Beilage 3
FD FDS 4.5 / 19 / 163446

**Erläuterungen zur Vollziehungsverordnung zum Gesetz über die Informationssicherheit (Informationssicherheitsverordnung, ISV)**

vom …

## 1. In Kürze

Die grundlegenden Bestimmungen über Einschränkungen verfassungsmässiger Rechte müssen in einem Gesetz im formellen Sinne 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 01. April 2025 in Kraft getretenen Bestimmung über die Bearbeitung von Personendaten die dazu notwendige gesetzliche Grundlage geschaffen. Dieser gesetzgeberische Schritt setzte den Kanton Zug unter Zugzwang. Mit der Gesetzesvorlage des ISG schafft der Kanton Zug hiermit ebenfalls die notwendige gesetzliche Grundlage. In der ISV finden sich daher keine Bestimmungen, welche die Bearbeitung der Personendaten regeln.

Die Bestimmungen der ISV, die im Bund überwiegend auf Gesetzesstufe geregelt werden, behandeln Themen unter anderem wie Grundsätze der Informationssicherheit, des Risikomanagements, der Klassifizierung von Informationen, der Sicherheit beim Einsatz von IT-Mitteln mit der Regelung der Massnahmen und dem physischen Schutz.

Erläuterungen zu den Grundlagen im Kanton Zug, welche Auswirkungen auf die Bestimmungen der Informationssicherheit im ISG und in der ISV haben, werden im Bericht zum ISG behandelt. Davon sind insbesondere datenschutzrechtliche Themen, Abgrenzungen zwischen der Personalgesetzgebung und der Personensicherheitsprüfung und Hinweise zum Geltungsbereich für die Gemeinden betroffen. Zudem wird im ISG die gesetzliche Grundlage für die Bildung einer Fachstelle für Informationssicherheit (Fachstelle) geschaffen. Diese wird direkt der Finanzdirektion als Stabsfachstelle zugeordnet. Organisation und Aufgaben der Fachstelle werden in den Erläuterungen zum ISG beschrieben.

## 2. Ausgangslage

Die kantonalen Organe dürfen nach § 5 Abs. 2 DSG besonders schützenswerte Personendaten sowie Persönlichkeitsprofile nur bearbeiten, wenn ein Gesetz dies ausdrücklich vorsieht. Diese Themen werden daher im ISG und nicht in der vorliegenden Verordnung behandelt.

Der gewählte Weg, wonach weitgehend technologische Themen der Informationssicherheit Gegenstand der Vollziehungsverordnung bilden, maximiert die dringend notwendige Flexibilität. Dem Regierungsrat wird eine Delegationskompetenz zur flexiblen Ausgestaltung und laufenden Anpassung der Ausführungsbestimmungen (Verordnung) eingeräumt. Die technologische Entwicklung im Bereich der Informationssicherheit und die sich ständig wandelnden Bedrohungslagen erfordern ein dynamisches und flexibles Regelwerk. Dieses wird mit der vorliegenden Verordnung geschaffen. Detailthemen können zudem in Weisungen des Regierungsrates geregelt werden.

## 3. Ergebnisse der Vernehmlassung

(Text folgt nach Auswertung der externen Vernehmlassung)

## 4. Erläuterungen zu den einzelnen Bestimmungen der ISV

Der Regierungsrat des Kantons Zug, gestützt auf § 25 Abs. 1 des Gesetzes über die Informationssicherheit (ISG) vom ..., im Einvernehmen mit dem Obergericht und dem Verwaltungsgericht, beschliesst:

### 1. Allgemeine Bestimmungen

§ 1 Zweck

[1] Diese Verordnung regelt Grundsätze und Verfahren zur Umsetzung der Informations- und Cybersicherheit beim Einsatz von IT-Mitteln durch Organe gemäss § 4 Abs. 1 Bst. b Informationssicherheitsgesetz.

*Die Umschreibung des Zwecks ergänzt die generelle Zweckbestimmung in § 1 ISG und greift insbesondere die besondere Bedeutung der Abwehrmassnahmen gegenüber Cyberbedrohungen auf.*

§ 2 Begriffe

[1] In dieser Verordnung bedeuten:
a) IT ist der Oberbegriff für Informations- und Kommunikationstechnologie;
b) IT-Mittel sind Mittel der Informations- und Kommunikationstechnik, namentlich Anwendungen, Informationssysteme und Datensammlungen sowie Einrichtungen, Produkte und Dienste, die zur elektronischen Verarbeitung von Informationen dienen;
c) Klassifizierung ist eine risikobasierte Einstufung von Informationen nach deren Schutzbedarf in definierte Schutzstufen;
d) Das Sicherheitsverfahren ist ein Prozess zur Beurteilung des Schutzbedarfs von Informationen, zur Festlegung, Umsetzung und Überprüfung angemessener Sicherheitsmassnahmen sowie zur Behandlung verbleibender Risiken beim Einsatz von IT-Mitteln.

*§ 2 definiert die zentralen Begriffe der Verordnung und stellt damit ein einheitliches Verständnis und eine einheitliche Anwendung sicher. Der Begriff der IT-Mittel ist bewusst weit und technologieneutral gefasst und entspricht wörtlich der Definition der Informatikmittel in Art. 5 Bst. a des Informationssicherheitsgesetzes des Bundes (SR 128), womit die Anschlussfähigkeit an das Bundesrecht gewährleistet ist.*

### 2. Massnahmen

2.1 Grundsätze

§ 3 Informationssicherheit

[1] Die Organe sorgen dafür, dass

a) dass der Schutzbedarf der Informationen in ihrem Verantwortungsbereich beurteilt wird;
b) diese 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); und
c) dass die IT-Mittel, welche die Organe zur Erfüllung ihrer gesetzlichen Aufgaben einsetzen, vor Missbrauch und Störung geschützt werden.

*Die Gewährleistung der Informationssicherheit gehört als Thema zum Risikomanagement eines jeden Organs. Sie umfasst die Gesamtheit aller Anforderungen und Massnahmen, mit denen die Vertraulichkeit, die Verfügbarkeit, die Integrität und die Nachvollziehbarkeit von Informationen sowie der Schutz von Informatikmittel vor Missbrauch und Störung, als Schutzziele bezeichnet, gewährleistet werden kann.*

*Die Schutzziele der ISV beziehen sich auf Informationen sämtlicher Art und ohne Rücksicht auf die Art des Informationsträgers. Die Informationssicherheit darf demnach nicht auf die IT-Sicherheit (Schutz elektronisch gespeicherter Informationen und deren Verarbeitung) reduziert werden. Vielmehr umfasst die Informationssicherheit alle Bearbeitungsvorgänge, also auch Papierdokumente und somit nicht nur die elektronische Bearbeitung.*
*Die Schutzziele der ISV sind vergleichbar mit den Schutzzielen der Sicherheitsmassnahmen gemäss der VIP (insbesondere § 4 VIP).*

