Act XXIII of 2023

on cybersecurity certification and cybersecurity supervision

Electronic information systems and digital devices have developed into a central feature of everyday life with the speedy digital transformation and interconnectedness of society. That development has lead also to the expansion of the digital threat landscape, which can impede the pursuit of economic activities, generate financial loss, and undermine user confidence, thus causing major damage to economic and social life. Moreover, cybersecurity is a key enabler for many critical sectors to successfully embrace the digital transformation and to fully grasp the economic, social and sustainable benefits of digitalisation. In view of the above, the National Assembly adopts the following Act:

Chapter I

GENERAL PROVISIONS

Section 1 For the purposes of this Act:

1. *data centre service* means a service that ensures centralised accommodation, interconnection and operation for IT and network equipment providing data storage, technical data processing, and data transfer services, including facilities and infrastructures for power supply and environmental control;

2. *penetration testing* means detecting the weaknesses and checking for the exploitable vulnerabilities of information and communications technology (hereinafter "ICT") systems and electronic information systems by simulating malicious attacks against security measures;

3. *internal IT security scan* means a security scanning process of assessing the vulnerability of an IT system directly from an internal network termination point;

4. *confidentiality* means the term as defined in the Act on the electronic information security of state and local government organs;

5. *incident* means the term as defined in the Act on the electronic information security of state and local government organs;

6. *DNS service provider* means an entity that provides any of the following services:

a) authoritative DNS service means a service directly enabling queries on domain name data processed by a domain name registration service provider that constitutes a part of the top-level domain name registration service;

b) recursive DNS service means a DNS service that directs domain name queries from users to the appropriate authoritative DNS service provider in the hierarchical distributed domain name system and forwards to the user the responses to queries by the authoritative DNS service provider;

c) DNS caching means the temporary storing of responses to domain name queries and serving user queries on the basis of stored domain name data;

7. *domain name* means the alphanumeric equivalent of an IP address used for communication over the internet;

8. *domain name registration service provider* means a service provider authorised to register a domain as a proxy of a top-level domain name registry;

9. *electronic information system* means the term as defined in the Act on the electronic information security of state and local government organs;

10. *European cybersecurity certification scheme* means a system as defined under point (9) of Article 2 of Regulation (EU) 2019/881 of the European Parliament and of the Council;

11. *cloud computing service* means a digital service that enables self-service network access to an elastic pool of on-demand scalable shared physical and virtual resources;

12. *cloud computing service provider* means an entity providing cloud computing services;

13. *manufacturer* means the manufacturer of an ICT product, the provider of an ICT service, and the manufacturer or provider of an ICT process;

14. *ICT process* means the term as defined in Regulation (EU) 2019/881 of the European Parliament and of the Council;

15. *ICT service* means the term ad defined by Regulation (EU) 2019/881 of the European Parliament and of the Council;

16. *ICT product* means the term as defined in Regulation (EU) 2019/881 of the European Parliament and of the Council;

17. *cybersecurity audit* means a scan or audit of compliance with cybersecurity requirements as regards an electronic information system;

18. *cyber threat* means the term as defined in Regulation (EU) 2019/881 of the European Parliament and of the Council;

19. *outsourced (managed) information and communication security service provider* means an outsourced (managed) information and communication service provider that provides cybersecurity risk management and related services;

20. *outsourced (managed) information and communication service provider* means an entity providing services related to the installation, management, operation and maintenance of ICT products, networks, infrastructure, applications or any other electronic information systems either at the establishment of the service user or remotely;

21. *social networking services platform* means a platform that enables end-users to connect, share, discover and communicate with each other across multiple devices;

22. *research organisation* means a research organisation within the meaning of the Act on scientific research, which has as its primary goal to conduct applied research or experimental development with a view to exploiting the results of that research for commercial purposes, but which does not include educational institutions;

23. *top-level domain name registry* means an entity which has been delegated a specific top-level domain and is responsible for administering the top-level domain, including the registration of domain names under the top-level domain, and the technical operation of the domain, including the operation of its name servers, the maintenance of its databases and the distribution of top-level domain zone files across name servers, irrespective of whether any of those operations are carried out by the entity itself or are outsourced, but excluding situations where top-level domain names are used by a registry only for its own use;

24. *conformity assessment* means an assessment procedure that confirms compliance with the requirements set for an ICT product, ICT process or ICT service;

25. *conformity assessment body* means the term as defined in Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93;

26. *statement of conformity* means a document issued by a manufacturer or service provider attesting that a given ICT product, ICT service or ICT process has been evaluated for compliance with specific security requirements laid down in a national cybersecurity certification scheme;

27. *conformity self-assessment* means the term as defined by Regulation (EU) 2019/881 of the European Parliament and of the Council;

28. *national cybersecurity certification scheme* means a comprehensive set of rules, technical requirements, standards and procedures developed in accordance with the principles of European cybersecurity schemes and adopted by the certification authority and that apply to the certification or conformity assessment of ICT products, ICT services and ICT processes in Hungary;

29. *national cybersecurity certificate* means a document issued by an independent third party, attesting that a given ICT product, ICT service or ICT process has been evaluated for compliance with specific security requirements laid down in a national cybersecurity certification scheme;

30. *online marketplace* means a service using software, including a website, part of a website or an application, operated by or on behalf of a trader which allows consumers to conclude distance contracts with other traders or consumers;

31. *availability* means the term as defined in the Act on the electronic information security of state and local government organs;

32. *integrity* means the term as defined in the Act on the electronic information security of state and local government organs;

33. *certification* means a conformity assessment activity carried out by an independent third party;

34. *content delivery network provider* means a network provider for a network of geographically distributed servers ensuring high availability, accessibility or fast delivery of digital content and services;

35. *remote vulnerability scan* means an IT security scan

a) scanning the external vulnerability of an electronic information system from the internet including free searches in public databases available on the internet, targeted information gathering, and mapping of the vulnerabilities of the services of accessible computers;

b) disclosing the vulnerabilities of web applications by automated and manual scanning;

c) searching for and mapping wireless access and connection points, evaluating encryption procedures and checking, using dedicated software or manually, whether encryption keys can be decrypted.

