

1. zufällige Bekanntgabe, Vernichtung oder Verlust
2. technische Fehler
3. unbefugte Kenntnisnahme
4. unbefugte Bearbeitung
5. Fälschung, Entwendung oder
6. widerrechtliche Verwendung.

Die erforderlichen technischen und organisatorischen Sicherheitsmassnahmen müssen dabei die Vertraulichkeit, die Integrität, die Verfügbarkeit, die Zurechenbarkeit sowie die Nachvollziehbarkeit von Datenbearbeitungen gewährleisten (§ 4 Abs. 1 VIP). Eine Anpassung der VIP im Zusammenhang mit dem Erlass des ISG ist nicht vorgesehen, die VIP wird daher nicht revidiert.

3.5. Informatikverordnung

Gegenstand der Informatikverordnung vom 13. November 2018 (ITV; BGS 153.53) ist gemäss § 1 die Organisation, die Steuerung, der Betrieb und die Kontrolle der Informatik. Der Begriff «Informatik» wird in § 2 Abs. 1 Bst. a als «Oberbegriff für Informations- und Kommunikationstechnologie» definiert. § 2 Abs. 1 Bst. i hält sodann fest, dass unter IT-Sicherheit «Massnahmen zum Schutz der Integrität und der Verfügbarkeit der IT-Mittel sowie zum Schutz der

Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Daten, die mit diesen Mitteln bearbeitet werden», verstanden werden.

Damit lehnt sich die ITV an die Bestimmungen in Art. 5 Bst. a ISG-Bund an: Danach gelten als «Informatikmittel» die Mittel der Informations- und Kommunikationstechnik.

Anders als das ISG beschränkt die ITV den Schutz jedoch nur auf «Daten», die mit Informatikmitteln bearbeitet werden. Nicht miterfasst von der ITV werden somit diejenigen Daten (Informationen), welche unabhängig von Informatikmitteln bearbeitet werden, beispielsweise physisch vorhandene Daten in Papierform.

Im Weiteren befasst sich § 18 ITV explizit mit der IT-Sicherheit, jedoch nur beschränkt auf die IT-Mittel und - für Personendaten - nach den Vorgaben des DSG und der VIP. Keinen ausdrücklichen Bezug nimmt die Bestimmung zu denjenigen Daten, welche gemäss § 2 Abs. 1 Bst. i) ITV von den Massnahmen zur «IT-Sicherheit» betroffen sind.

ISG und ISV regeln die Informationssicherheit in umfassender Weise; die ITV behandelt ergänzend insbesondere organisatorische Themen. Die ITV ist an das ISG und die ISV anzupassen, dieser Schritt erfolgt im Rahmen einer separaten Revision der ITV.

3.6. Cybersicherheit

Cybersicherheit (Cybersecurity) beschreibt den anzustrebenden Zustand, bei dem die Datenbearbeitung, insbesondere der Datenaustausch zwischen Personen und Organisationen, über Informations- und Kommunikationsinfrastrukturen wie beabsichtigt funktioniert.

Nach Art 74a ISG-Bund haben die Kantone dafür zu sorgen, dass dem Bundesamt für Cybersicherheit (BACS) Cyberangriffe gemeldet werden. Durch die Meldung eines Cyberangriffs können die meldepflichtigen Behörden nach Art. 74b ISG-Bund, namentlich Kantons- und Gemeindebehörden bei der Vorfallbewältigung im Rahmen der festgelegten Massnahmen und zur Verfügung gestellten Hilfsmittel unterstützt werden (Art. 74 Abs. 1 und 2 ISG-Bund). Die Meldepflicht dient ausschliesslich dazu, dass die Bundesbehörde BACS Angriffsmuster auf kritische Infrastrukturen frühzeitig erkennen und dadurch mögliche Betroffene warnen und ihnen geeignete Präventions- und Abwehrmassnahmen empfehlen kann.

Die Cybersicherheit umfasst sämtliche Risiken, Massnahmen, Prozesse und Aufgaben auf organisatorischer und technischer Ebene zur Identifikation, Analyse und Bewältigung von Cyberbedrohungen und -angriffen. Sie ist ein wichtiger Teil der Informationssicherheit. Im Bereich des Datenschutzes sorgen die zuständigen Organe durch angemessene technische und organisatorische Massnahmen für die Sicherheit aller Personendaten. Personendaten sind insbesondere vor Verlust, Fälschung, Entwendung, Kenntnisnahme, Kopieren und Bearbeiten durch Unbefugte zu sichern. Diese Ziele werden vom ISG erfasst.

Ist von Cybersicherheit die Rede, gilt es begrifflich zwischen Cybervorfall, Cyberangriff, Cyberbedrohung und Schwachstelle zu unterscheiden. Der Begriff Cybervorfall ist als Oberbegriff für alle Ereignisse zu verstehen, welche die Schutzziele der Informationssicherheit beeinträchtigen können. Ein Cybervorfall schliesst Ereignisse ein, die von Unbefugten absichtlich ausgelöst werden oder von Personen unbeabsichtigt, bspw. durch Fehlmanipulationen oder Fehlfunktionen der Informatikmittel, eintreten können.

Ein Cybervorfall gilt als Cyberangriff, wenn er absichtlich ausgelöst wird und zwar unabhängig davon, ob es sich um einen Mitarbeitenden bspw. eines kantonalen Organs oder um eine externe Quelle handelt. Entscheidend ist beim Cyberangriff, ob absichtlich die Schutzziele der Informationssicherheit beeinträchtigt werden sollen.

Eine Cyberbedrohung umfasst jedes Ereignis, welche das Potenzial für einen Cybervorfall aufweist. Hingegen bildet ein Cyberrisiko die Einschätzung einer Cyberbedrohung mit Blick auf ihre Eintretenswahrscheinlichkeit und ihres Schadensausmasses und ist gegenüber einer Cyberbedrohung abzugrenzen.

Im selben Zusammenhang ist von Schwachstellen zu sprechen. Wenn eine Cyberbedrohung auf Schwächen oder Fehler in Informatikmitteln zurückzuführen ist, muss von einer Schwachstelle ausgegangen werden. Daher stellt jede Schwachstelle stets eine Cyberbedrohung dar.

3.7. Personensicherheitsprüfung und Abgrenzung gegenüber dem Personalgesetz

Die Bestimmungen über die Personensicherheitsprüfung (PSP) stellen den wesentlichen Inhalt der Vorlage des ISG dar. Eine PSP kann im Sinne eines weiteren zusätzlichen Prüfschrittes im Rahmen eines Anstellungsverfahrens durchgeführt werden, wenn die gesetzlichen Voraussetzungen dazu erfüllt sind. Somit steht auch fest, dass die im Rahmen der Eignungsprüfung gemäss Personalgesetzgebung durchgeführten Abklärungen bei einer PSP nicht wiederholt werden müssen, sofern die Unterlagen, namentlich die verlangten Registerauszüge, weiterhin aktuell sind.

Die PSP kann als eine präventive Massnahme bezeichnet werden, die im Rahmen eines vorgegebenen Verfahrens die möglichen Eintretensrisiken von Verletzungen der Informationssicherheit durch internes Personal und Personal von mandatierten Dritten vermeiden oder zumindest verringern soll. Diese Risiken liegen in einer vorsätzlichen oder fahrlässigen Beeinträchtigung wesentlicher öffentlicher Interessen, die mit der Ausübung einer sicherheitsempfindlichen Tätigkeit durch eine bestimmte Person verbunden sind.

Für die meisten Stellenbesetzungen reichen die Auswahlverfahren gemäss der Personalgesetzgebung aus. Zudem entsteht bei einem allfälligen Vertrauensmissbrauch in den meisten Fällen allenfalls ein Reputationsverlust für die öffentliche Verwaltung, allenfalls werden Straftatbestände wie Amtsmissbrauch, Verletzung der Verschwiegenheit oder des Amtsgeheimnisses vorliegen. Ein Schadenseintritt, der aufgrund der Verletzung von öffentlichen Interessen eintritt, dürfte eher die Ausnahme darstellen. Muss jedoch mit einem solchen Schaden gerechnet werden, so kann eine PSP mögliche Risikofaktoren aufzeigen, die sich aus dem Vorleben oder dem Umfeld der geprüften Person ergeben.

Anlassgrund für eine PSP bilden stets die Risiken im Zusammenhang mit sicherheitsempfindlichen Tätigkeiten, fehlt ein solcher Bezug, ist von einer PSP abzusehen. Eine PSP bearbeitet Personendaten und vor allem besonders schützenswerte Personendaten. Die datenschutzrechtlichen Voraussetzungen für das Bearbeiten von Personendaten gemäss § 4 DSG, namentlich der Grundsatz der Verhältnismässigkeit (§ 4 Abs. 1 Bst. d DSG), müssen erfüllt sein, dies ist jeweils im konkreten Anwendungsfall zu prüfen.

Die Verhältnismässigkeit der Datenbearbeitung ist stets in einem direkten Zusammenhang zu den konkreten Massnahmen und Aufgaben zu stellen. Grundsätzlich dürfen Personendaten nur mit Blick auf einen bestimmten Zweck bearbeitet werden. Besteht eine gesetzliche Grundlage für die Datenbearbeitung - wie dies vorliegend zutrifft -, so ist diese Voraussetzung der Zweckbindung erfüllt. In diesem Fall verlangt die Beachtung der Verhältnismässigkeit, dass einzig diejenigen Personen die Personendaten bearbeiten dürfen, welche aufgrund ihrer Rolle und Funktion zur Datenbearbeitung berechtigt und auch verpflichtet sind. Diese Anforderungen werden ebenfalls erfüllt, zumal der Personenkreis (Antragsstellendes Organ, Fachstelle für Informationssicherheit, Zuger Polizei, Personalamt, HR-Stellen der Direktionen) der die PSP durchführt, eng begrenzt ist.

Datenschutzrechtlich nicht zulässig sind beispielsweise die Datenbearbeitung auf Vorrat wie das Sammeln von Personendaten für künftige Bearbeitungen oder die Aufbewahrung auf unbestimmte Zeit, auf jeden Fall länger als der Zweck der Bearbeitung dies erfordert.

Im Kapitel 4 nachstehend werden Aufgaben und Zuständigkeiten der Fachstelle für Informationssicherheit, der Zuger Polizei und des Personalamtes im Zusammenhang mit der Einleitung und Entscheidung der PSP behandelt.

In diesem aufgezeigten Rahmen sind die Bestimmungen verbunden mit den vorliegenden Erläuterungen zur PSP zu betrachten.

Mit der Regelung der Personensicherheitsprüfung (PSP) nach Art. 27 ff. ISG-Bund und §§ 12 ff. ISG soll die Vertrauenswürdigkeit von Personen überprüft werden, die im Rahmen ihrer Funktion oder eines Auftrages eine sicherheitsempfindliche Tätigkeit bzw. Funktionen ausüben (z.B. Systemadministration, Personen mit Zugang zu Sicherheitszonen). Mit dieser organisatorischen Massnahme können die Behörden des Bundes das Risiko, dass Sicherheitslücken durch vorsätzliches Fehlverhalten der eigenen Mitarbeitenden oder durch Beauftragte entstehen, reduzieren.

Der Kanton Zug führt für den Bund die PSP nach Bundesrecht (ISG-Bund und der Vollzugsverordnung zur PSP) durch, sofern für die betreffende Person eine PSP-Bund verlangt wird. Wenn für eine bestimmte Person eine PSP-Bund durchgeführt wird, dann kann der Kanton Zug dieses Ergebnis anerkennen, wenn eine kantonale PSP gemäss ISG erforderlich ist. Der Kanton Zug ist dazu aber nicht verpflichtet. Die kantonale Prüfung kann auch zu einem Ergebnis führen, das von demjenigen der PSP-Bund abweicht, wie die Praxis beweist.

Das Personalgesetz über das Arbeitsverhältnis des Staatspersonals (Personalgesetz) vom 1. September 1994 (PG, BGS 154.21) regelt in § 2bis die Eignungsprüfung von Mitarbeitenden des Kantons, die auf bestimmte oder unbestimmte Zeit im Voll- oder Teilpensum angestellt sind. Diese Bestimmung stellt die gesetzliche Grundlage für eine Eignungsprüfung dar, die eine registerbasierte, medizinische oder andere Eignungsprüfung umfasst (§ 2bis Abs. 1 PG). Der Zweck dieser umfassenden Eignungsprüfung wird in § 2bis Abs 2 Bst. a, b und c PG aufgaben- und funktionsbezogen umschrieben. Spezialregelungen bestehen für Lehrpersonen (Sonderprivatauszug) gemäss § 2ter PG und für Mitarbeitende u.a. der Polizei, Gerichtsinstanzen, in leitenden Funktionen usw. gemäss § 2^{quater} Abs. 4 und 5 PG.

Die Vorschriften der PSP und die Bestimmungen des PG über die Eignungsprüfungen sind nicht vollumfänglich deckungsgleich. Der Fokus der im PG geregelten Eignungsprüfung ist auf die Anstellung und Weiterbeschäftigung ausgerichtet. Hingegen dient eine PSP der Beurteilung, ob ein Risiko für die Informationssicherheit bestehen könnte, wenn eine Person im Rahmen ihrer Funktion oder eines Auftrages eine sicherheitsempfindliche Tätigkeit ausübt. Im Fokus der PSP steht nicht primär die Eignung als solche mit Blick auf die Erfüllung einer dienstlichen Aufgabe, sondern vielmehr die Vertrauenswürdigkeit der betreffenden Person, die eine entsprechende Tätigkeit mit sicherheitsrelevanten Bezug wahrnimmt.

Die gesetzlichen Bestimmungen des PG sind im Hinblick auf die Eignungsprüfung umfassend ausgestaltet. Daher kann auf entsprechende Massnahmen wie zum Beispiel registerbezogene und allenfalls persönliche Befragungen im Rahmen einer PSP gemäss ISG unter Umständen verzichtet werden. Eine Revision der Bestimmungen über die Eignungsprüfung des PG ist mit Blick auf die Ausgestaltung der PSP gemäss ISG nicht erforderlich.

Das ISG schliesst allerdings eine Lücke bei den PSP von Drittpersonen, die auf der Grundlage eines Auftragsverhältnisses öffentliche Aufgaben erfüllen. Drittpersonen sind vom Geltungsbereich des PG nicht erfasst und daher kann ihre Eignung gestützt auf die entsprechenden Bestimmungen des PG nicht überprüft werden. Wenn diese Personen Aufgaben ausüben, die vom Geltungsbereich des ISG erfasst werden, dann kann gestützt auf §§ 12 ff. ISG eine Personensicherheitsprüfung vorgenommen werden. Das heisst, die nicht vom PG erfassten Personen, die im Kanton Aufgaben erfüllen, können somit einer PSP im Rahmen der Sicherheitsprüfung unterzogen werden. In diesen Fällen wird eine umfassende PSP durchzuführen sein, zumal bspw. registerbasierte Unterlagen nicht vorliegen, wie dies bei kantonalen Mitarbeitenden regelmässig zutrifft.

