



Regierungsrat, Postfach, 6301 Zug

**Nur per E-Mail**

Eidgenössisches Departement für Verteidigung,  
Bevölkerungsschutz und Sport VBS  
Frau Bundesrätin Viola Amherd  
Bundeshaus Ost  
3003 Bern

Zug, 15. November 2022 sa

**Ausführungsrecht zum Informationssicherheitsgesetz (ISG)  
Stellungnahme des Kantons Zug**

Sehr geehrte Frau Bundesrätin Amherd  
Sehr geehrte Damen und Herren

Mit Schreiben vom 24. August 2022 hat uns das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport eingeladen, zum Ausführungsrecht betreffend das Informationssicherheitsgesetz (ISG) bis 24. November 2022 Stellung zu nehmen. Zum Ausführungsrecht äussern wir uns wie folgt:

**1. Allgemeines**

Das Ausführungsrecht zum ISG umfasst insgesamt drei neue Verordnungen:

- Informationssicherheitsverordnung (ISV),
- Verordnung über Personensicherheitsprüfungen (VPSP),
- Verordnung über das Betriebssicherheitsverfahren (VBSV)

und eine Änderung einer bestehenden Verordnung:

- Verordnung über Identitätsverwaltungs-Systeme (IAMV).

Ziel dieser Ausführungserlasse ist es, für alle Behörden und Organisationen des Bundes ein möglichst einheitliches Sicherheitsniveau zu erreichen, wobei die Kantone für eine gleichwertige Informationssicherheit sorgen müssen, wenn sie klassifizierte Informationen des Bundes bearbeiten oder auf seine Informatikmittel zugreifen. Das Inkrafttreten des ISG und seiner Verordnungen ist auf Mitte 2023 geplant. Für einen erfolgreichen Übergang ins neue Recht sehen sowohl das ISG (vgl. Art. 90) als auch die zugehörigen Ausführungsverordnungen (Art. 48 ISV, Art. 38 VPSP und Art. 25 VBSV) Übergangsfristen vor.

Der Regierungsrat des Kantons Zug unterstützt das vorerwähnte Ausführungsrecht, wobei nur im Bereich der ISV, die VPSP und die IAMV Umsetzungsbedarf für den Kanton Zug besteht, weil die VBSV die Wahrung der Informationssicherheit bei der Vergabe von Aufträgen der Bundesbehörden an Dritte (Betriebe) regelt und daher nur für Bundesbehörden gilt.

## **2. Fragen**

Zu den vier im Rahmen der Vernehmlassung gestellten Fragen äussern wir uns wie folgt:

### **2.1. Ist die Umsetzung der Verordnungen für die Kantone verständlich?**

Die Vorgaben sind zwar verständlich, gehen aber zu wenig ausführlich auf die Pflichten der Kantone ein. Zudem macht der verfolgte föderalistische Ansatz, wonach die Vorgaben des Bundes nur dann gelten, wenn die kantonalen Regelungen den Sicherheitsanforderungen des Bundes nicht genügen, das Ganze kompliziert.

### **2.2. Wie gedenken die Kantone die Verordnung umzusetzen?**

Die Hauptverantwortung für die Sicherheit bei der Bearbeitung von klassifizierten Informationen des Bundes liegt bei den kantonalen Organen, die diese Daten bearbeiten bzw. die auf die Informatikmittel des Bundes zugreifen (namentlich Amt für Zivilschutz und Militär, Notorganisation, Zuger Polizei, Verein für Arbeitsmarktmassnahmen). Diese Organe haben die erforderlichen Prozesse, Zuständigkeiten und Massnahmen festzulegen, um das vom Bund verlangte Sicherheitsniveau sicherstellen zu können. Dabei kommen die Vorschriften des Bundes nur dann zur Anwendung, wenn die Vorschriften und Massnahmen der Kantone den Sicherheitsanforderungen des Bundes nicht genügen.

Die Mitarbeitenden der Organe sind für die Einhaltung der Vorgaben beim Umgang mit den klassifizierten Informationen und den Informatikmitteln verantwortlich. Der richtige Umgang mit den klassifizierten Informationen und den Informatikmitteln setzt voraus, dass die Bundesbehörden den Organen entsprechende Vorgaben machen.

Auf Basis dieser Vorgaben wird der Chief Information Security Officer (CISO) des Amtes für Informatik und Organisation des Kantons Zug (AIO) eine auf die entsprechenden Organe angepasste Schulung erarbeiten und durchführen. Das AIO ist zudem dafür verantwortlich, die nötigen Informatikmittel anzubieten und deren Sicherheit im Betrieb zu gewährleisten.

Die Organe sind verpflichtet, die Wirksamkeit der getroffenen Schutzmassnahmen periodisch zentral durch das AIO überprüfen zu lassen. Der CISO des AIO stellt sicher, dass die Fachstellen des Bundes für Informationssicherheit periodisch über die Ergebnisse der Überprüfungen orientiert wird.