*In sachlicher Hinsicht werden meistens vier jeweils nach den Umständen zu gewichtende Schutzkriterien der Informationssicherheit erwähnt, nämlich die Wahrung der Vertraulichkeit, der Integrität, der Verfügbarkeit und der Nachvollziehbarkeit der Informationen.*
*Vertraulichkeit: Dieser Grundsatz wird dahingehend konkretisiert, dass Informationen nur Berechtigten zugänglich sein sollen. Der Kreis der Berechtigten ergibt sich aus dem Kontext der jeweiligen gesetzlichen Aufgabenerfüllung sowie dem Inhalt und der Bedeutung der Information.*
*Verfügbarkeit: Für die Entscheidungs- und Handlungsfähigkeit der Organe ist erforderlich, dass sie im Rahmen der gesetzlichen Aufgabenerfüllung die notwendigen Informationen rechtzeitig und vollständig abrufen können.*
*Integrität: Die Wahrung der Unversehrtheit und Richtigkeit der Informationen ist unter anderem für Informationen von Bedeutung, die zur Veröffentlichung oder Wiederverwendung bestimmt sind.*
*Nachvollziehbarkeit: Die nachvollziehbare Bearbeitung der Informationen ist insbesondere für alle öffentlichen Verfahren (Strafverfahren, Beschwerdeverfahren usw.) von Bedeutung, aber auch für die Erfüllung von Kontroll- und Aufsichtsaufgaben und das Vorgehen bei Missbräuchen. Die Organe müssen somit eine Beurteilung des Schutzbedarfs von Informationen vornehmen und bestimmen, in welcher Hinsicht und wie stark die Informationen geschützt werden müssen.*

*Obwohl sich die Anforderung nach einem angemessenen Schutz der Informatikmittel vor Missbrauch und Störung grundsätzlich bereits aus dem Bst. b) ergibt, wird sie noch ausdrücklich erwähnt (Bst. c), weil die Unterstützung der Geschäftsprozesse durch die Technik immer mehr an*

*Bedeutung gewonnen hat. Ihr gutes Funktionieren stellt heute eine unentbehrliche Voraussetzung für die effiziente Aufgabenerfüllung der Organe dar.*

## § 4 Risikomanagement

[1] Die Organe sorgen in ihrem Zuständigkeitsbereich dafür, dass die Risiken für die Informationssicherheit laufend beurteilt werden.

[2] Sie treffen die erforderlichen Massnahmen, um die Risiken zu vermeiden oder auf ein tragbares Mass zu reduzieren.

[3] Risiken, die getragen werden sollen, müssen vom Organ nachweislich akzeptiert werden.

*Unter dem Begriff «Risiko» werden gestützt auf die anerkannten Standards (bspw. ISO 27001) generell die Auswirkungen von Unsicherheiten auf Ziele verstanden. Ein Risiko kann durch die Kombination aus einem Ereignis, dessen Eintretenswahrscheinlichkeit und möglichen Konsequenzen für die Schutzziele wie Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit von Informationen entstehen. Risiken müssen identifiziert, analysiert und bewertet werden, um das Risikoniveau festzustellen, das aus dem Produkt der Eintretenswahrscheinlichkeit und den Auswirkungen ermittelt wird.*

*Das Risikomanagement im Bereich der Informationssicherheit umfasst die systematischen Prozesse, um potenzielle Gefahren wie Schwachstellen oder externe Bedrohungen in IT-Systemen und Infrastrukturen zu erkennen, zu analysieren und zu bewerten. Die erkannten Risiken, welche die Informationen und die IT-Mittel im Bereich der Informationssicherheit gefährden können, müssen mit geeigneten Massnahmen behandelt werden, damit die Einhaltung der Schutzziele der Informationssicherheit gewährleistet ist. Im Rahmen des Risikomanagements ist zudem eine Abwägung vorzunehmen, ob ein Risiko als tragbar erscheint oder ob ein Risiko mit geeigneten Massnahmen auf ein technisch und finanziell tragbares Mass zu reduzieren ist. Die vorliegende Bestimmung ist bewusst offen formuliert, um situationsbezogen und mit Blick auf die Gefährdung der Schutzziele die notwendigen Massnahmen zu treffen. Die Risikoanalyse und -bewertung erfolgen nach anerkannten Standards im IT-Security-Management-Bereich (bspw. ISO Normen).*

*Ein wirksames Risikomanagement ist eine unverzichtbare Voraussetzung für eine zweckmässige und wirtschaftliche Informationssicherheit. Die Beurteilung der Risiken setzt Kenntnisse der gesetzlichen Aufgaben und der entsprechenden Geschäftsprozesse, die regelmässige Beurteilung der Bedrohungen, die Analyse der Schwachstellen sowie die Einschätzung der Eintrittswahrscheinlichkeit und des potenziellen Schadensausmasses bestimmter Gefahren voraus. Das mit dieser Bestimmung verlangte Risikomanagement wird fachspezifisch von der Fachstelle für Informationssicherheit gesteuert und wird in das übergeordnete Risikomanagement eines jeden Organs integriert.*

*Allerdings können Risiken auch in Kauf genommen oder getragen werden. Risiken, die nach der Umsetzung der vorgesehenen Sicherheitsmassnahmen bestehen bleiben (sogenannte*

*Restrisiken), oder Risiken, die nicht vermindert werden sollen, sind klar auszuweisen. Die Entscheidungsträger sind für ihre diesbezügliche Güterabwägung in dokumentierter Form auf diese Risiken und die potenziellen Auswirkungen hinzuweisen. Die verbleibenden Risiken müssen nachweisbar akzeptiert und entsprechend getragen werden.*

*Eine detaillierte Regelung, was unter IT-Risikomanagement zu verstehen ist, wird in § 19 der Informatikverordnung vom 13. November 2018 (ITV, BGS 153.53) festgehalten. Diese Bestimmung ist bei der Anwendung von § 4 ISV heranzuziehen.*

*Abs. 2 schafft eine Grundlage, um die Massnahmen zu treffen, die zur Vermeidung von Risiken oder deren Reduzierung auf ein tragbares und vertretbares Mass erforderlich sind. Dazu gehören technische und organisatorische Massnahmen (als Business Continuity Management, BCM) bezeichnet. Mit diesen Massnahmen ist sicherzustellen, dass kritische Geschäftsprozesse oder IT-Systeme auch bei Störungen oder Krisensituationen weiter im Betrieb stehen oder die Betriebsausfälle so rasch als möglich behoben werden.*

*Der § 20 ITV ist als Grundlage für ein BCM anzuwenden, das jedoch gestützt auf die Tatbestandsvoraussetzungen Lücken enthält. Demnach ist beispielsweise das AIO auf die Sicherstellung des BCM beschränkt, dies betrifft die IT-Infrastruktur, die Basis-, Standard- und eigenen Fachanwendungen sowie die Datenlogistik. Hingegen sind Prozessverantwortliche (§ 33 Abs. 1 Bst. d ITV) und Anwendungsverantwortliche (§ 34 Abs. 1 Bst. f ITV) für das BCM Planning zuständig. Mit der vorliegenden Bestimmung wird eine Grundlage für ein umfassendes und vollständiges BCM geschaffen.*

*Bei der Umsetzung des Risikomanagements durch die Organe ist sicherzustellen, dass die Umsetzung in die bestehenden Instrumente wie IKS und Risikoinventar integriert wird. Es gilt den administrativen Aufwand zu begrenzen und Doppelspurigkeiten bei der Berichterstattung zu vermeiden.*

## § 5 Zusammenarbeit mit Dritten

[1] Beauftragen die Organe Dritte, so sorgen sie dafür, dass:
a) die Anforderungen und Massnahmen nach dieser Verordnung den Dritten vertraglich überbunden werden;
b) die Umsetzung angemessen überprüft wird und
c) die Nichteinhaltung sanktioniert wird.