Die Bestimmungen des ISG im Zusammenhang mit der PSP entfalten ihre Wirkungen mittelbar auch auf das Vorgehen in Submissionsverfahren. Wenn der Kanton als Auftraggeber im Rahmen eines Submissionsverfahrens eine Eignungsprüfung gestützt auf Art. 27 der Interkantonalen Vereinbarung über das öffentliche Beschaffungswesen vom 15. November 2019 (IVöB; BGS 721.52) vornimmt, dann können Registerauszüge der Firmen und / oder der Schlüsselperson (Betreibungs-, Strafregisterauszüge) verlangt werden. Diese Abklärungen erfolgen im Zusammenhang mit der Eignung der betreffenden Anbieterinnen und stellen Eignungskriterien dar, die zwingend erfüllt sein müssen. Wenn diese Kriterien nicht erfüllt sind, wird das Angebot aus dem Verfahren ausgeschlossen, bzw. ein erteilter Zuschlag kann widerrufen werden (Art. 44 IVöB).

3.8. Zu schliessende Lücken in den bestehenden Rechtsgrundlagen

Im geltenden kantonalen Recht bestehen Lücken bei der Regelung der Informationssicherheit. ISG und ISV schliessen diese Lücken. Es betrifft dies insbesondere:

1. der fehlende Schutz von Informationen (Sachdaten) des Kantons;
2. die Voraussetzungen zur Personensicherheitsprüfung und deren Abwicklung;
3. die Bearbeitung von Personendaten im Zusammenhang mit Informationssicherheitsvorfällen;
4. die Bearbeitung von als «vertraulich» und «geheim» klassifizierten Informationen;
5. Verwaltung, Betrieb, Wartung und Überprüfung von Informatikmitteln der Sicherheitsstufen «hoher Schutz»;
6. Zugang zu den Sicherheitszonen;

7. Festlegung von personellen Massnahmen;
8. Bestimmungen zum physischen Schutz von Informationen und Informatikmitteln;
9. Fachliche Unabhängigkeit der Fachstelle Informationssicherheit und des CISO durch direkte Zuordnung bei der Finanzdirektion.

Die Massnahmen zur Gewährleistung der Informationssicherheit sollen Sicherheitsrisiken begegnen und die Daten zum Beispiel vor Manipulation, Verlust oder von unberechtigter Kenntnisnahme schützen. Dabei ist unerheblich, ob es sich um digitale oder analoge Informationen handelt und ob diese einen Personenbezug haben. Diese Lücken bei der Informationssicherheit werden mit dem ISG und der ISV geschlossen. Eine Revision des DSG und der VIP sind indessen nicht erforderlich.

3.9. Geltungsbereich für die Gemeinden des Kantons Zug

Für die Gemeinden gelten gemäss § 2 Abs. 2 ISG nur die Bestimmungen über:

a) klassifizierte Informationen, soweit sie klassifizierte Informationen des Kantons oder des Bundes bearbeiten;
b) die Sicherheit beim Einsatz von IT-Mitteln, soweit sie auf IT-Mittel des Kantons oder des Bundes zugreifen.

Der Geltungsbereich des ISG erfasst demnach die Gemeinden, soweit diese klassifizierte Informationen des Kantons oder des Bundes bearbeiten. Dasselbe soll auch gelten, wenn sie auf Informatikmittel des Kantons zugreifen.

Die Vorschriften des Kantons über klassifizierte Informationen und die Sicherheit beim Einsatz von Informatikmitteln, die im Einklang mit den bundesrechtlichen Vorgaben stehen, sollen jedoch in Berücksichtigung des Subsidiaritätsprinzips ausschliesslich dann zur Anwendung kommen, wenn die Vorschriften und Massnahmen der Gemeinden den Sicherheitsanforderungen des Kantons nicht genügen. Soweit die Gemeinden bereits mit einer eigenen, mit derjenigen des Kantons vergleichbaren Informationssicherheit ausgestattet sind, gelangt das ISG demnach nicht zur Anwendung. Dies ist der Fall, wenn der IT-Minimalstandard des Bundes und des Kantons eingehalten werden.

Die Fachstelle für Informationssicherheit erlässt Richtlinien über die Sicherheitsanforderungen und unterstützt die Gemeinden bei der Erarbeitung ihrer internen Grundlagen wie Leitfäden, Merkblätter usw. im Bereich der Sicherheitsanforderungen an die Informationssicherheit.

3.10. Betriebssicherheitsverfahren wird im ISG nicht geregelt

Das Betriebssicherheitsverfahren befasst sich mit der Wahrung der Informationssicherheit bei der Vergabe von Aufträgen der kantonalen Beschaffungsstellen an Dritte (Betriebe). Das Verfahren dient einerseits der Prüfung der Vertrauenswürdigkeit der zu beauftragenden Betriebe, andererseits ermöglicht es, die notwendigen Massnahmen zur Gewährleistung der Informationssicherheit während der Ausführung des Auftrags zu kontrollieren und durchzusetzen.

Im Rahmen eines Betriebssicherheitsverfahren werden auch Personendaten und namentlich besonders schützenswerte Personendaten gemäss DSG bearbeitet. Daher ist für die Durchführung eines Betriebssicherheitsverfahrens eine gesetzliche Grundlage notwendig. Diese Grundlage wird im ISG-Bund geschaffen.

Der Bund sieht ein Verfahren vor (vgl. Art. 49 bis Art. 73 ISG-Bund), wonach bei der Vergabe von sicherheitsempfindlichen Aufträgen die Behörden dafür sorgen müssen, dass nur Unternehmen öffentliche Aufträge erhalten, welche befähigt sind, die Informationssicherheit zu gewährleisten. Das Verfahren soll der Prüfung der Vertrauenswürdigkeit der zu beauftragenden Betriebe dienen. Das Verfahren darf nur mit Einwilligung des Betriebs durchgeführt werden.

Auf eine gesetzliche Regelung des Betriebssicherheitsverfahrens im ISG wird jedoch aus folgenden Gründen verzichtet. Anknüpfungspunkt an ein Betriebssicherheitsverfahren bildet stets ein Auftrag einer Verwaltungsstelle (Beschaffungsstelle), vorliegend eines kantonalen Organs, an ein Unternehmen der Privatwirtschaft. Dieser Auftrag kann unter anderem auch sicherheitsempfindliche Tätigkeiten beinhalten. Daher müssen die entsprechenden Anforderungen an die Informationssicherheit im Zuge der Auftragserfüllung gemäss den Vorgaben der auftragsvergebenden Stelle erfüllt werden. Es gilt einen Aspekt der Eignung der Leistungserbringerin zu prüfen, wonach diese geeignet sein muss, die Aufträge mit einem allenfalls sicherheitsempfindlichen Inhalt auszuführen. Die Prüfung der Eignung erfolgt in der Regel im Rahmen eines Submissionsverfahrens. Die Eignungskriterien werden mit Blick auf die zu beschaffenden betrieblichen Leistungen festgelegt. Im Rahmen der Auswertung der Angebote wird überprüft, ob die Anforderungen an die Eignungskriterien auch im Bereich der Informationssicherheit erfüllt sind.

In Art. 27 der Interkantonalen Vereinbarung über das öffentliche Beschaffungswesen vom 15. November 2019 (IVöB, BGS 721.52) werden die Anforderungen an die Eignungskriterien festgehalten. Zudem besteht gestützt auf Art. 30 IVöB für die Beschaffungsstelle die Möglichkeit, die Anforderungen an die Informationssicherheit mit technischen Spezifikationen zu schärfen und zu präzisieren.

Da im Rahmen des Beschaffungsprozesses die Teilnahmebedingungen und Eignungskriterien vermehrt auch auf die Anforderungen im Bereich der Informationssicherheit ausgerichtet werden, kann daher auf eine zusätzliche gesetzliche Regelung des Betriebssicherheitsverfahrens im ISG verzichtet werden.

Die Anforderungen an die Sicherheitsvorgaben können im Rahmen der Beschaffung kontrolliert und im Zuge der Realisierung der Projekte durchgesetzt werden. Die IVöB bietet die entsprechenden Grundlagen (Art. 44 und Art. 45 IVöB).

Die Informationssicherheit bildet bei der Beschaffung von IT Leistungen stets einen zentralen Prüfpunkt.

Die Vergabestelle (Auftraggeberin) wird bei der Festlegung des Pflichtenheftes und der Ausschreibungsbedingungen die Anforderungen an die Informationssicherheit der Fachstelle für Informationssicherheit zur Stellungnahme unterbreiten und ihre Anträge berücksichtigen. Im Zuge der Auswertung der Angebote sind die Angaben der Anbieterinnen zur Informationssicherheit der Fachstelle zur Vernehmlassung zu unterbreiten, wenn die Frage zu klären ist, ob die Anforderungen erfüllt sind oder ob aufgrund mangelnder Eignung oder Erfüllung der Teilnahmebedingungen und / oder der technischen Spezifikationen das entsprechende Angebot aus dem Verfahren auszuschliessen ist. Ein solcher Schritt erfolgt gestützt auf eine Verfügung, die gemäss Art. 53 Abs. 1 Bst. h IVöB mit Beschwerde beim Verwaltungsgericht des Kantons Zug angefochten werden kann.

Mit den Instrumenten des Submissionsrechts kann den Anforderungen an die Betriebssicherheit mit Blick auf die Informationssicherheit entsprochen werden. Auf ein separates Betriebssicherheitsverfahren, wie dies im ISG-Bund vorgesehen ist, kann daher im ISG verzichtet werden. Der Rechtsschutz ist gewährleistet, zumal gestützt auf Art. 56 Abs. 3 IVöB Rechtsverletzungen, einschliesslich Überschreitung oder Missbrauch des Ermessens sowie unrichtige oder unvollständige Feststellung des rechtserheblichen Sachverhalts, gerügt werden können.

Gestützt auf Art. 24 der bundesrätlichen Verordnung über das Betriebssicherheitsverfahren vom 08. November 2023 (VBSV; SR 128.41) können die Kantone für sicherheitsempfindliche Aufträge nach kantonalem Recht bei der Fachstelle des Bundes die Durchführung einer Beurteilung der Eignung nach den Art. 55 bis Art. 57 ISG-Bund unter bestimmten Voraussetzungen beantragen. Die Leistungen des Bundes sind gebührenpflichtig.

3.11. Rechtsschutz und rechtliches Gehör vor Erlass der Erklärung der Fachstelle

Die Erklärung der Fachstelle für Informationssicherheit (Fachstelle) kann gestützt auf die Personensicherheitsprüfung PSP ein Sicherheitsrisiko feststellen, wenn aufgrund der erhobenen Daten konkrete Anhaltspunkte vorliegen, dass die geprüfte Person die sicherheitsrelevante Funktion oder den sicherheitsrelevanten Auftrag mit hoher Wahrscheinlichkeit vorschriftswidrig oder unsachgemäss ausüben wird.

Eine solche Erklärung der Fachstelle kann für die geprüfte Person negative Folgen für ihre berufliche Entwicklung haben und zudem ihre Persönlichkeitsrechte verletzen oder erheblich beeinträchtigen. Daher muss die Erklärung der Fachstelle gerichtlich überprüft werden können. Der Anspruch auf den gerichtlichen Rechtsschutz ist in Art. 29a Bundesverfassung (BV) verankert und stellt eine Ergänzung der verfassungsrechtlich gewährleisteten Verfahrensgarantien dar.

Vor dem Erlass einer Erklärung ist der geprüften Person grundsätzlich stets das rechtliche Gehör zu gewähren (Art. 29 Abs. 2 BV). Im Zusammenhang mit dem Recht zur Stellungnahme hat die geprüfte Person Anspruch auf Einsicht in die Verfahrensakten und kann sich zu ihrem Inhalt äussern, Berichtigungen verlangen oder Ergänzungen vorbringen. Die Fachstelle wird vor dem Erlass ihrer Erklärung stets eine Stellungnahme der geprüften Person einholen und ihre Anträge allenfalls berücksichtigen.

Verzichtet die geprüfte Person auf eine Stellungnahme und demnach die Wahrnehmung des rechtlichen Gehörs, dann kann in einem allfälligen Rechtsmittelverfahren der Einwand nicht mehr erhoben werden, dass die verfassungsmässigen Verfahrensrechte nicht gewährt wurden, es sei denn, die Erklärung der Fachstelle beruht auf Tatsachen, die der geprüften Person bisher nicht bekannt waren.

Mit der Erklärung der Fachstelle beginnt die Frist von 20 Tagen zur Beschwerde, die beim Regierungsrat einzureichen ist. Die geprüfte Person kann die Rechte nach § 21 Abs. 1 ISG geltend machen; im Beschwerdeverfahren können gemäss § 42 VRG alle Mängel des Verfahrens und des angefochtenen Entscheides gerügt werden.

4. Fachstelle für Informationssicherheit

4.1. Organisation

Eine einheitliche und konsequente Durchsetzung der Informationssicherheit ist von zentraler Bedeutung. Der Fachstelle für Informationssicherheit (Fachstelle) obliegt die Pflicht Überprüfungen vorzunehmen, ob die Vorgaben der Informationssicherheit eingehalten werden und bei erkannten Sicherheitslücken entsprechende Sofortmassnahmen zu ergreifen. Die Organe können jederzeit von sich aus einen Antrag auf Überprüfung ihrer Organisation an die Fachstelle richten.

Die Gefährdung der öffentlichen Interessen, die durch eine Verletzung der Informationssicherheit eintreten kann, rechtfertigt es, dass die Fachstelle bestimmte Kompetenzen erhält, wie beispielsweise die autonome Durchführung von Überprüfungen aber auch die Möglichkeit des Ergreifens von Sofortmassnahmen, wenn Verletzungen der Informationssicherheitsvorgaben festgestellt werden. Es gilt auch Kollateralschäden auf anderen Systemen zu verhindern und zudem ist die Gesamtstabilität der IT-Landschaft sicherzustellen.