Section 2 The provisions of the Act on the Code of General Administrative Procedure shall apply to authority proceedings under this Act with the derogations and supplementations laid down in this Act, the Act on consumer protection, the Act on the market surveillance of products, and the Act on the Supervisory Authority of Regulatory Affairs, and with the supplementations provided for by the government decree laying down the rules on civil aviation security and on the powers, responsibilities and operational order of the Aviation Security Committee, and by the decree issued by the president of the Supervisory Authority of Regulatory Affairs (hereinafter "SARA").

Chapter II.

CERTIFICATION SCHEMES

1. Tasks of the certification authority

Section 3 (1) The provisions of this chapter shall apply to the authority's activities related to ICT product, ICT service or ICT process certification.

(2) The provisions of the Act on the activity of conformity assessment bodies shall not apply to the cybersecurity certification regulated in this chapter and the activity of the certification authority.

Section 4 (1) The tasks of the national cybersecurity certification authority within the meaning of Regulation (EU) 2019/881 of the European Parliament and of the Council (hereinafter the "certification authority") shall be performed as follows:

a) the tasks other than those specified in point *b)* shall be performed by SARA;

b) the tasks of the cybersecurity certification authority related to defence industry research, development, manufacturing and trade shall be performed by an authority designated by the Government.

(2) The national cybersecurity certification schemes, except for defence industry research, development, manufacturing and trade, shall be established by the president of SARA in a decree. As regards defence industry research, development, manufacturing and trade, the certification schemes shall be established by the Government in a decree, taking account of the national cybersecurity certification schemes.

Section 5 (1) Regarding European cybersecurity certification schemes, the certification authority

a) shall monitor the development of European cybersecurity certification schemes and processes in standardisation;

b) shall participate in the work of the European Cybersecurity Certification Group;

c) shall gather information on sectors and fields that are not covered by a European cybersecurity certification scheme and for which it is necessary to enhance cybersecurity;

d) shall, as appropriate, provide information and support to stakeholders;

e) shall provide the information under Article 57 (4) of Regulation (EU) No 2019/881 of the European Parliament and of the Council.

(2) Regarding the maintenance of national cybersecurity certification schemes, the certification authority

a) shall at least every three years assess the national cybersecurity certification schemes in force with regard to current security risks;

b) shall without delay take measures to review a national cybersecurity certification scheme when a cause for review arises;

c) shall without delay take measures to review and set aside any national cybersecurity certification scheme on the same subject matter when a European cybersecurity certification scheme is issued.

(3) In respect of the tasks referred to in paragraph (1) *b)* and *e)*, SARA shall act as certification authority.

2. Requirements of national cybersecurity certification schemes

Section 6 The national cybersecurity certification scheme shall achieve the following security objectives:

a) to protect stored, transmitted or otherwise processed data against accidental or unauthorised storage, processing, access or disclosure during the entire life cycle of the ICT product, ICT service or ICT process;

b) to protect stored, transmitted or otherwise processed data against accidental or unauthorised destruction, loss or alteration or lack of availability during the entire life cycle of the ICT product, ICT service or ICT process;

c) to ensure that authorised persons, programs or machines are able only to access the data, services or functions to which their access rights refer;

d) to identify and document known dependencies and vulnerabilities;

e) to record which data, services or functions that require protection have been accessed, used or otherwise processed, at what times and by which authorised person, program or machine;

f) to make it possible to check which data, services or functions have been accessed, used or otherwise processed, at what times and by which authorised person, program or machine;

g) to verify that ICT products, ICT services and ICT processes do not contain known vulnerabilities;

h) to restore the availability of and access to data, services and functions in a timely manner in the event of a physical or technical incident;

i) to ensure that ICT products, ICT services and ICT processes are secure in proportion to the risks, by default and by design;

j) to ensure that ICT products, ICT services and ICT processes are provided with up-to-date software and hardware; and

k) to ensure that ICT products, ICT services and ICT processes do not contain publicly known vulnerabilities and are provided with mechanisms for secure updates.

Section 7 (1) The national cybersecurity certification scheme shall include the following:

a) the subject matter and scope of the certification scheme, and the type or categories of ICT products, ICT services and ICT processes;

b) a clear description of the purpose of the certification scheme and of how the selected standards, evaluation methods and assurance levels correspond to the needs of the intended users of the scheme;

c) references to the international, European or national standards applied in the evaluation or, where such standards are not available or appropriate, to technical specifications that meet the requirements set out in Annex II to Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council or, if such specifications are not available, to technical specifications or other cybersecurity requirements defined in the European cybersecurity certification scheme;

d) one or more assurance levels;

e) an indication of whether conformity self-assessment is permitted;

f) additional requirements to which persons and bodies carrying out conformity assessment are subject;

g) the specific evaluation criteria and methods to be used, including types of evaluation;

h) the conditions under which marks or labels may be used;

i) the content and the format of the national cybersecurity certificates and statements of conformity to be issued; and

j) the conditions for issuing, maintaining, continuing and renewing the national cybersecurity certificates issued under the scheme, as well as the conditions for the period of validity and for extending or reducing the scope of such certifications.