*Die Verwaltung ist im Rahmen ihrer Aufgabenerfüllung häufig auf Leistungen Dritter angewiesen. Als Dritte gelten nach dieser Bestimmung Organisationen und Personen des öffentlichen oder privaten Rechts, die nicht zu den Organen gemäss ISG und deren Verwaltungsorganisationen zu zählen sind und deshalb selbstständig handeln.*

*Die auftragserteilenden Stellen haben in beiden Fällen dafür zu sorgen, dass bei der Auftragserteilung und -ausführung die gesetzlich vorgesehenen Massnahmen eingehalten werden. Die einzelnen Sicherheitsmassnahmen werden in der Regel vertraglich festgehalten. Verletzungen können unabhängig vom Verschulden einer Vertragspartei mit Konventionalstrafen*

*sanktioniert werden. Zusätzlich können in der Regel Schadenersatzforderungen geltend gemacht werden, wenn die Vertragsverletzungen schuldhaft verursacht werden.*
*Entscheidend ist aber auch, dass die auftragserteilenden Stellen die Umsetzung der Massnahmen angemessen (d.h. risikoorientiert) überprüfen. Diese Bestimmung ermöglicht den Organen, im Rahmen eines Besuchs vor Ort oder mittels schriftlicher Bestätigung durch die Drittpartei zu überprüfen, ob die angeordneten Massnahmen vertragskonform umgesetzt werden.*
*Schliesst der Auftrag die Ausübung einer sicherheitsempfindlichen Tätigkeit ein, so müssen die Organe die erforderlichen Personensicherheitsprüfungen beantragen, die gemäss den Bestimmungen des ISG durchzuführen sind.*

## § 6 Vorgehen bei Verletzung der Informationssicherheit

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

[2] Sie melden Verletzungen der Informationssicherheit unverzüglich der Fachstelle für Informationssicherheit. Diese entscheidet über das weitere Vorgehen und über eine nach Art. 74a ff. des Bundesgesetzes über die Informationssicherheit erforderliche Meldung an das Bundesamt für Cybersicherheit (BACS) oder an die zuständige Stelle des Bundes.

[3] Die Fachstelle für Informationssicherheit meldet Verletzungen der Informationssicherheit der Zuger Polizei mit einer Einschätzung des Vorfalls und Empfehlungen für geeignete Massnahmen.

[4] Die Organe melden einen datenschutzrelevanten Vorfall direkt der kantonalen Datenschutzstelle und informieren zugleich die Fachstelle für Informationssicherheit.

*Verletzungen im Bereich der Informationssicherheit lassen sich nicht absolut vermeiden. Es ist deshalb nötig, einen einheitlichen und effektiven Ansatz für den Umgang mit solchen Vorfällen festzulegen. Die Organe müssen die erforderlichen Massnahmen treffen, um Informationssicherheitsvorfälle frühzeitig zu identifizieren und ein Verfahren festlegen, nach welchem vorgegangen werden soll, wenn Vorfälle oder Schwachstellen festgestellt werden. Die Fachstelle für Informationssicherheit legt das Vorgehen und die Abläufe fest. Sie informiert die Zuger Polizei, beschreibt den Vorfall und zeigt die möglichen Auswirkungen auf die Informationssicherheit auf.*
*Falls strafrechtlichen Massnahmen notwendig sind, werden diese gemeinsam zwischen der Fachstelle für Informationssicherheit und der Zuger Polizei festgelegt und ihre Umsetzung wird koordiniert.*

*Die Fachstelle für Informationssicherheit stellt fest, welche notwendigen Vorkehrungen zu treffen sind, und bestimmt das Vorgehen gemäss der Bundesgesetzgebung mit Blick auf die Meldung an das Bundesamt für Cybersicherheit, die kantonale Datenschutzstelle oder an die zuständige Stelle des Bundes (Eidgenössische bzw. Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragte bzw. Öffentlichkeitsbeauftragter; EDÖB).*

*Die Bestimmung nach Abs. 3 stellt eine Präzisierung der von der Fachstelle für Informationssicherheit zu erfüllenden Meldepflichten dar. Damit die Zuger Polizei ihre Ermittlungstätigkeiten unter anderem gestützt auf die Bestimmungen der Polizeigesetz- und Strafprozessgesetzgebung erfüllen kann, ist die unverzügliche Bekanntgabe von Sicherheitsvorfällen durch die Fachstelle für Informationssicherheit zwingend notwendig. Die Fachstelle wird ihre allenfalls bereits getroffenen Sofortmassnahmen nach einem Sicherheitsvorfall der Zuger Polizei mitteilen und im Weiteren die erforderlichen Massnahmen im Rahmen der polizeilichen Ermittlungen mit der Zuger Polizei festlegen bzw. ihre Anordnungen umsetzen, soweit diese vom Aufgaben- und Zuständigkeitsbereich der Fachstelle erfasst werden.*

*Die Bestimmung nach Abs. 4 entspricht § 7c DSG, wobei neben der kantonalen Datenschutzstelle die Organe zugleich die Fachstelle für Informationssicherheit informieren, damit notwendige Massnahmen sofort veranlasst und mit den betroffenen Organen abgestimmt werden können.*

## 2.2 Durchführung von Personensicherheitsprüfungen

### § 7 Antragstellung

[1] Das Organ hat den Antrag zur Durchführung einer Peronensicherheitsprüfung zu begründen und die notwendigen Informationen über die zu prüfende Person der Fachstelle für Informationssicherheit zu unterbreiten.