Aufgrund der Überwachungspflichten im Themenbereich Informationssicherheit muss die fachliche und funktionale Unabhängigkeit gegenüber allen Dienstleistern und Ämtern, die IT-Leistungen erbringen, gewährt werden. Durch die administrative Zuweisung bei der Finanzdirektion ist die organisatorische Unabhängigkeit in Informationssicherheitsfragen gewährleistet. Die gewählte Organisationsform folgt konsequent dem international anerkannten «Three Lines of Defense»-Modell, welches eine klare Trennung zwischen der operativen Umsetzung (1. Linie, Security Operation Center beim AIO) der unabhängigen Informationssicherheitsaufsicht (2. Linie, Fachstelle für Informationssicherheit) sowie einer unabhängigen Prüfung (3. Linie) vorsieht. Diese wird von der Finanzkontrolle des Kantons Zug sowie externen Auditoren, beispielweise im Rahmen von Zertifizierungsprozessen (ISO 27001:2022-Audit), wahrgenommen.

Durch diese Entflechtung wird sichergestellt, dass die Fachstelle als kontrollierende Instanz auch dem gegenüber AIO (IT-Dienstleister) verbindliche Sicherheitsvorgaben anordnen kann, ohne in einen Interessenskonflikt zu geraten, wie dies der Fall ist, wenn die Fachstelle in die Hierarchie des AIO eingebunden ist und somit in einem Abhängigkeitsverhältnis zur Leitung des AIO steht.

Die administrative Zuweisung der Fachstelle zu einer Direktion der kantonalen Verwaltung stellt ebenfalls eine notwendige Voraussetzung für die Umsetzung einer «Checks- and Balances-Struktur» dar und gewährleistet hiermit die Anwendung einer wirksamen Governance-Politik. Die Entscheide im Informationssicherheitsbereich können ohne Mitwirkung von hierarchisch vorgesetzten Stellen getroffen und durchgesetzt werden.

Die administrative Zuweisung zur Finanzdirektion erweist sich als eine vertretbare und zweckmässige Lösung. Die fachliche Unabhängigkeit bei der Ausübung der Aufgaben der Fachstelle bleibt gewährleistet. Die Aufgaben der Finanzdirektion beinhalten personalrechtliche und administrative Themen gegenüber der Fachstelle. Der Finanzdirektion stehen keine Entscheidungskompetenzen im Informationssicherheitsbereich zu. Daher kann einzig der Gesamtregierungsrat und nicht eine einzelne Direktion Massnahmen im Informationssicherheitsbereich anordnen, Sofortmassnahmen bei Sicherheitsvorfällen beschliessen oder Schritte zur Abklärung bei Cybervorfällen einleiten.

Der Leiter der Fachstelle Informationssicherheit ist zugleich Informationssicherheitsbeauftragter (CISO) des Kantons und zuständig für alle Informationssicherheitsfragen in den kantonalen Direktionen.

Die Anstellung der Leiterin bzw. des Leiters (CISO) der Fachstelle erfolgt durch den Regierungsrat. Die Anstellung der Mitarbeitenden der Fachstelle erfolgt durch die Leiterin bzw. den Leiter der Fachstelle.

Die Fachstelle kann im Rahmen dieser Organisationsstruktur ihre Aufgaben wahrnehmen, ohne in einen Interessenskonflikt zu geraten, wenn ein Organ von Sicherheitsvorfällen direkt betroffen sein könnte.
Bei festgestellten Sicherheitslücken und Sicherheitsvorfällen muss die Fachstelle zeitnah reagieren und Sofortmassnahmen anordnen können, welche verhältnismässig, geeignet und zweckgebunden sein müssen. Solche Eingriffe sind auf Fälle von unmittelbarer Gefahr für wesentliche Interessen (Gefahr im Verzug) beschränkt. Sie müssen den Grundsatz der Verhältnismässigkeit strikt wahren, um die operative Funktionsfähigkeit der Organe nicht unnötig zu beeinträchtigen. Die von der Fachstelle getroffenen Sofortmassnahmen präjudizieren allfällige Massnahmen oder Anordnungen des Regierungsrates nicht. Daher können die von der Fachstelle angeordneten Sofortmassnahmen durch den Regierungsrat angepasst, korrigiert oder aufgehoben werden, wenn die Voraussetzungen für ihre Beibehaltung oder Weiterführung nicht mehr erfüllt sind. Einzelheiten über die Berichterstattung von Sicherheitsvorfällen werden im § 17 ISV geregelt.

Die Fachstelle informiert den Regierungsrat und die Präsidien des Obergerichts und des Verwaltungsgerichts (Gerichte) sowie die Zuger Polizei über Sicherheitsvorfälle und Sicherheitslücken mit einem hohen Risiko für die Informationssicherheit und dagegen ergriffene Sofortmassnahmen so rasch als möglich und stellt Anträge, die im Einvernehmen mit den Gerichten erfolgen, für das weitere Vorgehen an den Regierungsrat. Dieser entscheidet innert 72 Stunden über die getroffenen Massnahmen. Die Kompetenz zur Anordnung von Massnahmen bei derartigen Sicherheitsvorfällen und Sicherheitslücken und zum Erlass von Weisungen im Bereich der Informationssicherheit liegt daher ausschliesslich beim Regierungsrat in Abstimmung mit den Gerichtspräsidien.

4.2. Aufgaben der Fachstelle für Informationssicherheit

Die Fachstelle ist zuständig für die Steuerung und Umsetzung der Informationssicherheit und arbeitet eng mit dem Security Operation Center (SOC), das im Amt für Information und Organisation (AIO) integriert ist, zusammen. Die Fachstelle unterstützt die kantonalen Organe und die übrigen vom ISG betroffenen Körperschaften und Organisationen bei der Gewährleistung der Informationssicherheit, beim Risikomanagement, beim Vorgehen bei Sicherheitsvorfällen (Verletzungen der Informationssicherheit), beim Sicherheitsverfahren und bei der Gewährleistung der Sicherheit der Informatikmittel vor deren Einsatz und während des Betriebs.

Weiter ist die Fachstelle mit Kontrollaufgaben betraut. Sie hat die Möglichkeit, im Anwendungsbereich des ISG bei kantonalen Organen sowie bei den Gemeinden und anderen Organisationen Überprüfungen der Informationssicherheit vorzunehmen. Stellt sie Mängel fest, kann sie Sofortmassnahmen ergreifen und Anträge für das weitere Vorgehen zuhanden des

Regierungsrats stellen. Die Fachstelle erstattet dem Regierungsrat und den Gerichten jährlich Bericht über die Informationssicherheit im Kanton Zug (§ 17 ISV).

Die Fachstelle nimmt im Zusammenhang mit der Personensicherheitsprüfung eine zentrale Rolle ein. Art. 31 ISG-Bund erteilt den Kantonen die formelle Kompetenz zur Festlegung der Zuständigkeiten für die Einleitung des Verfahrens für eine PSP; diese Stelle bildet im Kanton Zug die Fachstelle für Informationssicherheit, sie ist dem Bund bekanntzugeben. Die Fachstelle kann von sich aus keine PSP, weder für den Bund noch für den Kanton, einleiten. Es braucht dazu einen entsprechenden Auftrag. Ist eine PSP für den Bund gemäss Art. 29 Abs. 1 Bst. b ISG-Bund vorzunehmen, wonach eine PSP für Angestellte eines Kantons durchzuführen ist, die eine sicherheitsempfindliche Tätigkeit ausüben, so ist die Fachstelle die einleitende Behörde (Art. 31 Abs. 1 Bst. a ISG-Bund). Entscheidende Stelle nach Art. 31 Abs. 1 Bst. b ISG-Bund ist allerdings die vom Bund bezeichnete Fachstelle.

Die kantonale Fachstelle ist jedoch die einleitende und zugleich entscheidende Behörde bei der Durchführung einer kantonalen PSP. Die Fachstelle wird die zur Durchführung der PSP benötigten Daten vom Personalamt, von den zuständigen HR-Stellen der Direktionen und insbesondere von der Zuger Polizei beziehen. Die Fachstelle hat keinen direkten Zugriff auf diese Daten. Ein solcher ist ihr gestützt auf die datenschutzrechtlichen Bestimmungen auch nicht zu gewähren.
Die Fachstelle kann ein eigenes Informationssystem betreiben und im Rahmen ihrer Sicherheitsabklärungen zusätzliche Daten bei der zu prüfenden Person oder bei Dritten erheben bzw. Befragungen durchführen.

Zudem überprüft die Fachstelle periodisch die Umsetzung und Wirksamkeit der Informationssicherheit und orientiert die Fachstelle für Informationssicherheit des Bundes über die Ergebnisse. Sie ist einzige kantonale Kontaktstelle gegenüber dem Bundesamt für Cybersicherheit (BACS) und gegenüber den Fachstellen für Informationssicherheit der anderen Kantone (§ 19 ISV).

5. Gründe für die gewählte Lösung

5.1 Legalitätsprinzip

Nach Art. 5 Abs. 1 und Art. 36 Abs.1 zweiter Satz sowie Art. 164 Abs. 1 Bst. b Bundesverfassung vom 18. April 1999 (BV, SR 101) müssen die grundlegenden Bestimmungen über die Einschränkungen verfassungsmässiger Rechte in einem Gesetz im formellen Sinne geregelt werden.

Die kantonalen Organe dürfen nach § 5 Abs. 2 DSG besonders schützenswerte Personendaten sowie Persönlichkeitsprofile nur bearbeiten, wenn ein Gesetz dies ausdrücklich vorsieht. Formell-gesetzliche Grundlagen sind im Zusammenhang mit der Informationssicherheit nötig für:

a) den Einsatz von Informationssystemen zur zentralen Kontrolle von Identitäten, weil damit besonders schützenswerte Personendaten bearbeitet werden;
b) die PSP, weil die Durchführung einer PSP mit einem erheblichen Eingriff in die Grundrechte von Privatpersonen verbunden ist;
c) die Regelung der Berechtigungen für klassifizierte Informationen bzw. des Zugangs zu den Sicherheitszonen, die auf einer PSP beruht;

d) für die Bewältigung von Sicherheitsvorfällen ist die Bearbeitung von Daten über potenzielle Täterinnen oder Täter erforderlich. Diese Bearbeitung kann in Verbindung mit administrativen oder strafrechtlichen Verfolgungen und Sanktionen stehen, die als besonders schützenswerte Personendaten gemäss dem DSG gelten.

5.2 Welche Personendaten sind konkret betroffen?

Bei der Gewährleistung der Informationssicherheit im Kanton Zug müssen u.a. folgende besonders schützenswerte Personendaten bearbeitet werden:

- Vorfallbewältigung bei Cyberangriffen: Daten über potenzielle Täterinnen und Täter, Angriffsmuster, Identitäten, Handlungen und Beweggründe;
- Sicherheitszonen und Zutrittskontrollen: Personenkontrollen, Überwachungsmassnahmen, biometrische Daten;
- Personensicherheitsprüfung: Befragung über persönliche Daten (u.a. betreffend Gesundheit, politische Engagements, finanzielle Verhältnisse, Strafen usw.).

5.3 Flexibles Regelwerk erforderlich

Die rasante technologische Entwicklung im Bereich der Informationssicherheit und die sich ständig wandelnden Bedrohungslagen erfordern ein dynamisches und flexibles Regelwerk. Ein detailliertes, starres Gesetz könnte bereits bei Inkrafttreten zum Teil veraltet sein und müsste revidiert werden.

Das ISG stellt die dringend notwendige Flexibilität sicher, indem das ISG nur die verfassungsrechtlich zwingend auf Gesetzesstufe zu regelnden Aspekte normiert und dem Regierungsrat eine Delegationskompetenz zur flexiblen Ausgestaltung und laufenden Anpassung der Ausführungsbestimmungen (Verordnung) einräumt.

Vorteile dieser Lösung:

- Maximale Flexibilität: Der Regierungsrat kann die Verordnung laufend an neue Herausforderungen anpassen, ohne dass der Kantonsrat sich mit Gesetzesrevisionen befassen muss;
- Zukunftsfähigkeit: Technologieneutrale Formulierung im Gesetz gewährleistet Bestand auch bei technologischen Entwicklungen;
- Schnelle Reaktionsfähigkeit: Bei neuen Cyberbedrohungen oder geänderten Bundesvorgaben kann der Regierungsrat sofort reagieren;
- Verhältnismässigkeit: Regelungsdichte auf Gesetzesstufe wird den formell gesetzlichen Anforderungen entsprechend festgelegt;
- Praktikabilität: Erprobte und bewährte überwiegend technische und oder betriebliche Lösungen können auf Verordnungsebene rasch umgesetzt und bei Bedarf situationsbezogen und zeitgerecht angepasst werden.

6. Ergebnisse der Vernehmlassung

Text folgt nach Auswertung der externen Vernehmlassung.

7. Erläuterungen zu den einzelnen Bestimmungen der Gesetzesvorlage

1. Allgemeine Bestimmungen

§ 1 Regelungsgegenstand und Zweck

[1] Dieses Gesetz regelt
a) die Umsetzung der Informationssicherheit; und
b) die Bearbeitung von Personendaten zur Sicherstellung der Informationssicherheit.

[2] Es bezweckt den Schutz der folgenden öffentlichen Interessen:
a) Entscheidungs- und Handlungsfähigkeit der Organe;
b) öffentlichen Ordnung und Sicherheit;
c) wirtschafts- und finanzpolitischen Interessen des Kantons; und
d) Erfüllung von gesetzlichen und vertraglichen Verpflichtungen der Organe zum Schutz von Informationen.

Der Zweck ergibt sich grundsätzlich aus dem Begriff der Informationssicherheit. Bezweckt wird demnach der Schutz aller Informationen, für welche die kantonalen Organe zuständig sind, ungeachtet des Umstands, ob sie diese selbst erstellen, von Dritten erhalten oder Dritten zur Bearbeitung weitergeben. Ebenso wie für die Herkunft der Informationen soll das ISG auch in Bezug auf die Art und Form der Informationen umfassend gelten und daher technologieneutral sein. Es spielt demnach keine Rolle, ob die Information textlicher, akustischer oder graphischer Natur ist und ob sie elektronisch oder beispielsweise auf einem Papierdokument verfügbar ist. Im Zentrum steht immer die Information und wie diese Information gewonnen, transportiert, verarbeitet und dann weiterbearbeitet wird, um daraus Wissen zu kreieren.

Weiter soll das Gesetz auch sämtliche Informationstechnik erfassen, die von den kantonalen Organen eingesetzt, auf welche zugegriffen wird oder deren Betrieb sie auslagern. Der Schutz der Informationen dient bestimmten öffentlichen Interessen beziehungsweise Eigeninteressen des Kantons als Gemeinwesen. Das Gesetz soll durch Gewährleistung einer sicheren Bearbeitung von Informationen, für die der Kanton zuständig ist, die hohen eigenen Interessen des Kantons, namentlich die innere Sicherheit, die Entscheidungs- und Handlungsfähigkeit der Organe und ihrer Verwaltungseinheiten und die Erfüllung der gesetzlichen und vertraglichen Verpflichtungen des Kantons zum Schutz von Informationen schützen.

