[M05] Ergebnis 1. Lesung Regierungsrat vom 7. Juli 2026

Gesetz über die Informationssicherheit (Informationssicherheitsgesetz, ISG)

Vom [...]

Von diesem Geschäft tangierte Erlasse (BGS-Nummern)

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

Der Kantonsrat des Kantons Zug,

gestützt auf § 41 Abs. 1 Bst. b und § 47 Abs. 1 Bst. b und c der Verfassung des Kantons Zug (Kantonsverfassung, KV) vom 31. Januar 1894[1)],

beschliesst:

I.

Der Erlass BGS ???.???, Gesetz über die Informationssicherheit (Informationssicherheitsgesetz, ISG), wird als neuer Erlass publiziert.

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;

[1)] BGS 111.1

c) wirtschafts- und finanzpolitischen Interessen des Kantons; und
d) Erfüllung von gesetzlichen und vertraglichen Verpflichtungen der Organe zum Schutz von Informationen.

§ 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.

§ 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.

§ 4 Begriffe

[1] In diesem Gesetz bedeuten:

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 Tätigkeiten sind die 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.

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[2)] 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.

---

2) BGS 157.1

[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.

§ 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[3)].

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.

§ 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;

[3)] BGS 152.4

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.

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.

§ 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.

§ 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.

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 Datenschutzgesetz[4)] 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 nach § 18;
c) Datenerhebung bei Drittpersonen nach § 19;
d) die Beurteilung des Sicherheitsrisikos und Erklärung nach § 20;
e) Daten und Akten aus Beschwerdeverfahren nach § 21;
f) Listen und Statistiken, die Daten nach den Bst. a–e enthalten.

[3] Anhand der Daten des Informationssystems darf ein Profiling nach § 2 Abs. 1 Bst. b1 Datenschutzgesetz[5)] 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.

---

4) BGS 157.1
5) BGS 157.1

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.

§ 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.

§ 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[6)] vorlegt und die Wiederholungsfrist[7)] noch nicht abgelaufen ist.

§ 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.

§ 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.

§ 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;

---

6) Art. 39 Bundesgesetz über die Informationssicherheit; SR 128
7) Art. 43 Bundesgesetz über die Informationssicherheit; SR 128

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 § 2bis Personalgesetz[8)];
g) aus systematischen Sammlungen und Analysen von öffentlich zugänglichen Informationen;
h) durch Befragung der zu prüfenden Person; und
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.

§ 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.

§ 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.

8) BGS 154.21

[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.

§ 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 Datenschutzgesetz[9)].

[3] Die Erklärung kann gestützt auf § 21a Verwaltungsrechtspflegegesetz[10)] innert 20 Tagen beim Regierungsrat mit Beschwerde 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.

§ 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.

---

9) BGS 157.1
10) BGS 162.1

[2] Die Archivierung der Daten richtet sich nach den Vorschriften des Archivgesetzes[11)].

[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.

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[12)].

[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[13)] ist die Fachstelle für Informationssicherheit.

6. Vollziehungsverordnung

§ 25 Vollziehungsverordnung

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

II.

Keine Fremdänderungen.

III.

Keine Fremdaufhebungen.

[11)] BGS 152.4
[12)] SR 128
[13)] SR 128

IV.

Dieses Gesetz tritt nach unbenutztem Ablauf der Referendumsfrist (§ 34 Abs. 2 der Kantonsverfassung[14]) oder nach der Annahme durch das Stimmvolk nach der Veröffentlichung im Amtsblatt an dem vom Regierungsrat bestimmten Zeitpunkt in Kraft.[15]

Zug, ...

Kantonsrat des Kantons Zug

Der Präsident
Stefan Moos

Der Landschreiber
Tobias Moser

Publiziert im Amtsblatt vom ....

[14] BGS 111.1
[15] Inkrafttreten am ...