suisse.ing

Schweizerische Vereinigung Beratender Ingenieurunternehmungen
Union Suisse des Sociétés d'Ingénieurs-Conseils
Unione Svizzera degli Studi Consulenti d'Ingegneria
Uniun svizra dals biros d'inschigneria consultativs
Swiss Association of Consulting Engineers

Bern, August 2023

FACTSHEET ZUM NEUEN INFORMATIONS-SICHERHEITSGESETZ

Im Dezember 2020 verabschiedete die Bundesversammlung das Bundesgesetz über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG; AS 2022 232). Das zugehörige Ausführungsrecht war bis am 24. November 2022 in Vernehmlassung. Das ISG sowie die vier dazugehörigen Verordnungen werden voraussichtlich Anfang 2024 in Kraft treten. Obwohl das ISG grundsätzlich nur für Behörden und Organisationen gilt, erstreckt sich dessen Anwendungsbereich auch auf sämtliche Verträge, welche der Bund mit Dritten schliesst (vgl. Art. 9 ISG).

Das ISG bezweckt, die folgenden öffentlichen Interessen zu schützen (Art. 1 Abs. 2 ISG):

- *die Entscheidungs- und Handlungsfähigkeit der Behörden und Organisationen des Bundes;*
- *die innere und äussere Sicherheit der Schweiz;*
- *die aussenpolitischen Interessen der Schweiz;*
- *die wirtschafts-, finanz- und währungspolitischen Interessen der Schweiz; und*
- *die Erfüllung der gesetzlichen und vertraglichen Verpflichtungen der Behörden und Organisationen des Bundes zum Schutz vor Informationen.*

Der vorliegende Beitrag soll einen Überblick über die wesentlichen Regelungen des ISG liefern und einen ersten Anhaltspunkt für die zukünftige Zusammenarbeit mit dem Bund bieten.

Geltung nur für den Bund

Das ISG gilt für die Bundesversammlung, den Bundesrat, die eidgenössischen Gerichte, die Bundesanwaltschaft und die Aufsichtsbehörde über die Bundesanwaltschaft sowie die Schweizerische Nationalbank. Zudem gilt es für die Parlamentsdienste, die Bundesverwaltung, die Verwaltungen der eidgenössischen Gerichte, die Armee und die mit Verwaltungsaufgaben betrauten Personen (Art. 2 Abs. 1 und 2 ISG. N.B.: Der einfacheren Lesbarkeit zuliebe wird im Folgenden statt von «verpflichteten Behörden und Organisationen» jeweils vom «Bund» gesprochen). Für Kantone gelten gewisse Bestimmungen des ISG ebenfalls, es sei denn, sie gewährleisten eine mindestens gleichwertige Informationssicherheit (Art. 3 ISG).

Das ISG gilt auszugsweise auch für Organisationen des privaten Rechts, die kritische Infrastrukturen betreiben (vgl. Art. 2 Abs. 5 ISG). Als kritische Infrastrukturen gelten die Trinkwasser- und Energieversorgung, Informations-, Kommunikations- und Transportinfrastrukturen sowie weitere Prozesse, Systeme und Einrichtungen, die essenziell für das Funktionieren der Wirtschaft beziehungsweise das Wohlergehen der Bevölkerung sind (Art. 5 lit. c ISG).

Arbeitet der Bund mit Dritten zusammen, so sorgt er dafür, dass die Anforderungen und Massnahmen nach dem ISG in den entsprechenden Vereinbarungen und Verträgen festgehalten werden. Er sorgt für eine angemessene Überprüfung der Umsetzung der Massnahmen (Art. 9 ISG). Betriebe, die einen sicherheitsempfindlichen Auftrag des Bundes ausführen sollen, können einem Betriebssicherheitsverfahren unterzogen werden (vgl. Art. 50 Abs. 1 lit. a ISG).

Merke: Das ISG gilt grundsätzlich nur für den Bund. Arbeitet jedoch ein Ingenieurbüro mit dem Bund zusammen, wird es sich zukünftig an die Anforderungen und Massnahmen des ISG halten müssen. Bei sicherheitsempfindlichen Aufträgen kann ein Ingenieurbüro sogar Gegenstand eines Betriebssicherheitsverfahrens werden.