Der Schutz der öffentlichen Sicherheit beinhaltet auch die Individualinteressen der Bevölkerung und von Unternehmen (Persönlichkeitsrechte und Geschäftsgeheimnisse) im Verkehr mit den Organen.

Der Begriff Information wird im ISG nicht definiert, da sich der Begriff im ISG mit dem umgangssprachlichen Gebrauch deckt. Das Gesetz macht grundsätzlich auch keinen Unterschied zwischen Informationen und Daten: Beide Begriffe werden unter dem Begriff Informationen subsumiert. Der Begriff Daten wird nur dann verwendet, wenn Personendaten nach dem DSG betroffen sind.

§ 2 Geltungsbereich

[1] Dieses Gesetz gilt für die Organe des Kantons und der Gemeinden im Sinne von § 4 Abs. 1 Bst. b.

[2] Für Organe der Gemeinden gelten nur die Bestimmungen über:

a) klassifizierte Informationen, soweit sie klassifizierte Informationen des Kantons oder des Bundes bearbeiten;
b) die Sicherheit beim Einsatz von IT-Mitteln, soweit sie auf IT-Mittel des Kantons oder des Bundes zugreifen.

[3] Diese Bestimmungen gelten nicht, wenn die Organe nach Abs. 2 eine mindestens gleichwertige Informationssicherheit gewährleisten.

Die Vernetzung der Informatiksysteme der kantonalen Organe nimmt untereinander laufend zu. Dadurch wird das Risiko erhöht, dass sich Angriffe sowie Bedrohungen gegen ein Organ auf die Zuständigkeitsbereiche anderer Organe ausweiten könnten. Es ist daher unentbehrlich, dass die jeweiligen kantonalen Organe gleichwertige Risikobeurteilungskriterien und -methoden anwenden und dass ihre organisatorischen, personellen, technischen und physischen Sicherheitsmassnahmen bei der Bearbeitung von Informationen und beim Einsatz von Informatikmitteln aufeinander abgestimmt werden.

Der Geltungsbereich des ISG erfasst neben den kantonalen Organen und der Gemeinden natürliche oder juristische Personen oder Personengesellschaften des Handelsrechts, denen öffentliche Aufgaben übertragen worden sind, soweit diese klassifizierte Informationen des Kantons oder des Bundes bearbeiten. Dasselbe soll auch gelten, wenn sie auf Informatikmittel des Kantons oder des Bundes zugreifen.

Die Vorschriften des Kantons über klassifizierte Informationen und die Sicherheit beim Einsatz von Informatikmitteln sollen jedoch für die Gemeinden in Berücksichtigung des Subsidiaritätsprinzips nur dann zur Anwendung kommen, wenn die Vorschriften und Massnahmen der Gemeinden den Sicherheitsanforderungen des Kantons nicht genügen.

§ 3 Verhältnis zu anderen Erlassen

[1] Dieses Gesetz findet ergänzend Anwendung auf Informationen, deren Schutz auch in Erlassen des Bundes oder in anderen Erlassen des Kantons geregelt ist.

Im Verhältnis zu Gesetzen, die ebenfalls den Schutz von Informationen vorsehen, soll das ISG ergänzend Anwendung finden. Die spezialgesetzlichen Regelungen werden nicht derogiert. Daher hat beispielsweise das Öffentlichkeitsgesetz gegenüber dem ISG Vorrang. Im Verhältnis zum Datenschutz ist festzuhalten, dass Datenschutz und Informationssicherheit zwar eine gemeinsame thematische Schnittmenge haben, in dem Personendaten auch Informationen sind, jedoch der Schutzzweck jeweils unterschiedlich ist. Personendaten im Kanton werden weiterhin nach dem DSG und der VIP behandelt und bearbeitet.

§ 4 Begriffe

In diesem Gesetz bedeuten:

[1] a) Informationssicherheit gewährleistet die Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit von sämtlichen Informationen des Kantons oder des Bundes sowie die Verfügbarkeit und Integrität von IT-Mitteln ihrem Schutzbedarf entsprechend.

b) Organe sind Behörden und Dienststellen, die für den Kanton oder die Gemeinden handeln, und natürliche oder juristische Personen oder Personengesellschaften des Handelsrechts, soweit ihnen öffentliche Aufgaben übertragen sind.
c) Gemeinden sind die Einwohner-, Bürger-, Kirch- und Korporationsgemeinden.
d) Identitätsverwaltungs-Systeme prüfen die Identität und berechtigungsbezogene Eigenschaften von Personen, Maschinen und Systemen und übermitteln das Resultat der Prüfung an die angeschlossenen Informationssysteme.
e) Sicherheitsempfindliche Tätigkeit: Bearbeitung von «vertraulich» oder «geheim» klassifizierten Informationen; Verwaltung, Betrieb, Wartung und Überprüfung von IT-Mitteln der Sicherheitsstufe «hoher Schutz» und Zugang zu Sicherheitszonen.
f) Sicherheitszonen sind von den Organen bezeichnete Bereiche, in denen häufig als «vertraulich» oder «geheim» klassifizierte Informationen bearbeitet oder IT-Mittel der Schutzstufe «hoher Schutz» betrieben werden.
g) Schwachstelle ist eine Sicherheitslücke in einem IT-Mittel und stellt eine Cyberbedrohung dar.

Bst a) *Informationssicherheit: umfasst die Gewährleistung für Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit von sämtlichen Informationen des Kantons oder des Bundes sowie die Verfügbarkeit und Integrität von IT-Mitteln. IT ist der Oberbegriff und die Abkürzung für Informations- und Kommunikationstechnologie. IT-Mittel der Informations- und Kommunikationstechnik sind namentlich Anwendungen, Informationssysteme und Datensammlungen sowie Einrichtungen, Produkte und Dienste, die zur elektronischen Verarbeitung von Informationen dienen.*
Bst.d) Ein Informationsverwaltungssystem dient der wirksamen Verwaltung und Kontrolle von Identitäten (einzelne User oder User Gruppen) und Zugriffen. Es können die Authentifizierung eines Users, die Autorisierung im Sinne der Berechtigungen des Zugriffs oder die Verwaltung der Benutzer mit ihren Identitäten geregelt werden.

Bst. e) Die sicherheitsempfindliche Tätigkeit stellt einen zentralen Begriff dar. Die Ausübung einer solchen Tätigkeit ist Voraussetzung für die Durchführung von PSP. Die Sicherheitsempfindlichkeit einer Tätigkeit wird erst dann angenommen wenn die Interessen nach § 1 Absatz 2 ISG beeinträchtigt werden können. Sicherheitsempfindlich ist zudem nicht der blosse Zugang zu diesen Informationen, sondern deren tatsächliche und berechtigte Bearbeitung. Die blosse Benützung der IT-Mittel wird also nicht als sicherheitsempfindlich betrachtet. Erfasst werden vor allem Administratoren und Anwendungsverantwortliche der Systeme mit hohem Schutzbedarf. Als sicherheitsempfindlich wird auch der Zugang zu Sicherheitszonen bezeichnet, weil das Schadenspotenzial bei Spionage oder bei Sabotage in diesen Zonen aufgrund der darin befindlichen Informationen und IT-Mittel sehr hoch ist.
Bst. f) Die Bezeichnung von Sicherheitszonen stellt eine physische Massnahme der Informationssicherheit dar. Sie dient dem Schutz der IT-Mittel aber auch von Informationen. Eine Sicherheitszone muss bestimmt, konkret umschrieben und auf den Zweck der zu schützenden Informationen und Informatikmittel ausgerichtet sein. Die Massnahmen in den Sicherheitszonen werden risikogerecht auszugestalten sein.
Bst. g) Eine Schwachstelle stellt stets eine Cyberbedrohung dar, wenn diese auf Schwächen oder Fehler in IT-Mitteln zurückzuführen ist. Eine Cyberbedrohung umfasst jedes Ereignis, welche das Potenzial für einen Cybervorfall aufweist.

2. Bearbeiten von Personendaten

§ 5 Bearbeitung

[1] Die Organe können zur Gewährleistung der Informationssicherheit und zur Behebung von Schwachstellen Personendaten in dafür vorgesehenen Informationssystemen (ISMS-Anwendungen) bearbeiten.

[2] Sie können Personendaten nach Abs. 1 untereinander sowie mit nationalen, internationalen und ausländischen Organisationen des öffentlichen Rechts austauschen, sofern:
a) dies zur Gewährleistung der Informationssicherheit zweckmässig ist;
b) keine gesetzlichen oder vertraglichen Geheimhaltungspflichten verletzt werden;
c) die Vorgaben des Datenschutzes eingehalten werden; und
d) diese Organisationen gesetzliche Aufgaben im Bereich der Informationssicherheit wahrnehmen, die denjenigen der bekanntgebenden Organe entsprechen.

[3] Sie können ihre Informationssysteme, insbesondere die ISMS-Anwendungen, miteinander verknüpfen und Daten automatisch oder auf Anfrage über Schnittstellen austauschen.

[4] Sie können zur Einreichung und Bearbeitung von Anträgen und Meldungen im Bereich der Informationssicherheit digitale Formulare zur Verfügung stellen und diese mit ihren ISMS-Anwendungen oder anderen Informationssystemen verknüpfen.

[5] Sofern dies für die Bewältigung von Verletzungen der Informationssicherheit oder die Behebung von Schwachstellen erforderlich ist, können die Organe besonders schützenswerte Personendaten von Personen, die daran beteiligt oder davon betroffen sind, bearbeiten.

Diese zentrale Bestimmung des ISG schafft die gesetzliche Grundlage für die Bearbeitung von Personendaten und insbesondere den schützenswerten Personendaten gemäss dem DSG und die technische Bearbeitung gestützt auf Informationssysteme. Die Auflistung der technischen Möglichkeiten in den Abs. 2 bis 5 ist erforderlich, weil sämtliche Massnahmen die Bearbeitung von besonders schützenswerten Personendaten umfassen können. Die datenschutzrechtlichen Grundsätze beim Bearbeiten von Personendaten gemäss § 4 und § 5 DSG werden im Abs. 2 dieser Bestimmung summarisch festgehalten.

Diese Bestimmung bildet auch die gesetzliche Grundlage für die Bearbeitung von Personendaten im Zusammenhang mit der Bewältigung von Sicherheitsvorfällen. Diese setzt die Bearbeitung von Daten über potenzielle Täterschaften voraus, die in Verbindung mit administrativen oder strafrechtlichen Verfolgungen und Sanktionen stehen können und deshalb als besonders schützenswerte Personendaten im Sinne des DSG gelten. Bei diesen Personendaten handelt es sich insbesondere um Daten über die Identität, die Handlungen, das Vorgehen und die Beweggründe von potenziellen Täterschaften. Es werden auch Daten von Personen bearbeitet, die lediglich vom Vorfall betroffen sein können, weil sie beispielsweise einen Schaden erleiden.

§ 6 Aufbewahrung und Archivierung

[1] Die Organe können Personendaten und besonders schützenswerte Personendaten bis zwei Jahre nach der Bewältigung der Verletzungen der Informationssicherheit oder der Behebung der Schwachstellen aufbewahren, höchstens aber zehn Jahre.

[2] Die Archivierung der Daten richtet sich nach den Vorschriften des Archivgesetzes.

Für die Bearbeitung der Personendaten muss gemäss dem DSG das Prinzip der Verhältnismässigkeit eingehalten werden, weshalb die besonders schützenswerten Personendaten nur zwei Jahren nach der Bewältigung der Informationssicherheitsverletzung oder Behebung der Schwachstelle aufbewahrt werden dürfen.

3. Identitätsverwaltungs-Systeme

§ 7 Einsatz von Identitätsverwaltungs-Systemen

[1] Die Organe können zur zentralen Verwaltung der Daten Informationssysteme (Identitätsverwaltungs-Systeme) betreiben, die zur Identifizierung von Personen dienen, die Zugang zu sicherheitsrelevanten Informationen, IT-Mitteln, Räumlichkeiten oder anderen Infrastrukturen haben.

[2] Identitätsverwaltungs-Systeme prüfen die Identität und berechtigungsbezogene Eigenschaften von Personen, Maschinen und Systemen und übermitteln das Resultat der Prüfung an die angeschlossenen Informationssysteme, damit diese die Berechtigungen der identifizierten Person ermitteln können.

Eine der wirksamsten operativen Massnahmen zur Gewährleistung der Informationssicherheit ist eine wirksame Verwaltung und Kontrolle von Identitäten und Zugriffen. Mit dem stets wachsenden Umfang der Nutzung von Informationen aus unterschiedlichen Quellen und über die Organisationsgrenzen hinweg können die Anforderungen an Schutz und Funktionalität nur noch mit übergreifend koordinierten Systemen effizient gewährleistet werden.

Die Identifizierung von Personen stellt eine Bearbeitung von Personendaten dar und bedarf aus Datenschutzgründen einer formell-gesetzlichen Regelung.

Diese Bestimmung beschreibt den Zweck und die Funktionsweise der zentralen Identitätsverwaltungs-Systeme. Die Organe erhalten die Kompetenz, derartige Systeme für die zentrale Kontrolle von Personen, Maschinen und Systemen, die Zugang zu Informationssystemen und anderen Ressourcen verlangen, zu betreiben.

§ 8 Datenaustausch und -abgleich

[1] Die Identitätsverwaltungs-Systeme können mit den angeschlossenen Informationssystemen, mit Personal- und Benutzerverzeichnissen und mit anderen Identitätsverwaltungs-Systemen Daten austauschen und abgleichen.

[2] Der Austausch und Abgleich ist auf die Daten zu begrenzen, die im jeweiligen System bearbeitet werden dürfen.

[3] Der Austausch und Abgleich der Daten können erfolgen:

a) mit der Authentifizierung im laufenden Betrieb bei jeder Anmeldung einer Benutzerin oder eines Benutzers;
b) beim Aufbau eines neuen Identitätsverwaltungs-Systems mit dem Datenbezug aus bestehenden Mitarbeitenden- und Benutzerverzeichnissen; oder
c) bei der Übertragung der bisher für die Authentifikation verwendeten Daten an das Identitätsverwaltungs-System.

