Translation of Liechtenstein Law

Disclaimer

English is not an official language of the Principality of Liechtenstein. This translation is provided for information purposes only and has no legal force. The contents of this website have been compiled with utmost care and to the best of knowledge. However, the supplier of this website cannot assume any liability for the currency, completeness or accuracy of any of the provided pages and contents.

English title:	Cyber Security Law (CSG) of 4 May 2023
Original German title:	Cyber-Sicherheitsgesetz (CSG) vom 4. Mai 2023
Serial number (LR-Nr.):	784.13
First published:	30 June 2023
First publication no. (LGBl-Nr.):	2023-269
Last amended:	
Date of last amendment - publication no. (LGBl-Nr.):	
Translation date:	15 June 2023

Liechtenstein Law Gazette
Year 2023 No. 269 published on 30 June 2023

Cyber Security Law (CSG)

of 4 May 2023

I hereby grant My Consent to the following resolution adopted by the Liechtenstein Parliament:

I. General provisions

Art. 1

Subject matter and purpose

1) This Law lays down measures with a view to achieving a high level of security of the network and information systems of:

a) operators of essential services in the energy and transport sectors, banking, financial market infrastructures, the healthcare sector, drinking water supply and distribution, as well as digital infrastructure; and

b) providers of digital services.

2) The security and notification requirements laid down in this Law do not apply to:

a) companies subject to the requirements laid down in Art. 40 and 41 of Directive (EU) 2018/1972[1]; and

b) trust service providers subject to the requirements laid down in Art. 19 of Regulation (EU) No 910/2014[2].

1 Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (OJ L 321 of 17.12.2018, p. 36)

2 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257 of 28.8.2014, p. 73)

Art. 2

Transposition and implementation of EEA legislation

1) This Law serves to transpose and/or implement the following EEA legislation:

a) Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union[3];

b) Regulation (EU) 2021/887 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres[4].

2) The current version of the EEA legislation to which this Law makes reference is to be found in the publication of the decisions of the EEA Joint Committee in the Liechtenstein Legal Gazette pursuant to Art. 3 k) of the Publications Act.

Art. 3

Definition of terms and designations

1) For the purposes of this Law, the following definitions apply:

a) "network and information system" means:

1. an electronic communications network within the meaning of Art. 3 (1) no. 5 of the Communications Act;
2. a device or group of interconnected or related devices, one or more of which performs automatic processing of digital data pursuant to a programme; or
3. digital data stored, processed, retrieved or transmitted by elements covered under nos. 1 and 2 for the purposes of their operation, use, protection and maintenance;

3 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194 of 19.7.2016, p. 1)

4 Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (OJ L 202 of 8.6.2021, p. 1)

b) "security of network and information systems" means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or the related services offered by, or accessible via, those network and information systems;

c) "NIS strategy (national strategy on the security of network and information systems)" means a framework providing strategic objectives and priorities on the security of network and information systems at national level;

d) "essential service" means a service:

   1. provided in one of the sectors listed in Art. 1 (1) a);
   2. which is essential for the maintenance of critical societal or economic activities, in particular for the maintenance of the public health service, the public supply of water, energy and vital goods, public transport or the functional capability of public information and communications technology;
   3. the provision of which depends on network and information systems; and
   4. where a security incident having a real impact on the security of network and information systems would have a significant disruptive effect on the provision of that service;

e) "operators of essential services" means a public or private entity registered in Liechtenstein that provides an essential service;

f) "digital service" means a service within the meaning of Art. 3 (1) e) of the EEA Notification Law, which involves an online marketplace, an online search engine or a cloud computing service;

g) "digital service provider" means a legal person that provides a digital service and is not a small company or micro company as defined in Art. 1064 (1) and (1a) of the Persons and Companies Act:

   1. that is registered in Liechtenstein; or
   2. that is registered outside the European Economic Area (EEA) and has designated a representative pursuant to h);

h) "representative" means any natural or legal person domiciled or registered in Liechtenstein, explicitly designated to act on behalf of a digital service provider registered outside the EEA, which may be addressed by the National Cyber Security Unit, instead of the digital service provider, with regard to the obligations of that digital service provider under this Law;

i) "security incident" means any event that compromises the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or the related services offered by, or accessible via, network and information systems;

k) "security incident handling" means all procedures supporting the detection, analysis and containment of security incidents and the response thereto;

l) "risk" means any reasonably identifiable circumstance or event having a potentially adverse effect on the security of network and information systems;

m) "cooperation group" means a body established on the basis of Art. 11 of Directive (EU) 2016/1148, composed of representatives from EEA Member States, the European Commission and the European Union Agency for Network and Information Security (ENISA), that serves to support and facilitate strategic cooperation and exchange of information between the EEA Member States in order to develop trust and confidence, with a view to achieving a high common level of security of network and information systems in the EEA;

n) "CSIRTs network" means a body established pursuant to Art. 12 of Directive (EU) 2016/1148 composed of representatives of the Computer Emergency Response Teams of the EEA Member States and the European Computer Emergency Response Team, and designed to contribute to the development of confidence and trust between the EEA Member States and promote a swift and effective operational cooperation;

o) "online marketplace" means a digital service that allows consumers or traders to conclude online sales or service contracts with traders, either on the online marketplace's website or on a trader's website, that uses computing services provided by the online marketplace;

p) "online search engine" means a digital service that allows users to perform searches of, in principle, all websites or websites in a particular language, on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found;

q) "cloud computing service" means a digital service that enables access to a scalable and elastic pool of shareable computing resources.

2) The terms used in this Law to denote persons are to be understood as applying to all persons, irrespective of their gender, unless the personal terms explicitly refer to a specific gender.

II. Security and notification requirements

A. Operators of essential services

Art. 4

Security requirements

1) Operators of essential services shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations.

2) Having regard to the state of the art, the measures referred to under (1) shall ensure a level of security of network and information systems appropriate to the risk posed.

3) Operators of essential services shall take appropriate measures to prevent and minimise the impact of security incidents affecting the security of the network and information systems used for the provision of services, with a view to ensuring the continuity of their services.

4) The obligations under (1) to (3) do not apply if specific legislation is already in place in respect of security requirements, providing at least an equivalent level of security for network and information systems.

5) The Government may establish more specific regulations concerning security requirements for operators of essential services by Ordinance.

Art. 5

Notification requirements

1) Operators of essential services shall immediately notify the National Cyber Security Unit of a security incident having a significant impact, or likely to have a significant impact, on the continuity of one of the services they provide.

2) The notification must contain all relevant information concerning the security incident and the technical circumstances that are known at the time of the initial notification, in particular the probable or actual cause, the information technology concerned, the type of entity or facility concerned. Information on circumstances concerning the security incident that come to light later must be reported in follow-up notifications

and finally in a concluding report, immediately after the circumstances have been established.

3) Notifications are to be communicated in a secure electronic format, that is standardised, as far as possible.

4) Where an operator of essential services relies on a third-party digital service provider for the provision of an essential service, any impact on the continuity of these services as referred to in (1) due to an incident affecting the digital service provider shall be reported to the National Cyber Security Unit by that operator.

5) After consulting the notifying operator of essential services, the National Cyber Security Unit may inform the public of the actual security incidents, if public awareness is necessary in order to prevent security incidents or deal with ongoing security incidents.

6) The requirements listed in (1) to (5) do not apply if specific legislation in respect of notification requirements already exists and the criteria for reporting are at least equivalent. In such cases the recipients of the notification shall report the notifications they have received immediately to the National Cyber Security Unit.

7) The Government may establish more specific regulations concerning notification requirements applying to operators of essential services by Ordinance.

B. Digital service providers

Art. 6

Security requirements

1) Digital service providers shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in the context of providing digital services.

2) Having regard to the state of the art, the measures referred to in (1) shall ensure a level of security of network and information systems appropriate to the risk posed and shall take into account the following elements:

a) the security of systems and facilities;

b) handling of security incidents;

c) business continuity management;

d) monitoring, auditing and testing;

e) compliance with international standards.

3) Art. 4 (4) shall apply mutatis mutandis.

Art. 7

Notification requirements

1) Digital service providers shall notify the National Cyber Security Unit without delay of any security incident having a substantial impact on the provision of a service they have provided within the EEA.

2) After consulting the digital service provider concerned, the National Cyber Security Unit may inform the public about actual security incidents or require the digital service provider to do so, if:

a) public awareness is necessary in order to prevent security incidents or to manage ongoing security incidents; or

b) disclosure of the security incident is otherwise in the public interest.