Definition «sicherheitsempfindliche Tätigkeiten»

Sicherheitsempfindlich sind gemäss Art. 5 lit. b ISG folgende Tätigkeiten:

- **die Bearbeitung von «vertraulich» oder «geheim» klassifizierten Informationen**. Informati-

onen gelten als «vertraulich» oder «geheim, wenn deren Kenntnisnahme durch Unberechtigte die in der Einleitung erwähnten öffentlichen Interessen erheblich oder schwerwiegend beeinträchtigen kann (vgl. Art. 13 Abs. 2 und 3 ISG);

- **die Verwaltung, der Betrieb, die Wartung und die Überprüfung von Informatikmitteln** der Sicherheitsstufe «hoher Schutz» oder «sehr hoher Schutz». Diese Sicherheitsstufen gelten für Informatikmittel, wenn eine Verletzung der Vertraulichkeit, Verfügbarkeit, Integrität oder Nachvollziehbarkeit der Informationen, die damit bearbeitet werden, die in der Einleitung erwähnten öffentlichen Interessen erheblich oder schwerwiegend beeinträchtigen kann (vgl. Art. 17 Abs. 2 und 3 ISG);

- **der Zugang zu Sicherheitszonen, insbesondere zu Schutzzone 2 oder 3 einer Anlage nach der Gesetzgebung über den Schutz militärischer Anlagen**. Der Bund kann Räumlichkeiten oder Bereiche als Sicherheitszonen bezeichnen, wenn in diesen Räumlichkeiten oder Bereichen häufig «vertraulich» oder «geheim» klassifizierte Informationen bearbeitet werden oder Informatikmittel der Sicherheitsstufe «hoher Schutz» oder «sehr hoher Schutz» betrieben werden (Art. 23 Abs. 1 ISG).

Merke: Die Klassifizierung erfolgt durch den Bund (vgl. Art. 11 ISG). Es ist davon auszugehen, dass die grosse Mehrheit an Verträgen mit dem Bund nicht als sicherheitsempfindlich gelten wird.

Zukünftige Verträge mit dem Bund für nicht sicherheitsempfindliche Tätigkeiten

Das ISG wird auf sämtliche Verträge mit dem Bund einen Einfluss haben. Die Bundesbehörden sind verpflichtet, die Gewährleistung der Informationssicherheit im Rahmen der Zusammenarbeit mit Dritten zu stipulieren und für eine angemessene Kontrolle der Einhaltung der Vorgaben zu sorgen (Art. 9 ISG; Generalsekretariat VBS GS-VBS, Digitalisierung und Cybersicherheit VBS, Erläuternder Bericht zum Ausführungsrecht zum Informationssicherheitsgesetz, 2022 [hiernach: Erläuternder Bericht], S. 47). Im Folgenden werden die wichtigsten Verpflichtungen des Bundes aufgezeigt und wie sich diese auf die Aufträge des Bundes auswirken können:

- **Informationssicherheit:** Informationen sollen ihrem Schutzbedarf entsprechend nur Berechtigten zugänglich sein (Vertraulichkeit), verfügbar sein, wenn sie benötigt werden (Verfügbarkeit), nicht unberechtigt oder unbeabsichtigt verändert werden (Integrität) und nachvollziehbar bearbeitet werden (Nachvollziehbarkeit) (Art. 6 Abs. 2 ISG). Die Informatikmittel sind vor Missbrauch und Störung zu schützen (Art. 6 Abs. 3 ISG). Es gelten die Grundsätze der Zweckmässigkeit, Wirtschaftlichkeit und Benutzerfreundlichkeit (Art. 6 Abs. 4 ISG). Der Bund wird deshalb seine Vertragspartner voraussichtlich dazu verpflichten, diese Sicherheit zu gewährleisten. Dafür kann er im Vertrag konkrete Massnahmen vorsehen, die der Vertragspartner vorzunehmen hat.

- **Vorgehen bei Verletzungen der Informationssicherheit:** Verletzungen der Informationssicherheit sollen rasch erkannt, Ursachen abgeklärt und Auswirkungen minimiert werden (Art. 10 Abs. 1 ISG). Folglich wird der Bund seine Vertragspartner voraussichtlich dazu verpflichten, Verletzungen der Informationssicherheit innert einer kurzen Frist zu melden.

- **Überprüfung:** Der Bund sorgt für eine angemessene Überprüfung der Umsetzung der Massnahmen (Art. 9 Abs. 2 ISG). Es ist davon auszugehen, dass der Bund zukünftig jeweils vertraglich ein Auditrecht vereinbaren wird.