*Diese Bestimmung präzisiert den Grundsatz nach § 17 ISG, dass ein Organ die Durchführung einer PSP beantragen muss und dass dieser Antrag zu begründen ist. Unnötige, unverhältnismässige oder sachfremde PSP können vermieden werden, wenn der Antrag zur Durchführung einer PSP begründet werden muss. In der Begründung sind die Notwendigkeit der Durchführung einer PSP mit Blick auf Aufgaben und Funktion sowie die bekannten und bereits vorliegenden Informationen über die zu prüfende Person anzuführen. Es gilt sicherzustellen, dass im Rahmen der Datenerhebung die für die Durchführung der PSP ausschliesslich die absolut notwendigen Daten ausgewertet und beschafft werden und dass bereits vorhandene Daten über die betreffende Person mitgeteilt und zur Auswertung zur Verfügung gestellt werden. Den Prinzipien der Verhältnismässigkeit und der sparsamen Bearbeitung der Personendaten gemäss dem DSG wird somit entsprochen.*

### § 8 Eröffnung des Verfahrens

[1] Die Fachstelle für Informationssicherheit eröffnet als einleitende Stelle das Verfahren und überprüft, ob die nachstehenden Voraussetzungen erfüllt sind:
a) die betreffende Funktion setzt die Durchführung einer Personensicherheitsprüfung voraus
b) der Antrag zur Durchführung einer Personensicherheitsprüfung wird vom zuständigen Organ gestellt;
c) die zu prüfende Person hat der Durchführung der Personensicherheitsprüfung zugestimmt und die Einwilligung nicht zurückgezogen;

d) die beantragte Datenerhebung, namentlich aus Registern, Daten- und Informationssystemen sowie weiteren öffentlich zugänglichen Quellen gemäss § 18 Abs. 1 Bst. f ISG ist notwendig und verhältnismässig im Hinblick auf den Prüfzweck der Personensicherheitsprüfung und
e) die Angaben der zu prüfenden Person, die für Datenerhebung und die Durchführung des Prüfungsverfahrens notwendig sind, liegen vollständig vor.

[2] Die Fachstelle für Informationssicherheit weist einen unvollständigen Antrag an das betreffende Organ zurück.

*Die Fachstelle für Informationssicherheit prüft als einleitende Stelle einer PSP, ob die angeführten Voraussetzungen erfüllt sind und eröffnet das Verfahren. Sie kann das antragstellende Organ anweisen, zusätzlichen Daten zu beheben, und den Antrag zur Überarbeitung und Ergänzung an das antragstellende Organ zurückweisen. Dieses kann erneut einen Antrag in derselben Angelegenheit unterbreiten.*

*Der Fachstelle steht auch die Möglichkeit offen, fehlende Daten bei den Organen selber zu beschaffen, zusätzliche Informationen oder Registerauszüge einzuholen. Sie ist ebenfalls dafür zuständig, Befragungen von Drittpersonen vorzunehmen oder das antragstellende Organe mit Befragungen zu beauftragen. Die Fachstelle ist aber nicht dazu verpflichtet, die zusätzlichen Abklärungen vorzunehmen, damit ein vollständiger Antrag zur Durchführung einer PSP vorliegt und beurteilt werden kann.*

## § 9 Ablauf und Abschluss des Verfahrens

[1] Die Fachstelle für Informationssicherheit koordiniert das Verfahren mit den Organen und Dritten, die bei der Datenerhebung mitwirken, veranlasst die Befragungen und holt die Registerauszüge ein.

[2] Die Fachstelle teilt dem antragstellenden Organ und der zu prüfenden Person das Ergebnis der Beurteilung mit und lädt diese zur Stellungnahme ein, bevor sie eine Erklärung nach § 20 ISG erlässt.

[3] Das antragstellende Organ und die zu prüfende Person können in ihrer Stellungnahme insbesondere die Abwicklung des Prüfverfahrens, die Datenerhebung und die vorgesehene Erklärung rügen.

[4] Die Fachstelle eröffnet dem antragstellenden Organ und der zu prüfenden Person die begründete Erklärung mit Rechtsmittelbelehrung gemäss § 21 ISG.

*Die Fachstelle für Informationssicherheit ist gemäss § 17 ISG für die Durchführung der PSP zuständig. Zu ihrem Aufgabenbereich gehört insbesondere die koordinierte Datenerhebung gemäss § 18 ISG für die Durchführung der PSP. Die Fachstelle kann die Daten selber beheben oder – was die Regel sein dürfte – Organe mit der Durchführung der Datenerhebung und der Beschaffung der notwendigen Informationen gemäss § 17 Abs. 2 ISG beauftragen.*

*Die Absätze 2 bis 4 dieser Bestimmung befassen sich mit dem Ergebnis der Beurteilung und dem Rechtsschutz und stellen verfahrensrechtliche Präzisierungen zu den Bestimmungen gemäss den §§ 20 und 21 ISG dar. Abs. 2 stellt eine unmittelbare Umsetzung der verfassungsrechtlich verankerten Rechtsweggarantie dar und gewährleistet das rechtliche Gehör. Dem antragstellenden Organ und der zu prüfenden Person stehen die Möglichkeit offen, innert einer von der Fachstelle angesetzten angemessenen Frist insbesondere Verfahrensmängel, die Datenerhebung und das Ergebnis der Beurteilung zu rügen. Die geltend gemachten Rügen sind zu plausibilisieren und nach Möglichkeit zu beweisen. Die Fachstelle begründet eine Beurteilung mit einer Sicherheitserklärung mit Vorbehalt und ein Sicherheitsrisiko.*

*Nach der Anhörung des antragsstellenden Organs und der zu prüfenden Person eröffnet die Fachstelle das Ergebnis der Beurteilung mit einer Erklärung gemäss § 20 Abs. 1 Bst. a, b oder c ISG. Die Fachstelle begründet ihren Entscheid und erteilt Auskunft über die Datenerhebung, wobei die Einschränkung des Auskunftsrechts gemäss § 21 Abs. 2 ISG vorbehalten bleibt.*

*In der Rechtsmittelbelehrung gemäss § 21 Abs. 3 ISG sind namentlich die Beschwerde als zulässiges Rechtsmittel, die Rechtsmittelfrist von 20 Tage und der Regierungsrat als Beschwerdeinstanz anzuführen. Die formellen Voraussetzungen an die Beschwerdelegitimation und die Beschwerdeschrift sind im § 44 des Gesetzes über den Rechtsschutz in Verwaltungssachen vom 01. April 1976 (Verwaltungsrechtspflegegesetz; VRG; BGS 162.1) festgehalten.*

2.2 Sicherheit beim Einsatz von IT-Mitteln

§ 10 Sicherheitsverfahren

[1] Der Regierungsrat erlässt im Einvernehmen mit dem Obergericht und dem Verwaltungsgericht eine Weisung betreffend das Verfahren zur Gewährleistung der Informationssicherheit beim Einsatz von IT-Mitteln (Sicherheitsverfahren).

[2] Das Sicherheitsverfahren umfasst insbesondere:
a) die Beurteilung des Schutzbedarfs der Informationen vor dem Einsatz von IT-Mitteln;
b) die Bestimmung der sich aus dem Schutzbedarf ergebenden Sicherheitsstufe und der angemessenen Sicherheitsmassnahmen;
c) die Umsetzung der Sicherheitsmassnahmen und deren Überprüfung;
d) die Zuständigkeit für die Sicherheitsfreigabe von IT-Mitteln und für die Akzeptanz verbleibender Risiken und
e) das Vorgehen bei Veränderung der Risiken.

[3] Die Organe sind für die Durchführung des Sicherheitsverfahrens zuständig.