Im Mittelpunkt einer umfassenden Identitätsverwaltung stehen zentralisierte Identitätsverwaltungs-Systeme. Mit diesen Systemen können für die zentrale Kontrolle von Personen, Maschinen und Systeme, die Zugang zu Informationssystemen und anderen Ressourcen verlangen, betrieben werden. Es gilt sicherzustellen, dass die berechtigten Personen und Systeme gestützt auf ihre Zugriffsberechtigungen sich korrekt anmelden und dass die einzelnen Zugrifft transparent und nachvollziehbar bleiben. Für jedes System muss eine verantwortliche Stelle bezeichnet werden. Im Zusammenhang mit dem Datenaustausch ist zwischen den im Abs. 3 umschriebenen Tatbeständen auszugehen, bei denen ein Identitätsverwaltungs-System Personendaten mit anderen Systemen austauscht: Die häufigste Übermittlung von Daten geschieht im laufenden Betrieb bei jeder Anmeldung (Login) einer Benutzerin oder eines Benutzers. Das Identitätsverwaltungs-System authentifiziert die Benutzerin oder den Benutzer, komplettiert die von der Fachanwendung verlangten Identitätsdaten aus einem Verzeichnis oder aus externen Quellen und stellt diese Daten der Fachanwendung in der Form von Bestätigungen zur Verfügung, damit diese über die konkreten Zugriffsberechtigungen befinden kann.
Beim Aufbau eines neuen Identitätsverwaltungs-Systems bezieht dieses die notwendigen Identitätsdaten der Mitarbeitenden des abzudeckenden Bereichs aus den entsprechenden Mitarbeitenden- und Benutzerverzeichnissen. Im späteren Betrieb müssen periodisch Mutationen von diesen Systemen an das Identitätsverwaltungs-System gemeldet werden.

Ein weiterer Anlass ist der Anschluss einer Fachanwendung, die bisher die Authentifizierung der Benutzerinnen und Benutzer selbstständig durchgeführt hat. In diesem Fall werden die für die Authentifikation verwendeten Daten an das zentrale Identitätsverwaltungs-System übertragen und dort in die bestehenden Daten eingetragen.

4. Klassifizierung von Informationen

§ 9 Klassifizierung

[1] Die Organe klassifizieren die Informationen gemäss folgenden Stufen:
a) «öffentlich», wenn die Informationen für jedermann zugänglich sind;
b) «intern», wenn die öffentlichen Interessen aufgrund der Kenntnisnahme durch Unberechtigte beeinträchtigt werden können;
c) «vertraulich», wenn die öffentlichen Interessen aufgrund der Kenntnisnahme durch Unberechtigte erheblich beeinträchtigt werden können;
d) «geheim», wenn die öffentlichen Interessen aufgrund der Kenntnisnahme durch Unberechtigte schwerwiegend beeinträchtigt werden können.

[2] Die Klassifizierung ist auf das erforderliche Mindestmass zu beschränken und nach Möglichkeit zeitlich zu begrenzen. Nicht klassifizierte Informationen gelten als «intern».

[3] Die Gerichte können abweichende Regelungen vorsehen.

[4] Personendaten gelten nicht als klassifiziert, wenn sie bereits gesetzlich geschützt sind.

Bei der Klassifizierung wird der Schutzbedarf von Informationen hinsichtlich einer Beeinträchtigung der zu schützenden Interessen beurteilt. Sie bildet die Basis für die weiteren Massnahmen zum Schutz der Informationssicherheit. Die Grundzüge, das Verfahren und die Zuständigkeiten der Klassifizierung von Informationen sind mit Blick auf die Wichtigkeit der Klassifizierung für die Informationssicherheit zu regeln. Das Ziel besteht darin, dass bei allen kantonalen Organen und den ihnen unterstellten Organisationen die Klassifizierung von Informationen einheitlich erfolgt.

Zu den Grundzügen der Klassifizierung gehören dabei neben der Klärung der Frage, welche Informationen überhaupt zu klassifizieren sind, insbesondere auch Regelungen betreffend die Klassifizierungsstufen, die Zuständigkeiten, mithin auch die Zuständigkeit zur Änderung von Klassifizierungen, und den Zugang zu klassifizierten Informationen. Zur Klärung der Frage, welche Informationen überhaupt zu klassifizieren sind, nimmt diese Bestimmung direkten Bezug auf die durch Klassifizierung zu schützenden öffentlichen Interessen.

Das Amt für Informatik und Organisation kann den Organen zur Klassifizierung sämtlicher digitaler Dateiformate eine Klassifizierungsanwendung zur Setzung von Sensitivity Labels zur Verfügung stellen, mit denen Inhalte je nach Schutzbedarf klassifiziert und geschützt werden. Je nach Label können dann Regeln zur Durchsetzung beispielsweise Verschlüsselung, Vorgaben beim Weiterleiten, Drucken, Bearbeiten usw. festgelegt werden. Labels unterstützen Compliance Anforderungen und insbesondere eine einheitliche Datenklassifizierung bei den Organen.

Personendaten gemäss § 2 Abs, 1 insbesondere Bst. b und c DSG, welche bereits durch die Datenschutzgesetzgebung geschützt werden, oder Informationen, die gesetzlich oder vertraglich geschützt sind (Geschäfts-, Fabrikations- oder Berufsgeheimnisse), werden nicht klassifiziert.

In Abs. 3 wird den Gerichten im Zusammenhang mit der Klassifizierung die Möglichkeit einer differenzierte Regelung eingeräumt, zumal alle Informationen im Zusammenhang mit Verfahren grundsätzlich mit 'vertraulich' zu klassifizieren sind.

§ 10 Zuständigkeiten

[1] Die Organe legen fest, welche Stellen für das Klassifizieren der Informationen zuständig sind (klassifizierende Stellen).

[2] Klassifizierungen dürfen nur von der klassifizierenden Stelle oder von der Stelle, die dieser übergeordnet ist, geändert oder aufgehoben werden.

[3] Der Regierungsrat bzw. das Obergericht und das Verwaltungsgericht regeln die Klassifizierung in einer separaten Weisung.

Die Zuständigkeit zur Klassifizierung sollte in aller Regel derjenigen Stelle überlassen sein, die schutzwürdige Informationen in irgendeiner Form festhält oder herausgibt. Nebst dem Verfassen eines Dokuments können auch auf Bild- und Tonträger festgehaltene Informationen klassifizierungswürdig sein. Die in Absatz 1 definierte Stelle kann den Schutzbedarf der Informationen sowie allfällige Risiken am besten einschätzen.

Die Klassifizierung ist grundsätzlich verbindlich. Ist eine Information klassifiziert, wird sie auf ihrem weiteren Weg von dieser Klassifizierung begleitet. Wer Zugang zu einer solchen Information erhält, muss die Vorgaben einhalten, die mit der Klassifizierung verbunden sind. Eine Änderung oder Aufhebung der Klassifizierung darf im Grundsatz nur von derjenigen Stelle vorgenommen werden, welche die Klassifizierung festgelegt hat.

§ 11 Zugang zu klassifizierten Informationen

[1] Zugang zu klassifizierten Informationen der Stufen «vertraulich» und «geheim» erhalten nur Personen,
a) die Gewähr dafür bieten, dass sie damit sachgerecht umgehen und
b) die Informationen zur Erfüllung einer gesetzlichen Aufgabe benötigen.

Es gilt der Grundsatz «Kenntnis nur wenn nötig» für jede einzelne klassifizierte Information. Es besteht also kein allgemeines Recht, Zugang zu allen klassifizierten Informationen zu haben. Dies trifft auch für Prüf-, Kontroll- oder Aufsichtsorgane zu, die gegebenenfalls zwar ein allgemeines Informationsrecht haben, die aber für jede einzelne klassifizierte Information den Nachweis dafür erbringen, dass sie zur Erfüllung ihres Auftrags tatsächlich von den betreffenden Informationen Kenntnis haben müssen. Bei einem vertraglich vereinbarten Zugangsrecht müssen die entsprechenden Verträge den Zugang zu klassifizierten Informationen vorsehen und deren Bearbeitung regeln.

Gemäss Botschaft des Bundesrates vom 22.02.2017, BBl 2017 2953, S. 3025 setzt «Gewähr bieten» voraus, dass Personen, welche klassifizierte Informationen bearbeiten sollen, entsprechend ausgebildet wurden. Zudem sollen diese Personen bei Bedarf auch den Nachweis erbringen, dass sie die erforderlichen technischen und physischen Sicherheitsmassnahmen einhalten können. Für «vertraulich» oder «geheim» klassifizierte Informationen kann zudem die Durchführung einer Personensicherheitsprüfung eine weitere Bearbeitungsvoraussetzung darstellen.

5. Informationssystem und Personensicherheitsprüfung

5.1 Informationssystem für die Personensicherheitsprüfung

§ 12 Informationssystem für Personensicherheitsprüfungen Kanton und Bund

[1] Die Fachstelle für Informationssicherheit betreibt ein Informationssystem. Dieses dient der Durchführung von:
a) Personensicherheitsprüfungen;

b) Beurteilungen des Gefährdungs- oder Missbrauchspotenzials bezüglich der persönlichen Waffe;
c) Zuverlässigkeitskontrollen; und
d) Prüfungen der Vertrauenswürdigkeit.

[2] Im Informationssystem können Personendaten und besonders schützenswerte Personendaten nach § 2 Abs. 1 Bst. a und b DSG bearbeitet werden. Ein Informationssystem kann folgende Daten enthalten:
a) Daten zur Identität der zu prüfenden oder geprüften Personen, einschliesslich der AHV-Nummer und der Passnummer;
b) Daten im Zusammenhang mit der Datenerhebung (§ 18 ISG);
c) Datenerhebung bei Drittpersonen (§ 19 ISG);
d) die Beurteilung des Sicherheitsrisikos und Erklärung (§ 20 ISG);
e) Daten und Akten aus Beschwerdeverfahren (§ 21);
f) Listen und Statistiken, die Daten nach den Buchstaben a) bis e) enthalten.

[3] Anhand der Daten des Informationssystems darf ein Profiling nach § 2 Abs. 1 Bst. b1 Datenschutzgesetz durchgeführt werden, um die nachfolgenden persönlichen Aspekte einer natürlichen Person zu den Bearbeitungszwecken nach Abs. 1 zu analysieren, zu bewerten, zu beurteilen oder vorherzusagen:
a) Sicherheitsrisiko oder
b) Gefährdungs- und Missbrauchspotenzial bezüglich einer persönlichen Waffe.

Die von der Fachstelle für Informationssicherheit erhobenen Daten und insbesondere die Risikobeurteilungen stellen besonders schützenswerte Personendaten bzw. Persönlichkeitsprofile im Sinne von § 2 Abs. 1 b) und b1) DSG dar. Dabei ist festzuhalten, dass sich dieses Profiling technisch ausschliesslich auf die Zusammenführung der gesetzlich definierten Prüfkriterien im Rahmen einer bereits eingeleiteten PSP beschränkt. Es handelt sich ausdrücklich nicht um eine allgemeine Überwachung, Leistungs- oder Verhaltenskontrolle der Mitarbeitenden im Arbeitsalltag. Die automatisierte Auswertung dient einzig der effizienten und standardisierten Risikobeurteilung bei Personen in sicherheitsempfindlichen Funktionen und ist strikt auf diesen Sicherheitszweck begrenzt. Die Effizienz des Prüfverfahrens kann gesteigert werden, indem die der Fachstelle für Informationssicherheit gesetzlich zustehenden Zugriffe auf Informationssysteme automatisiert abgefragt werden können. Mit dieser Bestimmung wird die notwendige formell-gesetzliche Grundlage geschaffen, damit die Durchführung der gesetzlich geregelten Prüfverfahren und ein automatisierter Zugriff auf die Datenbanken ermöglicht werden.

Die Auflistung der im Informationssystem bearbeiteten Personendaten stellt eine Präzisierung der datenschutzrechtlichen Grundsätze dar. Die Bearbeitung der Personendaten im Informationssystem hat zweckgebunden und unter der Beachtung der Verhältnismässigkeit und des Grundsatzes nach Treu und Glauben zu erfolgen (§ 5 Abs. 1 Bst. d DSG) und stellt eine notwendige Voraussetzung dar, um die Anforderungen an die Informationssicherheit gemäss der Zweckbestimmung des ISG (§ 1 Abs. 2 ISG) zu erfüllen.

5.2. Personensicherheitsprüfung Kanton

§ 13 Prüfzweck und Prüfinhalt

[1] Die Personensicherheitsprüfung dient zur Beurteilung, ob ein Risiko für die Informationssicherheit bestehen könnte, wenn eine Person im Rahmen ihrer Funktion oder eines Auftrags Zugang zu sicherheitsrelevanten Informationen, IT-Mitteln oder Sicherheitszonen des Kantons hat.

[2] Um abzuklären, ob eine solche Person ein Risiko für die Informationssicherheit darstellen könnte, werden sicherheitsrelevante Daten über ihre Lebensführung, insbesondere über ihre engen persönlichen Beziehungen und familiären Verhältnisse, ihre finanzielle Lage und ihre Beziehungen zum Ausland, bearbeitet.

[3] Daten über die Ausübung verfassungsmässiger Rechte dürfen nur dann bearbeitet werden, wenn ein konkreter Verdacht besteht, dass die zu prüfende Person diese Rechte ausübt, um Tätigkeiten vorzubereiten oder auszuüben, welche die Interessen nach § 1 Abs. 2 erheblich beeinträchtigen können.

Die Personensicherheitsprüfung stellt eine vorbeugende Massnahme dar und hat zum Ziel, das Risiko einer vorsätzlichen oder fahrlässigen Beeinträchtigung wesentlicher öffentlicher Interessen, das mit der Ausübung einer sicherheitsempfindlichen Tätigkeit durch eine bestimmte Person verbunden ist, zu identifizieren. Es liegt in der Verantwortung des auftraggebenden bzw. anstellenden Organs zu entscheiden, ob es ein allfälliges erhöhtes Risiko tragen, ob es das Risiko mit bestimmten Auflagen reduzieren oder ob das Organ das Risiko durch Nichtanstellung oder Kündigung vermeiden will.