(2) If the national cybersecurity certification scheme specifies multiple assurance levels, the requirements shall include a precise distinction between the requirements for the various assurance levels.

(3) The national cybersecurity certification scheme shall specify the following:

a) the assessment procedures relating to the specific requirements or sets of requirements;

b) the critical security functions for which internal IT security or remote vulnerability scan or penetration testing, cryptographic assessments, or security source code analysis must be carried out, also allowing ex-post monitoring of the activity; and

c) the requirements for the documentation of evaluation results.

3. Assurance levels of national cybersecurity certification schemes

Section 8 (1) The national cybersecurity certification schemes may specify one or more of the following assurance levels for ICT products, ICT services and ICT processes: ‘basic’, ‘substantial’ or ‘high’.

(2) The assurance level shall provide assurance that the ICT products, ICT services and ICT processes concerned meet the corresponding security requirements and security functionalities, and that they have been evaluated

a) at assurance level ‘basic’ which is intended to minimise the known basic risks of incidents and attacks;

b) at assurance level ‘substantial’ which is intended to minimise the known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources;

c) at assurance level ‘high’ which is intended to minimise the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources.

(3) The assurance level shall be commensurate with the level of the risk associated with the intended use of the ICT product, ICT service or ICT process, in terms of the probability and impact of incidents.

(4) The evaluation activities to be undertaken shall include at least the following:

a) for assurance level ‘basic’, a review of the technical documentation with regard to compliance with the requirements of the given certification scheme;

b) for assurance level ‘substantial’:

ba) a review of the technical documentation with regard to compliance with the requirements of the given certification scheme;

bb) a review to demonstrate the absence of publicly known vulnerabilities; and

bc) testing to demonstrate that the ICT products, ICT services or ICT processes correctly implement the necessary security functionalities;

c) for assurance level ‘high’:

ca) a review of the technical documentation with regard to compliance with the requirements of the given certification scheme;

cb) a review to demonstrate the absence of publicly known vulnerabilities;

cc) testing to demonstrate that the ICT products, ICT services or ICT processes correctly implement the necessary security functionalities at the state of the art; and

cd) an assessment of their resistance to attacks carried out by skilled actors, using penetration testing.

4. Requirements for cybersecurity certifications and statements of conformity

Section 9 (1) The national cybersecurity certificate and the national statement of conformity shall specify the following:

a) the national cybersecurity certification scheme under which the certificate or statement is issued;

b) the assurance level; and

c) the technical specifications, standards and procedures related thereto.

(2) The national cybersecurity certificate and the national statement of conformity shall indicate the following:

a) name and address of the issuing body;

b) date of issuance;

c) name and address of the manufacturer;

d) reference to the entity on behalf of whom conformity assessment is carried out;

e) application areas or, if in the given application areas conformity only applies if certain conditions are fulfilled, these conditions;

f) period of validity;

g) identification of the ICT product, ICT service and ICT process to which certification relates, including, if applicable, its version number; and

h) signature by the issuer.

(3) The manufacturer of the ICT product, ICT service or ICT process that has been certified or for which a statement of conformity has been issued shall without delay inform the certification authority of any vulnerabilities or irregularities concerning the security of the ICT product, ICT service or ICT process.

Section 10 (1) A conformity mark in the form set out in the national or European cybersecurity certification scheme shall be affixed to ICT products, ICT services and ICT processes that have been certified or for which a statement of conformity has been issued in a manner provided for in a decree of the president of SARA or, where section 4 (1) *b)* applies, of the Government.

(2) The unauthorised affixing of the conformity mark referred to in paragraph (1) shall be prohibited; moreover, it shall be prohibited to affix a mark which resembles the form of the conformity mark or gives the impression that the ICT product, ICT service or ICT process is certified or a statement of conformity has been issued for it, and may thus mislead a third party.

5. Conformity self-assessment, conformity assessment

Section 11 (1) Conformity self-assessment may be carried out only if the national cybersecurity certification scheme permits it in relation to ICT products, ICT services and ICT processes that present a low risk corresponding to assurance level ‘basic’.

(2) The manufacturer shall issue a national statement of conformity stating that the fulfilment of the requirements set out in the national cybersecurity certification scheme has been checked. As part of the check, the fulfilment of the requirements set out in the national cybersecurity certification scheme shall be assessed in accordance with the methodology specified in the certification scheme.

(3) The manufacturer that carries out the conformity self-assessment shall send a copy of the statement of conformity, the technical documentation, the assessment report drawn up in accordance with the assessment method specified in the national cybersecurity certification scheme, and all other relevant assessment information relating to the conformity with the certification scheme indicated to the certification authority for them to be entered in a record within 15 days following the issuance of the statement of conformity referred to in paragraph (2).