*In einer Weisung des Regierungsrates ist das Verfahren zur Gewährleistung der Informationssicherheit beim Einsatz von IT-Mitteln zu regeln. Das Sicherheitsverfahren muss insbesondere die sicherheitsmässigen Aufgaben, Kompetenzen und Verantwortungen der Organe festlegen, die den Einsatz von Informatikmitteln planen und beschliessen. Die Aufgaben der Fachstelle für Informationssicherheit sind für das Sicherheitsverfahren ebenfalls festzuhalten. Die geltenden*

*Bestimmungen der ITV im Zusammenhang mit dem Erlass von Weisungen im Bereich Informationssicherheit, beispielsweise gemäss § 29 Abs. 2 Bst. a ITV, sind an die entsprechende Weisung des Regierungsrates im Zusammenhang mit dem Sicherheitsverfahren gegebenenfalls anzupassen.*

*Eckpunkte des Verfahrens, die in einer Weisung zu regeln sind, bilden namentlich folgende Themenbereiche:*
*Buchstabe a: Der erste Schritt in Bezug auf die Umsetzung der Informationssicherheit besteht darin, bei der Bestimmung des Einsatzzwecks des Informatikmittels die Geschäftsprozesse zu bestimmen, die mit dem einzusetzenden Informatikmittel unterstützt werden, sowie die Informationen zu identifizieren, die damit bearbeitet werden. Zu diesem Zeitpunkt muss das Organ den Schutzbedarf der Informationen erheben sowie im Rahmen einer Risikobewertung die potenziellen Auswirkungen einer Störung oder eines Missbrauchs des einzusetzenden Informatikmittels auf die Interessen nach § 1 Abs. 2 ISG beurteilen.*

*Buchstabe b: Der Schutzbedarf misst sich an den Auswirkungen eines Risikos, das die Schutzziele (Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit) der Informationen und Informatikmittel verletzen kann. Der Schutzbedarf bezeichnet den notwendigen Schutzgrad, um die Gewährleistung der Schutzziele sicherzustellen. Der Schutzbedarf wird im Rahmen einer Schutzbedarfsanalyse festgestellt. Diese bewertet die Auswirkungen eines Schadens, wenn die Schutzziele von Informationen oder die IT-Systeme verletzt werden. Aus der Schutzbedarfsanalyse ergeben sich die Anforderungen an den Schutz der Informationen sowie die Sicherheitseinstufung des Informatikmittels (§ 11). Die Anforderungen müssen wiederum in vollziehbaren Massnahmen festgehalten werden, damit diese gemäss Buchstabe c umgesetzt werden können. Diese Massnahmen müssen mit den Anforderungen aus der Schutzbedarfsanalyse im Einklang stehen.*

*Buchstabe c In einer Weisung ist festzuhalten, welche Massnahmen umgesetzt werden müssen und wie die Umsetzung dieser Massnahmen zu prüfen ist. Grundsätzlich sollen standardisierte Massnahmen zur Anwendung kommen. Die Überprüfung der Umsetzung der Massnahmen erfolgt durch die Fachstelle für Informationssicherheit.*

*Buchstabe d: Mit der Sicherheitsfreigabe soll sichergestellt werden, dass das Organ vor dem Einsatz eines Informatikmittels die identifizierten Restrisiken kennt und auch bereit ist, diese zu tragen. Ist das Organ der Meinung, die Restrisiken seien noch zu hoch, kann es die Freigabe verweigern und die Umsetzung ergänzender risikomindernder Massnahmen verlangen.*

*Buchstabe e: Die Organe müssen zudem ein Vorgehen festlegen, um eine Veränderung der Risiken bei bereits eingesetzten Informatikmitteln zu berücksichtigen. Die Fachstelle für Informationssicherheit berät die Organe und unterstützt diese bei der Festlegung von Massnahmen aufgrund von Veränderungen, die bei der Bewertung der Risiken eintreten.*

## § 11 Sicherheitsstufen

[1] Die Sicherheitsstufe «Grundschutz» gilt für sämtliche IT-Mittel, sofern diese nicht höher eingestuft werden müssen.

[2] Die Sicherheitsstufe «hoher Schutz» gilt für IT-Mittel, wenn:
a) eine Verletzung der Vertraulichkeit, Verfügbarkeit, Integrität oder Nachvollziehbarkeit der Informationen, die damit bearbeitet werden, die Interessen nach § 1 Abs. 2 ISG erheblich beeinträchtigen kann, oder
b) ein Missbrauch oder eine Störung des IT-Mittels die Interessen nach § 1 Abs. 2 ISG erheblich beeinträchtigen kann.

*Die Sicherheitseinstufung wird von der Schwere des Schadens abgeleitet, der verursacht werden kann, wenn die Informationen, die mit dem betroffenen Informatikmittel bearbeitet, oder das Informatikmittel selber missbraucht oder gestört werden. Massgebend für die Einstufung sind entsprechend sowohl der Schutzbedarf von Informationen in Bezug auf die Schutzziele als auch die Risiken einer zeitnahen und sachgemässen Erfüllung der Geschäftsprozesse, die mit dem Informatikmittel unterstützt werden. Die Zuweisung zu einer Sicherheitsstufe gibt auch vor, welche Sicherheitsanforderungen gelten und wie die Schutzmassnahmen definiert werden müssen.*

*Auszugehen ist vom Grundsatz, dass nicht alle Sicherheitsstufen für Informatikmittel als sicherheitsrelevant im Sinne dieser Verordnung gelten. Der Schutz der Informatikmittel soll vielmehr dort effizient ansetzen, wo das Schadenspotenzial als mögliche Folge einer Verletzung der Informationssicherheit hoch ist. Sicherheitsstufe «Grundschutz» gilt für alle Informatikmittel, die keine besonderen Schutzanforderungen aufweisen. Die grosse Mehrheit der Systeme der Organe soll dieser Sicherheitsstufe zugeordnet werden.*

§ 12 Sicherheit beim Betrieb

[1] Die Organe gewährleisten in ihrem Verantwortungsbereich die Sicherheit der IT-Mittel, die sie für sich selbst oder im Auftrag eines anderen Organs betreiben.

*Die Hauptverantwortung für die Sicherheit beim Einsatz von Informatikmitteln liegt bei den Organen. Sie sind dafür zuständig, beim Betrieb der Informatikmittel die Sicherheit nach dem Stand der Wissenschaft und Technik zu gewährleisten.*

*Die Fachstelle für Informationssicherheit kann die erforderlichen Massnahmen vornehmen, wenn die Organe Angriffe und Störungen feststellen, die den Betrieb beeinträchtigen. Gestützt auf die gesetzliche Bestimmung betreffend die Bearbeitung von Personendaten nach § 5 ISG kann die Fachstelle für Informationssicherheit die Aktivitäten von Personen überprüfen und allenfalls eine personenbezogene Auswertung der Daten vornehmen.*

2.3 Personelle Massnahmen

§ 13 Voraussetzungen für den Zugang zu Informationen sowie zu den IT-Mitteln

[1] Die Organe sorgen dafür, dass Personen, die Zugang zu behördlichen Informationen, IT-Mittel, Räumlichkeiten und anderen Infrastrukturen haben:

a) sorgfältig ausgewählt, risikogerecht identifiziert, funktionsgerecht aus- und weitergebildet sowie gegebenenfalls zur Geheimhaltung und besonderer Sorgfalt verpflichtet werden und
b) nur berechtigt werden, soweit dies zur Erfüllung ihrer gesetzlichen oder vertraglichen Aufgaben nötig ist.