Die gesetzlichen Grundlagen für die Eignungsprüfungen für die Mitarbeitenden in einem öffentlich-rechtlichen Anstellungsverhältnis im Rahmen der Anstellung und Weiterbeschäftigung bestehen im Personalgesetz (§ 2bis, 2ter und 2quater des Gesetzes über das Arbeitsverhältnis des Staatspersonals vom 1. September 1994 Personalgesetz; PG; BGS 154.21). Daher wird im Rahmen einer Anstellung eine PSP nur in Ausnahmefällen durchzuführen sein. Dies trifft dann zu, wenn neben der Eignung zusätzlich die Vertrauenswürdigkeit für die Ausübung einer sicherheitsempfindlichen Tätigkeit in einer bestimmten Funktion zusätzlich zu prüfen ist.
Als staatliche Massnahme der Informationssicherheit muss die PSP risikogerecht eingesetzt werden. Da sie zwangsläufig mit einem erheblichen Eingriff in die Persönlichkeitsrechte der zu prüfenden Person verbunden ist, muss sie zudem den hohen Anforderungen an die Verhältnismässigkeit genügen. Der mit der PSP verbundene Aufwand und der Eingriff in die Persönlichkeitsrechte lassen sich nur dann rechtfertigen, wenn die Funktion oder der Auftrag, für deren Ausübung eine PSP vorgesehen ist, tatsächlich die Möglichkeit einschliesst, wesentliche Interessen des Kantons erheblich zu beeinträchtigen. Daher ist der Einsatz einer PSP auf das notwendige Mindestmass zu beschränken.

§ 14 Voraussetzungen

[1] Eine Personensicherheitsprüfung kann durchgeführt werden, wenn die mit der Funktion oder dem Auftrag der zu prüfenden Person verbundenen Sicherheitsrisiken dies rechtfertigen, namentlich wenn die zu prüfende Person eine sicherheitsempfindliche Tätigkeit ausübt.

In dieser Bestimmung werden die konkreten Voraussetzungen festgehalten, welche die Durchführung einer Personensicherheitsprüfung (PSP) rechtfertigen. Die Organe stellen fest, bei welchen Personen eine PSP durchzuführen ist. Die Funktionen und Aufträge, welche die Ausübung einer sicherheitsempfindlichen Tätigkeit erfordern und deren Funktionsträgerinnen und Funktionsträger somit geprüft werden müssen, sind festzulegen und klar zu umschreiben. Entscheidend für die Unterstellung unter die PSP ist die Frage, ob die Inhaberin oder der Inhaber einer bestimmten Funktion zur Erfüllung ihrer oder seiner Aufgaben eine sicherheitsempfindliche Tätigkeit ausüben muss. Die Umsetzung dieses restriktiven Ansatzes setzt voraus, dass die Organe eine Übersicht der Geschäftsprozesse und Aufgabenbereiche haben, die notwendigerweise mit sicherheitsempfindlichen Tätigkeiten verbunden sind und zudem die PSP eine Massnahme im Bereich des Risikomanagements der Informationssicherheit darstellt.

Die Grundsätze beim Bearbeiten von Personendaten gemäss § 4 Abs. 1 DSG werden in dieser Bestimmung konkretisiert und mit den Sicherheits- und Schutzzielen des ISG verknüpft. Die «Kann»-Bestimmung öffnet einen Ermessensspielraum zur Durchführung einer PSP und trägt der Verhältnismässigkeit und insbesondere dem Umstand Rechnung, dass eine PSP einen erheblichen Eingriff in die geschützten Persönlichkeitsrechte jeder Person darstellt und daher gestützt auf die Risikoabschätzung stets restriktiv anzuwenden ist.

§ 15 Zu prüfende Personen und zuständige Stellen

[1] Folgende Personen können einer Personensicherheitsprüfung unterzogen werden:
a) Mitarbeitende vor Abschluss beziehungsweise während der Dauer des Anstellungsverhältnisses: durch anstellendes Organ;
b) Personen, die in ein Amt oder als Mitglied eines kantonalen Gremiums gewählt werden sollen: durch die Wahlbehörde oder die Behörde, die den Antrag zur Wahl stellt; oder
c) Dritte, die für ein Organ einen Auftrag ausführen oder eine übertragene Aufgabe wahrnehmen sollen: durch das auftraggebende Organ.

[2] Nicht durchgeführt wird die Personensicherheitsprüfung bei Anwärterinnen und Anwärtern auf folgende Funktionen:
a) Mitglied des Kantonsrats;
b) Mitglied des Regierungsrats;
c) Landschreiberin bzw. Landschreiber;
d) Richterin oder Richter eines kantonalen Gerichts.

[3] Auf eine Personensicherheitsprüfung kann verzichtet werden, wenn die zu prüfende Person eine Sicherheitserklärung der Fachstelle des Bundes vorlegt und die Wiederholungsfrist noch nicht abgelaufen ist.

Im Abs. 1 dieser Bestimmung wird festgelegt, welche Personen einer PSP unterzogen werden. Im Rahmen der Abwicklung einer PSP ist zwischen der für eine PSP zuständigen, der einleitenden und entscheidenden Stelle zu unterscheiden. Als zuständige Stelle ist das Organ bzw. die Wahlbehörde zu bezeichnen, die den Antrag um Durchführung einer PSP stellt. Dieser Antrag ist der Fachstelle für Informationssicherheit zu unterbreiten, welche das PSP-Verfahren einleitet, die Verfahrenskoordination übernimmt und die entsprechenden Daten und Informationen beschafft. Diese werden von der Zuger Polizei, vom Personalamt und allenfalls von einzelnen

HR-Abteilungen der Direktionen einzuholen sein, weil die Fachstelle für Informationssicherheit keinen Zugriff auf diese Daten und ihr aus Gründen des Datenschutzrechts auch kein Zugriff zu gewähren ist. Weil einzig Daten und Informationen im Hinblick auf den Prüfzweck und Prüfinhalt gemäss § 11 ISG auszuwerten sind, wird die Fachstelle für Informationssicherheit über das Ergebnis der PSP entscheiden. Somit ist die Fachstelle für Informationssicherheit im kantonalen PSP-Verfahren einleitende und zugleich entscheidende Stelle. Das Ergebnis der PSP wird der zu prüfenden Person, dem Organ, das eine PSP beantragt hat, der Zuger Polizei und dem Personalamt zugestellt.

Abs. 2 regelt die Funktionen bei denen keine PSP durchzuführen ist. Die entsprechenden Ausnahmen sind Mitglieder von Organen, die vom Volk oder vom Kantonsrat gewählt werden. Diese Personen werden für die Ausübung der entsprechenden Funktion nicht geprüft, obschon sie im Rahmen ihrer Funktion auch sicherheitsempfindliche Tätigkeiten ausüben können.

Die oder der Datenschutzbeauftragte und die Ombudsperson einschliesslich die Stellvertretungen werden vom Kantonsrat für eine Amtsdauer gewählt. Ihre Funktionen sind gemäss Abs. 2 von einer PSP nicht ausgenommen. Dennoch kann gestützt auf Abs. 1 grundsätzlich auf eine PSP verzichtet werden, wenn die Wahlbehörde von einer PSP aus gerechtfertigten Gründen absehen will.

Ein weiterer Ausnahmetatbestand ist in Abs. 3 festgehalten. Wenn der Fachstelle für Informationssicherheit eine Sicherheitserklärung des Bundes unterbreitet wird, dann kann auf eine PSP verzichtet werden. Allerdings hat die Fachstelle zu prüfen, ob die vorgelegte Sicherheitserklärung den Anforderungen an die vom Kanton durchzuführende PSP genügt. Daher kann die Fachstelle für Informationssicherheit verlangen, dass eine PSP gemäss dem ISG durchzuführen ist, selbst wenn eine Sicherheitserklärung des Bundes vorliegt.

§ 16 Einwilligung und Mitwirkung

[1] Eine Personensicherheitsprüfung darf nur mit der Einwilligung der zu prüfenden Person durchgeführt werden.

[2] Die zu prüfende Person ist verpflichtet, an der Feststellung des Sachverhalts mitzuwirken.

Die Durchführung der PSP erfordert die ausdrückliche Einwilligung der betroffenen Person. Die Fachstelle für Informationssicherheit hat dabei eine Aufklärungspflicht. Im Rahmen des Prüfverfahrens hat die zu prüfende Person an der Sachverhaltserhebung mitzuwirken. Diese beinhaltet neben der Auskunftserteilung anlässlich der Befragung auch die Einreichung von weiterführenden und für den Zweck der PSP hilfreichen Unterlagen. Insbesondere ist die Mitwirkung zur Abklärung der persönlichen Umstände und Verhältnisse notwendig, zu welchen die Fachstelle für Informationssicherheit keine Anhaltspunkte hat und die für sie nicht ohne weiteres erkennbar sind. Die befragte Person muss ihre Antworten wahrheitsgemäss erteilen. Es ist der zu prüfenden Person insbesondere anlässlich der Befragung unbenommen, bestimmte Fragen nicht beantworten zu wollen. Es ist dann aber Aufgabe der Fachstelle für Informationssicherheit, die Auskunftsverweigerung oder auch die Verweigerung, weitere Dokumente einzureichen, zu würdigen, da ein gewisser Spielraum für Fragen zur persönlichen Geheimsphäre bestehen muss. Verweigert die zu prüfende Person die Mitwirkung jedoch in einem Ausmass,

dass eine fachgerechte Beurteilung nicht möglich ist, so ist die PSP abzubrechen und die Prüfung gilt als nicht bestanden.

§ 17 Zuständige Stelle

[1] Zuständig für die Durchführung der Personensicherheitsprüfung ist die Fachstelle für Informationssicherheit.

[2] Die Fachstelle für Informationssicherheit kann Organe mit der Durchführung der Datenerhebung und der Beschaffung von Informationen beauftragen.

[3]Aufgaben, Kompetenzen, Organisation und Berichterstattung der Fachstelle für Informationssicherheit werden in der Vollziehungsverordnung geregelt.

Unter Ziffer 4 des vorliegenden Berichts finden sich nähere Erläuterungen zu den Aufgaben der Fachstelle für Informationssicherheit die als unabhängige Fachstelle der Finanzdirektion zugeordnet ist.

Für die Fachstelle für Informationssicherheit besteht mit der Bestimmung gemäss Abs. 2 die formalgesetzliche Rechtsgrundlage, die für die Datenerhebung zuständigen Stellen, beispielsweise die Zuger Polizei oder das Personalamt, zu beauftragen, bei der Datenerhebung mitzuwirken und insbesondere die im Rahmen einer PSP notwendigen Registerabklärungen vorzunehmen. Eine Datenerhebung durch die Fachstelle erfolgt gestützt auf das Verhältnismässigkeitsprinzip, wenn notwendige Abklärungen erforderlich sind, weil die zu beschaffenden Daten beispielsweise bei der Zuger Polizei, beim Personalamt oder bei dem antragsstellenden Organ nicht vorhanden und ebenfalls nicht abrufbar sind. Der Fachstelle ist bei der Beschaffung der Daten, beispielsweise aus entsprechenden Registern, ein Ermessensspielraum einzuräumen.

Eine pflichtgemässe Ermessensbetätigung setzt voraus, dass die Datenerhebung im Rahmen der Abklärungen gemäss § 14 ISG im Hinblick auf die Aufgaben und Funktion der zu prüfenden Person erfolgt. Zudem muss die Datenerhebung die Voraussetzungen gemäss § 13 ISG bezüglich Prüfzweck und Prüfinhalt der PSP unter Berücksichtigung der Verhältnismässigkeit und der sparsamen Bearbeitung der Personendaten gemäss DSG erfüllen. Die Fachstelle stimmt die Datenerhebung und insbesondere die Registerabklärungen mit dem auftraggebenden Organ ab und kann für diese Abklärungen insbesondere die Zuger Polizei und das Personalamt beiziehen.

Die Fachstelle für Informationssicherheit kann von sich aus keine PSP durchführen, sie benötigt einen Auftrag des zuständigen Organs. Die Fachstelle muss das Risiko für die Informationssicherheit objektiv, das heisst ausschliesslich gestützt auf die erhobenen Daten beurteilen. Daher darf sich die führungsverantwortliche Stelle des auftraggebenden Organs nicht in das Prüfverfahren einmischen.

§ 18 Datenerhebung

[1] Die Fachstelle für Informationssicherheit kann für die Personensicherheitsprüfung aus folgenden Quellen Daten über die zu prüfende Person erheben:

a) aus dem Strafregister;
b) bei den Strafbehörden durch Einholen von Auskünften und Akten über laufende, abgeschlossene oder eingestellte Strafverfahren;
c) aus den Datenbearbeitungs- und Informationssystemen der Kantonspolizei;
d) aus den Registern der Betreibungs- und Konkursbehörden;
e) aus den Akten bisheriger Personensicherheitsprüfungen; und
f) aus öffentlich zugänglichen Quellen.

[2] Die Fachstelle für Informationssicherheit kann bei Bedarf zudem aus folgenden Quellen Daten erheben:
a) bei den eidgenössischen und kantonalen Steuerbehörden;
b) aus den Registern der Einwohnerkontrollen;
c) durch Auskünfte oder Akteneinsicht über Administrativverfahren im Strassenverkehr;
d) durch Einholung von Referenzen bei früheren Arbeitgebern;
e) bei Finanzinstituten und Banken, mit welchen die zu prüfende Person Geschäftsbeziehungen unterhält;
f) aus den vorhandenen Akten bisheriger Eignungsprüfungen gemäss § 2[bis] Personalgesetz;
g) aus systematischen Sammlungen und Analysen von öffentlich zugänglichen Informationen;
h) durch Befragung der zu prüfenden Person;
i) durch Befragung von Dritten, sofern die zu prüfende Person zustimmt.

[3] Die Fachstelle für Informationssicherheit kann Befragungen nach Abs. 2 Bst. i mit technischen Geräten aufnehmen und auf Datenträgern aufbewahren.

Die Fachstelle für Informationssicherheit kann die Daten aus verschiedenen Quellen erheben. Dabei ist nicht verlangt, dass auf alle verfügbaren Mittel und Daten zurückgegriffen werden muss, um das Risiko zu beurteilen. Es gilt das Verhältnismässigkeitsprinzip zu beachten. Zudem muss aus Gründen des Datenschutzes auf die Erhebung von Daten, die allenfalls besonders schützenswert sind, teilweise oder vollständig verzichtet werden. Wenn im Rahmen der PSP die Erhebung von besonders schützenswerten Personendaten zur Beurteilung des Risikos nicht notwendig ist, dann dürfen diese Daten nicht beschafft werden. Eine Erhebung von Daten gleichsam auf Vorrat, ohne dass dazu ein berechtigter Anlass besteht, ist aus Gründen des Datenschutzes ebenfalls nicht zulässig.