Section 12 Third party conformity assessment activities may be carried out only by a body that

a) has been accredited by the accreditation body appointed pursuant to the Act on national accreditation having regard to the requirements set out in the applicable national or European cybersecurity certification scheme, or, if the body has been accredited in another country, this status of it is recognised by the said accreditation body;

b) meets the requirements laid down in a decree of the president of SARA for each assurance level; and

c) is registered with the certification authority.

6. Supervision of cybersecurity certification

Section 13 (1) Summary procedure shall not be applicable to proceedings of the certification authority.

(2) For the certification authority, administrative time limit shall be 120 days.

(3) In relation to a European cybersecurity certification scheme, the certification authority shall notify the conformity assessment body accredited by the national accreditation body to the European Commission (hereinafter the "Commission") within 15 days from when the decision on the entry into the official register reaches administrative finality. The applicant body shall provide evidence of its accreditation status by attaching the decision of the national accreditation body.

(4) The certification authority shall conduct an authorisation procedure for the conformity assessment body if the national or European cybersecurity certification scheme covering the ICT product, ICT service or ICT process

a) sets out additional requirements, and therefore, the conduct of an authorisation procedure becomes necessary; or

b) requires an assurance level 'high' for cybersecurity certifications to be issued under the scheme, and the certification authority delegates the task of issuing such certificates to the conformity assessment body either regarding certain national or European cybersecurity certificates or in general.

(5) Where paragraph (4) *b)* applies, authorisation shall be granted on the condition that the conformity assessment body qualifies as an economic operator entitled to perform a vulnerability scan within the meaning of the Act on the electronic information security of state and local government organs.

(6) The validity of the authorisation under paragraph (4) shall run until no later than the expiry of the accreditation status.

(7) In relation to a European cybersecurity certification scheme, if the certification authority conducts an authorisation procedure under paragraph (4), it shall notify the conformity assessment body to the Commission within 15 days from when the decision on granting the authorisation reaches administrative finality.

(8) Within its cybersecurity certification supervisory tasks the certification authority shall be entitled

a) to request conformity assessment bodies and issuers of statements of conformity to provide any information and data necessary for the performance of the tasks of the authority; and

b) to conduct administrative audits of conformity assessment bodies and issuers of statements of conformity.

(9) For proceedings by the certification authority, administrative service fee shall be paid. The level of the administrative service fee and the detailed rules concerning the collection, distribution, management, registration and reimbursement of this fee shall be determined

a) in a decree of the president of SARA on administrative service fee payable for cybersecurity certification in connection with proceedings by the national cybersecurity certificate with regard to proceedings conducted by the certification authority referred to in section 4 (1) *a)*,

b) in a ministerial decree issued to implement this Act with regard to proceedings conducted by the certification authority referred to in section 4 (1) *b).*

Section 14 (1) The certification authority shall keep records of, and process

a) the data of the statements of conformity made available by the manufacturer of ICT products, ICT services or ICT processes;

b) the technical documentation attached to statements of conformity, and other information relating to the conformity of the ICT products, ICT services or ICT processes with the certification scheme;

c) the data required for the identification of the conformity assessment body and its designated contact point, furthermore, if the conformity assessment body is a public body within the meaning of Article 56 (5) of Regulation (EU) 2019/881 of the European Parliament and of the Council, a reference thereto, and the documents that support that the requirements set out in the decree of the president of SARA are met;

d) information provided in the decision relating to the accreditation status of the conformity assessment body accredited by the national accreditation body and relating to any change in the accreditation status;

e) the application, data and documents connected to the authorisation proceeding under section 13 (4) if such a proceeding needs to be conducted;

f) data relating to the authorisation granted under the authorisation procedure, its suspension and partial or complete withdrawal, as well as reference to its becoming ineffective;

g) the data required for the identification of the delegated power if the certification authority delegated the right to issue cybersecurity certifications at assurance level ‘high’ to a conformity assessment body;

h) the identifier assigned to the conformity assessment body upon registration by the Commission;

i) the data required for the identification of any contributor employed by the conformity assessment body and the designated contact point;

j) the data of the certificate issued by the conformity assessment body;

k) the data required for the identification of the manufacturer and the designated contact point;

l) information related to the refusal of issuance, restriction, suspension, and withdrawal, of certificates;

m) information related to any vulnerabilities or irregularities referred to in section 9 (3);

n) data and documents of which it became aware in the course of carrying out supervisory activities; and

o) data and documents relating to complaints lodged.

(2) For data referred to in paragraph (1) *f)* and *g)*, a register under paragraph (1) shall qualify as publicly certified register.

(3) The purpose of the processing of the data referred to in paragraph (1) shall be to keep information related to the security of ICT products, ICT services or ICT processes updated, as well as to perform the tasks connected to vulnerabilities or irregularities affecting them and the audit and supervisory authority activities of the certification authority.

(4) Unless otherwise provided by the law, data transfer regarding the data contained in a register under paragraph (1) may be performed to the following organisations:

a) to the Commission for the compilation and updating of the list of the conformity assessment bodies notified;

b) to the accreditation body appointed pursuant to the Act on national accreditation for the performance of the tasks related to the accreditation and supervision of the activities of conformity assessment bodies; and

c) to incident management centres referred to in the Act on the electronic information security of state and local government organs for the performance of activities related to vulnerabilities or irregularities referred to in section 9 (3).

(5) The conformity assessment body and the manufacturer shall send to the certification authority for registration the data referred to in paragraph (1) and the changes in the data within 8 days from the date on which they become available and from the date on which the change occurs respectively.

