Auszug aus dem Protokoll
des Regierungsrates des Kantons Zürich

Sitzung vom 9. November 2022

1462. Ausführungsrecht zum Informationssicherheitsgesetz (Vernehmlassung)

Mit Schreiben vom 24. August 2022 hat das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport das Vernehmlassungsverfahren zum Ausführungsrecht zum Informationssicherheitsgesetz eröffnet.

Das Bundesgesetz vom 18. Dezember 2020 über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG, BBl 2020 9975 ff.) soll die sichere Bearbeitung der Informationen, für die der Bund zuständig ist, sowie den sicheren Einsatz der Informatikmittel des Bundes gewährleisten (Art. 1 Abs. 1 ISG). Das Gesetz gilt in erster Linie für die darin genannten Behörden und Organisationen des Bundes (Art. 2 Abs. 1–4 ISG). Die Bestimmungen über kritische Infrastrukturen (Art. 74–80 ISG) gelten zudem für Organisationen des öffentlichen und privaten Rechts, die solche Infrastrukturen betreiben (Art. 2 Abs. 5 ISG). Einzelne Bestimmungen des Gesetzes gelten schliesslich auch für die Kantone, wenn diese keine mindestens gleichwertige Informationssicherheit gewährleisten (Art. 3 Abs. 2 ISG). Dabei handelt es sich um die Bestimmungen über klassifizierte Informationen, soweit die Kantone klassifizierte Informationen des Bundes bearbeiten, und über die Sicherheit beim Einsatz von Informatikmitteln, soweit die Kantone auf Informatikmittel des Bundes zugreifen (Art. 3 Abs. 1 ISG).

Das Ausführungsrecht zum Informationssicherheitsgesetz umfasst drei neue Verordnungen und die Änderung einer bestehenden Verordnung:

- Die neue *Verordnung über die Informationssicherheit bei der Bundesverwaltung und bei der Armee (Informationssicherheitsverordnung, ISV)* regelt das Management der Informationssicherheit, den Schutz von klassifizierten Informationen, die Informatiksicherheit sowie die Massnahmen zur Gewährleistung der personellen und physischen Sicherheit. Sie legt dazu die Aufgaben, Kompetenzen, Verantwortlichkeiten und Verfahren fest.
- Die neue *Verordnung über die Personensicherheitsprüfungen (VPSP)* fasst die Ausführungsbestimmungen zu den verschiedenen Personensicherheitsprüfungen zusammen. Sie erlaubt den Kantonen, unter bestimmten Voraussetzungen Leistungen einer Fachstelle des Bundes in Anspruch zu nehmen.

– Die neue *Verordnung über das Betriebssicherheitsverfahren (VBSV)* regelt die Einzelheiten des vom Gesetz vorgesehenen Betriebssicherheitsverfahrens, dessen Anwendung auf Subunternehmen, die Organisation der Fachstelle Betriebssicherheit, die Datensicherheit in deren Informationssystem sowie die periodische Kontrolle der Bearbeitung von Personendaten durch eine externe Stelle.
– Die Änderung der *Verordnung über Identitätsverwaltungs-Systeme und Verzeichnisdienste des Bundes (IAMV, SR 172.010.59)* umfasst neben vorwiegend technischen Anpassungen eine Erweiterung des Geltungsbereichs auf die Verwaltungseinheiten der dezentralen Bundesverwaltung, sofern diese Zugriff auf Informatiksysteme der zentralen Bundesverwaltung haben.

Das Inkrafttreten des Informationssicherheitsgesetzes und des Ausführungsrechts ist auf Mitte 2023 geplant.

Auf Antrag der Finanzdirektion

beschliesst der Regierungsrat:

I. Schreiben an das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport, 3003 Bern (Zustellung auch per E-Mail als PDF- und Word-Version an sicherheit.vbs@gs-vbs.admin.ch):

Mit Schreiben vom 24. August 2022 haben Sie uns eingeladen, zum Ausführungsrecht zum Informationssicherheitsgesetz Stellung zu nehmen und vier konkrete Fragen zu beantworten. Wir danken für diese Gelegenheit und äussern uns wie folgt:

Die Bestrebungen des Bundes im Bereich der Informationssicherheit begrüssen wir. Zu den Verordnungsentwürfen schlagen wir keine Änderungen vor. Ihre Fragen beantworten wir gerne wie folgt:

1. Ist die Umsetzung der Verordnungen für die Kantone verständlich?

Die Verordnungsentwürfe betrachten wir grundsätzlich als verständlich. Sie lassen allerdings noch wesentliche Punkte offen, beispielsweise zur Frage, unter welchen Voraussetzungen die Informationssicherheit bei einem Kanton als «gleichwertig» im Sinne von Art. 3 Abs. 2 des Bundesgesetzes vom 18. Dezember 2020 über die Informationssicherheit beim Bund (ISG) zu betrachten ist. Unklar ist ferner, ob und inwieweit von den Kantonen gemäss Art. 16 Abs. 3 der Verordnung über die Informationssicherheit bei der Bundesverwaltung und bei der Armee (ISV) erwartet wird, nach Bundesrecht Gesuche um Zugang zu Informationen des Bundes zu behandeln.

