Kanton Zug **[Fundst. od. Gesch.-Nr.] (ID 2985)**

[D5] Ergebnis 1. Lesung Regierungsrat vom 7. Juli 2026

Vollziehungsverordnung zum Gesetz über die Informationssicherheit (Informationssicherheitsverordnung, ISV)

Vom [...]

Von diesem Geschäft tangierte Erlasse (BGS-Nummern)

Neu: **???.???**
Geändert: –
Aufgehoben: –

Der Regierungsrat des Kantons Zug,

gestützt auf § 25 Abs. 1 des Gesetzes über die Informationssicherheit (Informationssicherheitsgesetz, ISG) vom ...[1)], im Einvernehmen mit dem Obergericht und dem Verwaltungsgericht,

beschliesst:

I.

Der Erlass BGS ???.???, Vollziehungsverordnung zum Gesetz über die Informationssicherheit (Informationssicherheitsverordnung, ISV), wird als neuer Erlass publiziert.

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[2)].

---

1) BGS XXX.X
2) BGS XXX.X

§ 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. Massnahmen

2.1 Grundsätze

§ 3 Informationssicherheit

[1] Die Organe sorgen dafür, dass:

a) 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) die IT-Mittel, welche die Organe zur Erfüllung ihrer gesetzlichen Aufgaben einsetzen, vor Missbrauch und Störung geschützt werden.

§ 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.

§ 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.

§ 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[3)] 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.

2.2 Durchführung von Personensicherheitsprüfungen

§ 7 Antragstellung

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

[3)] SR 128

§ 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[4)] 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.

§ 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[5)] 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[6)] .

---

4) BGS XXX.X
5) BGS XXX.X
6) BGS XXX.X

2.3 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.

§ 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[7)] erheblich beeinträchtigen kann; oder
b) ein Missbrauch oder eine Störung des IT-Mittels die Interessen nach § 1 Abs. 2 ISG[8)] erheblich beeinträchtigen kann.

§ 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.

---

7) BGS XXX.X
8) BGS XXX.X

2.4 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.

§ 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.

2.5 Physischer Schutz

§ 15 Grundsatz

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

§ 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 Art. 34 Abs. 1ter des Fernmeldegesetzes[9)] betreiben.

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; und
e) sie erstattet dem Regierungsrat bzw. dem Obergericht und dem Verwaltungsgericht jährlich Bericht über die Informationssicherheit im Kanton Zug.

§ 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;

9) SR 784.10

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.

§ 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[10)] ist die Fachstelle für Informationssicherheit.

II.

Keine Fremdänderungen.

III.

Keine Fremdaufhebungen.

IV.

Diese Verordnung tritt am Tage nach der Veröffentlichung im Amtsblatt in Kraft.[11)]

Zug, ...

Regierungsrat des Kantons Zug

Der Landammann
Andreas Hostettler

Der Landschreiber
Tobias Moser

Publiziert im Amtsblatt vom ...

[10)] SR 128
[11)] Inkrafttreten am ...