Section 15 (1) If the certification authority becomes aware or, in the course of an audit, establishes that the conformity assessment body or the manufacturer does not meet, or does not comply with, the security requirements set out in the applicable EU or Hungarian law and the related procedural rules, it shall call upon the conformity assessment body or the manufacturer to meet the security requirements set out in the applicable EU and Hungarian law and the related procedural rules, setting a time limit in its decision on warning.

(2) If, despite what is stated in paragraph (1), the conformity assessment body or the manufacturer does not meet, or does not comply with, the security requirements set out in the law and the related procedural rules, the certification authority, having regard to all the circumstances of the case, may impose a fine in accordance with the provisions laid down in a government decree; in the case of continued non-compliance, the fine may be imposed again.

Section 16 (1) The certification authority shall process any classified data, personal data or sensitive data as well as any other data protected by law and classified as trade secret, bank secret, payment secret, insurance secret, securities secret, fund secret, medical secret or secret related to the exercise of a profession that it obtains when performing its task only for the period of performing the task, observing the purpose limitation principle. The certification authority shall record the data supporting the conclusions drawn from the administrative audit, and shall process the data thus recorded until the last day of the 10th year following the termination of the accreditation status of the conformity assessment body or until the last day of the 10th year from when the statement of conformity becomes ineffective, with the proviso that if, for the ICT product, ICT service or ICT process subject to the audit, both a certificate issued by the conformity assessment body and a conformity self-assessment are available, the date to be taken into account shall be the later of the date the accreditation status terminates and the date the statement of conformity becomes ineffective. Then the certification authority shall erase the data from its electronic information systems and data-storage mediums.

(2) Unless otherwise provided in an Act, the data generated in the course of the proceedings of the certification authority shall not be public.

(3) Subject to the exceptions provided for in the law, the staff members of the certification authority shall be under an obligation of secrecy with respect to the data obtained in accordance with paragraph (1); the secrecy obligation shall apply for a period of 5 years following the termination of the employment-related relationship or, for classified data, until the end of their period of validity or, for personal data, without a time limit.

(4) The certification authority shall perform its certification authority activity, the administrative audits and its tasks related to record-keeping in accordance with a decree of the president of SARA or, for a certification authority under section 4 (1) *b)*, of the Government.

(5) The manufacturer in carrying out conformity self-assessment and the conformity assessment body in the course of certification shall act in accordance with a decree of the president of SARA or, for a certification authority under section 4 (1) *b)*, of the Government.

Chapter III

CYBERSECURITY SUPERVISION

7. Entities subject to cybersecurity supervision

Section 17 (1) The provisions of this Chapter shall apply to the electronic information systems of

a) service providers and organisations operating in sectors of high criticality listed in Annex 1; and

b) service providers and organisations operating in critical sectors listed in Annex 2

(hereinafter jointly “supervised entity”).

(2) The rules laid down in this Chapter shall not apply to micro and small undertakings within the meaning of the Act on small and medium-sized undertakings and the support of their development, except where the supervised entity is

a) an electronic communications service provider;

b) a trust service provider;

c) a service provider providing DNS service;

d) a top-level domain name registry; or

e) a domain name registration service provider.

(3) The rules laid down in this Chapter shall not apply to supervised entities' electronic information systems and networks for national defence purposes within the meaning of the Act on the electronic information security of state and local government organs.

Section 18 The rules laid down in this Chapter shall not apply to the protection of electronic information systems contributing to critical activities of system elements designated, in accordance with the Act on the identification, designation and protection of critical systems and facilities, as European or national critical system elements within the meaning of the Act on the electronic information security of state and local government organs, and of programmable systems falling within the scope of the government decree on physical protection and the related authorisation, reporting and monitoring system in the context of nuclear energy use.

8. Basic requirements

Section 19 (1) A supervised entity shall ensure a level of security of electronic information systems and their physical environment appropriate to the degree of damage cyber threats may cause.

(2) Security referred to in paragraph (1) shall include the protection of electronic information systems and their physical environment against all incidents that might compromise the confidentiality, integrity and availability of

a) stored, transmitted or technically processed data and information; or

b) services provided by or available through electronic information systems.

(3) The protection specified in paragraph (2) shall include the following:

a) the system of information security management;

b) the identification and management of the risks of electronic information systems;

c) the application of administrative, logical and physical measures aimed at mitigating risks that correspond to the security class to be determined for each system in the risk assessment of the organisation;

d) the prevention, detection and management of security incidents and the mitigation of their impact;

e) the ensuring of business continuity; and

f) the acquisition, development and operation of electronic information systems and the software and hardware products used by them.

(4) If a supervised entity employs a contributor to establish, operate, maintain or repair the electronic information system, the contributor shall also meet the requirements set out in paragraph (3).

(5) The head of the supervised entity shall ensure that the requirements set out in paragraphs (1) to (3) are included in a contract for the contributor referred to in paragraph (4).

(6) The head of the supervised entity shall

a) determine the tasks and responsibilities of the person responsible for the security of electronic information systems;

b) determine the rules applicable to users of electronic information systems;

c) provide for regular information security trainings for, and maintaining the knowledge of, the staff members of the organisation.

Section 20 (1) The supervised entity shall assign electronic information systems and data stored, transmitted and technically processed in them to security classes observing the criteria specified in a decree by the Minister responsible for the direction of civilian national security services.