*Mit der Regelung der Voraussetzungen für den Zugang zu Informationen, zu den Informatikmitteln sowie mit dem Entzug der Berechtigungen soll verhindert werden, dass Unbefugte auf Daten lesend oder ändernd zugreifen oder unberechtigt Funktionen in IT-Systemen nutzen. Die sorgfältige Auswahl, die risikogerechte Identifikation, eine optimale, zielgerichtete Instruktion im Sinne einer funktionsgerechten Aus- und Weiterbildung und eine Verpflichtung zur Geheimhaltung und zu besonderer Sorgfalt sind unabdingbare Voraussetzungen für eine Gewährleistung der Informationssicherheit in personeller Hinsicht.*

*Es liegt in der Verantwortung der Anstellungsorgane beziehungsweise der Verwaltungseinheiten bei Vergaben öffentlicher Aufträge oder bei Auslagerung öffentlicher Aufgaben dafür zu sorgen, dass diesen Anforderungen im Rahmen der Aufgabenerfüllung entsprochen wird. Bei einer Aufgabenerfüllung durch Dritte ist dies durch vertragliche Überbindung sicherzustellen. Bei der Auswahl der anzustellenden oder zu beauftragenden Personen müssen die Auswahlkriterien dem Schutzbedarf der Informationen beziehungsweise der Sicherheitsstufe der Informatikmittel entsprechen.*
*Personen, die Zugang zu Informationen, Informatikmitteln oder Infrastrukturen haben, müssen Anforderungen erfüllen, die im Abs. 1 Bst. a festgelegt werden. Massnahmen, welche den besonders schützenswerten Personendaten und dem Profiling zuzuordnen sind, dürfen nicht angewendet werden, weil dazu eine entsprechende formelle gesetzliche Grundlage erforderlich ist und die vorliegende Bestimmung für eine solche Massnahme nicht genügt. Allenfalls ist eine Personensicherheitsprüfung gemäss ISG durchzuführen.*

## § 14 Entzug von Berechtigungen

[1] Die Berechtigungen werden vom Organ entzogen, sobald die Anstellung oder der Vertrag beendet oder die Aufgabe erfüllt ist.

[2] Die Berechtigungen dürfen bei einem Sicherheitsvorfall oder wenn Anhaltspunkte für eine Gefährdung der Sicherheit vorliegen vom Organ oder der Fachstelle für Informationssicherheit ohne Vorankündigung temporär gesperrt oder entzogen werden.

*Wenn eine Anstellung, ein Vertrag oder eine Aufgabe beendet ist, müssen die entsprechenden Berechtigungen entzogen werden. Besteht Grund zur Annahme, dass eine Gefährdung der Informationssicherheit vorliegt, müssen die Berechtigungen sofort gesperrt oder entzogen werden. Beide Massnahmen sollen insbesondere dazu beitragen, das Risiko einer Verletzung der Informationssicherheit zu reduzieren. Die Sperrung bzw. der Entzug der Berechtigung ist eine einschneidende Massnahme. Daher ist gestützt auf den Grundsatz der Verhältnismässigkeit diese Massnahme zeitlich zu begrenzen. Es gilt im Einzelfall zu prüfen, ob eine temporäre Sperrung oder ein zeitlich befristeter Entzug der Berechtigung als verhältnismässige Massnahme in Frage kommt.*

## 2.4 Physischer Schutz

### § 15 Grundsatz

[1] Die Organe sorgen in ihrem Verantwortungsbereich für einen angemessenen physischen Schutz der Informationen und der IT-Mittel.

*Bei den physischen Schutzmassnahmen geht es darum, die Risiken durch physische Bedrohungen zu reduzieren. Zu diesen Risiken gehören unter anderem menschliche Handlungen oder Elementarschäden. Diese Bestimmung legt den Grundsatz fest, dass die Organe den physischen Schutz ihrer Informationen und Informatikmittel in ihrem Verantwortungsbereich gewährleisten müssen. Der unberechtigte Zugang zu den Informationen oder Informatikmitteln ist zu verhindern. Die Organe können für Zugangskontrollen technische Hilfsmittel einsetzen. Wenn der Einsatz von Videokameras vorgesehen ist, dann sind die Bestimmungen über die Videoüberwachung im öffentlichen und im öffentlich zugänglichen Raum vom 26. Juni 2014 (Videoüberwachungsgesetz; VideoG, BGS 159.1) anzuwenden. Eine Videoüberwachung, die nicht vom Gegenstand und Geltungsbereich des VideoG erfasst wird, ist nicht zulässig, weil besonders schützenswerte Personendaten bearbeitet werden.*

### § 16 Sicherheitszonen

[1] Die Organe können Räumlichkeiten und Bereiche als Sicherheitszone bezeichnen, in denen:
a) häufig «vertraulich» oder «geheim» klassifizierte Informationen bearbeitet werden oder
b) IT-Mittel der Sicherheitsstufe «hoher Schutz» betrieben werden.

[2] Die Organe können in Sicherheitszonen:
a) das Mitführen bestimmter Gegenstände, insbesondere von Aufnahmegeräten, verbieten;
b) sicherheitsempfindliche Bereiche mit Aufnahmegeräten überwachen;
c) Taschen- und Personenkontrollen durchführen;
d) unangemeldet Raumkontrollen durchführen, auch in Abwesenheit der Angestellten oder
e) störende Fernmeldeanlagen gemäss Artikel 34 Absatz 1$^{ter}$ des Fernmeldegesetzes betreiben.

*Die Ausscheidung bestimmter Räume beziehungsweise Bereiche als Sicherheitszone stellt eine physische Massnahme der Informationssicherheit dar, die bereits heute beispielsweise bei der Kantonspolizei ergriffen wird. Aber auch dort, wo es um den Schutz von Serverräumen (Rechenzentrum) geht, sind entsprechende Massnahmen unabdingbar. Eine Sicherheitszone muss vordefiniert werden, identifizierbar sein und entsprechend geschützt werden. Die Massnahmen in den Sicherheitszonen der jeweiligen Stufen sind risikogerecht auszugestalten. Über ihre tatsächliche Einrichtung entscheidet das Organ nach einer Risikobeurteilung. Sicherheitszonen sollen nur für Informationen und Informatikmittel der vertraulichen und höchsten Klassifizierungs- beziehungsweise Sicherheitsstufe gelten.*

*Die Organe legen fest, ob für den Zugang zu den Sicherheitszonen ausschliesslich Personen zugelassen werden, die einer Personensicherheitsprüfung (PSP) nach § 13 ff. ISG unterzogen wurden. Eine PSP als Voraussetzung für den Zugang zu einer Sicherheitszone steht im*

*Einklang mit der Bestimmung von § 13 Abs. 1 ISG wonach die PSP zur Beurteilung dient, 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.*

