HÄRTING

HÄRTING Rechtsanwälte AG

Landis + Gyr-Strasse 1
6300 Zug
+41 41 710 28 50
office@haerting.ch
www.haerting.ch

Generalsekretariat des Eidgenössischen
Finanzdepartements
Nationales Zentrum für Cybersicherheit (NCSC)
3003 Bern

Per E-Mail an: ncsc@gs-efd-admin.ch

BETREFF

Stellungnahme zum Entwurf des Bundesgesetzes über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG)

DATUM

14. März 2022

Sehr geehrter Herr Bundesrat Maurer,
sehr geehrte Damen und Herren,

Wir bedanken uns für die Möglichkeit zum rubrizierten Geschäft Stellung zu beziehen und nehmen diese gerne fristgerecht wahr.

HÄRTING Rechtsanwälte AG ist eine national und international tätige, auf Informations-, Kommunikations- und Technologierecht (ICT) spezialisierte Wirtschaftsanwaltskanzlei mit Sitz in Zug. Wir beraten KMU, börsenkotierte Unternehmen als auch Kantone und Bundesbehörden.

Gerne schlagen wir Ihnen die nachfolgenden Änderungen bzw. Ergänzungen vor:

1. Informationsschutzgesetz (ISG)

Art. 1 - Ergänzung

[1] Dieses Gesetz soll:

a. die sichere Bearbeitung der Informationen, für die der Bund zuständig ist, sowie den sicheren Einsatz der Informatikmittel des Bundes gewährleisten, es sei denn eine Spezialgesetzgebung sehe eine gesonderte Zuständigkeit vor;

Begründung

Es sollte explizit erwähnt werden, dass eventuelle Spezialgesetzgebungen vorgehen können.

Art. 2 – Präzisierung

[5] Für Organisationen des öffentlichen und privaten Rechts, die kritische Infrastrukturen gemäss Artikel 74b betreiben, die aber nicht unter die Absätze 1–3 fallen, gelten die Artikel 73a–79. Die Spezialgesetzgebung kann weitere Teile dieses Gesetzes für anwendbar erklären.

Begründung

Es sollte klar sein, dass man die kritischen Infrastrukturen gemäss der Definition im ISG meint.

Art. 5 Bst. f-g - Ergänzung

Hinzufügen von lit. f mit der Definition von Cyberrisiko.

Hinzufügen von lit. g mit der Definition von Schwachstellen von Informatikmitteln

Begründung

Beide Begrifflichkeiten werden in Art. 73a ff. ISG erwähnt, jedoch erscheint deren Unterscheidung nicht geläufig. Deren Abgrenzung ist für die Erfüllung der Meldepflicht jedoch von grosser Bedeutung, weswegen wir empfehlen, die beiden Begriffe in Art. 5 ISG zu definieren.

Zudem sollten Begrifflichkeiten gesetzesübergreifend definiert und mit dem revDSG abgeglichen werden. Art. 5 Abs. 1 lit. h. revDSG spricht von Verletzung der Datensicherheit. Eine Verletzung der Datensicherheit liegt vor, wenn eine Verletzung der Sicherheit, die dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden.

Art. 73a Grundsatz Ergänzung

f. Subsidiäre Unterstützung von Betreiberinnen von kritischen Infrastrukturen.

Begründung

Da die Subsidiarität auch im erläuternder Bericht aufgewiesen wird, sollte diese auch im Gesetzestext statuiert werden. Das NCSC soll nur unterstützen, wenn die freie Wirtschaft dazu nicht in der Lage ist, weil es sich z.B. um einen Fall nationaler Bedeutung handelt.

Art. 73b Bearbeitung von Meldungen zu Cybervorfällen und Schwachstellen - Ergänzung

[2] Das NCSC kann Informationen zu Cybervorfällen veröffentlichen oder an interessierte Behörden und Organisationen weiterleiten, sofern der Geheimhaltungs- und Datenschutz sichergestellt ist und sofern dies dazu dient, Cyberangriffe zu verhindern oder zu bekämpfen. Diese Informationen dürfen Personendaten und Daten juristischer Personen enthalten, sofern es sich um missbräuchlich verwendete Identifikationsmerkmale und Adressierungselemente handelt und die betroffene Person einwilligt. Gleiches gilt für Immaterialgüterrechte im weitesten Sinne.

[3] Werden dem NCSC Schwachstellen gemeldet, so informiert es umgehend den Hersteller und setzt ihm zur Behebung der Schwachstelle eine angemessene Frist. Behebt der Hersteller die Schwachstelle nicht innert dieser Frist, so veröffentlicht das NCSC die Schwachstelle unter Angabe der betroffenen Soft- oder Hardware und des Herstellers, sofern dies zum Schutz vor Cyberrisiken beiträgt. Diese Meldungen werden vom Öffentlichkeitsprinzip ausgeschlossen.

Begründung

Betr. Abs. 1: Es muss präziser geregelt werden, welche Schwachstellen vom NCSC den Herstellern gemeldet werden müssen. Auch sollte aufgezeigt werden, ob diese Meldung lediglich optional erfolgen kann. Ebenfalls muss diese Meldung mit anderen Meldungen koordiniert werden, sodass Doppelspurigkeiten vermieden werden.

