

## Das neue Cyber-Sicherheitsgesetz

**Mit 1. Februar 2025 trat das neue Cyber-Sicherheitsgesetz (CSG) in Kraft. Dabei handelt es sich um eine Totalrevision des erst im Juli 2023 in Kraft getretenen CSG. Abweichend vom alten CSG haben Einrichtungen der kritischen Infrastruktur gemäss dem neuen CSG nunmehr die Verpflichtung, selbst zu prüfen, ob sie unter das Gesetz fallen.**

### Vorabumsetzung von NIS-2

In Liechtenstein wurde die Network-and-Information-Security-Richtlinie (NIS-2) der EU – losgelöst von einer Übernahme in den EWR – anhand des neuen CSG vorab umgesetzt. Dies unterstreicht die Bedeutung des neuen CSG im Umgang mit Cybersicherheit.

### Registrierungspflicht

Die Anwendbarkeit des neuen CSG wurde auf zusätzliche (Teil-)Sektoren wie etwa Fernwärme und -kälte sowie Wasserstoff (Energie), Abwasser, Weltraum, die öffentliche Verwaltung sowie Post- und Kurierdienste, Abfallbewirtschaftung, Produktion, Verarbeitung und Vertrieb von Lebensmitteln oder auch die Forschung ausgeweitet.

Es besteht für Einrichtungen der kritischen Infrastruktur die Verpflichtung zur Registrierung bei der Stabstelle Cyber-Sicherheit. Nach dem alten CSG war es die Aufgabe der Stabstelle Cyber-Sicherheit, die kritische Infrastruktur (abgesehen von Anbietern digitaler Dienste) zu ermitteln. Neu ist, dass nunmehr grundsätzlich jede Einrichtung, worunter auch ein Unternehmen fallen kann, die Pflicht hat, selbst zu prüfen, ob sie unter das neue CSG fällt (Selbsteinschätzung). Um Schwierigkeiten bei der Selbsteinschätzung zu begegnen, veröffentlichte die Stabstelle Cyber-Sicherheit eine Hilfestellung auf ihrer Website (unter Rechtliches/Geltungsbereich Cyber-Sicherheitsgesetz). Vor allem richtet sich das Gesetz

an mittelgrosse oder grosse Gesellschaften, welche ihre Dienste oder Tätigkeiten in Liechtenstein erbringen bzw. ausüben. Es bestehen jedoch Ausnahmen, die eine Registrierungspflicht unabhängig von der Grösse der Einrichtung vorsehen.

### Risikomanagementmassnahmen

Einrichtungen der kritischen Infrastruktur müssen ein Cyber-Sicherheitskonzept ausarbeiten. Risiken müssen beherrscht und Auswirkungen von Sicherheitsvorfällen auf andere verhindert oder zumindest möglichst geringgehalten werden.

### Berichtspflichten

Wesentliche und wichtige Einrichtungen haben erhebliche Sicherheitsvorfälle der Stabstelle Cyber-Sicherheit unverzüglich zu melden. Dies umfasst eine Frühwarnung innerhalb von 24 Stunden, eine Meldung über den Sicherheitsvorfall innerhalb von 72 Stunden ab Kenntnisnahme des erheblichen Sicherheitsvorfalls sowie einen Abschlussbericht spätestens einen Monat nach der Meldung.

Gegebenenfalls sind zusätzlich zu der Meldung an die Stabstelle Cyber-Sicherheit auch die Empfänger der Dienste unverzüglich über den erheblichen Sicherheitsvorfall zu informieren und entsprechende Abhilfemassnahmen mitzuteilen, die die Empfänger als Reaktion auf die Bedrohung ergreifen können.

Es sei erwähnt, dass Einrichtungen, die laut dem CSG nicht zur kritischen Infrastruktur gehören, eine freiwillige Meldung über Sicherheitsvorfälle, Cyberbedrohungen oder Beinahe-Vorfälle der Stabstelle Cyber-Sicherheit erstatten können. Eine freiwillige Meldung kann anonym erfolgen.

### Weitere Meldungen

Je nach Art des Sicherheitsvorfalls sind allenfalls spezialgesetzlich verpflichten-

de Meldungen vorgesehen. Betrifft der Sicherheitsvorfall etwa eine Verletzung des Schutzes personenbezogener Daten, besteht grundsätzlich die zusätzliche Verpflichtung zu einer Meldung gemäss der Datenschutzgrundverordnung an die Datenschutzstelle innerhalb von 72 Stunden ab Bekanntwerden der Datenschutzverletzung. Sofern strafrechtlich relevante Anhaltspunkte vorliegen, empfiehlt sich ergänzend eine (freiwillige) Anzeige bei der Landespolizei.

### Fazit

Bei Verstössen gegen das CSG drohen empfindliche Strafen. Vor diesem Hintergrund ist es ratsam, dass jedes Unternehmen eine Selbsteinschätzung vornimmt und diese dokumentiert. Ungeachtet einer Anwendbarkeit des CSG ist es zudem ratsam, dass jedes Unternehmen präventiv ein Cyber-Sicherheitskonzept erstellt sowie mit den infrage kommenden Meldungen und Meldestellen vertraut ist. Rechtsanwälte unterstützen bei Bedarf die Unternehmen bei dieser Herausforderung.



● Mag. iur. Peter Pacher, LL.M.  
Juristischer Mitarbeiter

W O H L W E N D  
N Ä S C H E R  
S C H Ä C H L E

Stuffen Egg 1, 9495 Triesen  
T +423 375 13 00  
office@wns.li, www.wns.li