3) Art. 5 (6) shall apply mutatis mutandis.

C. Other entities

Art. 8

Voluntary notification

1) Entities which have not been identified as operators of essential services and are not digital service providers may report risks and security incidents to the National Cyber Security Unit.

2) The voluntary notification does not have to contain the identity of the entity or information that would enable it to be identified.

III. Organisation and implementation

A. General

Art. 9

Responsibilities

1) The implementation of this Law is assigned to:

a) the National Cyber Security Unit;

b) the Computer Security Incident Response Team (CSIRT).

2) The National Cyber Security Unit and the CSIRT may instruct qualified third parties to perform their duties.

3) The Government may establish more specific regulations concerning the requirements for qualified third parties as referred to in (2) by Ordinance.

Art. 10

Professional confidentiality

The bodies entrusted with the implementation of this Law and any qualified third parties instructed by them shall be subject to professional confidentiality and shall maintain secrecy towards other official bodies and persons in respect of observations made in the performance of this activity and refuse access to the processed data and official files. Art. 14 is reserved.

Art. 11

Processing and disclosure of personal data

1) In order to guarantee a high level of security of network and information systems in the performance of its duties under this Law, the National Cyber Security Unit is authorised to process the personal data that is required under Art. 4 no. 1 of Regulation (EU) 2016/679[5].

5 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119 of 4.5.2016, p. 1)

2) It may divulge such data as referred to in (1), of which it becomes aware in the performance of its duties under this Law to domestic and foreign authorities and agencies, if:

a) it proves to be necessary for the performance of its duties under this Law or Directive (EU) 2016/1148;

b) confidentiality of the data is guaranteed; and

c) the security and the business interests of the operators of essential services and the digital services providers are protected.

B. National Cyber Security Unit

Art. 12

Responsibilities

1) The National Cyber Security Unit is the competent national authority responsible for the security of network and information systems pursuant to Art. 8 (1) of Directive (EU) 2016/1148. It is responsible for the monitoring and implementation of this Law.

2) The National Cyber Security Unit is also the single point of contact for the security of network and information systems as referred to in Art. 8 (3) Directive (EU) 2016/1148. It also exercises a liaison function to ensure cross-border cooperation with international bodies and groups, such as, in particular, the competent bodies in other EEA Member States, the cooperation group and the CSIRTs network.

Art. 13

Duties

1) The National Cyber Security Unit shall adopt the measures required within the context of its mandate to ensure compliance with this Law. It is responsible, in particular, for:

a) monitoring the security requirements set out in Art. 4 and 6 and compliance with the notification requirements set out in Art. 5 and 7;

b) establishment and coordination of the CSIRT pursuant to Art. 19;

c) receipt and analysis of notifications of risks or security incidents, drawing up a survey of the situation and forwarding the notifications and the survey of the situation, together with additional relevant

information, to the domestic authorities or other concerned bodies, where required;

d) drawing up and disclosure of relevant information to guarantee the security of network and information systems or for the prevention of security incidents;

e) identification of operators of essential services and drawing up a schedule listing essential services, to be reviewed and updated regularly, but at least once every two years;

f) communication and forwarding of information provided by the operator of essential services to the single point of contact of the EEA Member States concerned, if a security incident has a significant impact on the continuity of essential services in those EEA Member States;

g) coordinating public-private cooperation in respect of the security of network and information systems;

h) informing the public of security incidents, raising public awareness in order to prevent or manage security incidents and publishing general information in connection with the security of network and information systems;

i) cooperation and exchange of information with other domestic authorities and bodies, in particular the National Police, the Office of the Public Prosecutor, the Data Protection Authority, the Office of Information Technology, the Office for Communications, the Financial Intelligence Unit and the Financial Market Authority of Liechtenstein;

k) cross-border cooperation and cross-border exchange of information with the competent authorities and agencies in other EEA Member States, ENISA, the cooperation group and CSIRTs network;

l) cross-border cooperation and cross-border exchange of information in relation to the security of network and information systems with the competent authorities and agencies in third countries;

m) coordination and establishment of an NIS strategy pursuant to Art. 20;

n) representing Liechtenstein in the cooperation group, the CSIRTs network and in other cross-border organisations in the EEA and international bodies for the security of network and information systems.