#### **2.2.1. ISV**

Aktuell verfügt nur das AIO für Dienste, die es selber zur Verfügung stellt, über ein ISMS (Informationssicherheitsmanagementsystem) nach ISO27001. Die Bereitstellung des vom Bund geforderten ISMS Light führt zu beachtlichen Aufwendungen für Organe, die klassifizierte Informationen des Bundes auf ihren eigenen IT-Anwendungen bearbeiten oder auf Informatikmitteln

des Bundes zugreifen. Dies ist beispielsweise der Fall bei der Zuger Polizei, die noch nicht wie das AIO über ein ISMS verfügt.

### **2.2.2. VPSP**

Der Kanton verfügt mit den §§ 2<sup>bis</sup> und 2<sup>quater</sup> des Gesetzes über das Arbeitsverhältnis des Staatspersonals (Personalgesetz; PG) vom 1. September 1994 (BGS 154.21) über eine allgemeine Grundlage für die Vornahme von Eignungsprüfungen, wobei gemäss § 2 Abs. 1 PG abweichende spezialgesetzliche Bestimmungen ausdrücklich vorbehalten sind.

Im Bereich Personensicherheitsüberprüfungen können die Kantone gar keine gleichwertige Sicherheit gewährleisten wie der Bund, weshalb schon aus diesem Grund hier die Vorschriften des Bundes gelten. Die Kantone haben nämlich keine direkte Möglichkeit, Daten über ihre Angestellten beim Nachrichtendienst des Bundes oder bei anderen Sicherheitsbehörden des Bundes zu erheben. Deshalb wird gemäss Artikel 29 Absatz 1 Buchstabe b des Informationssicherheitsgesetzes (ISG) eine Personensicherheitsprüfung des Bundes bei Angestellten der Kantone durchgeführt, die eine sicherheitsempfindliche Tätigkeit ausüben. Der Bund trägt gemäss Artikel 36 Absatz 3 ISG die Kosten dieser Prüfungen. Die Kantone müssen nach Artikel 31 Absatz 1 ISG dem Bund die zuständigen Stellen melden für:

- die Einleitung der Personensicherheitsprüfungen (einleitende Stellen);
- den Entscheid über die Ausübung der sicherheitsempfindlichen Tätigkeit (entscheidende Stellen).

Der Bund wird nach erfolgter Vernehmlassung Kontakt mit den Kantonen aufnehmen, um die entsprechenden Listen der Funktionen zu liefern, welche der Personensicherheitsprüfung unterstellt werden müssen.

### **2.2.3. IAMV**

Mit der Verordnung über die elektronische Übermittlung im Verwaltungsverfahren vom 1. September 2015 (BGS 162.13) verfügt der Kanton Zug über Vorgaben an ein Identitätsverwaltungssystem (ZUGLOGIN). Mit dem Bund wird derzeit die Föderation ZUGLOGIN zum CH-Login bereits realisiert. Über das interne kantonale IAM-System stehen Admin-PKI-Zugänge bei erhöhtem Schutzbedarf auf Bundesanwendungen zur Verfügung.

## **2.3. Mit welchen finanziellen Auswirkungen rechnen die Kantone**

Für die Schulung, die Sicherstellung der Sicherheit des Informatikbetriebs, die Einleitung der Personensicherheitsprüfungen und die Überprüfung der Informatiksicherheit bei den Organen wird beim AIO eine zusätzliche Vollzeitstelle (Informationssicherheits-Spezialist) benötigt.

Zu den finanziellen Auswirkungen, insbesondere zu einem allfälligen personellen Mehraufwand bei den Organen, die klassifizierte Informationen des Bundes bearbeiten oder auf seine

Informatikmittel zugreifen, können derzeit keine Aussagen gemacht werden. Die konkreten Auswirkungen werden sich erst bei bzw. nach der Umsetzung der Verordnungen zeigen

**2.4. Die Kantone sollen für Fragen der Informationssicherheit eine Dienststelle als Ansprechpartner für die Bundesbehörden bezeichnen. Wer ist die Ansprechperson bei Ihrem Kanton?**

Ansprechperson ist der CISO des AIO.

Zug, 15. November 2022

Freundliche Grüsse  
Regierungsrat des Kantons Zug

sign.

Martin Pfister  
Landammann

sign.

Tobias Moser  
Landschreiber

Versand per E-Mail an:

- [sicherheit.vbs@gs-vbs.admin.ch](mailto:sicherheit.vbs@gs-vbs.admin.ch) (Word- und PDF-Format)
- Zuger Mitglieder der Bundesversammlung
- Staatskanzlei ([info.staatskanzlei@zg.ch](mailto:info.staatskanzlei@zg.ch), Geschäftskontrolle)
- Datenschutzstelle ([datenschutz.zug@zg.ch](mailto:datenschutz.zug@zg.ch))
- Sicherheitsdirektion ([info.sd@zg.ch](mailto:info.sd@zg.ch))
- Volkswirtschaftsdirektion ([info.vds@zg.ch](mailto:info.vds@zg.ch))
- Finanzdirektion ([info.fd@zg.ch](mailto:info.fd@zg.ch))
- Amt für Informatik und Organisation ([info.aio@zg.ch](mailto:info.aio@zg.ch))
- Personalamt ([info.pa@zg.ch](mailto:info.pa@zg.ch))