(2) As a result of security classification, security classes ‘basic’, ’substantial’ and ’high’ shall apply according to the risk of harming confidentiality, integrity and availability.

(3) The specific protective measures to be applied for each security class shall be determined in a decree by the Minister responsible for the direction of civil national security services.

(4) To certify compliance with the specific requirements set out in section 19 (1) to (4), an ICT product, ICT service or ICT process certified under a European or national cybersecurity certification scheme may be used where available.

(5) Supervised entities listed in a decree by the president of SARA shall use ICT products, ICT services or ICT processes certified under a European or national cybersecurity certification scheme that is specified in the decree by the president of SARA.

Section 21

9. Tools of cybersecurity supervision

Section 22 (1) The SARA shall carry out the cybersecurity supervision of supervised entities and their electronic information systems as regards the requirements set out in sections 19 and 20.

(2)

(3)

(4)

(5)

(6)

(7)

(8)

(9)

Section 23 (1) To evidence compliance with the cybersecurity requirements under this Act, a supervised entity shall have an independent auditor entitled to perform such an activity (hereinafter the "auditor") carry out a cybersecurity audit every two years.

(2)

(3)

(4) An auditor shall be entitled to carry out a cybersecurity audit if the auditor has the skills and meets the infrastructural conditions for the performance of such a task and who qualifies as an economic operator entitled to perform a vulnerability scan within the meaning of the Act on the electronic information security of state and local government organs. The requirements for an auditor shall be set out in a decree by the president of SARA.

(5)

(6) The SARA shall keep a register of economic operators entitled to carry out audit in accordance with the provisions of the decree by the president of SARA.

(7) The register shall include the following:

a) data of the auditor and the natural identification data, telephone number and electronic mailing address of the designated contact point of the auditor required for identification;

b) the identifier of the auditor received upon registration;

c) data of the contributor engaged by the auditor and the natural identification data, telephone number and electronic mailing address of his designated contact point of the contributor required for identification; and

d) the document containing the findings of the audit.

(8)

(9)

(10)

(11) The auditor shall specify in regulations the positions the holders of which may access trade secrets and learn their contents in the course of an audit. Persons participating in an audit shall be under the obligation of secrecy with respect to personal data and trade secrets obtained in the course of the audit; the secrecy obligation shall apply for a period of 5 years following the termination of the employment-related relationship or, for personal data, without a time limit.

(12) A cybersecurity audit under this Chapter shall be without prejudice to any certification obligation prescribed by another law.

(13)

Section 24

Section 25

Section 26 (1) The SARA shall keep a register of supervised entities in accordance with the provisions of the decree by the president of SARA that contains the following:

a) data for the identification of the supervised entity;

b) for a supervised entity that is not an organisation established in the European Union but that offers services in Hungary and designates a representative established in Hungary, the name or company name, mailing address, telephone number and electronic mailing address of the representative;

c) natural identification data, telephone number and electronic mailing address of the person responsible for the security of the electronic information system;

d) further data specified in the decree by the president of SARA not qualifying as personal data.

(2) A supervised entity shall send for registration the data specified in paragraph (1) to SARA within 30 days after the commencement of its operation.

(3) A supervised entity shall

a) enter into an agreement for the performance of a cybersecurity audit referred to in section 23 (1) with an auditor included in the register referred to in section 23 (6) within 120 days following its registration; and

b) have a cybersecurity audit referred to in section 23 (1) carried out for the first time within two years following its registration.

(4) A supervised entity shall send for registration any changes to the data referred to in paragraph (1) within 15 days following the change.

(5) Unless otherwise provided by the law, data transfer from the register under paragraph (1) may be performed exclusively to organisations performing the tasks of an authority and to incident management centres specified in the Act on the electronic information security of state and local government organs.

(6) The Government shall lay down in a decree the detailed rules on cooperation and data provision between SARA and authorities referred to in the Act on the electronic information security of state and local government organs.

(7) If a supervised entity no longer performs any activity falling under the scope of this Act, SARA shall delete from the register the data referred to in paragraph (1) five years after the notification of the termination of the activity.

(8) Should a supervised entity notify any change to the data referred to in paragraph (1), SARA shall delete from the register the original data five years after the notification of the change to the data concerned.

10.

Section 27

Chapter IV

FINAL PROVISIONS

11. Authorising provisions

Section 28 (1) Authorisation shall be given to the Government to determine in a decree

a) the level of the fine that the certification authority can impose, the criteria for determining this fine, and the detailed procedural rules on the manner in which this fine is to be paid,

b) the detailed rules on the task of the certification authority under section 4 (1) *b)*, the procedure governing the certification authority activity, the authorisation procedure, the administrative audit and the record-keeping, as well as the content excluding personal data of the records, as well as the rules for affixing the conformity mark,

c) the detailed rules on conformity self-assessment, certification and the obligations and activity of the conformity assessment bodies with respect to defence industry research, development, manufacturing and trade,

d) the certification schemes with respect to defence industry research, development, manufacturing and trade, taking account of the national cybersecurity certification schemes,

e)

f)

g)

(2) Authorisation shall be given to the Government to appoint in a decree the certification authority under section 4 (1) *b).*