2) The National Cyber Security Unit may, after consulting the appropriate member of the Government, conclude agreements with other domestic and foreign authorities concerning the cooperation arrangements and cooperate with private individuals under public-private partnerships for the performance of its duties.

3) The Government may establish more specific regulations concerning the duties of the National Cyber Security Unit by Ordinance.

Art. 14

Powers with regard to operators of essential services

1) In the performance of its duties under this Law, the National Cyber Security Unit may require operators of essential services to:

a) provide it with the information necessary to assess the security of their network and information systems, including documented security policies;

b) produce evidence of the effective implementation of security policies;

c) disclose information free of charge, in particular technical and statistical data, for statistical purposes or the creation of physical surveys of the situation.

2) Operators of essential services may not refuse to disclose the information referred to in (1) c) on grounds of professional, commercial or industrial confidentiality.

Art. 15

Powers with regard to digital service providers

The National Cyber Security Unit may, when provided with evidence that digital service providers do not meet the requirements laid down in this Law, require the providers to provide, without delay, the information necessary to assess the security of their network and information systems pursuant to Art. 2 (2) of Commission Implementing Regulation (EU) 2018/151[6], including documented security policies.

Art. 16

Powers in the event of infringements

1) If the National Cyber Security Unit has evidence that an operator of essential services or a digital service provider is in breach of the provisions of this Law, the ordinances enacted in connection with them, or decisions or orders based on them, it shall notify the operator of essential

6 Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for the application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact (OJ L 26 of 31.1.2018, p. 48)

services or the digital service provider of this informally, subject to (5), and set it an appropriate deadline to:

a) comment on the notification; or

b) restore the situation to a lawful state of affairs.

2) The National Cyber Security Unit may extend the deadline referred to in (1) b) in justified cases on request, if the operator of essential services or the digital service provider can thereby be expected to restore the situation to the lawful state of affairs.

3) If the operator of essential services or the digital service provider is a public-sector body or an entity that is charged with public functions, the National Cyber Security Unit shall also inform the Government about the notice referred to in (1).

4) If there is evidence of infringements against the provisions of this Law or ordinances enacted in connection with them by operators of essential services or digital service providers, the National Cyber Security Unit shall inform the competent supervisory authority and give it the opportunity to comment before a notice as referred to in (1) is issued.

5) If an operator of essential services or a digital service provider fails to comply with the notice referred to in (1) the National Cyber Security Unit shall issue an appropriate order on the matter; in urgent cases an order may be issued without a notice. The National Cyber Security Unit shall inform the competent supervisory authority for the operator of essential services or the digital service provider, of the decision.

6) The imposition of fines pursuant to Art. 22 is reserved.

Art. 17

Use of information and communications technology solutions (ICT solutions)

In order to perform its duties, the National Cyber Security Unit is authorised to:

a) employ ICT solutions or commission third parties to employ them, in order to identify the risks or security incidents arising in network and information systems in good time;

b) employ ICT solutions, or use them after obtaining the consent of the entity concerned, in order to identify the patterns of attacks on network and information systems.

Art. 18

Control measures

1) The National Cyber Security Unit may carry out control measures to check compliance with the requirements pursuant to this Law or instruct qualified third parties to perform this function.

2) In order to carry out control measures the National Cyber Security Unit, or the qualified third parties it has instructed, may inspect the network and information systems used for the provision of essential services or digital services and inspect the relevant documents. They have the right to enter premises in which network and information systems are located in order to perform such inspections. The right of access must be exercised proportionately and with the highest possible level of protection for the rights of the entity and third parties concerned and for the business operation.

3) The Government may establish more specific regulations concerning the performance of control measures by Ordinance.

C. Computer security incident response team (CSIRT)

Art. 19

Purpose and responsibilities

1) In order to guarantee the security of network and information systems a CSIRT shall be established at the National Cyber Security Unit. It is responsible, in particular, for:

a) provision of information that may be useful for dealing with a security incident on receipt of notifications of risks or security incidents as referred to in Art. 5, 7 and 8;

b) providing early warning, alerts, announcements and dissemination of information to relevant stakeholders about risks and security incidents;

c) the initial general assistance in responding to a security incident;

d) observation and analysis of risks and security incidents and situational awareness;

e) participating in the CSIRTs network.