Die Beschaffungskonferenz des Bundes BKB hat den Beschaffungsstellen der Bundesverwaltung eine Musterklausel betreffend Schutz vor Cyberangriffen zur Verfügung gestellt. Die Klausel kann unter diesem Link abgerufen werden. Sie bietet einen Einblick, wie sich die neuen Verpflichtungen auf die einzelnen Verträge auswirken können. Zu beachten ist, dass sich diese Klausel gemäss Erläuterungen der BKB in erster Linie auf Verträge mit einem hohen Risiko für Cyberangriffe bezieht. Es kann deshalb davon ausgegangen werden, dass in Verträgen mit geringerem Risiko tiefere Hürden vorgesehen werden.

Merke: Auch bei nicht sicherheitsempfindlichen Tätigkeiten werden zukünftige Verträge mit dem Bund gewisse zusätzliche Klauseln zur Informationssicherheit beinhalten. Insbesondere werden Vertragspartner voraussichtlich die Sicherheit (Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit) der Informationen gewährleisten müssen. Zudem werden voraussichtlich eine Meldepflicht von Verletzungen der Informationssicherheit sowie ein Auditrecht zugunsten des Bundes vorgesehen sein.

Zukünftige Verträge mit dem Bund für sicherheitsempfindliche Tätigkeiten

Betriebe, die sicherheitsempfindliche Aufträge des Bundes erfüllen, werden im Rahmen des Betriebssicherheitsverfahrens auf deren Vertrauenswürdigkeit hin überprüft und anschliessend regelmässig kontrolliert (Erläuternder Bericht, S. 47).

Das Betriebssicherheitsverfahren läuft wie folgt ab:

1. **Antrag auf Einleitung des Betriebssicherheitsverfahrens:** Der Bund beantragt bei der für die Durchführung des Betriebssicherheitsverfahrens zuständigen Fachstelle (Fachstelle BS) die Einleitung des Verfahrens, wenn er beabsichtigt, einen sicherheitsempfindlichen Auftrag zu vergeben (Art. 52 Abs. 1 ISG).

2. **Einleitung des Betriebssicherheitsverfahrens oder Verzicht:** Die Fachstelle BS prüft den Antrag und leitet das Verfahren ein (Art. 53 Abs. 1 ISG). Die Fachstelle BS kann mit Einverständnis der Auftraggeberin auf die Einleitung verzichten, wenn das Sicherheitsrisiko mit anderen Massnahmen, welche die Fachstelle BS empfiehlt, auf ein tragbares Mass reduziert werden kann (Art. 53 Abs. 2 ISG).

3. **Beurteilung der Betriebe:** Die Fachstelle BS legt in Absprache mit der Auftraggeberin die Anforderungen an die Informationssicherheit für das Vergabeverfahren und die Auftragserfüllung fest (Art. 54 ISG).

   Die Auftraggeberin teilt der Fachstelle BS mit, welche Betriebe in Frage kommen (Art. 55 Abs. 1 ISG).

   Die Fachstelle BS beurteilt, ob diese Betriebe zur Ausführung geeignet sind oder ob ein Sicherheitsrisiko besteht (Art. 55 Abs. 2 ISG). Sie kann zur Beurteilung Daten beim Betrieb, beim Nachrichtendienst des Bundes (NDB) und aus öffentlich zugänglichen Quellen erheben (Art. 56 Abs. 1 ISG). Sie kann ausländische und internationale Dienststellen um Zustellung entsprechender Daten ersuchen; Anfragen an ausländische Nachrichtendienste erfolgen über den NDB (Art. 56 Abs. 2 ISG). Ein Sicherheitsrisiko wird dabei so definiert, dass aufgrund der erhobenen Daten konkrete Anhaltspunkte vorliegen, dass der Betrieb den sicherheitsempfindlichen Auftrag mit hoher Wahrscheinlichkeit vorschriftswidrig oder unsachgemäss ausführen wird (Art. 57 Abs. 1 ISG). Ob das Sicherheitsrisiko durch den Betrieb verschuldet ist oder nicht spielt keine Rolle (vgl. Art. 57 Abs. 3 ISG).