Eine abschliessende Beurteilung ist deshalb erst möglich, wenn die weiteren Vorgaben gemäss Kapitel 3.8 des erläuternden Berichts vorliegen. Diese sollten wirksam, zweckmässig und wirtschaftlich sein.

2. Wie gedenken die Kantone, die Verordnungen umzusetzen?

Die Umsetzung im Kanton Zürich muss sinnvollerweise darauf ausgerichtet sein, eine mindestens gleichwertige Informationssicherheit im Sinne von Art. 3 Abs. 2 ISG zu gewährleisten. Sie erfolgt nach den Vorgaben von § 7 des Gesetzes über die Information und den Datenschutz vom 12. Februar 2007 (LS 170.4), §§ 12 ff. der Verordnung über die Informationsverwaltung und -sicherheit vom 3. September 2019 (LS 170.8) und der Allgemeinen Informationssicherheitsrichtlinie des Regierungsrates für die kantonale Verwaltung vom 3. September 2019 (RRB Nr. 795/2019) sowie der gestützt darauf erlassenen Besonderen Informationssicherheitsrichtlinien.

Die Sicherheit beim Betrieb gemäss Art. 30 E-ISV kann das Amt für Informatik schon heute mit dem Cyber Defence Center (CDC) gemäss der kantonalen Cybersicherheitsstrategie vom 4. Mai 2022 (RRB Nr. 676/2022) gewährleisten. Das CDC überprüft die Infrastruktur auch regelmässig auf Schwachstellen und Lücken. Die Sicherheitsakkreditierung von Informatikmitteln gemäss Art. 23 E-ISV erfolgt mit einer Kombination aus Schwachstellenmanagement, Pentesting, Bug-Bounty und einem konzeptionellen Review der Lösung. Bei der Umsetzung der physischen Schutzmassnahmen gemäss Art. 34 E-ISV ist im Kanton Zürich das Immobilienamt federführend. Im Bereich der Personensicherheitsprüfungen wird eine Präzisierung der Rechtsgrundlagen zu prüfen sein.

Die Umsetzung durch die Kantone kann jedoch erst dann abschliessend festgelegt werden, wenn die weiteren Vorgaben gemäss Kapitel 3.8 des erläuternden Berichts vorliegen.

3. Mit welchen finanziellen Auswirkungen rechnen die Kantone?

Grundsätzlich gehen wir davon aus, dass dem Kanton Zürich durch das neue Informationssicherheitsrecht des Bundes Zusatzkosten entstehen. Dies gilt beispielsweise für die Sicherheitsakkreditierung von Informatikmitteln gemäss Art. 23 E-ISV. Die Kosten dafür belaufen sich – abhängig vom Umfang und der Komplexität einer Lösung – jeweils auf ungefähr Fr. 10 000 bis 50 000. Weiter entstehen in diesem Zusammenhang auch Zusatzkosten für die regelmässige Prüfung der Sicherheit während des Lebenszyklus. Aufgrund der noch offenen Fragen zur Umsetzung des neuen Informationssicherheitsrechts (vgl. Antwort auf Frage 2) können dessen finanzielle Auswirkungen aber noch nicht abschliessend abgeschätzt werden.

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

Die Bezeichnung einer zentralen Ansprechstelle für Fragen der Informationssicherheit in jedem Kanton erachten wir grundsätzlich als sinnvoll. In der kantonalen Verwaltung Zürich steht den Bundesbehörden dafür grundsätzlich die oder der Informationssicherheitsbeauftragte des Kantons Zürich zur Verfügung. Je nach dem Gegenstand der Anfrage erfordern Auskünfte indessen eine Rücksprache mit den betroffenen kantonalen Organisationseinheiten. Für die tägliche Arbeit ist ausserdem der direkte Austausch zwischen den «Peer»-Abteilungen von Bund und Kantonen notwendig, da die Themen in den verschiedenen Organisationseinheiten sehr unterschiedlich sind und ein spezifisches Detailwissen erfordern.

II. Mitteilung an die Mitglieder des Regierungsrates sowie an die Finanzdirektion.

Vor dem Regierungsrat
Die Staatsschreiberin:

Kathrin Arioli