2) The CSIRT may also perform the duties listed in (1) a) to d) with respect to other entities or individuals, if they are affected by a risk or a security incident in their network and information systems.

3) The Government may establish more specific regulations concerning the purpose and responsibilities of the CSIRT by Ordinance.

D. NIS strategy

Art. 20

Basic principle

1) The NIS strategy shall define in particular the strategic objectives and appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of security of network and information systems.

2) The National Cyber Security Unit shall communicate the NIS strategy to the EFTA Surveillance Authority within three months from its adoption. Elements of the strategy which relate to national security do not have to be communicated.

3) The NIS strategy must be approved by the Government and once approved will be published on the National Cyber Security Unit website.

IV. Legal remedy

Art. 21

Appeal

1) Appeals may be lodged with the Board of Appeal for Administrative Matters against decisions and orders of the National Cyber Security Unit within 14 days from notification.

2) Appeals may be lodged with the Administrative Court against decisions and orders of the Board of Appeal for Administrative Matters within 14 days from notification.

3) The powers of review of the Board of Appeal for Administrative Matters and the Administrative Court are restricted to legal and substantive issues. The exercise of discretion is examined purely in a legal context.

4) In other respects, the provisions of the Law on General National Administration shall apply to the procedure.

V. Penal provisions

Art. 22

Administrative offences

1) Provided the offence in question does not constitute criminal offence falling within the jurisdiction of the courts, the National Cyber Security Unit shall impose fines of up to 100 000 Francs for an offence, on any person who:

a) as an operator of essential services fails to take the measures prescribed in Art. 4 (1) to (3);

b) as an operator of essential services fails to comply with the notification requirements laid down in Art. 5 (1) to (4);

c) as a digital service provider fails to take the measures prescribed in Art. 6 (1) and (2);

d) as a digital service provider fails to comply with the notification requirements laid down in Art. 7 (1);

e) as an operator of essential services fails to supply the information, including the documented security policies required under Art. 14 (1) a);

f) as an operator of essential services fails to provide evidence as referred to in Art. 14 (1) b);

g) as an operator of essential services fails to disclose information as referred to in Art. 14 (1) c) to the National Cyber Security Unit;

h) as a digital service provider fails to provide without delay the information, including documented security policies, necessary to assess the security of their network and information systems pursuant to Art. 15;

i) as an operator of essential services or a digital service provider hinders, obstructs or renders impossible the proper performance of a control measure pursuant to Art. 18;

k) as an operator of essential services or a digital service provider contravenes a legally binding order or decision of the National Cyber Security Unit.

2) In the event of negligence, the upper limit of the penalty stated in (1) is reduced by half. If there is a repeat offence the upper limit of the penalty is doubled.

Art. 23

Liability

If criminal offences are committed in the course of business of a legal entity, a partnership or a sole trader, the penal provisions shall apply to those persons who acted, or should have acted on their behalf, but subject to the joint and several liability of the legal entity, the partnership or the sole trader for the fines and costs.

VI. Final provisions

Art. 24

Implementing regulations

The Government shall enact the Ordinances required for the implementation of this Law.

Art. 25

Applicability of EU legislation

1) Until they are adopted into the EEA Agreement the following shall apply as national legislation:

a) Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union;

b) Regulation (EU) 2021/887 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres;

c) the implementing acts in respect of the EU legislation referred to in a) and b).

2) The full text of the legislation referred to in (1) is published in the Official Journal of the European Union at https://eur-lex.europa.eu; it can be viewed on the National Cyber Security Unit website at https://scs.llv.li.

Art. 26

Entry into force

1) Provided that the referendum deadline expires unutilised, this Law shall enter into force on 1 July 2023, otherwise on the day after promulgation.

2) Art. 2 (1) a) shall enter into force at the same time as the Decision of the EEA Joint Committee no. 21/2023 of 3 February 2023 amending Annex XI (Electronic communication, audio-visual services and information society) to the EEA Agreement.

3) Art. 2 (1) b) shall enter into force at the same time as the Decision of the EEA Joint Committee no. 27/2023 of 3 February 2023 amending Protocol 31 (cooperation in specific fields outside the four freedoms) to the EEA Agreement.

In representation of the Prince Regnant:
sig. *Alois*
Hereditary Prince

sig. *Daniel Risch*
Prime Minister of the
Principality of Liechtenstein