(3) Authorisation shall be given to the president of SARA to determine in a decree

a) the detailed rules on the procedure governing the certification authority activity, the authorisation procedure, the administrative audit and the record-keeping, and the content excluding personal data of the records, as well as the rules for affixing the conformity mark, except for the certification authority activity under section 4 (1) *b),*

b) the detailed rules on conformity self-assessment, certification, the requirements for conformity assessment bodies, as well as the obligations and activity of the conformity assessment bodies, except for defence industry research, development, manufacturing and trade,

c) the national cybersecurity certification schemes except for defence industry research, development, manufacturing and trade,

d) ICT products, ICT services and ICT services certified under national or European cybersecurity certification scheme the use of which is mandatory under section 20 (5), and the supervised entities obliged to use them;

e)

f) the rules governing the registration of supervised entities in the cybersecurity supervision official register and the detailed rules on data included in the register not qualifying as personal data;

g)

h) the rules governing the registration of auditors and the requirements for auditors;

i)

j)

(4) Authorisation shall be given to the Minister responsible for national defence to determine in a decree

a) in agreement with the Minister responsible for taxation policy, the level of the administrative service fee payable for proceedings by the certification authority under section 4 (1) *b)* and the detailed rules concerning the collection, distribution, management, registration and reimbursement of this fee, and

b) the requirements for conformity assessment bodies with respect to defence industry research, development, manufacturing and trade.

(5) Authorisation shall be given to the Minister responsible for the direction of civilian national security services to determine in a decree the requirements for security classification and the specific protective measures to be applied for each security class.

(6) The Minister responsible for the direction of civilian national security services shall issue the decree referred to in paragraph (5) after seeking the opinion of the president of SARA.

12. Provisions on entry into force

Section 29 (1) With the exceptions specified in paragraphs (2) to (4), this Act shall enter into force on the 8th day following its promulgation.

(2) Section 15 and section 28 (1) *a)* shall enter into force on the 16th day following the promulgation of this Act.

(3) Subtitle 7, section 19, section 20, section 22 (1), section 23 (1), (4), (6), (7), (11) and (12), section 26, section 28 (3) *d), f)* and *h),* section 28 (5) and (6), section 30 (1), (2), (4) and (5), section 40, section 42, section 48 and annexes 1 and 2 shall enter into force on 1 January 2024.

(4) Section 21, section 22 (2) to (9), section 23 (2), (3), (5), (8) to (10) and (13), section 24, section 25, subtitle 10), section 28 (1) *e)* to *g),* section 28 (3) *e), g), i)* and *j),* section 30 (3), sections 33 to 37, section 38 *a)* and *c),* section 46 and section 49 shall enter into force on 18 October 2024.

13. Transitional provisions

Section 30 (1) A supervised entity that commenced its operation before 1 January 2024 shall send he data referred to in section 26 (1) to SARA for registration by 30 June 2024 for the first time.

(2) A supervised entity that commenced its operation before 1 January 2024 shall apply the specific protective measures referred to in section 20 (3) determined in a decree by the Minister responsible for the direction of civilian national security services from 18 October 2024.

(3)

(4) A supervised entity that commenced its operation before 18 October 2024 shall meet its obligation under section 26 (3) *a)* by 31 December 2024 at the latest.

(5) A supervised entity that commenced its operation before 1 January 2024 shall have the first cybersecurity audit referred to in section 23 performed by 31 December 2025.

14. Compliance with the requirement of the Fundamental Law on cardinality

Section 31 Sections 39 to 42, sections 47 to 49 and section 51 qualify as cardinal on the basis of Article 23 of the Fundamental Law.

15. Compliance with the law of the European Union

Section 32 (1) This Act contains provisions for the implementation of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

(2) This Act serves the purpose of compliance with Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

16. Amending provisions

Section 33

Section 34

Section 35

Section 36

Section 37

Section 38 The following shall be repealed in Act L of 2013 on the electronic information security of state and local government organs:

a)

b)

c)

d)

e)

f)

g)

h)

i)

j)

k)

Section 39

Section 40

Section 41

Section 42

Section 43

Section 44

Section 45

Section 46

Section 47

Section 48

Section 49

Section 50

Section 51

Annex 1 to Act XXIII of 2023

Service providers and organisations operating in sectors of high criticality

	A	B	C
1	Sector	Subsector	Organisation
2	Energy	Electricity	electricity undertakings within the meaning of the Act on electricity with the exception of public lighting operating licence holders;
3		District heating and cooling	licence holders within the meaning of the Act on district heating
4		Oil	*a)* licence holders establishing and operating hydrocarbon transmission lines; *b)* operators of facilities used for processing and storing oil under the Act on mining;
5			central stockholding entities under the Act on emergency stockholding of imported petroleum and petroleum products;
6		Gas	gas industry undertakings engaged in activities requiring a licence under the Act on gas supply with the exception of one-stop-shop capacity sellers, organised gas market licence holders and piped LPG providers;
7		Hydrogen	operators of hydrogen production, storage and transmission;
8	Transport	Air transport	organisations contributing to air transport security within the meaning of the government decree on the rules of civil aviation security and on the powers, tasks and operational rules of the Aviation Security Committee;
9		Rail transport	railway infrastructure managers other than managers of private railways infrastructure and industrial sidings, railway undertakings, and rail capacity allocation organisations within the Act on rail transport;
10		Road transport	*a)* service providers operating intelligent road transport systems; *b)* traffic management organisations; within the meaning of the decree issues on the basis of authorisation by the Act on road traffic;
11		Water transport	legal persons and economic operators without legal personality engaged in shipping activitites within the meaning of the Act on waterway traffic;