Betr. Abs. 2: Da die Bekanntgabe von Cybervorfällen negative Konsequenzen für die Reputation des angegriffenen Unternehmens nach sich ziehen kann, sollte präziser geregelt werden, unter welchen Umständen der Cybervorfall unter Nennung welcher Angaben veröffentlicht werden soll. Idealerweise ist mit dem betroffenen Unternehmen die Kommunikation sogar abzustimmen. Zudem muss der Daten- und Geheimhaltungsschutz von vertraulichen Informationen gewährleistet sein, es sei denn die betroffene Person hat zugestimmt Wenn eine Kommunikation eine Firma, Marke oder dergleichen einer Firma beinhaltet, so gilt die Zustimmung auch für diese Immaterialgüterrechte.

Betr. Abs. 3: Da auch der erläuternde Bericht die Angabe des Herstellers erwähnt, empfehlen wir auch eine explizite Nennung des Herstellers im Gesetzestext.

Art. 74 Unterstützung von Betreiberinnen von kritischer Infrastruktur - Ergänzung

[2] Es stellt ihnen dazu insbesondere folgende Hilfsmittel zur Verfügung:

a. ein Kommunikationssystem für den sicheren Informationsaustausch sowie eine sichere Datenablage;

[3] Es berät und unterstützt sie bei der Bewältigung von Cybervorfällen und der Behebung von Schwachstellen in subsidiärer Weise zu IT-Dienstleistungen, die auf dem Markt erhältlich sind, wenn für die kritische Infrastruktur ein unmittelbares Risiko von gravierenden Auswirkungen besteht und, sofern es sich um private Betreiberinnen handelt, die Beschaffung gleichwertiger Unterstützung auf dem Markt nicht rechtzeitig möglich ist.

[4] Es kann zur Analyse eines Cybervorfalls mit dem Einverständnis der betroffenen Betreiberin auf deren Informationen und Informatikmittel zugreifen. Der Zugriff kann gewährt werden ohne allfällige Geheimhaltungspflichten zu verletzen.

Begründung

Betr. lit. a: Es sollte explizit auch erwähnt werden, dass der NCSC eine sichere Datenablage gewährleistet.

Betr. lit. c: Was ist unter technischen Hilfsmittel zu verstehen?

Betr. Abs. 2: Da die Subsidiarität auch im erläuternder Bericht aufgewiesen wird, sollte diese auch im Gesetzestext statuiert werden.

Art. 74a Meldepflicht - Präzisierung

Die Betreiberinnen von kritischen Infrastrukturen müssen dem NCSC Cyberangriffe und -vorfälle nach deren Entdeckung so rasch als möglich melden, damit das NCSC Angriffsmuster frühzeitig erkennen, mögliche Betroffene warnen und ihnen geeignete Präventions- und Abwehrmassnahmen empfehlen kann.

Begründung

Bereits Cybervorfälle sollen gemeldet werden. Auch Schwachstellen sollte man freiwillig melden können, damit das NCSC Hersteller darauf hinweisen kann.

Art. 74b Bereiche - Ergänzung

r. Unternehmen, die die Bevölkerung mit unentbehrlichen Gütern des täglichen Bedarfs versorgen. Der Bundesrat bezeichnet die betroffenen Unternehmen.

Oder alternativ ganz streichen und eine gesetzliche Grundlage schaffen, um dies auf Verordnungsstufe zu definieren.

Begründung

Da der erläuternde Bericht die Präzisierung durch den Bundesrat auf dem Verordnungsweg explizit erwähnt, sollte dies auch im Gesetzestext aufgenommen werden. Es fragt sich, ob nicht die gesamte Definition der Kritischen Infrastrukturbetreiber durch den Bundesrat erfolgen soll.

Art. 74d Zu meldende Cyberangriffe – und Vorfälle– Ergänzung und Löschung

[1] Ein Cyberangriff oder ein Cybervorfall auf eine kritische Infrastruktur muss gemeldet werden, wenn die ernsten Befürchtungen bestehen, dass:

Streichung von lit. b.

Begründung

Die Ausführungen in lit. a-d verdeutlichen, dass Bagatellfälle nicht gemeldet werden sollen, sondern lediglich, wenn der Cyberangriff weitgehende Konsequenzen beinhalten kann und somit schweizweit zum Tragen kommt. Dass bereits Anzeichen der Meldepflicht gemäss Art. 74d unterliegen, widerspricht demnach der ratio legis. Lit. b ist zu streichen, da in der Regel oft nicht belegt werden kann, dass ein fremder Staat einen Cyberangriff tätigt. Lit. d ist auch zu streichen.

Art. 74e Inhalt der Meldung – Ergänzung + Bemerkung

[1] Die Meldung muss Informationen zur kritischen Infrastruktur, zur Art und Ausführung des Cyberangriffs, des Cybervorfalles, zu seinen Auswirkungen und zum geplanten weiteren Vorgehen der Betreiberin der kritischen Infrastruktur enthalten.