*Wenn eine PSP durchgeführt wurde, können die in Abs. 2 festgehaltenen Massnahmen ergriffen werden. Diese stellen zum Teil eine Bearbeitung von besonders schützenswerten Personendaten dar, wie bspw. die Taschen- oder Personenkontrollen. Diese Kontrollen können unter Anwendung der Verhältnismässigkeit und gestützt auf die gesetzlichen Bestimmungen der PSP durchgeführt werden. Wird auf eine PSP verzichtet oder kann diese nicht abgewickelt werden, bspw. wegen der fehlenden Einwilligung der betroffenen Person, ist der Zugang zur Sicherheitszone nicht zu gewähren. Eine Personen- oder Taschenkontrolle bei einer nicht durchgeführten PSP ist aus datenschutzrechtlichen Gründen nicht zulässig.*

*Absatz 2 regelt die besonderen Befugnisse derjenigen Verwaltungseinheit, die eine Sicherheitszone einrichtet. Die Massnahmen müssen verhältnismässig und geeignet sein, die Schutzziele zu erreichen. Das Mitführen bestimmter Gegenstände in eine Sicherheitszone kann eingeschränkt werden. Namentlich ist das Mitführen von Bild- oder Tonaufnahmegeräten (inkl. Smartphones oder Notebooks mit entsprechenden Funktionen) in der Regel nur mit separater Bewilligung erlaubt.*

*Bereiche der Sicherheitszone, die für die Informationssicherheit besonders wichtig sind (z.B. die Zutrittszone zu einem Serverraum, der Administratorarbeitsplatz oder der Archivraum mit "geheim" klassifizierten Informationen), können mittels Videoaufnahmegeräten überwacht werden. Beim Ein- oder Ausgang können Taschen- oder Personenkontrollen durchgeführt werden. Die Überwachungsmassnahme durch Videoaufnahmegeräte unterliegt nicht dem VideoG, zumal die Sicherheitszonen weder öffentlich noch öffentlich zugänglich sind und somit vom Geltungsbereich des VideoG nicht erfasst werden. Ob in nicht öffentlichen Räumen, die allerdings nicht den Sicherheitszonen zuzuordnen sind, eine Videoüberwachung als adäquate Sicherheitsmassnahme in Frage kommen kann, ist im Einzelfall unter Würdigung der datenschutzrechtlichen Bestimmungen zu beurteilen.*

*Auch Bürokontrollen sollen im Bereich der Sicherheitszonen möglich sein. Dabei geht es um die Überprüfung der Einhaltung der sogenannten Clean Desk Policy. Die Kontrolle darf auch in Abwesenheit der betroffenen Personen, beispielsweise während der Nacht, stattfinden. Die Aufzählung ist nicht abschliessend. So könnte auch der Betrieb einer störenden Fernmeldeanlage nach dem Fernmeldegesetz (FMG) vom 30. April 1997 (SR 784.10) in Betracht kommen, wenn die Sicherheitszone besonders kritisch ist.*

*Im Zusammenhang mit den Sicherheitszonen sind ebenfalls die Vorgaben gemäss dem Konzept Betriebliche Sicherheit Kantonale Verwaltung und Gerichte (Sicherheitskonzept; RRB vom 9. April 2013) zu beachten. Die Stossrichtungen der ISV-Bestimmungen und derjenigen des Sicherheitskonzepts stimmen zum Teil überein, wenn die Sicherheit der Infrastrukturen (Bauten, Räumlichkeiten der kantonalen Verwaltung) betroffen sind. Die Regelung in der ISV umfasst allerdings auch die Sicherheitszonen in einzelnen Räumen und stellt daher eine Erweiterung zu den Vorgaben des Sicherheitskonzepts dar. Ebenfalls ist von differenzierten Schutzzielen*

*auszugehen. Gleichwohl bestehen Schnittstellen zwischen den Aufgaben der beiden Fachstellen für die Informationssicherheit und für Sicherheit der BD.*

*Das Sicherheitskonzept definiert unter Berücksichtigung der Sicherheitsrisiken die Minimalanforderungen an die betriebliche Sicherheit in der kantonalen Verwaltung (inkl. Schulen) und der Gerichte. Zudem werden die sicherheitsrelevanten Funktionen und notwendigen baulich-technischen und organisatorischen Sicherheitsstandards definiert.*

*Das Sicherheitskonzept fokussiert auf die betriebliche Sicherheit innerhalb der kantonseigenen und gemieteten Liegenschaften, in welchen Mitarbeiterinnen und Mitarbeiter von kantonalen Organe arbeiten. Die betriebliche Sicherheit wird an die Leitung der Baudirektion delegiert, welche die operative Umsetzung via der Fachstelle Sicherheit durchsetzt oder nötigenfalls direkt Empfehlungen und Weisungen an die Direktionen erteilt.*
*Die Leitungen der beiden Fachstellen für Informationssicherheit und für Sicherheit werden ihre Aufgaben und Tätigkeiten im Bereich der Umsetzung der Vorgaben gemäss der ISV im Bereich der Sicherheitszonen koordinieren und sich bei der Erfüllung ihrer Aufgaben gegenseitig abstimmen.*

2.6 Fachstelle für Informationssicherheit, Unterstützungsleistungen und periodische Prüfung

§ 17 Fachstelle für Informationssicherheit

[1] Die Fachstelle für Informationssicherheit ist der Finanzdirektion zugeordnet. Die Leitung der Fachstelle für Informationssicherheit wird vom Regierungsrat gewählt.

[2] Die Fachstelle nimmt folgende Aufgaben wahr:
a) sie überprüft die Einhaltung der Vorgaben zur Informationssicherheit;
b) sie ergreift bei Nichteinhaltung der Vorgaben, festgestellten Sicherheitslücken und Sicherheitsvorfällen die erforderlichen Sofortmassnahmen;
c) sie informiert die Vorsteherin bzw. den Vorsteher der Finanzdirektion bzw. das Obergericht und das Verwaltungsgericht über Sicherheitsvorfälle und Sicherheitslücken mit einem hohen Risiko für die Informationssicherheit und teilt die ergriffenen Sofortmassnahmen mit. Der Regierungsrat bzw. das Obergericht und das Verwaltungsgericht entscheidet innerhalb von maximal 72 Stunden über diese Massnahmen für die Verwaltung bzw. für die Gerichte;
d) sie erarbeitet Anträge und Weisungen zur Informationssicherheit zuhanden des Regierungsrats bzw. des Obergerichts und des Verwaltungsgerichts ;
e) sie erstattet dem Regierungsrat bzw. dem Obergericht und dem Verwaltungsgericht jährlich Bericht über die Informationssicherheit im Kanton Zug.