12		Public transport	public service operators within the meaning of Article 2 *d)* of Regulation (EC) No 1370/2007 of the European Parliament and of the Council of 23 October 2007 on public passenger transport services by rail and by road and repealing Council Regulations (EEC) Nos 1191/69 and 1107/70;
13	Health		healthcare providers within the meaning of the Act on healthcare; operators of high-security biological laboratories; organisations managing healthcare reserves and blood supplies; entities carrying out research and development activities of medicinal products; entities manufacturing basic pharmaceutical products and pharmaceutical preparations; medicinal product wholesalers; entities manufacturing medical devices considered to be critical included in the list of devices considered to be critical during a public health emergency; organisations holding a distribution authorisation under Article 79 of Directive 2001/83/EC of the European Parliament and the Council of 6 November 2001 on the Community code relating to medicinal products for human use;
14	Drinking water, waste water	Water utility services	water utility service providers within the meaning of the Act on water utility services;
15	Electronic communications services		*a)* electronic communications service providers and *b)* internet exchange service providers within the meaning of the Act on electronic communications;
16			trust service providers within the meaning of the Act on the general rules on electronic administration and trust services;
17	Digital infrastructure		cloud computing service providers;
18			data centre service providers;
19			top-level domain name registries;
20			DNS service providers;
21			content delivery network providers;
22	Outsourced ICT services		*a)* outsourced (managed) information and communication service providers; *b)* outsourced (managed) information and communication security service providers;
23	Space-based services		operators of ground-based infrastructure supporting the provision of space-based services

Annex 2 to Act XXIII of 2023

Service providers and organisations operating in critical sectors

	A	B	C
1	Sector	Subsector	Type of entity
2	Postal and courier services		postal service providers within the Act on postal services;
3	Production, processing and distribution of food		food businesses within the meaning of the Act on the food chain and its authority supervision;
4	Waste management		entities carrying out an activity under the Act on waste
5	Production and distribution of chemicals		manufacturers and distributors within the meaning of Article 3 of Regulation (EC) No 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH), establishing a European Chemicals Agency, amending Directive 1999/45/EC and repealing Council Regulation (EEC) No 793/93 and Commission Regulation (EC) No 1488/94 as well as Council Directive 76/769/EEC and Commission Directives 91/155/EEC, 93/67/EEC, 93/105/EC and 2000/21/EC;
6	Manufacturing	Manufacture of medical devices and in vitro diagnostic medical devices	entities manufacturing medical devices within the meaning of Article 2, point (1) of Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, or in vitro diagnostic medical devices within the meaning of Article 2, point (2) of Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU other than entities manufacturing medical devices considered to be critical included in the list of devices considered to be critical during a public health emergency;
7		Manufacture of computer, electronic and	economic operators carrying out the activity of 'Manufacture of computer, electronic and optical products' under Division 26 of Regulation (EC)

		optical products	No 1893/2006 of the European Parliament and of the Council of 20 December 2006 establishing the statistical classification of economic activities NACE Revision 2 and amending Council Regulation (EEC) No 3037/90 as well as certain EC Regulations on specific statistical domains;
8		Manufacture of electrical equipment	economic operators carrying out the activity of 'Manufacture of electrical equipment' under Division 27 of Regulation (EC) No 1893/2006 of the European Parliament and of the Council of 20 December 2006 establishing the statistical classification of economic activities NACE Revision 2 and amending Council Regulation (EEC) No 3037/90 as well as certain EC Regulations on specific statistical domains;
9		Manufacture of machinery and equipment n.e.c.	economic operators carrying out the activity of 'Manufacture of machinery and equipment n.e.c.' under Division 28 of Regulation (EC) No 1893/2006 of the European Parliament and of the Council of 20 December 2006 establishing the statistical classification of economic activities NACE Revision 2 and amending Council Regulation (EEC) No 3037/90 as well as certain EC Regulations on specific statistical domains;
10		Manufacture of motor vehicles, trailers and semi-trailers	economic operators carrying out the activity of 'Manufacture of motor vehicles, trailers and semi-trailers' under Division 29 of Regulation (EC) No 1893/2006 of the European Parliament and of the Council of 20 December 2006 establishing the statistical classification of economic activities NACE Revision 2 and amending Council Regulation (EEC) No 3037/90 as well as certain EC Regulations on specific statistical domains;
11		Manufacture of other transport equipment	economic operators carrying out the activity of 'Manufacture of other transport equipment' under Division 30 of Regulation (EC) No 1893/2006 of the European Parliament and of the Council of 20 December 2006 establishing the statistical classification of economic activities NACE Revision 2 and amending Council Regulation (EEC) No 3037/90 as well as certain EC Regulations on specific statistical domains;
12		Manufacture of cement, lime and plaster	economic operators carrying out the activity of 'Manufacture of cement, lime and plaster' under Division 23.5 of Regulation (EC) No 1893/2006 of the European Parliament and of the Council of 20 December 2006 establishing the statistical classification of economic activities NACE

			Revision 2 and amending Council Regulation (EEC) No 3037/90 as well as certain EC Regulations on specific statistical domains;
13	Digital providers		*a)* providers of online marketplaces; *b)* search provider within the meaning of Act CVIII of 2001; *c)* providers of social networking services platforms; *d)* domain name registration service provider;
14	Research		research organisations