Begründung

Der Inhalt der Meldung sollte präziser formuliert werden, auch im Hinblick auf die Gefahr von Bussgeldern. Vorstellbar wäre die Präzisierung auch auf Stufe der Verordnung vorzunehmen.

Auch sollte der Inhalt der Meldung mit anderen Meldungspflichten an anderen Behörden abgestimmt werden, um Doppelspurigkeiten zu vermeiden.

Art. 74f Übermittlung der Meldung – Bemerkung + Streichung

[1] Für die elektronische Meldung von Cyberangriffen stellt das NCSC ein sicheres System zur Übermittlung der Meldung an das NCSC zur Verfügung.

[2] Das System muss der Betreiberin einer kritischen Infrastruktur ermöglichen, die Meldung des Cyberangriffs oder seiner Auswirkungen gesamthaft oder in Teilen an weitere Stellen und Behörden zu übermitteln.

Neuer Vorschlag

Abs. 3 ist zu streichen.

Begründung

Es kann nicht angehen, dass hier Meldungen an das NCSC und an die Datenschutzbehörde, BAKOM oder FINMA vermischt wird. Es ist sicherzustellen, dass andere «Stelle» und Behörden, nur den Umfang an Information erhalten, zu dem sie gesetzlich berechtigt sind oder im Rahmen des Zweckes der zugrundeliegenden Gesetzgebung eine Rechtfertigung besteht.

Abs. 3 ist zu streichen oder sonst ist eine klare Governance-Regelung aufzunehmen, welche es der betroffenen Infrastruktur ermöglicht zu erkennen, an welche andere(n) Behörde, Stelle oder Dritten die Informationen über ihren Cybervorfall oder -angriff mitgeteilt wurden. Das Transparenzgebot staatlichen Handelns gebietet dies.

Art. 74g Auskunftspflicht - Ergänzung

Es ist festzulegen, wie weit eine Auskunftspflicht gehen kann.

Begründung

Mit der Meldung sollte die Pflicht der kritischen Infrastrukturanbieter erfüllt sein. U.U. müsste man sich überlegen, ob man die Meldepflicht detaillierter in einer Verordnung fasst. Ausserdem ist mit der Erteilung der ergänzenden Auskünfte die Meldepflicht erfüllt. Auch die ergänzenden Auskünfte dürfen nicht zu einer Belastung in einem Strafverfahren führen und sie können nicht endlos sein.

Art. 74i Widerhandlungen gegen Verfügungen des NCSC

Neuer Vorschlag

Komplett streichen

Begründung

Die Verletzung der Meldepflicht wie auch die nachträgliche Auskunft soll nicht unter Strafe gestellt werden. Dies ist kontraproduktiv und verhindert freiwillige Meldungen, die über die reine Pflicht hinausgehen.

4. Abschnitt: Datenschutz und Informationsaustausch

Art. 77 Internationale Zusammenarbeit

[1]Das NCSC kann mit ausländischen und internationalen Stellen, die für die Cybersicherheit zuständig sind, Informationen austauschen, wenn sie diese zur Erfüllung von Aufgaben benötigen, die denjenigen des NCSC entsprechen. Umfasst der Informationsaustausch auch Personendaten nach Artikel 75, ist Artikel 6 und Art. 10a DSG zu beachten.

[2] Der Informationsaustausch nach Absatz 1 ist nur dann zulässig, wenn die ausländischen und internationalen Stellen die bestimmungsgemässe datenschutzkonforme Verwendung gewährleisten.

Begründung

Der Transfer von Personendaten hat sich an die allgemeinen datenschutzrechtlichen Grundsätze zu halten, insbesondere auch Art. 10a DSG.

Art. 79 Abs. 1

[1] Das NCSC bewahrt Personendaten nur so lange auf, wie dies zur Abwehr von Gefahren oder zur Erkennung von Vorfällen zweckmässig ist, höchstens jedoch ein Jahr ab der letzten Verwendung; bei besonders schützenswerten Personendaten beträgt die Frist 6 Monate. In anonymisierter Form sowie als erkannte Muster dürfen die aus Personendaten gewonnen Erkenntnisse unbefristet aufbewahrt werden.

Begründung

Das Verhältnissmässigkeitsprinzip im Datenschutz gebietet, dass Daten nur so lange aufbewahrt bleiben, wie sie für die Zweckerfüllung benötigt werden. Aus den Personendaten können anonymisierte Muster generiert werden.

II. Die nachstehenden Erlasse werden wie folgt geändert:

2. Datenschutzgesetz vom 25. September 2020

Art. 24 Abs. 5bis

Streichen.

Begründung

Sofern eine zentrale Stelle zu schaffen wäre, welche sämtlichen Meldungen aufnimmt, erübrigt sich diese Ergänzung.

Nach dem Gesagten danken wir Ihnen, sehr geehrter Herr Bundesrat Maurer, sehr geehrte Damen und Herren, bestens für die Berücksichtigung unserer Anliegen und stehen Ihnen für allfällige Rückfragen gerne zur Verfügung.

Freundliche Grüsse

Nicole Beranek Zanon

Olivia Boccali