*Organisation und Aufgaben der Fachstelle für Informationssicherheit werden im Bericht zum ISG im Kapitel 4 umschrieben. Insbesondere wird auf die Unabhängigkeit der Fachstelle im Zusammenhang mit der Aufgabenerfüllung hingewiesen. Die Leitung der Fachstelle für Informationssicherheit wird vom Regierungsrat gewählt.*

*Bst. c) Diese Bestimmung öffnet der Fachstelle einen breiten Entscheidungsspielraum in der Frage, welche Sicherheitslücken und Sicherheitsvorfälle zu melden sind. Auszugehen ist von einem risikobasierten Ansatz. Demnach besteht die Pflicht zu rapportieren, wenn die Sicherheitslücke bzw. der Sicherheitsvorfälle ein hohes Risiko für Verletzungen der Informationssicherheit bzw. der Schutzobjekte gemäss § 1 Abs. 1 und 2 ISG bedeuten. Von*

*einem hohen Risiko ist stets auszugehen, wenn Personendaten und namentlich besonders schützenswerte Personendaten gemäss DSG von einem Sicherheitsvorfall betroffen sind. Gegenstand der Berichterstattung bilden zudem Ausführungen zur Schwere des Vorfalls.*

*Die Fachstelle entscheidet über die zu treffenden Sofortmassnahmen und zeigt diese dem Regierungsrat bzw. dem Obergericht oder dem Verwaltungsgericht sofort an. Der Regierungsrat bzw. das Obergericht oder das Verwaltungsgericht, allenfalls deren Präsidien, entscheidet innerhalb von 72 Stunden über die von der Fachstelle getroffenen Massnahmen.*

*Bst. e: Die Fachstelle legt den Inhalt des Berichts fest. Die Berichterstattung behandelt Themen wie: Handlungsbedarf im Bereich der Informationssicherheit, Umsetzung und Wirksamkeit der vom Regierungsrat angeordneten Massnahmen, Schulungs- und Sensibilisierungsmassnahmen der Organe im Bereich der Informationssicherheit und künftige Herausforderungen mit Blick auf die technischen Entwicklungen. Die Fachstelle prüft, ob einzelne Sicherheitsvorfälle darzulegen sind. Eine entsprechende Publikation erfolgt, wenn der Vorfall von allgemeinem Interesse ist. Die Berichterstattung darf jedoch keine schützenswerten Interessen der Öffentlichkeit und privaten Personen verletzen. Die Fachstelle unterbreitet den Bericht zu Beginn eines jeden Kalenderjahres dem Regierungsrat. Dieser nimmt vom Bericht Kenntnis.*

## § 18 Unterstützungsleistungen der Fachstelle für Informationssicherheit

[1] Die Fachstelle für Informationssicherheit unterstützt die Organe bei:

a) der Gewährleistung der Informationssicherheit nach § 3 Abs. 1;
b) der Durchführung des Risikomanagements nach § 4 Abs. 1 und 2;
c) dem Vorgehen im Falle einer Verletzung der Informationssicherheit nach § 6 Abs. 2;
d) der Durchführung des Sicherheitsverfahrens nach § 10 Abs. 3 und
e) der Gewährleistung der Sicherheit im Betrieb nach § 12 Abs. 1.

*Die Fachstelle für Informationssicherheit steht den Organen beratend und unterstützend bei der Erfüllung ihrer Aufgaben zur Seite. Die Fachstelle kann generelle Leitfäden, Arbeitshilfen, Ablaufschemata, Formulare und weitere Vollzugshilfen erarbeiten und diese den Organen zur Verfügung stellen.*

*In Einzelfällen kann die Fachstelle auch konkrete Beratung und Unterstützung leisten. Ein Anspruch darauf besteht jedoch nicht. Die Fachstelle setzt aber im Interesse der Informationssicherheit und im Rahmen ihrer zur Verfügung stehenden Ressourcen und ihres Fachwissens alles daran, die Organe in ihrer Aufgabenerfüllung zu beraten und zu unterstützen.*

*In der der Verordnung über die Informationssicherheit von Personendaten vom 16. Januar 2007 (VIP; BGS 157.12) werden das Verfahren und die Verantwortlichkeiten zur Gewährleistung der Sicherheit von Personendaten, die mit elektronischen Hilfsmitteln oder auf andere Weise bearbeitet werden, geregelt. In diesem Zusammenhang ist auf § 8a der VIP hinzuweisen, welcher das Security Board verpflichtet, Merkblätter für die Instruktion von Mitarbeitenden zur Informationssicherheit sowie eine Vorlage für die Erarbeitung eines Massnahmenkataloges nach § 4 Abs. 3 VIP zu erstellen (siehe auch § 8 Abs. 2 VIP). Zudem ist auf die Weisung zur Überprüfung der Datensicherheit vom 16. Januar 2007 (mit Änderung betr. A11 und B13 gemäss RRB vom 13. April 2010) hinzuweisen. Diese Weisung wird auf den aktuellen Stand gebracht.*

*Das Security Board hat im Jahr 2024 das Dokument «Merkblätter Informationssicherheit» (Ausgabe 2024_2) veröffentlicht. Im Fokus dieser Merkblätter sind nicht nur Personendaten gemäss DSG und VIP, sondern generell «Personendaten und vertrauliche Informationen», welche nach ihrem Schutzbedarf zu «bewirtschaften» sind. Dazu gehören u.a. auch Daten von Firmen oder Geschäftspartnern. Sodann wird auch darauf hingewiesen, dass die zu treffenden Schutzmassnahmen von der Klassifikation der bearbeiteten Daten abhängen. Die Merkblätter wurden vom AIO überarbeitet. Sie werden ergänzt und mit den Bestimmungen des ISG und der ISV abgestimmt.*

§ 19 Periodische Prüfung und Ansprechpartnerin des Bundes

[1] Die Fachstelle für Informationssicherheit überprüft die Umsetzung und Wirksamkeit der Informationssicherheit periodisch und orientiert das Bundesamt für Cybersicherheit (BACS) über die Ergebnisse.

[2] Ansprechpartnerin des Bundes für Fragen zur Informationssicherheit gemäss Art. 86 Abs. 3 des Informationssicherheitsgesetzes des Bundes ist die Fachstelle für Informationssicherheit.

*Gestützt auf Art. 86 Abs. 1 ISG-Bund sorgen die Kantone für die periodische Prüfung der Umsetzung und Wirksamkeit der Informationssicherheit. Nach Artikel 3 ISG-Bund ist der Kanton Zug daher verpflichtet, einen gleichwertigen Schutz zu gewährleisten, wenn klassifizierte Informationen des Bundes bearbeitet oder auf seine Informatikmittel zugegriffen wird. Es muss sichergestellt sein, dass die Massnahmen geeignet sind, das erforderliche Sicherheitsniveau zu erreichen. Der Umfang dieser Prüfung ist auf die Sicherheit bei der Bearbeitung von klassifizierten Informationen und beim Zugriff auf Informatikmittel des Bundes beschränkt. Für diese Kontrolle ist der Kanton Zug selbst zuständig. Die kantonale Fachstelle für Informationssicherheit ist gemäss Art. 86 Abs. 2 ISG-Bund verpflichtet, das Bundesamt für Cybersicherheit über die Ergebnisse der Prüfungen zu orientieren.*

## 5. Finanzielle Auswirkungen

Die personellen und finanziellen Auswirkungen sind bereits im Bericht und Antrag des Regierungsrats vom … zum ISG (Vorlage Nr. ….) detailliert dargestellt worden.

## 6. Inkrafttreten

Der Regierungsrat bestimmt den Termin des Inkrafttretens der Informationssicherheitsverordnung.