Eine persönliche Befragung kann in jedem Fall durchgeführt werden, wenn sicherheitsrelevante Umstände im Rahmen der Datenerhebung festgestellt werden. Auf eine Wiederholung der Befragung über Themen, die bereits im Rahmen der personalrechtlichen Eignungsprüfung erfolgt ist, muss aus Gründen der Verhältnismässigkeit und des Datenschutzes verzichtet werden. Die Befragung muss sich im Rahmen der Datenbeschaffung einzig auf Prüfthemen beziehen, die zusätzlich zu den bereits erhobenen Daten vertiefter abzuklären sind und die stets im Zusammenhang mit der Funktion bzw. der zu erfüllenden Aufgabe stehen müssen.

Auf die Daten aus den Personalakten, welche im Rahmen von Eignungsprüfungen gemäss dem Personalgesetz vorliegen, oder welche von früheren Personensicherheitsprüfungen aktuell sind und verwendet werden können, muss zurückgegriffen werden, um dem Prinzip der Verhältnismässigkeit gemäss DSG zu entsprechen. Die Zuger Polizei, das Personalamt oder die HR-Abteilungen weisen auf diese Daten hin, welche im Rahmen der durchzuführenden PSP

verwendet werden können. Die Fachstelle für Informationssicherheit entscheidet, ob diese bereits vorhandenen Daten weiterhin verwendet werden können oder ob diese neu beschafft werden müssen.

Die Informationen aus OSINT (Open Source Intelligence) stellen heute eine weit verbreitete und auch häufig verwendete Quelle von öffentlich zugänglichen Informationen dar, zumal diese Informationen aus frei verfügbaren Quellen gesammelt, verknüpft und ausgewertet werden. Als Quellen kommen insbesondere Websites, Blogs, soziale Netzwerke mit beruflichen Profilen, Posts, Bilder oder Nachrichten aus Presse, Medien usw. in Frage Das Anführen dieser Quelle dient der Transparenz im Datenschutzrecht und ermöglicht die Auswertung der in diesen Quellen festgestellten Informationen gemäss den datenschutzrechtlichen Grundsätzen der Bearbeitung von Personendaten.

Abs. 3 schafft die rechtliche Grundlage für die Tonaufnahme der Befragungen und den Einsatz von weiteren technischen Mitteln. Der Einsatz der entsprechenden technischen Mittel und die Bearbeitung und Löschung der auf diesem Weg erhobenen Daten im Sinne der Transparenz der Datenbearbeitung ist vor der Befragung bekanntzugeben. Auf Verlangen ist die Aufzeichnung zur Anhörung zur Verfügung zu stellen. Dieser Anspruch folgt aus dem Recht, Auskunft über die erhobenen personenbezogenen Daten zu erhalten. Zudem kann eine Berichtigung der erhobenen Personendaten verlangt werden (Art. 44 Abs. 1 ISG-Bund).

§ 19 Datenerhebung bei Drittpersonen

[1] Befragt die Fachstelle für Informationssicherheit Drittpersonen nach § 18 Abs. 2 Bst. i, so macht sie diese darauf aufmerksam, dass die Auskunft freiwillig ist.

[2] Daten über Dritte, die untrennbar mit Daten über die zu prüfende Person verbunden sind, dürfen nur bearbeitet werden, wenn dies für die Beurteilung des Sicherheitsrisikos unerlässlich ist. Die Fachstelle für Informationssicherheit informiert die betroffenen Dritten über die Bearbeitung.

Zur Abklärung besonderer sicherheitsrelevanter Umstände oder zum Erhalt ergänzender Daten über einen längeren Zeitraum kann die Fachstelle für Informationssicherheit auch Drittpersonen befragen. Solche Befragungen dürfen nur mit dem Einverständnis der zu prüfenden Person und der betroffenen Drittperson durchgeführt werden. Die betroffene Drittperson kann trotz des Einverständnisses der betroffenen Person, die sich der PSP unterzieht, jederzeit auf die Erteilung jeglicher Auskunft verzichten.

§ 20 Ergebnis der Beurteilung

[1] Die Fachstelle für Informationssicherheit stellt das Ergebnis der Beurteilung als eine der folgenden Erklärungen mit der nachstehenden Bedeutung aus:
a) Sicherheitserklärung: Es besteht kein Sicherheitsrisiko.
b) Sicherheitserklärung mit Vorbehalt: Es besteht ein Sicherheitsrisiko, das mit Auflagen auf ein tragbares Mass reduziert werden kann. Die Fachstelle für Informationssicherheit empfiehlt entsprechende Auflagen.
c) Risikoerklärung: Es besteht ein Sicherheitsrisiko.

[2] Ein Sicherheitsrisiko besteht, wenn aufgrund der erhobenen Daten konkrete Anhaltspunkte vorliegen, dass die geprüfte Person die sicherheitsrelevante Funktion oder den sicherheitsrelevanten Auftrag mit hoher Wahrscheinlichkeit vorschriftswidrig oder unsachgemäss ausüben wird.

[3] Die Wahrscheinlichkeit einer vorschriftswidrigen oder unsachgemässen Ausübung der sicherheitsempfindlichen Tätigkeit kann insbesondere dann als hoch gelten, wenn konkrete Anhaltspunkte für folgende persönliche Eigenschaften vorliegen:
a) mangelnde persönliche Integrität oder Vertrauenswürdigkeit;
b) Erpressbarkeit oder Bestechlichkeit; oder
c) beeinträchtigtes Urteils- oder Entscheidungsvermögen.

[4] Die Fachstelle für Informationssicherheit teilt der geprüften Person sowie dem Antrag stellenden Organ das Ergebnis der Personensicherheitsprüfung schriftlich mit. Diese Mitteilung ergeht in der Form einer Erklärung der Fachstelle.

Das Ergebnis der Beurteilung beruht auf einer qualitativen Methode, bei welcher das Vorhandensein und das Zusammenwirken von Risikofaktoren bewertet werden. Der für die Durchführung einer PSP massgebende Ausdruck sicherheitsempfindliche Tätigkeit enthält in seiner Definition die Auswirkungen, deren Eintreten vermieden werden soll.

Es handelt sich dabei um eine erhebliche bzw. schwerwiegende Beeinträchtigung der Interessen nach § 1 Abs. 2 ISG. Ein Sicherheitsrisiko muss angenommen werden, wenn die Wahrscheinlichkeit hoch ist, dass die geprüfte Person die sicherheitsempfindliche Tätigkeit vorschriftswidrig oder unsachgemäss ausüben wird und dadurch die Interessen nach § 1 Abs. 2 mindestens erheblich beeinträchtigen wird. Die Fachstelle für Informationssicherheit muss sich einzig auf die Eintrittswahrscheinlichkeit des Ereignisses fokussieren. Bei der Bewertung einer solchen Wahrscheinlichkeit wird es sich zwangsläufig immer um eine Prognose über ungewisse künftige Sachverhalte handeln. Grundlage für diese Prognose bildet die Gesamtheit aller Umstände, wie beispielsweise die Persönlichkeit der betroffenen Person, ihr Vorleben und ihre Lebensverhältnisse, soweit diese Rückschlüsse auf ihr künftiges Verhalten zulassen.

Nach Abs.2 stellt die PSP auf eine objektive Gefährdung und nicht auf ein schuldhaftes Verhalten ab. Die Annahme eines Sicherheitsrisikos muss durch Fakten und tatsächliche Umstände, welche die zu beurteilende Person betreffen, begründet werden. Reine Vermutungen, insbesondere wenn sie beispielsweise die politische Gesinnung der zu prüfenden Person betreffen, sind nicht zulässig.

In Abs. 3 werden deshalb die Risikofaktoren konkretisiert, die zur Annahme einer hohen Wahrscheinlichkeit für eine Beeinträchtigung führen. Diese Bestimmung umschreibt persönliche Eigenschaften, die besonders risikoträchtig sind. Die Umschreibungen zielen zwar im Grundsatz auf möglichst objektiv feststellbare Eigenschaften ab. Mit Integrität und Vertrauenswürdigkeit werden vorweg der Charakter sowie die Gewohnheiten und Beziehungen einer Person zu ihrem Umfeld anvisiert. Diese Eigenschaften sind bei der Ausübung einer sicherheitsempfindlichen Tätigkeit die Eignungserfordernisse, die erfüllt sein müssen. Liegen diese Eigenschaften vor, kann mit hoher Wahrscheinlichkeit darauf vertraut werden, dass die mit einer solchen

Tätigkeit betraute Person loyal zu ihrer Aufgabe steht und die Sicherheitsinteressen des Arbeitgebers oder der Institution wahrt.

Die Fachstelle teilt das Ergebnis der PSP in der Form einer Erklärung der geprüften Person und dem antragstellenden Organ mit. Gestützt auf die schriftliche Mitteilung der Fachstelle gemäss Abs. 4 kann die geprüfte Person gegen die Erklärung der Fachstelle gemäss § 21 ISG vorgehen und die entsprechenden Schritte im Rahmen des Rechtsschutzes nach § 21 ISG einleiten.

§ 21 Rechtsschutz

[1] Die geprüfte Person kann nach Erhalt der Erklärung der Fachstelle gemäss § 20 Abs. 4 innerhalb von 20 Tagen
a) Einsicht in die Prüfungsunterlagen nehmen;
b) eine Berichtigung falscher Daten oder die Vernichtung nicht mehr aktueller Daten verlangen; oder
c) einen Bestreitungsvermerk anbringen lassen.

[2] Die Einschränkung des Auskunftsrechts richtet sich nach § 14 DSG.

[3] Die Erklärung kann gestützt auf § 21a Verwaltungsrechtspflegegesetz innert 20 Tagen beim Regierungsrat mit Beschwerde angefochten werden.

Absatz 1 Bst. a entspricht dem Auskunftsrecht der betroffenen Person. Die geprüfte Person muss ihre Ansprüche auf Information gestützt auf die in § 18 Abs. 1 und Abs. 2 bearbeiteten Daten geltend machen können, um den Rechtsschutz wahrzunehmen.
Abs 1 Bst. b stellt eine Mindestanforderung an die Bearbeitung der Personendaten im Rahmen einer Personensicherheitsprüfung dar und Abs. 1 Bst. c gewährleistet eine Vorgehensmassnahme, die der geprüften Person zusteht. Diese Bestimmungen sind mit Art. 44 Abs. 1 ISG-Bund vergleichbar.

Absatz 2 regelt die Einschränkung des Auskunftsrechts. Im ISG-Bund wird im Art. 44 Abs. 2 im Zusammenhang mit der Einschränkung des Auskunftsrechts auf Artikel 26 des Datenschutzgesetzes des Bundes verwiesen (Bundesgesetz über den Datenschutz vom 25. September 2020, DSG, SR 235.1). Eine vergleichbare Regelung ist im ISG vorgesehen. Massgebende Grundlage bildet § 14 DSG. Demnach darf ein Organ die Auskunft über Personendaten aus überwiegenden Interessen der Öffentlichkeit oder Dritter begründet einschränken, mit Auflagen versehen, aufschieben oder verweigern. Die Anwendung dieser Bestimmung setzt eine Interessensabwägung voraus. Die öffentlichen Interessen sind gegenüber den privaten Interessen der geprüften Person, mithin dem Anspruch auf Auskunft und damit verbunden der Ausübung der verfahrensrechtlichen Möglichkeiten, abzuwägen. Die privaten Interessen an der Auskunft der geprüften Person sind als erheblich zu bewerten, weil besonders schützenswerte Personendaten im Rahmen einer PSP bearbeitet werden und daher die geprüfte Person allein deswegen ein hohes Interesse an einer Auskunftserteilung nachweisen kann. Die Bestimmung nach § 14 DSG verlangt eine Massnahme, die dem Verhältnismässigkeitsprinzip nach § 4 Abs. 1 Bst. d DSG entspricht. Eine vollständige Verweigerung der Auskunftserteilung dürfte dem Verhältnismässigkeitsprinzip kaum standhalten und muss als absolute Ausnahme betrachtet werden.

Im Absatz 3 wird der Rechtsweg gestützt auf das Gesetz über den Rechtsschutz in Verwaltungssachen vom 01. April 1976 (Verwaltungsrechtspflegegesetz; VRG; BGS 162.1) umschrieben. § 21a VRG setzt die Rechtsweggarantie von Art. 29a Bundesverfassung um, wonach jede Person bei Rechtsstreitigkeiten Anspruch auf Beurteilung einer richterlichen Behörde hat. Gestützt auf diese Bestimmung kann eine anfechtbare Verfügung beantragt werden, wenn jemand von einer behördlichen Handlung betroffen ist und ein schutzwürdiges Interesse geltend machen kann.

Die Erklärung der Fachstelle stellt einen Entscheid über Realakte der Verwaltung gemäss § 21a Abs. 2 VRG dar, der unter bestimmten Voraussetzungen angefochten werden kann. Demnach können Personen, die ein schutzwürdiges Interesse nachweisen, was im Falle einer Erklärung betreffend die PSP regelmässig der Fall sein dürfte, verlangen, dass die im Abs. 1 Bst. b und c festgehaltenen Massnahmen getroffen werden. In diesem Sinne stellt die vorliegende Bestimmung nach § 21 Abs. 1 ISG einen Spezialtatbestand zu § 21a Abs. 1 VRG dar.

Die Erklärung der Fachstelle kann gestützt auf § 21 Abs. 3 ISG mit Beschwerde beim Regierungsrat angefochten werden.

§ 22 Wiederholung der Personensicherheitsprüfung

[1] Die Personensicherheitsprüfung ist spätestens nach fünf Jahren zu wiederholen. Für Personen in einer Funktion mit Amtsdauer wird die Personensicherheitsprüfung jeweils vor der Wiederwahl wiederholt.

[2] Die Personensicherheitsprüfung kann bei begründetem Anlass jederzeit wiederholt werden.

Das ISG schreibt keine festen ordentlichen Wiederholungsintervalle vor. Es setzt diesbezüglich lediglich Leitplanken fest. Diese werden im Abs. 1 geregelt.

Eine PSP bzw. eine Wiederholung der PSP soll dem tatsächlichen Sicherheitsbedarf entsprechend erfolgen. Eine vorzeitige Wiederholung der PSP ist beispielsweise aufgrund der Entstehung neuer Risiken bei der betroffenen Person durchzuführen, wenn diese Risiken einen Bezug zur sicherheitsempfindlichen Tätigkeit aufweisen (Abs. 2).

§ 23 Datenaufbewahrung, -archivierung und -vernichtung

[1] Die Fachstelle für Informationssicherheit bewahrt die Daten so lange auf, wie die betreffende Person ihre Funktion oder ihren Auftrag ausübt, längstens jedoch zehn Jahre.

[2] Die Archivierung der Daten richtet sich nach den Vorschriften des Archivgesetzes.