   Die Fachstelle BS teilt ihre Beurteilung der Auftraggeberin mit, dem Betrieb eröffnet sie die Beurteilung durch Verfügung (Art 58 Abs. 1 ISG). Ist bei einem Betrieb ein Sicherheitsrisiko vorhanden, wird er vom Vergabeverfahren ausgeschlossen (vgl. Art. 58 Abs. 2 ISG). Ist bei allen in Frage kommenden Betrieben ein Sicherheitsrisiko vorhanden, so kann die Auftraggeberin trotzdem einer dieser Betriebe den Auftrag erteilen. Das Betriebssicherheitsverfahren wird eingestellt und die Massnahmen nach den Artikeln 69, 60, 63 und 64 (Sicherheitskonzept inkl. Pflicht, dieses laufend umzusetzen, Personensicherheitsprüfungen, Meldepflicht für sicherheitsrelevanten Änderungen und Vorfälle, Inspektions- und Einsichtsrecht der Fachstelle BS, Schutzmassnahmen der Fachstelle BS bei Gefährdung Informationssicherheit) werden sinngemäss angewendet (vgl. Art. 58 Abs. 3 ISG).

4. **Sicherheitskonzept:** Die Auftraggeberin teilt der Fachstelle BS mit, welcher Betrieb den Zuschlag erhält (Art. 59 Abs. 1 ISG). Der Betrieb erstellt nach Vorgaben der Fachstelle BS ein Sicherheitskonzept, welches die Fachstelle BS prüft (Art. 59 Abs. 2 und 3 ISG). Personen des Betriebs, die für eine sicherheitsempfindliche Tätigkeit vorgesehen sind, werden einer Personensicherheitsprüfung unterzogen (Art. 60 Abs. 1 ISG).

5. **Ausstellung Betriebssicherheitserklärung:** Die Fachstelle BS stellt dem Betrieb eine Betriebssicherheitserklärung aus (Verfügung, fünf Jahre gültig), sobald dieser das Sicherheitskonzept nachweislich umgesetzt hat (Art. 61 Abs. 1 und 5 ISG). Wenn der Betrieb das Sicherheitskonzept nicht umsetzt, verweigert die Fachstelle BS ihm die Betriebssicherheitserklärung und erlässt eine entsprechende Verfügung (Art. 61 Abs. 2 ISG). Die Verfügungen werden der Auftraggeberin mitgeteilt und sie ist daran gebunden (Art. 61 Abs. 3 und 4 ISG).

6. **Ausführung Auftrag:** Erst wenn die Fachstelle BS die Betriebssicherheitserklärung ausgestellt hat, darf die Auftraggeberin den sicherheitsempfindlichen Auftrag ausführen lassen (Art. 62 ISG). Die Betriebe müssen das Sicherheitskonzept laufend umsetzen und der Fachstelle BS und der Auftraggeberin alle sicherheitsrelevanten Änderungen und Vorfälle unverzüglich melden (Art. 63 ISG). Die Fachstelle BS hat ein Inspektions- und Einsichtsrecht und kann bei konkreten Anhaltspunkten einer Gefährdung der Informationssicherheit die erforderlichen Schutzmassnahmen treffen (vgl. Art. 64 ISG).

7. **Weitere Aufträge:** Betriebe, die über eine Betriebssicherheitserklärung verfügen, gelten für weitere sicherheitsempfindliche Aufträge als geeignet. Die Fachstelle BS prüft den Bedarf einer Anpassung des Sicherheitskonzeptes (Art. 65 ISG). Die Betriebe können eine internati-

onale Betriebssicherheitsbescheinigung beantragen (Art. 66 ISG).

Aufträge, für welche ein solches Betriebssicherheitsverfahren notwendig ist, werden voraussichtlich eine kleine Minderheit sein. Die Kosten des Betriebssicherheitsverfahrens werden in der Regel weniger als 0.5% des Auftragsvolumens darstellen und werden direkt oder indirekt auf die Auftraggeberin überwälzt (Erläuternder Bericht, S. 47).

Merke: Dass ein Betriebssicherheitsverfahren durchgeführt werden muss, wird die Ausnahme darstellen. Es ist zwar mit einem gewissen Mehraufwand verbunden, bietet jedoch auch einen Mehrwert: Die Betriebe können eine internationale Betriebssicherheitsbescheinigung beantragen, wenn sie sich für einen sicherheitsempfindlichen Auftrag im Ausland bewerben wollen. Zudem können die Kosten direkt oder indirekt auf die Auftraggeberin überwälzt werden.

Fazit

Das ISG wird ab seinem Inkrafttreten für sämtliche zukünftigen Verträge mit dem Bund eine Rolle spielen. Für nicht sicherheitsempfindliche Aufträge wird der Bund die Gewährleistung der Informationssicherheit in den Verträgen vorsehen, inklusive einer angemessenen Kontrolle der Einhaltung der Vorgaben. Für sicherheitsempfindliche Aufträge wird ein Betriebssicherheitsverfahren notwendig.