[3] Wird das Prüfverfahren eingestellt, tritt eine geprüfte Person die vorgesehene Funktion nicht an oder lehnt sie den Auftrag ab, so werden alle mit der Personensicherheitsprüfung zusammenhängenden Daten und Akten spätestens nach drei Monaten vernichtet.

Diese Bestimmung beruht auf Art. 47 des ISG-Bund und regelt ebenfalls die Datenaufbewahrung, -archivierung und -vernichtung von Personendaten im Zusammenhang mit PSP. Die Aufbewahrungsdauer von höchstens zehn Jahren dürfte mit Blick auf die datenschutzrechtlichen Grundsätze wie Verhältnismässigkeit und Dauer und Aufbewahrung von Personendaten nur in Ausnahmefällen relevant sein. Personendaten sollen nur so lange aufbewahrt werden, wie dies für die Erkennung von Vorfällen und die Abwehr von Gefahren zweckmässig und notwendig ist. In den meisten Fällen sind bearbeitete Daten sehr kurzlebig und werden kurz nach der Bearbeitung wieder gelöscht werden.

Falls eine Person bereits mehreren Prüfungen unterzogen wurde, sind diejenigen Daten von Prüfungen zu löschen, die länger als zehn Jahre zurückliegen. Das Archivgesetz vom 29. Januar 2004 (BGS 152.4) regelt die Grundsätze der Aufbewahrung, der Verwaltung der Unterlagen, der Feststellung der Archivwürdigkeit und die Archivierungsprozesse. Die Regelungen der ordentlichen bzw. verlängerten Schutzfristen gemäss § 11 und § 12 Archivgesetz von 30 Jahren übersteuern die Bestimmungen des ISG und DSG.

Ein bereits eingeleitetes Prüfverfahren wird eingestellt, wenn die zu prüfende Person im Verlauf des Verfahrens ihre Einwilligung zurückzieht oder wenn sie aus einem anderen Grund für die vorgesehene Funktion oder für den fraglichen Auftrag nicht mehr in Frage kommt. In diesem Fall sind sowohl die zu prüfende Person als auch die einleitende Stelle über die Einstellung des Verfahrens zu informieren und die bei der entscheidenden Stelle PSP bereits erhobenen Daten und Akten sind zu vernichten. Die betroffene Person gilt in der Folge als nicht sicherheitsgeprüft und darf die fragliche sicherheitsempfindliche Tätigkeit nicht ausüben bzw. die entsprechende Funktion nicht übernehmen.

5.3 Personensicherheitsprüfung Bund

§ 24 Anwendbares Recht und zuständige Stelle

[1] Bei Personen, die klassifizierte Informationen des Bundes bearbeiten oder auf IT-Mittel des Bundes zugreifen, erfolgt die Personensicherheitsprüfung gemäss den Bestimmungen des Bundesgesetzes über die Informationssicherheit.

[2] Zuständige Stelle für die Einleitung der Personensicherheitsprüfung und den Entscheid über die Ausübung der sicherheitsempfindlichen Tätigkeit gemäss Art. 31 Abs. 1 des Bundesgesetzes über die Informationssicherheit ist die Fachstelle für Informationssicherheit.

Diese Bestimmung präzisiert den Auftrag des Bundes an die Kantone, die Zuständigkeit für die Einleitung und Durchführung einer PSP zu regeln. Der Anwendungsbereich dieser PSP ist gemäss Abs. 1 begrenzt und betrifft einzig diejenigen kantonalen Angestellten, die klassifizierte Informationen des Bundes bearbeiten oder auf IT-Mittel des Bundes zugreifen. Voraussetzungen und Anforderungen an die PSP werden im ISG-Bund geregelt. Die entsprechenden Kosten für die Durchführung der PSP trägt der Bund (Art. 36 Abs. 3 ISG-Bund).

8. Vollziehungsregelung

§ 25 Vollziehungsverordnung

[1] Der Regierungsrat erlässt zu diesem Gesetz im Einvernehmen mit dem Obergericht und dem Verwaltungsgericht eine Vollziehungsverordnung.

Der Regierungsrat erlässt eine Vollziehungsverordnung (Informationssicherheitsverordnung) gestützt auf diese Bestimmung. Sie tritt gleichzeitig mit dem ISG in Kraft. Zusätzlich kann der Regierungsrat Weisungen erlassen, welche Einzelfragen der Informationssicherheit behandeln.

9. Finanzielle und personelle Auswirkungen und Anpassungen von Leistungsaufträgen

Die nachfolgend dargestellten personellen und finanziellen Auswirkungen ergeben sich sowohl aus dem Informationssicherheitsgesetz (ISG) und der dazugehörigen Informationssicherheitsverordnung (ISV) als auch aus den damit zusammenhängenden Anpassungen von bestehenden Verordnungen (Informatikverordnung ITV) sowie von Weisungen zur Informationssicherheit. Dies ermöglicht eine gesamthafte Darstellung aller anfallenden Kosten.

9.1. Finanzielle Auswirkungen auf den Kanton Zug

Mit dem neuen ISG und der dazugehörigen Vollzugsverordnung ISV entstehen für den Kanton Zug neben dem separat ausgewiesenen Personalbedarf (siehe nachstehend) insbesondere einmalige und wiederkehrende Sach- und IT-Kosten. Diese ergeben sich namentlich aus den folgenden im ISG angelegten Umsetzungsnotwendigkeiten:

Informationssysteme: Die betroffenen Organe können zur Bewältigung von Verletzungen der Informationssicherheit respektive zur Behebung von Schwachstellen Personendaten in dafür vorzusehenden Informationssystemen (ISMS-Anwendungen) bearbeiten und dürfen hierfür bestehende Informationssysteme verknüpfen, Daten über Schnittstellen austauschen sowie digitale Formulare bereitstellen und anbinden. Daraus ergeben sich sowohl (einmalige) Projektkosten (Konzeption, Implementierung/Integration, Tests etc.) als auch wiederkehrende Betriebs- und Wartungskosten (Betrieb, Support, Weiterentwicklungen, Sicherheitsmassnahmen etc.) Das Amt für Informatik hat 2025 wegen der ISO 27001:2022 Zertifizierung ein offiziell anerkanntes ISMS eingeführt (Lizenzierung für FD). Durch die notwendige Erweiterung des ISMS auf den gesamten Kanton erhöhen sich die Lizenzkosten um ca. 15 000 Franken jährlich.

Identity-/Access-Management und Systemanbindungen: Das ISG sieht auch den Datenaustausch und -abgleich zwischen Identitätsverwaltungssystemen sowie angebundenen Informationssystemen und Verzeichnissen vor (z.B. für Authentifizierung, Datenübernahme beim Aufbau neuer Systeme [Bsp. Einführung von AGOV für eTax], Migration bestehender Authentifikationsdaten etc.). Dies führt praxisgemäss zu Aufwendungen für die IAM-/Directory-Integration, Schnittstellenpflege, Gewährleistung der Identitätsprüfung und -qualität sowie zu Lizenz- und Betriebskosten entsprechender Plattformen. Diese belaufen sich auf ca. 10 000 Franken jährlich

Informationssystem für Personensicherheitsprüfungen (PSP): Die Fachstelle für Informationssicherheit betreibt ein Informationssystem für Personensicherheitsprüfungen. Daraus ergeben sich Investitionen die Erweiterung der aktuellen Lizenz, den Betrieb inklusive Sicherheit und die Wartung eines solchen Systems, dies wird durch das bestehende ISMS abgedeckt.

Physische Schutzmassnahmen und Sicherheitszonen: Das ISG und die ISV regeln den physischen Schutz von Informationen und IT-Mitteln sowie den Zugang zu Sicherheitszonen (Bereiche, in denen häufig als «vertraulich» oder «geheim» klassifizierte Informationen bearbeitet oder IT-Mittel mit «hohem Schutz» betrieben werden). Je nach aktuellem Reifegrad können dadurch einmalige Investitionen (z.B. Zutrittskontrollen, Schutzeinrichtungen) sowie laufende Kosten (Betrieb, Unterhalt, Kontrollen) bei den betroffenen Organen entstehen. Für die Prüfung von Lieferanten und z.B. Gemeinden entsteht ein Mehraufwand für Audits, sowie die Lizenzierung unserer Schwachstellenprüf Software müsste erweitert werden. Gesamthaft führt das zu jährlich ca. 50 000 Franken an Mehrkosten.

Sicherheitsverfahren und Sicherheitsstufen: Der Regierungsrat erlässt eine Weisung u.a. zum Verfahren der Gewährleistung der Informationssicherheit beim Einsatz von IT-Mitteln (Sicherheitsverfahren), welche Bestimmungen zur Schutzbedarfsbeurteilung, zu den Sicherheitsstufen und den Sicherheitsmassnahmen sowie deren Umsetzung und Überprüfung umfasst. Auch wenn die Durchführung beim jeweiligen Organ liegt, entstehen kantonsweit Sachkosten. Zur Umsetzung und Ablage der Kontrolle wird wiederum das ISMS verwendet, es führt zu den unter Informationssystem aufgeführten Mehrkosten. Soweit im Einzelfall für sicherheitsempfindliche Aufträge durch Dritte eine Beurteilung der Eignung bei der Fachstelle Betriebssicherheit des Bundes beantragt wird, sind dessen Leistungen gebührenpflichtig. Die Gebühren werden über eine Leistungsvereinbarung zwischen dem Bund und dem Kanton festgelegt.

Die ab 2028 wiederkehrenden Kosten von 415 000 Franken jährlich setzen sich zusammen aus Sach- und IT-Kosten von insgesamt rund 75 000 Franken (Erweiterung der ISMS-Lizenzen: ca. 15 000 Franken; IAM-Integration und Schnittstellen: ca. 10 000 Franken; physischer Schutz, Audits und Schwachstellenprüfung: ca. 50 000 Franken) sowie aus den Personalkosten von 340 000 Franken für die beiden Stellen der Fachstelle für Informationssicherheit (siehe nachfolgend Kapitel 9.2). Im Einführungsjahr 2027 beläuft sich der Aufwand auf 245 000 Franken, da zunächst nur eine der beiden Stellen besetzt ist.

A	Investitionsrechnung	2027	2028	2029	2030
1.	Gemäss Budget oder Finanzplan: bereits geplante Ausgaben				
	bereits geplante Einnahmen				
2.	Gemäss vorliegendem Antrag: effektive Ausgaben				
	effektive Einnahmen				
B	**Erfolgsrechnung (nur Abschreibungen auf Investitionen)**				
3.	Gemäss Budget oder Finanzplan: bereits geplante Abschreibungen				
4.	Gemäss vorliegendem Antrag: effektive Abschreibungen				
C	**Erfolgsrechnung (ohne Abschreibungen auf Investitionen)**				
5.	Gemäss Budget oder Finanzplan: bereits geplanter Aufwand	0	0	0	0
	bereits geplanter Ertrag				
6.	Gemäss vorliegendem Antrag: effektiver Aufwand	245’000	415’000	415’000	415’000
	effektiver Ertrag				

9.2. Personelle Auswirkungen auf den Kanton

Mit dem Inkrafttreten des neuen ISG sowie der neuen Vollziehungsverordnung ISV entstehen dem Kanton Zug zusätzliche personelle Aufwände. Der Schwerpunkt der personellen Auswirkungen liegt bei der neu zu schaffenden Fachstelle für Informationssicherheit. Diese wird der Finanzdirektion als Fachstelle zugeordnet und durch den Informationssicherheitsbeauftragten (Chief Information Security Officer; CISO) geleitet. Der CISO sowie der ISO (Information Security Officer) mit insgesamt 200 Stellenprozenten wechseln vom Team Informationssicherheit beim AIO in die Fachstelle Informationssicherheit bei der Finanzdirektion.

Diese Aufgaben führen zu einem dauerhaften Personalaufwand (Planung, Durchführung von Kontrollen, Dokumentation, Nachverfolgung von empfohlenen Massnahmen, Reporting etc.). Für den Ausbau der vorerwähnten Leistungen bei der Finanzdirektion werden somit zusätzliche Personalressourcen im Umfang von 200 Stellenprozenten benötigt.

Die Besetzung der Stellenprozente ist ab dem Jahr 2027 vorgesehen mit einer Vollzeitstelle für 2027 und einer zweiten ab 2028. Für die Finanztabelle wird mit dem Jahreslohnansatz von 170 000 Franken pro Vollzeitstelle gerechnet.

9.3. Personelle und finanzielle Auswirkungen auf die Gemeinden

Für die Organe der Gemeinden gilt die ISV nicht umfassend, sondern nur hinsichtlich der Bearbeitung von klassifizierten Informationen des Bundes oder des Kantons, respektive hinsichtlich des Zugriffs auf IT-Mittel des Bundes oder des Kantons. Die Bestimmungen gelten dann nicht, wenn eine mindestens gleichwertige Informationssicherheit gewährleistet wird.

Daraus folgt, dass ein finanzieller und personeller Aufwand der Gemeinden nur fallbezogen entsteht und sofern die Gemeinden keine gleichwertige Informationssicherheit nachweisen können. In diesen Fällen können Aufwände für die Umsetzung der einschlägigen Vorgaben (z.B. organisatorische Massnahmen, technische Anpassungen etc.) anfallen. Die Feststellung der Gleichwertigkeit und des Bedarfs an Unterstützungsleistungen liegt bei der Fachstelle für Informationssicherheit.

9.4. Anpassungen von Leistungsaufträgen

Das neue ISG führt zu keinen Anpassungen von Leistungsaufträgen.

10. Zeitplan

17. Dezember 2026	Kantonsrat, Kommissionsbestellung
Januar bis Februar 2027	Kommissionssitzung(en)
März/April 2027	Kommissionsbericht
Mai 2027	Beratung Staatswirtschaftskommission
Mai 2027	Bericht Staatswirtschaftskommission
24. Juni 2027	Kantonsrat, 1. Lesung
26. August 2027	Kantonsrat, 2. Lesung
2. September 2027	Publikation Amtsblatt
2. September 2027	Beginn der Referendumsfrist (60 Tage)
2. November 2027	Ablauf Referendumsfrist
4. November 2027	Publikation Amtsblatt
5. November 2027	Inkrafttreten (ohne Volksabstimmung)
19. März 2028	Allfällige Volksabstimmung
23. März 2028	Publikation Amtsblatt
24. März 2028	Inkrafttreten (bei Volksabstimmung)

11. Antrag

Gestützt auf die vorliegenden Ausführungen beantragen wir Ihnen:

1. Auf die Vorlage Nr einzutreten und ihr zuzustimmen.

Mit vorzüglicher Hochachtung
Regierungsrat Kanton Zug

Der Landammann:

Der Landschreiber: