Act LXIX of 2024

on the cybersecurity of Hungary

[1] It is essential for our nation, having regard to current threats to information society, to reduce threats to electronic information systems and to ensure the continuity of services in key sectors.

[2] Society expects the closed, comprehensive, continuous and risk-proportionate protection of the confidentiality, integrity, availability of data and information processed in electronic information systems that are indispensable for the State and its citizens, and through this, the security of cyberspace, which contributes to ensuring the security and bolstering the resiliency and competitiveness of both Hungary and the European Union.

[3] Electronic information systems and digital devices have developed into a central feature of everyday life amidst the rapid digital transformation and interconnectedness of society. This development has also led 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 harness the economic, social and sustainable benefits of digitalisation.

[4] In view of the above and the EU Directive on measures for a high common level of cybersecurity across the Union, the National Assembly adopts the following Act:

Chapter I

GENERAL PROVISIONS

1. Scope of the Act

Section 1 (1) The provisions of this Act on the obligations of entities and on cybersecurity authority supervision shall apply to the following:

a) entities within the administrative sector listed in Annex 1,

b) economic operators under majority state control to which point a) does not apply and that meet at least one of the following conditions:

ba) the total number of employees reaches or exceeds 50 persons; or

bb) the annual net turnover and balance sheet total both exceed a forint amount corresponding to 10 million euro;

c) entities beyond the scope of points a), b) and d) to f) as well as Regulation (EU) 2022/2554 of the European Parliament and of the Council that are identified as essential or important entities in accordance with paragraph (6) by the national cybersecurity authority referred to in section 23 (1) a) (hereinafter the "national cybersecurity authority") or the national defence cybersecurity authority referred to in section 23 (2) (hereinafter "national defence cybersecurity authority");

d) entities listed in Annex 2 or 3 that qualify as medium-sized undertakings within the meaning of the Act on small and medium-sized undertakings and the support of their development, or exceed the threshold set for medium-sized undertakings, and to which point a) does not apply;

e) entities listed in Annex 2 or 3, regardless of size, to which point a) does not apply provided that the entity concerned qualifies as one of the following:

ea) an electronic communications service provider;

eb) a trust service provider;

ec) a DNS service provider;

ed) a top-level domain name registry; or

ee) a domain name registration service provider; as well as

f) companies carrying out activities relating to national defence interests.

(2) For critical entities and critical infrastructure designated in accordance with the Act on the resilience of critical entities (hereinafter the "Critical Entity Resilience Act") (hereinafter jointly "critical entity") and entities and infrastructure important for the defence and security of the country designated in accordance with the Act on the coordination of defence and security activities (hereinafter the "Defence and Security Activities Coordination Act") (hereinafter jointly "entity important for the defence and security of the country"), the classification of an entity under paragraph (1) shall be observed in the application of the provisions of this Act, except where the critical entity or the entity important for the defence and security of the country falls within the scope of Regulation (EU) 2022/2554 of the European Parliament and of the Council.

(2a) Except for the provisions of sections 9 and 13 to 15, the provisions of this Act applicable to entities referred to in section 1 (1) a) shall apply to critical entities or entities important for the defence and security of the country that do not qualify as an entity listed in paragraph (1).

(3) Depending on the critical nature of the service provided for the operation of the State, the society or the economy and, in certain cases, the size of the entity, an entity is either am essential or an important entity.

(4) From among the entities referred to in paragraph (1), the following shall qualify as essential entities:

a) entities listed in Annex 1 other than offices of representative bodies of settlements of which the number of inhabitants does not exceed 20000;

b) entities referred to in paragraph (1) b);

c) entities identified as an essential entity by the national cybersecurity authority or the national defence cybersecurity authority;

d) critical entities designated in accordance with the Critical Entity Resilience Act;

e) entities important for the defence and security of the country designated in accordance with the Defence and Security Activities Coordination Act;

f) entities listed in Annex 2 that qualify as medium-sized undertakings within the meaning of the Act on small and medium-sized undertakings and the support of their development, or exceed the threshold set for medium-sized undertakings; and

g) qualified trust service providers and top-level domain name registries as well as DNS service providers, regardless of size;

h) companies carrying out activities relating to national defence interests.

(5) From among the entities listed in paragraph (1), the following shall qualify as important entities to which the provisions on entities shall apply with the derogations set out in this Act:

a) offices of representative bodies of settlements of which the number of inhabitants does not exceed 20000;

b) entities identified as an important entity by the national cybersecurity authority or the national defence cybersecurity authority;

c) entities listed in Annex 2 other than those qualifying as an essential entity; and

d) entities listed in Annex 3 other than those qualifying as an essential entity in accordance with paragraph (4) b) to e).

(6) As a condition for an identification proceeding referred to in paragraph (1) c), the entity shall

1. be the sole provider in Hungary of a service which is essential for the maintenance of critical societal or economic activities;

2. provide a service the disruption of which could have a significant impact on public order, public safety or public health;

3. provide a service the disruption of which could have a significant impact on critical societal or economic activities;

4. provide a service the disruption of which could induce a significant systemic risk, in particular for sectors where such disruption could have a cross-border impact;

5. be of specific importance at national or regional level for the particular sector or type of service, or for other interdependent sectors in Hungary;

6. be under national security protection in accordance with the government decision on the scope of organs and facilities under national security protection or its identification shall be considered justified by the national cybersecurity authority for a national security reason or by the national defence cybersecurity authority for a national defence or military national security reason;

7. provide a service in a sector under Annex 2 or 3 or a service that is necessary for the operation of the State to at least 20 000 persons;

8. provide a service to at least five entities within the scope of this Act;

9. be under majority state control;

10. be processor of state registers forming part of national data assets as set out by law;

11. provide processing for an essential or important entity;

12. qualify as a company under public ownership other than those within the scope of paragraph (1) b); or

13. develop an electronic information system as part of a project subsidised from budget and European Union funds

(7) The provisions of this Act on cybersecurity certification shall apply to activities relating to certification of information and communication technology (hereinafter "ICT") products, ICT services and ICT processes.

(8) The provisions of this Act on post-quantum cryptography shall apply to the following entities specified in a decree by the president of the Supervisory Authority of Regulatory Affairs (hereinafter the "SARA") (hereinafter "entity required to use post-quantum cryptography") and the activities for their authority supervision:

a) an entity subject to usage obligation within the meaning of the government decree on government networks; and

b) a public utility service provider within the scope of any of the following Acts and an entity providing a public service within the scope of laws adopted on the basis of authorisation by any of the following Acts:

ba) the Act on the supply of natural gas;

bb) the Act on emergency stockholding of natural gas;

bc) the Act on electricity;

bd) the Act on district heating;

be) the Act on water utility services;

bf) the Act on waste.

(9) The provisions on vulnerability scan of this Act shall apply to vulnerability scans relating to the following:

a) an electronic information system of an entity referred to in paragraph (1) a) to c) and f); and

b) an electronic information system specified in an agreement under section 61, with the derogations laid down in the agreement.

(10) The provisions of this Act on cybersecurity incident handling shall apply to the handling of cybersecurity incidents relating to the electronic information systems of the following:

a) entities referred to in paragraph (1); and

b) entities within the scope of Regulation (EU) 2022/2554 of the European Parliament and of the Council.

(11) In the event of a cybersecurity incident reported voluntarily by an entity other than an entity referred to in paragraph (10) or a person, the national cybersecurity incident handling centre shall proceed in accordance with this Act.

Section 2 (1) The provisions of this Act shall apply to the following:

a) entities referred to in section 1 that are established in Hungary or that have a representative established in Hungary;

b) electronic communications service providers providing services within the territory of Hungary;

c) DNS service providers, top-level domain name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, outsourced (managed) information and communication service providers, outsourced (managed) information and communication security service providers, providers of online market places, of online search engines and of social networking services platforms if the main establishment is within the territory of Hungary.

(2) The main establishment of an entity referred to in paragraph (1) c) shall be considered to be in Hungary if

a) decisions relating to cybersecurity risk management measures are predominantly taken in Hungary;

b) cybersecurity operations relating to the electronic information systems of the entity are carried out in Hungary; or

c) the establishment with the highest number of employees of the entity is within the territory of Hungary.

Section 3 (1) The scope of this Act shall not cover the following:

a) electronic information systems processing classified data;

b) electronic information systems for operational purposes;

c) 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; and

d) cybersecurity services provided by an organ designated in a decree by the Government.

(2) The Government shall determine in a decree the cybersecurity services referred to in paragraph (1) d) and the entities that are subject to an obligation to use them or that are entitled to use them.

(3) The provisions of this Act shall apply to electronic information systems for national defence purposes with the derogations provided for in this Act.

2. Interpretative provisions

Section 4 For the purposes of this Act:

1. *data* means the carrier of information, a formalised representation of facts, concepts and instructions suitable for communication, presentation and processing by human beings or automated devices;

2. *technical processing* means the term as defined by the Act on the right to informational self-determination and on the freedom of information;

3. *processor* means the term as defined by the Act on the right to informational self-determination and on the freedom of information;

4. *processing* means the term as defined by the Act on the right to informational self-determination and on the freedom of information;

5. *controller* means the term as defined by the Act on the right to informational self-determination and on the freedom of information;

6. *data exchange service* means the term as defined by the Act on electronic communications;

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

8. *data classification* means classification of data and information processed by the entity in an electronic information system based on their confidentiality, integrity and availability;

9. *sector-related cybersecurity incident handling centre* means a cybersecurity incident handling centre operated by one or more entities related to a single sector within the scope of this Act for the centralised and uniform handling of cybersecurity incidents occurring within a specific field within that sector;

10. *auditor* means an independent economic operator entitled to carry out cybersecurity audit activities within the meaning of this Act;

11. *penetration testing* means a vulnerability scanning method as part of which the weaknesses of an ICT system or an electronic information system are detected and their exploitable vulnerabilities are checked by simulating malicious attacks against security measures;

12. *internal IT security scan* means a vulnerability scanning method for assessing the vulnerability of an IT system as part of which the vulnerability scan of the IT system is performed directly from an internal network termination point or the scan of a tool or component used in the internal network is performed;

13. *confidentiality* means the property of an electronic information system whereby only authorised persons may access and use the data and information stored and make provisions as regards the use thereof, in accordance with the level of their authorisation.

14. *trust service* means the term as defined by the Act on digital State and laying down certain rules relating to the provision of digital services;

15. *trust service provider* means the term as defined by the Act on digital State and laying down certain rules relating to the provision of digital services;

16. *security class* means the expected strength of protection of an electronic information system;

17. *security classification* means determining the expected strength of protection of an electronic information system based on the risks;

18. *digital service* means the term as defined by the Act on digital State and laying down certain rules relating to the provision of digital services;

19. *DNS* means a hierarchical distributed naming system, in other words, domain name system, which enables the identification of internet services and resources, allowing end-user devices to use internet routing and connectivity services to reach those services and resources;

20. *DNS service provider* means an entity that provides any of the following services to another entity or person outside the entity:

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;

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

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

23. *electronic communications service provider* means the term as defined by the Act on electronic communications;

24. *electronic information system* means the following:

a) an electronic communications network within the meaning of the Act on electronic communications;

b) any device or a group of interconnected or related devices, one or more of which, pursuant to a program, carry out automatic processing of digital data, including a cyber-physical system; or

c) digital data stored, processed, retrieved or transmitted by elements covered under subpoints a) and b) for the purposes of their operation, use, protection and maintenance.

25. *security of electronic information systems* means the ability of electronic information systems to resist, at a given level of confidence, any event that may compromise the availability, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, those network and information systems;

26. *lifecycle* means the period covering the design, development, operation and termination of an electronic information system;

27. *event* means any change to the status of an electronic information system;

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

29. *user entity* means an entity relying on a central system or central service;

30. *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;

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

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

33. *putting into use* means filling an electronic information system with data and commencing its designated use;

34. *electronic information system for national defence purposes* means the following:

a) the totality of electronic information systems of national defence entities, multi-purpose vocational training institutions not qualifying as a national defence entity under the direction of the Minister responsible for national defence as a maintainer, companies over which the ownership rights are exercised by the Minister responsible for national defence as well as companies carrying out activities relating to national defence interests under the law, which supports, in a sector-specific manner, operation within the national defence sector and among sectors;

b) electronic information systems of entities and infrastructure within the national defence sector that are important for the defence and security of the country;

c) electronic information systems of entities and infrastructure not affected by dual designation that are important for the defence and security of the country; and

d) electronic information systems of entities identified as essential or important entities by the national defence cybersecurity authority;

35. *national defence cybersecurity incident handling centre* means an organ designated in accordance with section 63 (2);

36. *rendering temporarily inaccessible* means temporarily preventing access to electronic data;

37. *ICT process* means the term as defined in Article 2, point (14) of Regulation (EU) 2019/881 of the European Parliament and of the Council;

38. *ICT service* means the term as defined in Article 2, point (13) of Regulation (EU) 2019/881 of the European Parliament and of the Council;

39. *ICT product* means the term as defined in Article 2, point (12) of Regulation (EU) 2019/881 of the European Parliament and of the Council;

40. *significant cybersecurity incident* means any of the following:

a) a cybersecurity incident defined as such in a directly applicable legal act of the European Union

b) absent a directly applicable legal act of the European Union, a cybersecurity incident that

ba) leads to or threatens at least 5 per cent reduction in the business services of an entity or the services provided by the entity or at least 5 per cent loss of annual income of the entity;

bb) causes or is capable of causing a severe operational disruption of the services or a financial or reputational loss for the entity or the person affected by the cybersecurity incident; or

bc) affects or is capable of affecting another natural or legal person by causing significant material or non-material damage;

41. *significant cyber threat* means a cyber threat which, based on its technical characteristics, can be assumed to have the potential to have a severe impact on the electronic information systems of an entity or the users of the entity's services by causing significant material or non-material damage;

42. *representative* means any natural or legal person established in Hungary explicitly designated to act on behalf of an entity that is not established in Hungary, which may be addressed by the cybersecurity authority and the cybersecurity incident handling centre in place of the entity concerned;

43. *cybersecurity* means the term as defined in Article 2, point (1) of Regulation (EU) 2019/881 of the European Parliament and of the Council;

44. *cybersecurity audit* means classifying electronic information systems and assessing whether protective measures applied based on security classification are adequate;

45. *cybersecurity authority* means an authority referred to in section 23 (1) a) or b) or section 23 (2);

46. *cybersecurity incident* means an event compromising the availability, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, electronic information systems;

47. *cybersecurity incident handling* means any actions and procedures aiming to prevent, detect, analyse, and contain or to respond to and recover from a cybersecurity incident;

48. *cybersecurity incident handling centre* means an organ referred to in section 63 (1) or (2);

49. *cybersecurity near miss* means an event that could have compromised the availability, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, electronic information systems, but that was successfully prevented from materialising or that did not materialise;

50. *cyber threat* means the term as defined in Article 2, point (8) of Regulation (EU) 2019/881 of the European Parliament and of the Council;

51. *cyber-physical system* means a programmable electronic information system that interacts with the physical environment or manages devices that interact with the physical environment. By monitoring or controlling devices, processes and events, these electronic information systems directly detect or induce physical changes;

52. *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;

53. *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;

54. *risk* means the level of threat that depends on the frequency and likelihood of the occurrence of the threat and the magnitude of loss caused by it;

55. *risk assessment* means identifying and evaluating risks by appraising the value and vulnerability of, and threats to, an electronic information system, along with any potential damage and its frequency;

56. *risk management* means elaborating a system of measures to reduce risks affecting an electronic information system and implementing such measures;

57. *risk management framework* means a structured yet flexible approach and set of organisational processes that integrates cybersecurity-related risk management activities into a system development lifecycle through the identification, introduction, evaluation, operation and follow-up of risk-proportionate protective measures in order to ensure the continuous detection of threats and the effective handling of risks to both new and existing systems;

58. *administrative organ* means an entity referred to in points 1 to 13 of Annex 1;

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

60. *central system* means an electronic information system facilitating the performance of certain state and local government tasks that is developed or operated in a centralised manner for a closed group of clients; functions provided through such a system are used mandatorily or optionally by user entities within a defined set of institutions;

61. *central service* means a service to be provided, either mandatorily or upon individual request, by a central service provider;

62. *central service provider* means an entity that has the exclusive right under the law to provide IT and electronic communications services to an entity carrying out a state and local government task;

63. *research organisation* means a research organisation within the meaning of the Act on scientific research, development and innovation, other than an educational institution, 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;

64. *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;

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

66. *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;

67. *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;

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

69. *milestone* means the term as defined, for the development of a central system financed using European Union funds, in Article 2, point (4) of Regulation (EU) 2021/241 of the European Parliament and of the Council of 12 February 2021 establishing the Recovery and Resilience Facility and in Article 2, point (4) of Regulation (EU) 2021/1060 of the European Parliament and of the Council of 24 June 2021 laying down common provisions on the European Regional Development Fund, the European Social Fund Plus, the Cohesion Fund, the Just Transition Fund and the European Maritime, Fisheries and Aquaculture Fund and financial rules for those and for the Asylum, Migration and Integration Fund, the Internal Security Fund and the Instrument for Financial Support for Border Management and Visa Policy and, for other development projects, the term as defined in the project;

70. *qualified trust service* means the term as defined by the Act on digital State and laying down certain rules relating to the provision of digital services;

71. *qualified trust service provider* means the term as defined by the Act on digital State and laying down certain rules relating to the provision of digital services;

72. *technical specification* means the term as defined in Article 2, point (4) of 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 (hereinafter "Regulation (EU) 1025/2012");

73. *electronic information system for operational purposes* means the following:

a) an electronic information system used by law enforcement organs and national security services to perform their public safety and national security tasks set out in an Act; and

b) an electronic information system used by national defence entities to perform their military operations tasks set out in an Act, in particular direct operations support, planning and command as well as direct situational tracking;

74. *large-scale cybersecurity incident* means a cybersecurity incident which causes a level of disruption that exceeds Hungary's capacity to respond to it or which has a significant impact on Hungary and at least one other country;

75. *non-private cloud computing service* means a cloud computing service provided by a service provider in such a way that it is accessible to anyone or exclusively to a specific set of entities;

76. *national cybersecurity incident handling centre* a cybersecurity incident response unit operating in accordance with the recommendations of the European Network and Information Security Agency, which holds membership in international network security organisations and international entities specialised in critical information infrastructure protection [in European terminology: CSIRT (Computer Security Incident Response Team), in American terminology: CERT (Computer Emergency Response Team)]

77. *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 that applies to the certification or conformity assessment of ICT products, ICT services and ICT processes in Hungary;

78. *national cybersecurity strategy* means a document providing strategic objectives and priorities in the area of cybersecurity and the governance to achieve them;

79. *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;

80. *national crisis management plan* means a national plan for response to large-scale cybersecurity incidents and crises in accordance with Directive (EU) 2022/2555 of the European Parliament and of the Council that sets out the objectives of and arrangements for the management of large-scale cybersecurity incidents and crises;

81. *online search engine* means the term as defined in Article 2, point (5) of Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services;

82. *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;

83. *registered user rights* means rights created specifically for the purpose of carrying out vulnerability scan for the person who conducts a security scan;

84. *availability* means ensuring that an electronic information system is accessible and the data processed within is usable by authorised persons

85. *ICT vulnerability* means a weakness, susceptibility or flaw of an ICT product, ICT service or ICT process, the exploitation of which compromises or damages the confidentiality, integrity or availability of the ICT product, ICT service or ICT process;

86. *integrity* means a property of data whereby the content and properties of the data conform to expectations, including confidence that it originates from the expected source, *i.e.* it is authentic, and the verifiability and certainty, *i.e.* non-repudiation, of such an origin as well as a property of an element of an electronic information system, whereby the element of the electronic information system is fit for designated use;

87. *vulnerability* means a weakness, susceptibility or flaw of an electronic information system, the exploitation of which compromises or damages the confidentiality, integrity or availability of the electronic information system;

88. *vulnerability management plan* means a planning document for eliminating vulnerabilities;

89. *vulnerability scan* means a vulnerability management tool or method through which information systems, hardware and software are examined from a security perspective; the scan is performed using both automated tools and direct expert examinations;

90. *standard* means the term as defined in Article 2, point (1) of Regulation (EU) 1025/2012;

91. *entity* means State organs and organisations as well as legal persons and organisations without legal personality within the meaning of the Act on the Civil Code;

92. *supporting system* means an electronic information system that is not involved directly in the performance of the core tasks of an entity within the meaning of section 1 (1) a) to c), but that is necessary for the operation of the systems performing core tasks;

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

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

95. *remote vulnerability scan* means a vulnerability scan that involves

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 ICT vulnerabilities of the services of accessible computers;

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

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

96. *upgrade* means developing the existing electronic information system concerned to an extent that involves substantial change to its functionality or affects the expected level of its protection;

97. *operational cybersecurity incident* means a cybersecurity incident unintentionally reducing or eliminating the availability of data stored, transmitted or processed in electronic information systems, or of the services offered by, or accessible via, such systems;

98. *operator* means a natural person, legal person, organisation without legal personality or a private entrepreneur who operates, and is responsible for the operation, of an electronic information system or its parts;

99. *closed, comprehensive, continuous and risk-proportionate protection* means the protection of an electronic information system

a) that is ensured without interruption even under circumstances and conditions that change over time;

b) that covers all parts of the electronic information system;

c) that takes into consideration all potential threats and dangers; and

d) the costs of which are proportionate to the potential value of damage caused by the threats.

3. General principles

Section 5 (1) Throughout the entire lifecycle of an electronic information system covered by this Act, closed, comprehensive, continuous and risk-proportionate protection shall be ensured relating to

a) confidentiality, integrity and availability of data and information processed in the electronic information system and of services provided by or accessible through it; and

b) integrity and availability of elements of the electronic information system.

(2) As part of the protection of an electronic information system the joint protection of the following shall also be ensured, when used by the entity with the right of disposal over the electronic information system, the controller and the processor for a specific objective:

a) devices for data and information processing, including the environmental infrastructure, hardware, network and data-storage media;

b) procedures for data and information processing, including regulation, software and related processes; and

c) persons managing the devices and procedures under points a) and b).

(3) Adequate budget funds shall be allocated to the operation of

a) the national cybersecurity authority and the national defence cybersecurity authority;

b) the state organ authorised to perform vulnerability scan in accordance with section 57 (1) (hereinafter the "state organ authorised to perform vulnerability scan"); and

c) the national cybersecurity incident handling centre and the national defence cybersecurity incident handling centre under section 63.

Chapter II

OBLIGATIONS OF ESSENTIAL AND IMPORTANT ENTITIES

4. General obligations of essential and important entities

Section 6 (1) An electronic information system at the disposal of an entity shall be regarded as the electronic information system of the entity.

(2) The head of an entity shall create and operate a risk management framework for the protection of electronic information systems in accordance with a directly applicable legal act of the European Union or, absent that and for matters not regulated by a directly applicable legal act of the European Union, a decree by the Minister responsible for information technology.

(3) As part of the activity specified in paragraph (2), the head of an entity shall

1. provide for the assessment and registration of electronic information systems and central services used by the entity, broken down as follows:

a) electronic information systems at the disposal of the entity;

b) central systems used by the entity;

c) services and supporting systems used by the entity that are provided by a central service provider;

d) other supporting systems at the disposal of or used by the entity.

2. specify the roles, the persons responsible and the tasks as well as the powers required relating to the protection of electronic information systems at the disposal of or used by the entity; appoints or assigns the person responsible for the security of the security of the electronic information system;

3. for an entity referred to in Annex 1, ensure the assessment and classification of data processed in an electronic information system referred to in point 1 a).

4. perform impact analysis and risk management activities in accordance with a decree by the Minister responsible for information technology relating to electronic information systems referred to in point 1 a) and their environment;

5. assign electronic information systems referred to in point 1 a) to security classes in accordance with the law;

6. determine the risk-proportionate protective measures for electronic information systems referred to in point 1 a);

7. issue the information security regulations relating to users and electronic information security requirements and ensure their review every two years and in the cases specified by law;

8. ensure that protective measures specified relating to the protection of electronic information systems are implemented;

9. where applicable, provide for the assessment of whether the protective measures selected in accordance with a legal act of the European Union and the decree by the Minister responsible for information technology are appropriate at the time of initial security classification;

10. regularly provide for the periodic assessment of protective measures and, as part of this, verify whether the protective measures determined in accordance with the law in a risk-proportionate manner adequately ensure the security of the entity and the electronic information systems at minimum by conducting risk assessments, inspections as well as independent internal cybersecurity evaluations in line with a recommendation issued by the cybersecurity authority;

11. ensure that deficiencies discovered in the course of the assessment of protective measures relating to security class are remedied;

12. decide, within the entity, on putting into use or continuing to use an electronic information system;

13. ensure that obligations imposed by the cybersecurity authority are fulfilled.

(4) The head of the entity shall carry out the tasks set out in paragraph (3), point 10 at minimum every two years together with reviewing the information security regulations and, where he is subject to such an obligation, the security classification.

(5) To ensure the protection of the electronic information system, the head of the entity shall

a) ensure education of protection tasks relating to electronic information systems and the related responsibilities, as well as cybersecurity training and further training for both himself and the employees of the entity as provided for in a decree by the Minister responsible for information technology;

b) ensure participation in mandatory national cybersecurity exercises and the independent conduct of cybersecurity exercises;

c) ensure that events in an electronic information system can be monitored;

d) ensure that cybersecurity requirements relating to an activity performed by a contributor in connection with an electronic information system are complied with as contractual obligations in accordance with the provisions of this Act, where the entity relies on a contributor in the course of the establishment, audit, maintenance and repair of the electronic information system and in the course of cybersecurity incident handling or for the performance of processing or technical processing tasks relating to the electronic information system;

e) with all necessary and available resources, provide for swift and effective response, reporting to the competent cybersecurity incident handling centre, cybersecurity incident handling, and recovery, should a cyber threat, cybersecurity near miss or cybersecurity incident occur relating to the electronic information system;

f) ensure that the persons concerned are immediately informed of any cybersecurity incidents and potential threats;

g) ensure that the recommendations and guidelines of the cybersecurity authority and the competent cybersecurity incident handling centre are taken into account with a view to the protection of the electronic information system;

h) endeavour to perform the tasks set out in this law in the shortest possible time;

i) for an entity referred to in section 1 (1) a) to c), ensure that, in the given year, the entity allocates an amount for cybersecurity development that corresponds to at least 5 per cent of the IT development expenditure for that year; and

j) take any other measure required for the protection of the electronic information system.

(6) The head of an entity shall be responsible for the tasks referred to in paragraphs (3) to (5), even if paragraph (5) d) applies, except where the entity is required to use a central service provider or a central system, up to the extent of services received.

(7) Performance of the reporting obligation under paragraph (5) e) shall be without prejudice to any other reporting obligations under another Act.

(8) To certify compliance with the specific requirements set out in paragraphs (1) to (5), an ICT product, ICT service or ICT process certified under a European or national cybersecurity certification scheme may be used where available.

(9) Entities referred to in section 1 (1) a) to c) and f) listed in a decree by the Minister responsible for information technology or, for electronic information systems for national defence purposes, the Minister for national defence, as well as entities referred to in section 1 (1) d) and e) listed in a decree by the president of SARA shall be required to use ICT products, ICT services or ICT processes certified under a European or national cybersecurity certification scheme that are specified in the decree by the Minister responsible for information technology, the Minister for national defence, or the president of SARA.

(10) In relation to an electronic information system at the disposal of an important entity falling within the scope of section 1 (1) a) and c) or an entity other than an entity referred to in Annex 2 or 3 falling within the scope of section 1 (1) b),

a) a comprehensive risk management framework referred to in paragraph (2) need not be operated;

b) the provisions of paragraph (3), points 4 to 5 and 9 need not be complied with; and

c) at least the requirements for "basic" security class shall be complied with.

(11) An entity holding the right of disposal over an electronic information system for national defence purposes shall contact the national defence cybersecurity authority in the authority procedure relating to the electronic information system for national defence purposes and shall fulfil its reporting and other obligations prescribed by this Act to the national defence cybersecurity authority.

(12) Detailed rules on the conduct of national cybersecurity exercises and detailed provisions on the obligations of entities falling within the scope of section 1 (1) a) to c) and f) shall be laid down in a government decree.

Section 7 (1) Except for budgetary organs, an entity referred to in section 1 (1) b), which is also an entity listed in Annex 2 or 3, as well as an entity referred to in section 1 (1) d) and e) or, where that entity is a controlled member of an acknowledged group of companies within the meaning of the Act on the Civil Code (hereinafter "acknowledged group of companies"), in place of that entity, the controlling member shall be required to pay cybersecurity supervision fee for cybersecurity supervision activities in an amount determined, in accordance with paragraph (2), in a decree by the president of SARA.

(2) The maximum amount of annual cybersecurity supervision fee shall be 0.015 per cent of the net turnover of the entity referred to in paragraph (1) in the previous business year or, absent such turnover, the *pro rata temporis* part of the turnover for the entire year in question, but it shall not exceed 10 million forints. For entities in the same acknowledged group of companies, *de facto* group of companies within the meaning of the Act on the Civil Code, or group of undertakings in the same scope of consolidation containing a parent company, subsidiaries and jointly managed undertakings included in the consolidation, the joint amount of annual cybersecurity supervision fee to be paid shall not exceed 50 million forints. An entity referred to in paragraph (1) shall prove operating as a *de facto* group of companies or a group of undertakings in the same scope of consideration in accordance with a decree of the president of SARA.

(3) An obligor under paragraph (1) shall pay to SARA the cybersecurity supervision fee in the manner and at the time specified in the decree by the president of SARA.

Section 8 (1) An entity registered in Hungary that operates an electronic information system falling within the scope of this Act shall designate in writing a representative operating within the territory of Hungary who shall be responsible for compliance with the provisions of this Act in accordance with the rules applicable to the head of an entity. Designation of a representative shall not affect the responsibility of the entity and the head of the entity.

(2) The head of the entity shall ensure that the entity cooperates with the cybersecurity authority.

(3) As part of the cooperation, the head of the entity shall

a) ensure that data, documents and any changes thereto are sent to the cybersecurity authority for registration within fifteen days of the change, in accordance with the provisions set out in law or on the website of the authority; and

b) ensure the conditions for conducting checks.

(4) With the exceptions set out in subtitle 51, an entity referred to in section 1 (1) a) to c) and f) shall

a) within 30 days of becoming subject to this Act, submit to the national cybersecurity authority the data specified in section 28 (1), point 1 a) to e) and j);

b) within 30 days of becoming subject to this Act, submit to the national cybersecurity authority the data of the person responsible of electronic information system security;

c) within 90 days of becoming subject to this Act, assess the electronic information systems used by the entity in accordance with the provisions of section 6 (3), point 1;

d) within 120 days of becoming subject to this Act, carry out the data classification referred to in section 9, where applicable;

e) within 180 days of becoming subject to this Act, send to the national cybersecurity authority the information security regulations of the entity;

f) within 180 days of becoming subject to this Act, together with the establishment of the risk management framework referred to in section 6, carry out, where the entity is required to do so, the security classification of existing electronic information systems and assess protective measure relating to electronic information systems, their adequacy and status, and submit a notification to the cybersecurity authority with the content prescribed by a decree of the Government.

(5) An entity covered by section 1 (1) b), which is also an entity listed in Annex 2 or 3, and an entity referred to in section 1 (1) d) or e) shall, within 30 days of commencing activities or becoming subject to this Act, send the data specified in section 29 (1) a) other than data specified in section 29 (1) a) ab) to SARA for registration.

(6) For the purposes of paragraphs (4) and (5), the date of becoming subject to this Act shall be

a) the day of the establishment of the entity, for a new entity;

b) the first day of the year following the year when the size threshold for medium-sized undertakings set out in the Act on small and medium-sized undertakings and the support of their development is reached;

c) the day of entry into force of the legal act establishing the legal status resulting in becoming subject to this Act.

(7) An entity may conclude cybersecurity information-sharing agreements for the implementation of a cooperation specified in a decree by the Minister responsible for information technology in order to share cybersecurity information other than information relating to electronic information systems for national defence purposes. The entity shall inform the cybersecurity authority of the conclusion of, participation in, and unilateral termination of a cybersecurity information-sharing agreement.

5. Data classification

Section 9 (1) To ensure the risk-proportionate protection of data processed by an entity, the entity referred to in section 1 (1) a) shall classify data processed by it in an electronic information system based on confidentiality, integrity and availability in accordance with the provisions of a government decree.

(2) Entities referred to in section 1 (1) b) and c) and, as regards electronic information systems for national defence purposes, f) shall perform data classification in the case of using a non-private cloud computing service or carrying out foreign processing with a view to the assessment of the risks of foreign processing or processing using a non-private cloud computing service.

(3) Data classification shall take into account the collective security requirements of electronic data that are processed together logically as a unit, such as databases, data repositories, individual documents or other data sets.

(4) Entities referred to in section 1 (1) a) to c) and, as regards electronic information systems for national defence purposes, f) may use a non-private cloud computing service or process data abroad exclusively on the basis of data classification, taking into account its outcome, provided that the use of the cloud computing service or the foreign processing is not prohibited or restricted by another law.

(5) The entity shall review data classification in the course of security classification and if the scope of data to be processed in the electronic information system changes.

6. Security classification

Section 10 (1) To ensure risk-proportionate protection for the electronic information systems of an entity and data processed in and services provided by them, the entity shall assign electronic information systems at the disposal of the entity that fall within the scope of this Act to ‘basic’, ‘substantial’ or ‘high’ security classes on the basis of the integrity and availability of the electronic information system concerned and the risk to the confidentiality, integrity and availability of data processed by the entity, with the protection requirements increasing in stringency according to classification.

(2) The head of the entity shall decide on security classification and shall be responsible for it being in compliance with the law and adequate to the risks as well as the completeness and timeliness of the data used. The entity shall record the outcome of security classification in the register of electronic information systems or another internal regulations.

(3) The Minister responsible for information technology shall determine in a decree the requirements for security classification and the specific protective measures to be applied for each security class.

(4) For an electronic information system, the entity shall determine and implement the protective measures prescribed in the decree of the Minster responsible for information technology on the basis of the security class of the electronic information system concerned.

(5) As regards electronic information systems of entities referred to in section 1 (1) a) and, as regards electronic information systems for national defence purposes, f) as well as entities other than an entity referred to in Annex 2 or 3 covered by section 1 (1) b), at the time of them becoming subject to this Act, the protective measures prescribed in the decree of the Minister responsible for information technology for at least the 'basic' security class shall be implemented.

(6) Where in the course of security classification a security class above 'basic' is assigned to an electronic information system referred to in paragraph (5), a maximum of two years from security classification shall be available for the entity to implement the security measures attached to the security class in order to reach the expected level of protection.

(7) Security classification shall be reviewed in a documented manner at least every two years or, in case of a change under a law that affects the security of the electronic system, as a matter of priority.

7. Person responsible for electronic information system security

Section 11 (1) The head of the entity shall designate a person responsible for electronic information system security within the entity, or enter into an agreement with a person outside the entity, for the purpose of performing tasks relating to the protection of the electronic information system, operating the risk management framework, reporting cybersecurity incidents and communicating with the cybersecurity incident handling centre.

(2) For entities referred to in section 1 (1) a) to c) and f), the mandatory content of an agreement under paragraph (1) shall be set out in a government decree. The natural person who performs the tasks of the person responsible for electronic information system security shall be specified, even if an agreement is concluded.

(3) A person may carry out the tasks of the person responsible for electronic information system security only if

a) he has capacity to act and no criminal record; and

b) the entity is an entity referred to in section 1 (1) a) to c) or f) or designated as a critical entity under the Critical Entity Resilience Act or designated as an entity important for the defence and security of the country under the Defence and Security Activities Coordination Act and he holds the qualification prescribed in a decree by the Minister responsible for information technology as required for the performance of his tasks and

ba) holds a professional qualification or accredited international qualification published by the national coordination centre referred to in section 75 (1) in accordance with the provisions of a decree by the Minister responsible for information technology (hereinafter jointly "professional qualification"); or

bb) has professional experience in the field specified in a decree by the Minister responsible for information technology.

(4) With the exception specified in paragraph (5), a person who performs financial management tasks at the entity and a person holding a position relating to IT operations or IT development within the entity or a person who is directly subordinated to such a person shall not be designated or assigned as person responsible for electronic information system security.

(5) Paragraph (4) shall not apply to the following entities:

a) important entities referred to in section 1 (1) a) to c);

b) entities referred to in section 1 (1) d) and e).

(6) The head of the entity shall ensure that the person responsible for electronic information system security

a) participates in the preparation of all decisions relating to the protection of electronic information systems;

b) has at his disposal all conditions, rights, information and human and material resources required for ensuring the protection of the electronic information system;

c) has access to all the systems, data and information required for the performance of the tasks to be carried out by him; and

d) participates in further training required to maintain his professional knowledge, as specified in a decree by the Minister responsible for information technology, should he be designated within the entity.

(7) The person responsible for electronic information system security shall be subject to an obligation of confidentiality concerning data and information he became aware of in connection with the performance of his tasks. Exemption from the obligation of confidentiality may be granted by the head of the entity.

(8) The person responsible for electronic information system security shall participate in further training specified in a decree by the Minister responsible for information technology.

(9) The person responsible for electronic information system security may request information as regards compliance with security requirements from contributors involved in the performance of electronic information security obligations and tasks of the entity. In this context, he has the right to access data relating to the activities of contributors that are required for substantiating compliance with the requirements and all documents produced as regards electronic information system security.

(10) Where justified, the entity may designate or assign a person authorised to substitute for the person responsible for electronic information system security, who shall carry out the tasks of the person responsible for electronic information system security in case of prolonged absence or other impediment. The head of the entity shall provide for the division of tasks and responsibility between the person responsible for electronic information system security and his substitute. The provisions applicable to the person responsible for electronic information system security shall apply to the substitute.

(11) Where justified by the number, size or security requirements of the electronic information systems of an entity, an organisational unit for electronic information security led by the person responsible for electronic information system security may be established within the entity.

(12) For an entity referred to in section 1 (1) a) to c) or f), an entity designated as critical entity under the Critical Entity Resilience Act and an entity designated as an entity important for the defence and security of the country under the Defence and Security Activities Coordination Act, detailed rules on the functions and powers of the person responsible for electronic information system security shall be laid down in a government decree.

(13) The national cybersecurity authority shall keep a register of persons suitable for performing the tasks of a person responsible for electronic information system security.

(14) The objective of the register of persons responsible for electronic information system security shall be to enable entities to select a person suitable for performing the tasks of a person responsible for electronic information system security from among the registered persons.

(15) The procedure for registration and deregistration in the register of persons responsible for electronic information system security shall be laid down in a government decree.

(16) The national cybersecurity authority may verify whether a person responsible for electronic information system security meets the requirement of having no criminal record set out in paragraph (3) a). For the purpose of such a verification, it may request data from the criminal records system.

8. Education and training as regards electronic information system security

Section 12 (1) A higher education institution providing cybersecurity-related training may, relating to its training activities,

a)

b) be involved in information security, cyber protection and, for critical entities, complex resilience exercises.

(2) An entity providing cybersecurity-related training may organise

a) training for heads of essential entities and important entities and for employees at organisational units managed by persons responsible for electronic information system security;

b) further training for heads of essential entities and important entities, persons responsible for electronic information system security, as well as employees at organisational units managed by persons responsible for electronic information system security.

9. Development and upgrade of electronic information systems

Section 13 (1) The provisions of this subtitle shall apply to the development of new electronic information systems and the upgrading of existing electronic information systems (hereinafter jointly "development") as regards the following entities qualifying as essential entities:

a) an entity referred to in section 1 (1) a) or c); and

b) an entity that qualifies as an entity under both section 1 (1) b) and Annex 2 or 3.

(2) In the case of the development of an electronic information system, the entity shall proceed in accordance with a government decree in order to ensure that information security requirements are met and the operation of the electronic information system is approved by the national cybersecurity authority.

(3) In the course of development, as part of the development lifecycle of the electronic information system, data intended to be processed in the system shall be classified where this Act imposes a data classification obligation, and the security classification of the electronic information system shall be carried out; the resulting classifications have to be submitted to the national cybersecurity authority for approval in accordance with a government decree

a) in the case of internal development, before the allocation of resources,

b) in the case of external development, before the conclusion of the relevant contract setting out the information security requirements in the contract for electronic information system development, observing also the legislative provisions on public procurement.

(4) In the development contract the entity shall specify the requirements for the classification approved by the national cybersecurity authority and, in the course of development, make arrangements for their implementation by the developer entity.

(5) Development shall be carried out in accordance with the protection requirements laid down in a decree by the Minister responsible for information technology for the security class that were approved by the national cybersecurity authority.

(6) Should the entity become aware of a circumstance with an impact on the security of the electronic information system concerned during development, the tasks referred to in paragraphs (2) to (4) shall be carried out repeatedly.

(7) In the course of its proceeding, the national cybersecurity authority may order a vulnerability scan.

(8) In the course of the introduction of a new electronic information system and the upgrading of an existing electronic information system, the requirements for the established security class shall be complied with by the time of the putting into use of the system.

(9) The head of the entity may take the decision under section 6 (3), point 12 on putting into use or continuing to use an electronic information system only if the requirements arising from the security classification approved by the national cybersecurity authority are complied with in accordance with paragraph (8).

(10) At the time of taking the decision referred to in section 6 (3), point 12, it shall be ensured that the data specified in a government decree of the electronic information system is notified to the national cybersecurity authority.

(11) In addition to the provisions of paragraphs (1) to (10), in the course of the development of a central system, the entity holding the right of disposal over the electronic information system shall inform the national cybersecurity authority of matters relating to the security of the central system, initially during the development phase and subsequently upon reaching each milestone.

Section 13/A The provisions of this subtitle shall apply also to the development of electronic information systems for national defence purposes of an entity referred to in section 1 (1) f).

Section 14 (1) In place of the provisions of section 13, the provisions of this section shall apply if the electronic information system is developed by

a) an essential entity under section 1 (1) b) other than an entity under Annex 2 or 3; or

b) an important entity under section 1 (1) a) or c).

(2) The entity referred to in paragraph (1) shall make arrangements that the protection requirements are implemented by the developer entity.

(3) The entity referred to in paragraph (1) shall notify the cybersecurity authority

a) of the electronic information system in its development lifecycle, before the development commences; and

b) following the decision under section 6 (3), point 12 by the head of the entity on putting into use or continuing to use the electronic information system.

(4) The cybersecurity authority may order a vulnerability scan if justified.

(5) The requirements for the security class shall be complied with by the time of putting into use the electronic information system; the head of the entity may take the decision referred to in section 6 (3), point 12 on putting into use or continuing to use the electronic information system only if the requirements are complied with.

Section 15 (1) Where vulnerability scan of an electronic information system of an entity referred to in section 1 (1) a) to c) is mandatory under the law or a decision of the national cybersecurity authority, the decision under section 6 (3), point 12 shall be conditional upon the approval of the vulnerability management plan prepared concerning vulnerabilities identified by the national cybersecurity authority.

(2) For an electronic information system referred to in paragraph (1) that is assigned to 'substantial' or 'high' security class, it shall be mandatory to request a comprehensive vulnerability scan in accordance with the government decree. Pursuant to a decision by the state organ authorised to perform vulnerability scan specified in a government decree, the entity may be exempted from the obligation to perform a vulnerability scan.

(3) Detailed rules to be observed in the course of the development of the electronic information systems of an entity referred to in section 1 (1) a) to c) shall be laid down in a government decree.

10. Cybersecurity audit

Section 16 (1) An entity referred to in section 1 (1) b), which is also an entity listed in Annex 2 or 3, as well as an entity referred to in section 1 (1) d) and, other than a micro undertaking within the meaning of the Act on small and medium-sized undertakings and the support of their development, an entity referred to in section 1 (1) e), shall be required to provide proof of compliance with the cybersecurity requirements under this Act every two years and to undergo cybersecurity audit if ordered by the competent cybersecurity authority under section 23 (1).

(2) An entity shall be required

a) to enter into an agreement for the performance of a cybersecurity audit with an auditor included in the register referred to in section 21 (3) within 120 days following its registration; and

b) to have an initial cybersecurity audit conducted within two years following its registration.

(3) No cybersecurity audit shall be conducted as regards an electronic information system for national defence purposes.

(4) Where an entity referred to in paragraph (1) holds the right of disposal over also an electronic information system for national defence purposes, the head of the entity shall be responsible for compliance with the provisions of paragraph (3).

(5) For electronic information systems of companies carrying out activities relating to national defence interests under the law and entities and national defence infrastructure important for the defence and security of the country that are not affected by dual designation, the national defence cybersecurity authority shall inform SARA of registration as electronic information system for national defence purposes.

11. Special provisions on supporting systems

Section 17 (1) The entity shall ensure that the same level of protection applies to the supporting system as the electronic information system supported by that system in accordance with a decree by the Minister responsible for information technology, provided that the protective measures in question can be applied to the supporting system concerned in a risk-proportionate manner. The entity shall be required to assess the protective measures applied in the supporting system.

(2) Where the entity provides the supporting system as a service, it shall inform the entity using the supporting system of the security class with the requirements of which the supporting system complies.

(3) A supporting system may be used only if it meets the protection requirements for the electronic information system supported by it.

12. Special provisions on central systems

Section 18 (1) As regards a central system provided to the user entity, the entity exercising the right of disposal over the central system

a) shall carry out the tasks listed in subtitle 4;

b) shall notify the national cybersecurity authority of the entity to which it provides the central system at its disposal;

c) shall set out as a contractual obligation or, absent a contract, make available on its website for the user entity the electronic information security requirements to be complied with, as a condition for the use of the central system, by the user entity with a view to the protection of the central system;

d) may monitor the performance of the tasks referred to in point c);

e) shall request, setting a time limit, the user entity to remedy deficiencies or rectify errors identified during monitoring under point d); should the request yield no result, the national cybersecurity authority shall be informed so that it may take further measures;

f) shall cooperate with the user entity and, as part of this cooperation,

fa) notify the user entity of planned events affecting the central system at least five days before the event;

fb) inform it of cybersecurity incidents affecting the central system as a matter of priority;

fc) inform it of available preventive measures, measures necessary for restoration and other measures in the event of a cyber threat, cybersecurity near miss or cybersecurity incident affecting the electronic information system;

fd) arrange for the remedy of any error or deficiency affecting the central system, should one be identified in the course of a vulnerability scan performed as regards an electronic information system of the user entity;

g) shall report cyber threats and cybersecurity near misses affecting the central system to the competent cybersecurity incident handling centre; and

h) shall take the measures prescribed by the competent cybersecurity incident handling centre in order to prevent, remedy or handle cyber threats, cybersecurity near misses and cybersecurity incidents affecting a central system and reduce their consequences, and, if a service used by it is affected, arrange for the service provider to take the necessary measures.

(2) As regards a central system used by a user entity, the user entity

a) shall, in the course of reporting its electronic information systems to the national cybersecurity authority, report, indicating the data suitable for the identification of the central system as well as the entity exercising the right of disposal over the central system, the use of the central system;

b) shall comply with the electronic information security requirements set out by the entity exercising the right of disposal over the central system and record them in its information security regulations; and

c) report cybersecurity incidents affecting the central system to the competent cybersecurity incident handling centre and the entity exercising the right of disposal over the central system.

(3) For an entity exercising the right of disposal over a central system the use of which is mandatory under the law, the allocation of tasks and responsibilities between the central system provider and the user entity shall be laid down by the law on the central system concerned. Absent this, and for a central system that use of which is voluntary, the entity exercising the right of disposal over the central system and the user entity shall enter into a service contract.

(4) The national cybersecurity authority shall keep a register of central systems.

(5) As regards a central system, the national cybersecurity authority shall be entitled to check compliance with electronic information security requirements at both the central system provider and the user entity.

13. Special provisions on systems provided by central service providers

Section 19 (1) The central service provider shall inform the user entity which security class the services it provides comply with or which security class the systems implementing central services comply with. The user entity shall use the service if the protective measures ensured by the central service provider are appropriate for the security class of the electronic information system affected by the service provided by the central service provider. Otherwise, the user entity shall not use the service or, in the case of mandatory use, the user entity shall provide for using risk-proportionate substitute measures the user entity has the power to implement.

(2) The central service provider

a) shall maintain continuous contact with the national cybersecurity authority;

b) shall notify the national cybersecurity authority of the entity to which it provides the central service or the supporting system;

c) shall provide for the implementation of the risk-proportionate protective measures of the central service or the supporting system;

d) shall set out and make available to the user entity the electronic information security requirements to be complied with as a condition of use by the user entity with a view to the protection of the central service or the supporting system;

e) shall cooperate with the user entity and, as part of this cooperation,

ea) notify it of planned events affecting the central service or the supporting system at least five days before the event;

eb) inform it of cybersecurity incidents affecting the central service or the supporting system as a matter of priority;

ec) inform it of available preventive measures, measures necessary for restoration and other measures in the event of a cyber threat, cybersecurity near miss or cybersecurity incident;

ed) arrange for the remedy of any error or deficiency affecting the central service or the supporting system, should one be identified in the course of a vulnerability scan performed as regards an electronic information system of the user entity;

f) shall report cyber threats, cybersecurity near misses and cybersecurity incidents impacting the central service or the supporting system to the competent cybersecurity incident handling centre; and

g) shall take the measures prescribed by the competent cybersecurity incident handling centre in order to prevent, remedy or handle cyber threats, cybersecurity near misses and cybersecurity incidents impacting the central service or the supporting system and reduce their consequences, and, if a service used by it is affected, arrange for the service provider to take the necessary measures.

(3) As regards the central eservice or the supporting system provided by the central service provider to the entity, the user entity

a) shall notify the national cybersecurity authority of the use of the central service or the supporting system, specifying the central service provider;

b) shall comply with the electronic information security requirements set out by the central service provider, and record them in its information security regulations; and

c) shall report cybersecurity incidents affecting the central service or the supporting system to the cybersecurity incident handling centre and the central service provider.

(4) If the use of the central service or the supporting system is mandatory under the law, the allocation of tasks and responsibilities between the central service provider and the user entity shall be laid down by the law on the central service or the supporting system concerned. Absent this and for a central service or a supporting system the use of which is voluntary, the central service provider and the user entity shall enter into a direct funding contract.

(5) Detailed rules on IT and electronic communications service tasks the central service provider provides with exclusive right on the basis of a law to an entity carrying out a state and local government task shall be laid down in a government decree.

(6) The national cybersecurity authority shall keep a register of central services and supporting systems provided by the central service provider.

(7) The national cybersecurity authority shall be entitled to check compliance with electronic information security requirements at both the central service provider and the user entity.

14. Top-level domain name registry

Section 20 (1) The top-level domain name registry shall keep a central register of domain names under the top-level domain.

(2) The central domain name register shall include the following:

a) the domain name concerned;

b) the date of domain name registration;

c) the name, electronic mailing address suitable for communication and telephone number of the domain name user; and

d) the name, electronic mailing address and telephone number of the point of contact administering the domain name if different from the data referred to in point c).

(3) The data referred to in paragraph (2) shall be processed for the purpose of keeping up-to-date the identification and contact data of the point of contact administering the domain name and the natural or legal person using the domain name.

(4) The top-level domain name registry shall make available to the public the verification procedure approved in advance by SARA with a view to verifying the authenticity and ensuring the integrity of data in the central domain name register.

(5) The top-level domain name registry shall make accessible to the public the data in the central domain name register except for personal data.

(6) The top-level domain name registry shall provide direct access to data in the central domain name register for the prosecution service, national security services, investigating authorities, organs conducting preparatory proceedings within the meaning of the Act on the Code of Criminal Procedure, the cybersecurity authority and the cybersecurity incident handling centre.

Chapter III

CYBERSECURITY SUPERVISION

15. Provisions on cybersecurity audit

Section 21 (1) In the course of cybersecurity audit, the auditor shall assess whether the security classification of electronic information systems and the protective measures based on security classification are appropriate.

(2) An auditor shall be entitled to carry out a cybersecurity audit if he has the skills and meets the infrastructural conditions for the performance of such a task and qualifies as an economic operator under section 57 (1) c) (hereinafter "economic operator authorised to perform vulnerability scan"). The requirements for an auditor shall be set out in a decree by the president of SARA.

(3) SARA shall enter into the register of economic operators authorised to perform audit in accordance with the detailed rules laid down in a decree by the president of SARA if compliance with the requirements under paragraph (2) is proved.

(4) The register referred to in paragraph (3) shall contain 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 the designated contact point of the contributor required for identification; and

d) the document containing the findings of the audit.

(5) By way of derogation from the Act on the general rules on taking up and pursuit of service activities, where SARA did not decide on entry into the register under paragraph (3) within the applicable administrative time limit, the applicant shall not be entitled to take up or pursue the activity specified in the application and the rules on an omission by the authority as laid down in the Act on the Code of General Administrative Procedure shall apply.

(6) If an auditor no longer performs any auditor activity, SARA shall delete from the register the data referred to in paragraph (4) five years after the notification of the termination of the activity.

(7) Should the auditor notify any change to the data referred to in paragraph (4), five year after the registration of the change to the data, SARA shall delete from the register the data that was recorded before the registration of the change.

(8) The objective of the processing of the data referred to in paragraph (4) shall be to keep up-to-date the information relating to auditors and to enable SARA to perform monitoring activities.

(9) Unless otherwise provided by the law, data transfer from the register referred to in paragraph (4) may be performed exclusively to cybersecurity authorities and cybersecurity incident handling centres.

Section 22 (1) To assess the appropriateness under section 21 (1), the auditor shall be entitled to carry out the following inspections in a manner that enables monitoring:

a) internal IT security and remote vulnerability scanning, and, for 'substantial' or 'high' security class, penetration testing;

b) cryptographic conformity assessment; and

c) for security classes ‘substantial’ and ‘high’, security source code analysis of custom-developed software implementing critical security functionalities.

(2) The auditor shall send to SARA and the entity the findings of the audit without delay following the completion of the audit.

(3) The auditor shall inform SARA without delay in writing if, relating to the electronic information system of the entity,

a) the auditor establishes a fact that seriously compromises the continued functioning of the entity; or

b) the auditor detects circumstances that indicate the commission of a criminal offence, a violation of law or a serious breach of the internal regulations of the entity, or the risk thereof.

(4) SARA shall send the findings of the audit and the information provided under paragraph (3) to the national cybersecurity authority

a) *ex officio*, if the entity falls under section 1 (1) b);

b) at a request of the national cybersecurity authority, if the entity falls under section 1 (1) d) or e).

(5) The auditor shall handle the documents received from the auditee that are managed by the auditee and are necessary for carrying out the audit, including also personal data and data qualifying as trade secret, for the purpose of verifying compliance with the requirements subject to audit to the extent necessary to conduct the audit and until the completion of the audit; such documents shall not be transferred to third parties.

(6) The auditor shall specify in regulations the positions the holders of which may access trade secrets and learn their content in the course of an audit. Persons participating in an audit shall be under the obligation of confidentiality with respect to personal data and trade secrets obtained in the course of the audit; the confidentiality 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.

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

(8) SARA shall monitor, applying section 25 (1) and (3), whether the auditor complies with his obligations.

(9) The maximum fee for an audit, excluding value added tax, and the procedure for carrying out a cybersecurity audit shall be determined in a decree by the president of SARA.

16. General provisions on the cybersecurity authority

Section 23 (1) With the exception of electronic information systems for national defence purposes, the following shall be responsible for the cybersecurity supervision of electronic information systems falling within the scope of this Act:

a) for electronic information systems of entities referred to in section 1 (1) a) to c), the national cybersecurity authority designated in a decree by the Government;

b) for electronic information systems of entities referred to in section 1 (1) d) and e), to which point a) does not apply, SARA.

(2) For electronic information systems for national defence purposes, the national defence cybersecurity authority responsible for cybersecurity supervision under this Act shall be designated, from within the national defence sector, in a decree by the Government. The provisions on the national defence cybersecurity authority shall apply to the activities of the national defence cybersecurity authority.

(3) The national cybersecurity authority shall be an organ with independent tasks and official authority that is subordinated only to the law in the performance of its administrative activities and is independent from all other organs and that shall not be instructed as regards administrative cases within its function, with the exception of instructions to perform a task or to rectify an omission.

17. Tasks of the cybersecurity authority

Section 24 (1) The national cybersecurity authority

1. shall examine whether the person responsible for electronic information system security and his substitute comply with the requirements set out by law, and if so, record them in the register;

2. shall examine whether security classification is justified and, based on its findings, decide on recording it in the register;

3. shall record data listed in section 28 (1) in the register and maintain the register;

4. shall establish principles, recommendations and requirements for electronic information system security;

5. may issue guidelines relating to convergence between protective measures set out in the laws of the European Union and in the decree by the Minister responsible for information technology;

6. with a view to certifying compliance with electronic information security requirements, may prescribe the use of European and national standards and technical specifications that are relevant to the security of electronic information systems, without requiring or giving preference to the use of any specific type of technology;

7. shall verify whether the requirements for the classification of electronic information systems that are set out by law or by the national cybersecurity authority itself are complied with;

8. shall order the remediation of the security deficiencies that were identified or of which it became aware during an audit as well as the measures necessary for their elimination, and shall monitor the effectiveness of those measures;

9. may take and monitor all measures for the protection of electronic information systems that are suitable for handling threats compromising the electronic information system concerned;

10. in case of a cybersecurity incident, shall launch an authority proceeding and inform immediately the national cybersecurity incident handling centre about reports received of cybersecurity incidents;

11. may participate in exercises relating to information security and cybersecurity and shall, upon invitation, represent Hungary at international information security and cybersecurity exercises;

12. shall represent Hungary at Hungarian and international information security and cybersecurity events;

13. may participate in peer reviews referred to in Article 19 of Directive (EU) 2022/2555 of the European Parliament and of the Council, and initiate such a review;

14. shall monitor the implementation in Hungary of Directive (EU) 2022/2555 of the European Parliament and of the Council;

15. shall contribute to awareness-raising activities for the protection of the Hungarian cyberspace;

16. shall monitor whether information security requirements are complied with during the development of electronic information systems;

17. shall approve the putting into use of electronic information systems in accordance with the government decree and may prohibit or restrict the use of the electronic information system, the processing of data abroad and the use of a cloud computing service until the established deficiencies are remedied;

18. may identify an entity as essential entity or important entity in accordance with a government decree;

19. may put forward a proposal to the designating authority under the Critical Entity Resilience Act for designation as a critical entity, and to the designating authority under the Defence and Security Activities Coordination Act for designations as an entity important for the defence and security of the country;

20. may organise Hungarian information security and cybersecurity exercises and order an entity to participate in an exercise, and may issue guidelines as regards exercises organised by the entity;

21. shall act as a specialist authority as regards professional issues specified in the government decree on the designation of specialist authorities acting upon a compelling reason of public interest;

22. shall represent Hungary in European Union and international organisations and committees responsible for electronic information system security; and

23. shall perform the tasks of a single point of contact under Regulation (EU) 2022/2555 of the European Parliament and of the Council.

(2) In the context of the performance of its audit tasks, the national cybersecurity authority shall prepare an annual audit plan based on risk assessment, seeking in advance the proposals of a designating authority under the Critical Entity Resilience Act and the Defence and Security Activities Coordination Act.

(3) The national defence cybersecurity authority shall carry out the tasks listed in paragraph (1), points 1 to 11 and 15 to 21; the provisions of section 11 (13) and section 28 (4) and (7) need not be applied to its activities. If paragraph (1), point 10 applies, the national defence cybersecurity authority shall inform the national defence cybersecurity incident handling centre.

(4) Functions and powers and detailed rules of procedure of the national cybersecurity authority and the national defence cybersecurity authority shall be laid down in a government decree.

(5) SARA

a) shall proceed in accordance with paragraph (1), points 4, 5, 7, 8 and 11 to 15 and paragraphs (3) and (4) as well as a decree by the president of SARA;

b) may order and monitor all measures for the protection of electronic information systems that are suitable for handling threats compromising the electronic information system concerned;

c) shall keep a register of data listed under section 29 (1);

d) may conduct an extraordinary check or order an extraordinary audit if a significant cybersecurity incident occurs or non-compliance with security requirements is suspected;

e) specifying the objective, shall be entitled to request from the entity and access the following:

ea) documents supporting the appropriateness of security classification and security arrangements;

eb) the document drawn up of the performance of internal IT security scan; and

ec) for the purpose of carrying out supervisory tasks, other data, information or documents demonstrating compliance with the laws.

(6) Detailed rules on carrying out an administrative audit by SARA shall be set out in a decree by the president of SARA.

(7) The cybersecurity authority shall be entitled to take supervision measures and to impose legal consequences as regards

a) entities providing services within the territory of Hungary or the network and information system of which is located within the territory of Hungary, provided that a relevant request for mutual assistance is received from the cybersecurity authority of a European Union Member State, or

b) entities providing services in Hungary without having a designated representative in any of the European Union Member States.

(8) To carry out its tasks set out by law, the cybersecurity authority may prioritise the conduct of supervision tasks on the basis of risk assessment.

(9) For the purposes of carrying out tasks relating to cybersecurity supervision under section 23 (1) b), food-chain supervision organs specified in a decree by the Government shall inform SARA, by 1 February each year, of the designation, seat and tax number of entities referred to in line 3 of the table in Annex 3.

18. General rules of authority procedure

Section 25 (1) The application of summary procedure in the proceedings of the cybersecurity authority shall be prohibited.

(2) For an audit of the implementation of protective measures and an administrative proceeding for the investigation of cybersecurity incidents, the administrative time limit for an authority proceeding conducted by the national cybersecurity authority shall be one hundred twenty days.

(3) The administrative time limit for an administrative audit carried out by SARA shall be one hundred twenty days and, for a proceeding relating to the official registration of auditors and economic operators authorised to carry out vulnerability scan or incident investigation or the audit of entities certifying the use of post-quantum cryptography or entities authorised to provide a post-quantum cryptography application, ninety days.

(4) The proceeding referred to in paragraph (3) may be suspended until the completion of the company check.

19. Identification procedure

Section 26 (1) The national cybersecurity authority may identify an entity as essential entity or important entity (hereinafter “identification proceeding”), provided that it is not covered by section 1 (1) and was not designated as a critical entity under the Critical Entity Resilience Act or an entity important for the defence and security of the country under the Defence and Security Activities Coordination Act, and at least one of the conditions listed in section 1 (6) is met.

(2) If the conditions under section 1 (6), points 6 to 9 are met simultaneously, the national cybersecurity authority shall identify the entity as an essential entity.

(3) In an identification proceeding, the national cybersecurity authority shall proceed observing the provisions of section 2.

Section 27 (1) In an identification proceeding, the national cybersecurity authority shall proceed *ex officio*.

(2) The national cybersecurity authority shall adopt a conclusive decision on the conditions for recording an entity in the register of essential or important entities; in this context, the national cybersecurity authority shall specify the tasks of the entity under this Act and inform the entity accordingly.

(3) With a view to conducting an identification proceeding, the national cybersecurity authority may request data other than personal data from the following:

a) an entity;

b) an entity exercising authority, supervision or control powers over the entity; and

c) a publicly certified register.

(4) If an entity identified as an essential entity or an important entity does not agree to the identification, the entity shall prove that it does not meet the conditions set out in the decision on identification as an essential or important entity.

20. Official register

Section 28 (1) For the purpose of performing its tasks laid down in this Act, the national cybersecurity authority shall record and process the following:

1. for an entity,

a) data required for the identification of the entity;

b) contact details of the entity, including electronic contact details; public IP addresses and IP ranges used by the entity; as well as the seat, establishment and branch of an entity other than an entity listed in Annex 1;

c) whether the entity qualifies as an essential entity or an important entity;

d) sector, subsector and entity type under Annexes 2 and 3;

e) list of European Union Member States in which the entity provides service, if applicable;

f) designation, summary description, security classification, and specification of security classification at the time of registration and review, of the electronic information systems of the entity;

g) data relating to the classification of data processed in the electronic information system, and location of processing, including name of the country and type of the cloud;

h) data relating to cloud computing services used in connection with the electronic information system;

i) protective measures relating to the electronic information system and their status;

j) name or company name, mailing address, phone number and electronic mailing address of the representative operating within the territory of Hungary of an entity registered outside Hungary;

k) data suitable for the identification of a person or entity carrying out the tasks of the person responsible for electronic information system security as well as personal identification data, phone number ensuring direct contact, electronic contact details, education, professional qualification and professional experience of the natural person who actually carries out the activity;

l) information security regulations of the entity;

m) data relating to further training of the head of the entity and the person responsible for electronic information system security;

n) outcome of audit, except for electronic information systems for national defence purposes;

o) information relating to administrative audits;

p) outcome of vulnerability scan as well as vulnerability management plan for the elimination of vulnerabilities;

2. for an entity connected to a central system:

a) designation and unique identification number of the central system used by the user entity;

b) name of the entity exercising the right of disposal over the central system;

3. for a central system, in addition to those listed in point 1:

a) unique identification number of the central system;

b) designation of the user entities;

4. for a central service provider, in addition to those listed in point 1:

a) unique identification number of the electronic information system involved in the service provided by the central service provider;

b) data suitable for the identification of the supporting system provided by the central service provider;

c) designation of the user entities;

5. notifications relating to cybersecurity incidents received from the cybersecurity incident handling centre and data relating to persons referred to therein;

6. personal identification data and contact details, including electronic contact details as well as data relating to expertise, of the natural persons suitable for carrying out the tasks of a person responsible for electronic information system security;

7. further data prescribed in a government decree, other than personal data.

(2) For the purpose of the performance of its tasks under this Act, the national defence cybersecurity authority shall register data referred to in paragraph (1), point 1 a) to m) and p) and points 2 to 5 and 7.

(3) The national cybersecurity authority and the national cybersecurity incident handling centre may access data listed in paragraph (1), point 1 a) to c), j) to k) and p) from the register of the national defence cybersecurity authority.

(4) The national cybersecurity authority shall compile, and review every two years, a list of essential entities and important entities, taking into account also data provision by SARA.

(5) Unless otherwise provided by the law, data from the register referred to in paragraphs (1) and (2) may be transferred exclusively to

a) SARA;

b) the national cybersecurity incident handling centre;

c) the single point of contact under Regulation (EU) 2022/2555 of the European Parliament and of the Council;

d) the National Authority for Data Protection and Freedom of Information;

e) the designating and registration authority under the Critical Entity Resilience Act;

f) the designating and registration authority under the Defence and Security Activities Coordination Act;

g) a public authority within the meaning of Regulation (EU) 2022/2554 of the European Parliament and of the Council;

h) the national defence cybersecurity authority;

i) cyberspace operational forces of the Hungarian Defence Forces;

j) the national defence cybersecurity incident handling centre; and

k) the national cybersecurity authority.

(6) The national cybersecurity authority shall transmit information security regulations received from a critical entity or an entity important for the defence and security of the country to the registration authority under the Critical Entity Resilience Act or the Defence and Security Activities Coordination Act, respectively.

(7) The national cybersecurity authority shall publish on its website a list of natural persons suitable for the performance of the tasks of the person responsible for electronic information system security.

Section 29 (1) For the purpose of performing its tasks laid down in this Act, SARA shall, in accordance with a decree by the president of SARA, register and process the following:

a) for an entity referred to in section 1 (1) b), d) or e):

aa) data required for the identification of the entity;

ab) seat, establishment and branch of the entity;

ac) for an entity that is not an entity 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;

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

ae) list of European Union Member States in which the entity provides services;

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

b) data required for the identification of the entity authorised to carry out a vulnerability scan, and contact details, including electronic contact details, of the entity;

c) natural personal identification data required for the identification of a natural person authorised to carry out a vulnerability scan, including electronic contact details as well as data relating to the professional expertise of the natural person authorised to carry out a vulnerability scan; and

d) data required for the identification of economic operators authorised to handle cybersecurity incidents and contact details of the entities, including electronic contact details.

(2) SARA shall prepare, and review every two years, a list of essential entities and important entities falling within the scope of section 1 (1) d) and e) as well as a list of entities providing domain name registration services. After the preparation and review of the list, SARA shall inform the national cybersecurity authority of the data specified in a government decree.

(3) Unless otherwise provided by the law, data transfer from the register referred to in paragraph (1) may be performed exclusively to cybersecurity authorities, cybersecurity incident handling centres and entities referred to in section 24 (9).

(4) SARA shall provide the national cybersecurity authority and the national cybersecurity incident handling centre with direct access to registration data processed by SARA of the entity.

(5) If an entity recorded in the register under paragraph (1) a) declares that it no longer qualifies as an entity under section 1 (1) b), d) or e), SARA shall delete from the register the data referred to in paragraph (1) a) five years after the declaration,

21. Legal consequences

Section 30 (1) Should an entity fail to fulfil or comply with the security requirements laid down by the law or the related procedural rules, to eliminate the security deficiencies, to take the measures necessary for compliance, or to cease the activity, the cybersecurity authority

a) shall warn the entity to comply with the security requirements laid down by the law and the related procedural rules and, setting an appropriate time limit, call upon it to eliminate security deficiencies relating to the requirements or identified or brought to its attention during a check or an audit, to take the measures for ensuring compliance and to fulfil the reporting and data provisions obligations;

b) may require the entity to cease the unlawful conduct and to refrain from the repeated commission of the unlawful act;

c) may contact the organ supervising the entity or those exercising ownership rights within the meaning of the Act on national assets and request their assistance; and

d) shall be entitled to appoint an information security officer at the expense of the entity in accordance with the provisions of a government decree or, for an entity referred to in section 1 (1) d) or e), a decree issued by the president of SARA.

(2) If, despite the application of a measure referred to in paragraph (1), the entity concerned does not meet, or does not comply with, the security requirements set out in the law and the related procedural rules, does not eliminate the security deficiencies, fails to take the measures ensuring compliance or does not cease the activity concerned, the cybersecurity authority, weighing all the circumstances of the case, may impose a fine as specified in a government decree.

(3) Should the head of the entity fail to comply with its obligation imposed by the law, the national cybersecurity authority, weighing all circumstances of the case, may impose a fine, or in the event of a repeated violation shall impose a fine, as specified in a government decree.

(4) The amount of the fine that the cybersecurity 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 shall be laid down in a government decree.

(5) The cybersecurity authority

a) may require the entity to make public, in a manner specified by the cybersecurity authority, the fact that a violation occurred and the circumstances of the violation, observing the rules on data protection and trade secret;

b) may order that the users of services provided by the entity be informed of any threats potentially affecting them as well as any preventive, protection or remedial measures that are required for eliminating such a threat or that may be taken, and the likely effects of such measures;

c) in the event of the occurrence of a cybersecurity incident, shall inform the public and may, in a conclusive decision, require entities to provide information, should this be necessary to prevent a specific cybersecurity incident or to handle an ongoing cybersecurity incident; and

d) may require an entity to inform the cybersecurity authority if taking a crisis management or emergency management measure becomes necessary.

(6) If an essential entity other than an administrative organ fails to comply with a requirement by the cybersecurity authority within the time limit set by the authority, the cybersecurity authority

a) may request the competent authority to temporarily suspend the certification or permit, in whole or in part, relating to the essential services or activities provided by the essential entity that are affected by the violation;

b) may request the company registration court to temporarily ban the head of the essential entity from performing executive tasks within the entity concerned.

(7) The legal consequences referred to in paragraphs (1), (2) and (5) and (6) may also be applied together and repeatedly.

(8) If the entity takes the necessary measure to remedy deficiencies or complies with the requirements by the authority, the cybersecurity authority shall arrange for the lifting of temporary measures referred to in paragraph (6).

(9) When imposing a legal consequence, the cybersecurity authority shall observe the criteria of proportionality and graduation, taking into account the effectiveness and the dissuasive effect of the legal consequence.

(10) If an entity referred to in section 1 (1) a) to c) or f) ignores a requirement by the authority or fails, due to its own fault, to implement the protective measures recommended by the national cybersecurity authority and, thus, a cybersecurity incident or a cybersecurity near miss occurs, the national cybersecurity authority may require the entity to reimburse the costs incurred in averting the occurrence of the cybersecurity incident or the cybersecurity near miss.

(11) If an entity referred to in section 1 (1) d) or e) does not meet or does not comply with the cybersecurity requirements set out in the law or the related procedural rules, SARA, in addition to the provisions of paragraphs (1) to (5),

a) may prohibit, observing the opinion of the authority permitting or supervising the activity of the entity, the entity concerned from an activity directly jeopardising compliance with security requirements;

b) shall, if a fine is imposed, inform the authority permitting or supervising the activity of the entity about the imposition of the fine and the underlying facts.

Section 31 (1) The cybersecurity authority shall designate the information security officer referred to in section 30 (1) d) for a fixed period or until a specific condition is met. The information security officer shall supervise compliance with security requirements set out by the law and observance of related procedural rules at the entity. The cybersecurity authority shall be in charge of the professional direction of the information security officer.

(2) For an entity referred to in

a) section 1 (1) a) to c), requirements for an information security officer and the detailed rules on his designation, rights and tasks shall be laid down in a government decree, while requirements relating to his education, further education obligations and professional experience as well as the procedure for the publication of professional qualifications by the national coordination centre referred to in section 75 (1) shall be laid down in a decree by the Minister responsible for information technology;

b) section 1 (1) d) or e), requirements for an information security officer and detailed rules on his designation, rights and tasks shall be laid down by the president of SARA in a decree.

Section 32 (1) If SARA detects or becomes aware, including on the basis of indication by the national cybersecurity authority, that an auditor does not meet, or does not comply with, the cybersecurity requirements set out in the law and the related procedural rules, SARA may

a) warn the auditor to comply with the requirements set out in the law and the related procedural rules;

b) order, setting a time limit, the remedying of identified security deficiencies or the taking of measures necessary for compliance; or

c) temporarily ban the auditor from acting as an auditor, and inform the national cybersecurity authority accordingly.

(2) If, despite the application of the measures referred to in paragraph (1), the auditor does not meet, or does not comply with, the requirements set out in the law and the related procedural rules, does not remedy the identified deficiencies, fails to take the measures ensuring compliance or does not cease the activity concerned, SARA, weighing all the circumstances of the case, may impose a fine as specified in a government decree; in the event of continued non-compliance, the fine may be imposed repeatedly.

(3) Should the SARA disclose any violation in accordance with paragraph (1) that affects the entity audited by the auditor, SARA shall notify immediately the person responsible for electronic information system security who is designated at that specific entity audited by the auditor and provide information on the circumstance of the possible cybersecurity incident or data leak.

22. Rendering data temporarily inaccessible

Section 33 (1) The cybersecurity authority may, in a conclusive decision, order that data published via an electronic communications network be rendered temporarily inaccessible if it poses a threat to Hungarian cyberspace security and it is subject to cybersecurity incident handling by the national cybersecurity incident handling centre.

(2) The national defence cybersecurity authority shall be in charge of ordering that data published via an electronic communications network be rendered temporarily inaccessible if it violates or jeopardises national defence interests or poses a threat to the security of an electronic information system for national defence purposes.

(3) Rendering electronic data temporarily inaccessible shall be ordered by the cybersecurity authority in a conclusive decision which is declared immediately enforceable. The period for which the cybersecurity authority orders rendering electronic data temporarily inaccessible shall not exceed ninety days; this period may be extended by ninety days, if justified.

(4) The cybersecurity authority shall communicate a conclusive decision ordering electronic data to be rendered temporarily inaccessible by public notice and send it to the National Media and Infocommunications Authority (hereinafter the "NMHH").

(5) The public notice shall be published on the website of the cybersecurity authority for 3 days. The day of the communication of the conclusive decision shall be the day following the publication of the public notice.

(6) NMHH shall send the conclusive decision to its addressees through the delivery system referred to in the Act on electronic communications.

(7) An obligation imposed by the conclusive decision referred to in paragraph (3) shall apply to all electronic communications service providers, even if they are not specifically named in the conclusive decision.

(8) NMHH shall organise and monitor the implementation of rendering data temporarily inaccessible in compliance with the Act on electronic communications.

(9) An obligation to render data temporarily inaccessible shall be terminated once the time limit specified in the conclusive decision expires.

(10) The cybersecurity authority shall lift rendering data temporarily inaccessible before its termination if

a) the grounds for ordering it have ceased;

b) the coercive measure of rendering electronic data temporarily inaccessible or the measure of rendering electronic data permanently inaccessible was ordered or is being implemented as regards the electronic data according to information provided by the court, prosecution office or investigating authority proceeding in the criminal case, or NMHH; or

c) there are doubts as to whether the provision can be implemented by electronic communications service providers on the basis of the data content provided.

(11) Where the cybersecurity authority ordered that electronic data be rendered inaccessible pursuant to paragraphs (1) or (2), and established, after the conclusive decision reaches administrative finality, that the unlawful act performed by the publication of the electronic data indicated in the conclusive decision is performed also by the making accessible or publication of other electronic data with content that is identical for the purposes of establishing unlawfulness, in particular other IP address, domain-domain or domain-subdomain, the cybersecurity authority shall, without conducting a repeated authority proceeding and without decision making under paragraph (3), notify, sending data required for rendering data inaccessible by electronic means using a secure delivery service, NMHH (hereinafter "simplified follow-up"); NMHH shall communicate such data exclusively by electronic means to the electronic communications service providers providing access. Electronic communications service providers shall ensure that electronic data as specified by the data required for rendering data inaccessible sent for the purpose of simplified follow-up is rendered inaccessible for as long as the related conclusive decision adopted in accordance with paragraph (3) remains enforceable.

Section 34 (1) In order to eliminate a significant cyber threat or to interrupt a series of ongoing cybersecurity incidents, the head of the national cybersecurity incident handling centre may order rendering data temporarily inaccessible with immediate effect until a decision is adopted by the cybersecurity authority, but for no longer than a period of seventy-two hours.

(2) If rendering data temporarily inaccessible is ordered with immediate effect, it shall be implemented in the shortest time possible given the state of the art.

Section 35 (1) The cybersecurity authority may impose a fine ranging from 1 million forints to 5 million forints on an electronic communications service provider that fails to comply with its obligations set out in this subtitle. The fine may be imposed repeatedly, setting a new time limit, after the time limit set for compliance with the obligation expires without result.

(2) The cybersecurity authority, NMHH and the electronic communications service provider shall not be held liable for any damage arising from the fact that the electronic data that is rendered inaccessible includes, in addition to the content specified in section 33 (1) and (2), also other content that cannot be separated technically or the technical separation of which cannot be expected in the course of the implementation of rendering data inaccessible.

23. Temporary removal of electronic data

Section 36 (1) The subject of an obligation to temporarily remove electronic data shall be the hosting service provider or the intermediary service provider providing also hosting services within the meaning of the Act on certain issues of electronic commerce services and information society services that processes the electronic data concerned (hereinafter the "subject of the removal obligation"). The subject of the removal obligation shall be required to temporarily remove the electronic data within one working day from the communication of the conclusive decision.

(2) A conclusive decision under paragraph (1) shall be served on those entitled to dispose of the data only if their identity and contact details are known from the data of the proceeding available at that time.

(3) Section 33 (1) to (5) and (9) to (11) as well as sections 34 to 35 shall apply accordingly to temporary removal.

Chapter IV

PROVISIONS ON CYBERSECURITY CERTIFICATION

Section 37 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 national cybersecurity certification authority referred to in Regulation (EU) 2019/881 of the European Parliament and of the Council (hereinafter "certification authority").

24. Requirements of national cybersecurity certification schemes

Section 38 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 lifecycle 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 lifecycle 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 ICT 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 event;

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 ICT vulnerabilities and are provided with mechanisms for secure updates.

Section 39 (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) 1025/2012 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 entities 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 analyses must be carried out, also allowing *ex-post* monitoring of the activity; and

c) the requirements for the documentation of evaluation results.

25. Assurance levels of national cybersecurity certification schemes

Section 40 (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 cybersecurity incidents and attacks;

b) at assurance level ‘substantial’ which is intended to minimise the known cybersecurity risks, and the risk of cybersecurity 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 cybersecurity 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.

26. Requirements for cybersecurity certifications and statements of conformity

Section 41 (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 entity;

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 ICT vulnerabilities or irregularities concerning the security of the ICT product, ICT service or ICT process.

Section 42 (1) A conformity mark shall be affixed in the manner and form set out in a decree by the president of SARA or, if section 45 (1) b) applies, the Government, to ICT products, ICT services and ICT processes that have been certified or for which a statement of conformity has been issued.

(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.

27. Conformity self-assessment, conformity assessment

Section 43 (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 to the certification authority 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 conformity with the indicated certification scheme for them to be entered in a register within 15 days following the issuance of the statement of conformity referred to in paragraph (2).

Section 44 (1) Third party conformity assessment activities may be carried out only by an entity 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 entity has been accredited abroad, its accreditation status is recognised by the said accreditation body;

b) meets the requirements laid down in a decree by the president of SARA or, for a certification authority referred to in section 45 (1) b), the Government for each assurance level, unless the European certification scheme applies; and

c) is registered with the certification authority.

(2) Detailed rules on conformity self-assessment, the certification procedure and, for a European certification scheme, the conditions for registration under paragraph (1) c), as well as the obligations and activities of conformity assessment bodies, shall be laid down in a decree

a) by the president of SARA, except for defence industry research, development, manufacturing and trade;

b) by the Government as regards defence industry research, development, manufacturing and trade.

(3) By way of derogation from the Act on the general rules on taking up and pursuit of service activities, where the certification authority did not decide on entry into the register under paragraph (1) c) within the applicable administrative time limit, the applicant shall not be entitled to take up or pursue the activity specified in the application, and the rules on an omission by the authority as laid down in the Act on the Code of General Administrative Procedure shall apply.

28. Supervision of cybersecurity certification

Section 45 (1) The following shall act as a certification authority:

a) SARA;

b) by way of derogation from point a), for tasks relating to defence industry research, development, manufacturing and trade, the 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 46 (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, if a European certification scheme is issued, take measures without delay to review or set aside any national cybersecurity certification scheme on the subject matter covered by the European cybersecurity certification scheme.

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

Section 47 (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 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) If paragraph (4) b) apply, authorisation shall be granted on the condition that the conformity assessment body qualifies as an economic operator referred to in section 57 (1) c).

(6) The validity of the authorisation issued in an authorisation proceeding 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 proceeding under paragraph (4), it shall notify the conformity assessment body to the European Commission within 15 days from when the decision on granting the authorisation reaches administrative finality.

(8) As part of 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) The certification authority shall proceed against an entity that does not meet the requirements under section 44 and carries out conformity assessment activities without authorisation.

(10) An administrative service fee shall be paid for proceedings conducted by a certification authority referred to in section 45 (1) b). The amount of the administrative service fee and the detailed rules concerning the collection, distribution, management, registration and reimbursement of this fee shall be determined in a decree issued by the Minister responsible for national defence for the implementation of this Act.

Section 48 (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 to this fact, and the documents that support that the requirements set out in the decree by the president of SARA are met;

d) information provided in the conclusive 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 47 (4) if such a proceeding is 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 European 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 ICT vulnerabilities and irregularities referred to in section 41 (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 ICT vulnerabilities and 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 entities:

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

b) to the accreditation body designated 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 cybersecurity incident handling centres referred to in section 63, for the performance of activities related to ICT vulnerabilities and irregularities referred to in section 41 (3).

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

Section 49 (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 containing a 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 an amount prescribed by a government decree; in the case of continued non-compliance, the fine may be imposed repeatedly.

(3) The certification authority may impose an administrative fine in an amount prescribed by a decree of the Government on a person carrying out unauthorised conformity assessment activities. When determining the amount of the fine, the Authority shall take into account the criteria set out in the Act on sanctions for administrative violations. A warning shall not be applicable as an administrative sanction.

Section 50 (1) The certification authority shall process any classified data, personal data or sensitive data as well as any other data protected by law and qualifying 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 when the accreditation status terminates and the date when the statement of conformity becomes ineffective. Subsequently, the certification authority shall erase the data from its electronic information systems and data-storage media.

(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 confidentiality with respect to the data obtained in accordance with paragraph (1); the confidentiality 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 register keeping in accordance with a decree by the president of SARA or, for a certification authority under section 45 (1) b), the Government.

(5) The manufacturer in carrying out conformity self-assessment and the conformity assessment body in the course of a certification proceeding, shall act in accordance with a decree by the president of SARA or, for a certification authority under section 45 (1) b), the Government.

Chapter V

POST-QUANTUM CRYPTOGRAPHY

29. General rules on the use of post-quantum cryptography

Section 51 Throughout the entire lifecycle of an electronic information system of an entity required to use post-quantum cryptography, the closed, comprehensive, continuous and risk-proportionate protection of the following shall be ensured:

a) confidentiality, integrity and availability of data and information processed in the electronic information system; and

b) by means of a post-quantum cryptography application that provides security beyond a traditional cryptography application, protection of integrity and availability of the electronic information system and its elements in the course of using a service provider within the meaning of the Act on electronic communications or its information-society-related services both on a government network between the physically separate locations of entities required to use post-quantum cryptography and on public internet platforms.

30. Protection of an entity required to use post-quantum cryptography

Section 52 In the context of the performance of tasks set out in a law, an entity required to use post-quantum cryptography shall be required to obtain, with a view to the deployment of a post-quantum cryptography application, a post-quantum cryptography application if using a service provider within the meaning of the Act on electronic communications or other information-society-related service both on a government network between its physically separate locations and on public internet platforms from a registered entity authorised to provide such an application, and to establish protection on the networks managed by it, in order to ensure that the electronic information flow is secured against cyberattacks by quantum computers.

31. Requirements for entities providing a post-quantum cryptography application

Section 53 (1) An entity may provide a post-quantum cryptography application (hereinafter "post-quantum cryptography application provider") to an entity required to use post-quantum cryptography only if it

a) poses no national security risk; and

b) complies with the requirements under paragraph (3).

(2) In accordance with paragraph (1), an entity may carry out an activity for post-quantum cryptography application provision only if

a) it holds a facility security clearance referred to in the Act on the protection of classified data; and

b) its relevant employee or subcontractor holds a personal security clearance referred to in the Act on the protection of classified data.

(3) An entity may carry out an activity for post-quantum cryptography application provision only if that electronic information system used by it ensures that the components are closed and prevents unauthorised access to the information system and any undetected modification thereof. The electronic information system of a post-quantum cryptography application provider shall comply with the requirements under this Act.

32. Certification of compliance with post-quantum cryptography requirements

Section 54 (1) An entity that intends to provide a post-quantum cryptography application shall provide evidence of compliance with the requirements listed in section 53 (3) by means of a certificate of the closed nature of the information system issued by a certifying entity registered in the register referred to in section 56 (3) b) (hereinafter "certifying entity").

(2) The certifying entity shall issue an expert opinion for the entity that intends to provide a post-quantum cryptography application that its end-to-end application is capable of providing post-quantum cryptography offering security beyond cryptographic applications.

(3) Should a certifying entity find a fact as regards the information system of a certified entity that has a negative impact on the continuous operation of the entity or indicates the commission of a criminal offence, the violation of a law or the danger thereof, it shall notify SARA without delay.

33. Provisions on certifying entities

Section 55 (1) Only an entity that does not pose a national security risk and complies with the requirements listed in section 53 (2) may serve as a certifying entity.

(2) A certifying entity may process data processed by an entity that intends to provide a post-quantum cryptography application or a certified entity, including accessed certified data, personal data and sensitive data, trade secret, bank secret, payment secret, insurance secret, securities secret, fund secret, and secret related to the exercise of a profession, that are required for the conduct of the certification proceeding only for the purpose of assessing the fulfilment of requirements to be certified, to the extent required for the conduct of the certification proceeding, and until the completion of the certification proceeding; such data shall not be transferred to third parties.

(3) The certifying entity shall specify in regulations the positions the holder of which may access trade secrets and learn their content in the course of a certification proceeding. Employees participating in the proceeding shall be subject to an obligation of confidentiality as regards any trade secret they became aware in the course of the certification proceeding even after the termination of their legal relationship with the entity certifying the post-quantum cryptography application.

34. Supervision of post-quantum cryptography

Section 56 (1) As regards the certifying entity and entities authorised to provide a post-quantum cryptography application, SARA, exercising its supervisory powers, may

a) carry out an administrative audit;

b) conduct an extraordinary check if non-compliance with the requirements set out in this chapter is suspected.

(2) SARA shall monitor, applying section 25 (1) and (3), whether the certifying entity and the entity authorised to provide a post-quantum cryptography application comply with their obligations, in accordance with the detailed rules set out in a decree by the president of SARA.

(3) For the purpose of performing its tasks laid down in this Act, SARA shall keep a register of the following:

a) entities authorised to provide a post-quantum cryptography application; and

b) certifying entities providing certification in accordance with section 54.

(4) The register referred to in paragraph (3) shall contain the following:

a) designation and seat of the entity and natural identification data, phone number and electronic mailing address of its designated contact person;

b) identifier of the entity received upon registration;

c) further data specified in a decree by the president of SARA that do not qualify as personal data.

(5) If an entity registered in the register referred to in paragraph (3) no longer performs a post-quantum cryptography application provision activity or a certification activity, SARA shall delete from the register the data referred to in paragraph (3) five years after the notification of the termination of the activity.

(6) Should the entity authorised to provide a post-quantum cryptography application or a certifying entity notify any change to the data referred to in paragraph (3), SARA shall delete from the register the data that was recorded before the registration of the change to the data five years after the registration of the change.

(7) Unless otherwise provided by the law, data transfer from the register referred to in paragraph (3) may be performed exclusively to cybersecurity authorities and cybersecurity incident handling centres.

Chapter VI

VULNERABILITY SCAN

35. Holders of authorisation to carry out vulnerability scan

Section 57 (1) The following shall be authorised to carry out vulnerability scan:

a) state organ designated in a decree by the Government, except for electronic information systems for national defence purposes;

b) national defence cybersecurity incident handling centre, for electronic information systems for national defence purposes; and

c) an economic operator recorded in the register of economic operators authorised to perform vulnerability scan that is maintained by SARA that holds a facility security clearance, and meets the infrastructural conditions and has the expertise for the performance of the task.

(2) A person may carry out a scan on behalf of an economic operator authorised to perform vulnerability scan only if

a) his national security vetting is completed and no national security risk was established in the course of the national security vetting;

b) he has the expertise necessary for carrying out a vulnerability scan;

c) has at least two years of professional experience within the field of vulnerability scanning; and

d) he is recorded in the register of persons authorised to carry out a vulnerability scan that is maintained by SARA.

(3) Registration in accordance with paragraph (1) c) shall be conditional upon at least two experts meeting the requirements set out in paragraph (2) being employed by the economic operator authorised to perform vulnerability scan. Detailed rules on registration in accordance with paragraph (1) c) and (2) d) and the infrastructural conditions and expertise required for carrying out the task shall be set out in the decree issued by the president of SARA seeking the opinion of the Minister responsible for information technology.

(4) SARA shall involve the state organ authorised to perform vulnerability scan in the proceedings for registration under paragraphs (1) and (2), for the purpose of establishing whether the expertise and the infrastructural conditions required for carrying out the task are available.

(5) Except for electronic information systems for national defence purposes, the state organ authorised to perform vulnerability scan shall carry out the vulnerability scan

a) of the electronic information system of entities listed in Annex 1, points 1 to 9, 11, 14 and 15;

b) of the electronic information system specified by the national cybersecurity authority of entities identified as essential or important entities by the national cybersecurity authority.

(6) Should the state organ authorised to perform vulnerability scan not have sufficient human resources to carry out a vulnerability scan, it may consent to the entity referred to in paragraph (5) having the vulnerability scan carried out by an economic operator authorised to perform vulnerability scan, selected by the entity.

(7) The state organ authorised to perform vulnerability scan may take over or assist in the vulnerability scan of an electronic information system of paramount importance for the operation and security of the state, the economy and the society.

(8) If there is no economic operator authorised to perform vulnerability scan that meets the requirements for carrying out a vulnerability scan set out in this Act as regards the electronic information system, other than an electronic information system referred to in paragraph (5) a), of a critical entity within the meaning of the Critical Entity Resilience Act or an entity designated as entity important for the defence and security of the country pursuant to the Defence and Security Activities Coordination Act, the vulnerability scan shall be carried out by the state organ authorised to perform vulnerability scan.

(9) The organ referred to in paragraph (1) at which the vulnerability scan was requested shall assess whether it is authorised to carry out the vulnerability scan and, if it finds that another organ referred to in paragraph (1) has exclusive authorisation, transmit the request to the competent organ without delay.

36. Launching a vulnerability scan

Section 58 (1) The national cybersecurity authority may impose an obligation to have a vulnerability scan carried out on an entity. Should the entity fail to fulfil the obligation imposed by the authority, the national cybersecurity authority may impose a fine.

(2) In the event of an obligation imposed by an authority referred to in paragraph (1), the national cybersecurity authority shall take account of the importance of the electronic information system for the operation of the state.

(3) When imposing an obligation referred to in paragraph (1), the national cybersecurity authority shall specify the electronic information systems covered by the vulnerability scan, and may specify the vulnerability scanning tool or method to be applied.

Section 59 The state organ authorised to perform vulnerability scan may, at its own initiative, launch and carry out a vulnerability scan if it holds registered user rights or, as regards the electronic information system of entities referred to in section 57 (5), even absent such rights.

Section 60 (1) Except for entities referred to in section 1 (1) d) and e), the head of an entity falling within the scope of this Act may request the vulnerability scan of an electronic information system even without being subject to an obligation imposed by an authority, provided that the system is subject to security classification and registered with the cybersecurity authority.

(2) The head of the entity shall request the vulnerability scan referred to in paragraph (1) sixty days before its planned commencement with a view to its planning and preparation. In scheduling the commencement date of the vulnerability scan, the entity shall take account of also the time requirement of the vulnerability scanning method as set out in a government decree, taking into consideration also the planned date of putting into use the electronic information system.

(3) The state organ authorised to perform vulnerability scan may, after the assessment of received requests, establish an order of priority; having regard to this order of priority, it may set the commencement date of the scan at a date not more than fifteen days later than the date previously established.

(4) The state organ authorised to perform vulnerability scan shall prioritise carrying out vulnerability scans ordered by the cybersecurity authority or launched *ex officio* over those required by an entity. In establishing the order, the organ shall act assessing the available resources and, applying a risk-based approach, the importance of the electronic information system for the operation of the State. Where carrying out a request by an entity does not interfere with the performance of mandatory tasks, the state organ authorised to perform vulnerability scan shall carry out the vulnerability scan, within the limits of its available capacity.

Section 61 As regards electronic information systems not falling within the scope of this Act, the state organ authorised to perform vulnerability scan may carry out a vulnerability scan on the basis of an agreement entered into with the entity with the right of disposal over the electronic information system.

37. General provisions on vulnerability scans

Section 62 (1) A vulnerability scan may target also a specific part of an electronic information system.

(2) Due to its nature, a vulnerability scan may cause a loss or reduction in service; the entity carrying out the vulnerability scan shall not be liable for any damage arising therefrom, except where such damage is caused intentionally.

(3) Vulnerability scanning methods and the detailed rules on carrying out a vulnerability scan shall be laid down in a government decree.

(4) The entity carrying out the scan shall issue a statement on its position as regards the findings of the vulnerability scan, which shall include the classification of vulnerabilities detected. The detailed content of the position statement shall be set out in a government decree.

Chapter VII

PROVISIONS ON CYBERSECURITY INCIDENTS

38. Cybersecurity incident handling centres

Section 63 (1) The Government shall operate a national cybersecurity incident handling centre through the organ designated by it in a decree with a view to handling threats, cybersecurity incidents and crises affecting the open electronic information systems of the entities referred to in section 1 (10), other than electronic information systems for national defence purposes.

(2) The Government shall operate a cybersecurity incident handling centre through the organ designated by it in a decree with a view to handling threats, cybersecurity incidents and crises affecting electronic information systems for national defence purposes.

(3) Except for the national defence sector, a sector-related cybersecurity incident handling centre (hereinafter "sector-related cybersecurity incident handling centre") may be established in accordance with the provisions of a government decree, subject to approval of the national cybersecurity incident handling centre. The national cybersecurity incident handling centre shall carry out, or have carried out, the assessment and examination of the capabilities of the national cybersecurity incident handling centre, on the basis of which a cooperation agreement shall be concluded. In the course of the examination, the conditions laid down in the decree by the president of SARA referred to in section 70 (3) b) shall also be taken into account.

Section 64 (1) The national defence cybersecurity incident handling centre shall carry out tasks specified in a government decree as regards the following:

a) threats relating to the cyberspace, early warnings, and cybersecurity incident prevention;

b) cybersecurity incident handling;

c) cybersecurity crisis management;

d) vulnerabilities;

e) information and awareness raising activities as regards cybersecurity; and

f) representation of Hungary in European Union and international cooperation.

(2) Except for activities relating to cyber activities and entities endangering national defence interests and military cyberspace operations, the national defence cybersecurity incident handling centre

a) shall carry out the tasks against threats and attacks from cyberspace as regards entities falling within the scope of this Act, in accordance with the rules on competence laid down herein;

b) shall control preparation for threats from cyberspace and related security tasks, except for the national defence sector;

c) shall analyse traffic on electronic communications networks without accessing the content of communication conducted on them, detect threats and attacks from cyberspace;

d) shall carry out or initiate measures necessary to interrupt an attack from cyberspace and to determine its causes and those responsible.

(3) The national cybersecurity incident handling centre shall carry out the coordination and other tasks set out in a government decree as regards ICT vulnerabilities and other vulnerabilities reported by any natural or legal person concerning the electronic information system of an entity referred to in section 1 (10) or an ICT product or ICT service falling within the scope of this Act. Detailed rules on the detection and reporting of ICT vulnerabilities and other vulnerabilities shall be laid down in a decree by the Government. If the ICT vulnerability or other vulnerability is reported as regards the electronic information system of an entity other than those listed in section 1 (10) or an ICT product or ICT service other than those falling within the scope of this Act, the national cybersecurity incident handling centre shall carry out the tasks set out in the government decree within the limits of available resources and assessing the extent of danger. As regards the latter reports, the national cybersecurity incident handling centre shall be obliged to act only if doing so does not impose a disproportionate or unreasonable burden on the national cybersecurity incident handling centre or if the report concerns the electronic information system of an entity falling within the scope of this Act.

(4) The national defence cybersecurity incident handling centre may take over, or assist in, the handling and the investigation of cybersecurity incidents seriously endangering Hungarian cyberspace.

(5) The national defence cybersecurity incident handling centre shall carry out the tasks listed in paragraph (1) as regards the national defence sector.

(6) The sector-related cybersecurity incident handling centre shall carry out the tasks set out in the cooperation agreement concluded with the national cybersecurity incident handling centre.

(7) The functions and powers of the national cybersecurity incident handling centre and the national defence cybersecurity incident handling centre, the detailed rules on the performance of their tasks, as well as the detailed rules on early warnings, the system thereof, the provisions on the designation of the operator of the system, and the procedure for using the related early warning service shall be laid down in a government decree.

39. Cybersecurity incident prevention

Section 65 (1) The national cybersecurity incident handling centre may apply protective and preventive means for the detection of threats from cyberspace, and provide such services (hereinafter jointly “preventive means”) to entities referred to in section 1 (1).

(2) An entity referred to in section 1 (1) may request the national cybersecurity incident handling centre to apply preventive means at the expense of the entity; the national cybersecurity incident handling centre shall decide on the application of preventive means within the limits of available resources and assessing the extent of danger.

(3) On a proposal by the national cybersecurity incident handling centre, the national cybersecurity authority may also impose an obligation to apply preventive means on an entity referred to in section 1 (1) a) to c); the national cybersecurity incident handling centre may, on the basis of risk assessment, decide on the application of preventive means also on its own, following prior information provision to the entity concerned.

(4) At the request of the national cybersecurity incident handling centre, an entity referred to in section 1 (1) a) to c) shall be required to use preventive means.

(5) At the request of the national cybersecurity incident handling centre, an entity referred to in section 1 (1) a) to c) shall be required to join the system for sharing information on threats that is operated by the national cybersecurity incident handling centre; the entity may also itself apply to join that system. The national cybersecurity incident handling centre shall require the entity referred to in section 1 (1) a) to c) to join or consent to its joining assessing the extent of danger and taking account of available resources.

(6) The national cybersecurity incident handling centre shall be entitled to collect information intended for exclusively general cybersecurity purposes as regards all internet addresses with Hungarian use and geolocation and the services hosted on them, from which threats and cybersecurity incidents can be clearly identified.

(7) The activity referred to in paragraph (6) shall not lead to disproportionate harm to the service operator and shall not cause the inaccessibility of the system.

(8) The national cybersecurity incident handling centre shall utilise and use data established in the course of a vulnerability scan solely in an anonymised form, for the purpose of evaluating the state of the cyberspace.

40. Reporting and handling of cybersecurity incidents

Section 66 (1) Entities referred to in section 1 (1) a to c) and f) shall immediately report to the national cybersecurity incident handling centre all threats, cybersecurity near misses, cybersecurity incidents, including operational cybersecurity incidents, that occurred within their electronic information systems or of which they became aware, in accordance with the provisions of a government decree.

(2) Entities referred to in section 1 (1) d) and e) shall report to the national cybersecurity incident handling centre all threats, cybersecurity near misses and cybersecurity incidents, including operational cybersecurity incidents, that occurred within their electronic information systems or of which they became aware and that cause a serious disruption or pecuniary loss as regards the operation of the entity or the service provided by it or a significant material or non-material damage to another natural or legal person, in accordance with the provisions of a government decree.

(3) Entities referred to in section 1 (1) d) and e) may report to the national cybersecurity incident handling centre also cybersecurity incidents other than cybersecurity incidents referred to in paragraph (2).

(4) The entity shall report any threats, cybersecurity near-misses and cybersecurity incidents relating to an electronic information system for national defence purposes to the national defence cybersecurity incident handling centre specified in a decree by the Government.

(5) The national defence cybersecurity incident handling centre and the sector-related cybersecurity incident handling centre shall transfer the data of any threats, cybersecurity near misses and cybersecurity incidents of which they became aware to the national cybersecurity incident handling centre without delay.

(6) Should the national cybersecurity incident handling centre, the national defence cybersecurity incident handling centre or the sector-related cybersecurity incident handling centre find that it lacks competence, it shall send the report to the competent cybersecurity incident handling centre without delay.

Section 67 (1) Entities and persons not falling within the scope of section 1 (10) may voluntarily report to the national cybersecurity incident handling centre all threats, cybersecurity near misses and cybersecurity incidents that have or can have a significant impact on Hungarian cyberspace security.

(2) The national cybersecurity incident handling centre may prioritise reports from entities falling within the scope of this Act over voluntary reports. The national cybersecurity incident handling centre shall handle voluntary reports within the limits of available resources and assessing the extent of danger.

(3) As regards voluntary reports, the national cybersecurity incident handling centre shall be obliged to act only if doing so does not impose a disproportionate or unreasonable burden on the national cybersecurity incident handling centre or if the voluntary report concerns the electronic information system of an entity falling within the scope of this Act.

(4) Based on a voluntary report, no obligation may be imposed on those making the report to which they would otherwise not be subject, even in the absence of such a report.

Section 68 (1) If a significant cybersecurity incident occurs in an electronic information system, which involves damaging fundamental information or personal data required for the operation of the entity with the right of disposal over the system or the user entity, or the electronic information system is threatened by the direct occurrence of such an incident, the national cybersecurity incident handling centre may, for the performance of its protection tasks, require the entity with the right of disposal over the system to take the necessary measures for the resolution of the significant cybersecurity incident or the elimination of the threat.

(2) If an information security officer was designated for the entity, he shall, without delay, inform the national cybersecurity incident handling centre of the occurrence of circumstances referred to in paragraph (1). In cases requiring immediate intervention, the national cybersecurity incident handling centre may, through the information security officer, apply a provisional measure to the extent necessary to avoid any damage to the information.

41. Measures necessary to interrupt an attack from cyberspace

Section 69 (1) Measures necessary to interrupt an attack from cyberspace referred to in section 64 (2) d) may be implemented on the basis of the relevant decision of the person designated by the Government. After the attack is interrupted, consideration shall be given to the extent of possible further measures to strengthen protection as well as the necessity of further decisions relating to the protection of the country.

(2) A measure referred to in section 64 (2) d)

a) shall be proportionate to the harm caused or the direct threat and shall be limited to the extent necessary; efforts shall be made to ensure that it does not lead to an outcome beyond the interruption of the attack or to harm;

b) shall ensure consistency with national security, national defence, law enforcement and foreign policy interests and objectives.

(3) In the event of a significant cyberattack from abroad, the Minister responsible for foreign policy shall be informed of the measures taken and their justification, with a view to taking further measures.

42. Cybersecurity incident handling

Section 70 (1) If a cybersecurity incident occurs, the entity shall provide for handling the cybersecurity incident concerned.

(2) The cybersecurity authority may require the entity to handle the cybersecurity incident concerned. Should the entity fail to comply with the request of the authority, the cybersecurity authority may impose a fine.

(3) The cybersecurity incident concerned shall be handled by the following:

a) the entity itself, provided that it employs an employee with appropriate expertise;

b) an economic operator registered in the registry referred to in paragraph (4) kept by SARA that is mandated by the entity, holds a facility security clearance and possesses the expertise and infrastructural conditions, as specified by the president of SARA in a decree, required for the performance of the task;

c) the sector-related cybersecurity incident handling centre;

d) the national cybersecurity incident handling centre; or

e) the national defence cybersecurity incident handling centre.

(4) SARA shall keep a register of economic operators authorised to handle a cybersecurity incident in accordance with the detailed rules laid down by the president of SARA in a decree.

(5) The register referred to in paragraph (4) shall contain the following:

a) designation and seat of the economic operator, and natural identification data, phone number and electronic mailing address of its designated contact person;

b) identifier of the economic operator received upon registration;

c) further data specified in a decree by the president of SARA that do not qualify as personal data.

(6) SARA shall involve the national cybersecurity incident handling centre in the proceeding for registration in the register referred to in paragraph (4) for the purpose of establishing whether the expertise and infrastructural conditions required for the performance of the task, as specified by the president of SARA in a decree, are available.

(7) An entity referred to in section 1 (1) d) or e) that does not itself handle a cybersecurity incident shall choose from among the economic operators entered in the register referred to in paragraph (4). Where the handling of a cybersecurity incident exceeds the capacities of the economic operator, the entity may contact the sector-related cybersecurity incident handling centre or the national cybersecurity incident handling centre for the purpose of handling the cybersecurity incident concerned.

(8) An entity referred to in section 1 (1) a) to c) that does not itself handle a cybersecurity incident shall choose from among the economic operators entered into the registered referred to in paragraph (4) or contact the sector-related cybersecurity incident handling centre or the national cybersecurity incident handling centre for the purpose of handling the cybersecurity incident.

(9) For an entity referred to in section 1 (1) a) to c) or designated as a critical entity under the Critical Entity Resilience Act or an entity important for the defence and security of the country under the Defence and Security Activities Coordination Act, a person may handle incidents on behalf and in the employment of an economic operator referred to in paragraph (3) b) only if his national security vetting was completed without any national security risk being identified.

(10) The national cybersecurity incident handling centre shall handle the cybersecurity incident concerned within the limits of available resources, assessing the extent of danger.

(11) The cybersecurity incident shall be handled by the national cybersecurity incident handling centre if, for the electronic information system of a critical entity under the Critical Entity Resilience Act and for entities important for the defence and security of the country designated under the Defence and Security Activities Coordination Act, there is no economic operator for the handling of cybersecurity incidents that would meet the conditions set out by the law or the economic operator lacks sufficient capacity.

(12) Cybersecurity incidents as regards the electronic information systems of a national security service carrying out civilian information activities shall be handled exclusively by employees of the national cybersecurity incident handling centre whose national security vetting was completed without any national security risk being identified.

(13) The national cybersecurity incident handling centre may inform the head of the Operational Corps referred to in section 73 (3) about any cybersecurity incident that comes to its attention if the cybersecurity incident also affects an entity represented by another member of the Operational Corps.

(14) Detailed rules on the handling of the cybersecurity incidents concerned shall be laid down in a government decree.

(15) The provisions of this section shall apply also to cybersecurity near miss handling.

43. Provisions on handling cybersecurity incidents of entities covered by Regulation (EU) 2022/2554 of the European Parliament and of the Council

Section 71 (1) The provisions of sections 63 to 64, section 67, section 68 (1), section 69 and section 70 (10), (13) and (14) shall apply to the handling of cybersecurity incidents of entities covered by Regulation (EU) 2022/2554 of the European Parliament and of the Council.

(2) Where the handling of a cybersecurity incident exceeds the capacities of the entity covered by Regulation (EU) 2022/2554 of the European Parliament and of the Council or the contributor used by it, the entity may contact the sector-related cybersecurity incident handling centre or the national cybersecurity incident handling centre for the purpose of handling the cybersecurity incident concerned.

Chapter VIII

ORGANISATIONAL STRUCTURE FOR THE COORDINATION OF CYBERSECURITY-RELATED TASKS

44. Commissioner for cybersecurity

Section 72 (1) The commissioner for cybersecurity shall be designated by the Minister responsible for information technology.

(2) The commissioner for cybersecurity shall be in charge of the preparation of

a) the national cybersecurity strategy; and

b) the national crisis management plan

and the coordination with the entities concerned in accordance with the directive on measures for a high common level of cybersecurity across the Union.

(3) The commissioner for cybersecurity shall head the National Cybersecurity Task Force.

45. The National Cybersecurity Task Force

Section 73 (1) The National Cybersecurity Task Force shall be the organ of the Government that makes proposals and delivers opinions on cybersecurity matters.

(2) The National Cybersecurity Task Force shall provide for the coordination of the tasks set out in an Act and its implementing decrees.

(3) The activities of the National Cybersecurity Task Force shall be supported by the Operational Corps, the cybersecurity sub-task forces and the National Cybersecurity Forum that provides a framework for cooperation with non-governmental actors.

(4) The commissioner for cybersecurity shall control the activities of the Operational Corps. The Operational Corps shall, with the involvement of the central organ of defence and security administration, classify defence and security events arising from a significant or large-scale cybersecurity incident, and shall initiate taking crisis management and emergency management measures.

(5) The rules relating to the establishment and operation of the National Cybersecurity Task Force and the bodies supporting its operation as well as their functions and powers shall be laid down in a government decree.

46. Organisational structure of cybersecurity crisis management

Section 74 (1) In the event of a significant or large-scale cybersecurity incident, the Operational Corps of the National Cybersecurity Task Force may, at the initiative of the national cybersecurity incident handling centre, propose that a cybersecurity incident be classified as cybersecurity crisis.

(2) Cybersecurity crisis means a defence and security event in case of which the Government may, upon submission by the Minister responsible for information technology, order a coordinated defence activity.

(3) In the event of a cybersecurity crisis, the provisions of the Defence and Security Activities Coordination Act shall apply, unless otherwise provided by this Act or a government decree issued for its implementation.

(4) In the event of a cybersecurity crisis and a coordinated defence activity ordered due to it, the Government may introduce the following as a measure:

1. increasing the readiness and preventive activities of an organ or entity involved in the management of the cybersecurity crisis;

2. the operational or manned protection of organs and entities referred to in point 1 and its intensification;

3. intensification of reconnaissance and counterintelligence activities, and the activities of cyberspace operations forces, of national defence entities, law enforcement organs and national security services in order to prevent the threat from spreading to Hungary, to repel the attack and to prevent its consequences;

4. coordinated or joint action by the organs and entities referred to in point 3 within the framework of a coordinated defence activity;

5. ordering the immediate identification of a service essential for maintaining critical social or economic activities and of the service provider that is the sole provider of such a service but has not yet been identified as an essential or important entity;

6. suspension, restriction or monitoring of electronic communications services, rendering accessing them impossible, and using electronic information technology networks and tools and electronic communications devices free of charge, allowing others to use them, refraining from using them, and making them inaccessible;

7. using free of charge, and allowing others to use, the operational premises, technical equipment, electronic information systems and facilities of a service provider required for cybersecurity crisis management;

8. with a view to ensuring the continuous operation of the information and communication systems of a state organ or entity or an organ or entity involved in cybersecurity crisis management, using free of charge repair capacities and spare part inventories, restricting their use, and providing repair and maintenance services the owners and employees of companies with repair capacities are obliged to provide;

9. stockholding and reserve storing products and tools that are important for ensuring cybersecurity;

10. mandatory information provision to the European cyber crisis liaison organisation network (hereinafter the "EU-CyCLONE"), and the European Commission and the European Union Agency for Cybersecurity (hereinafter the "ENISA"), and shall decide on its content;

11. mandatory official information provision by the Government to those concerned; and

12. information provision, through diplomatic channels, to the Member States of the European Union and to allied countries within the North American Treaty Organisation about the measures taken by the Government in connection with the cybersecurity crisis.

(5) In the course of information provision under paragraph (4), points 10 to 12, the provisions of EU and national rules on classified data protection and of general data protection legislation shall be observed.

(6) In order to prevent, identify, detect a cybersecurity crisis, to prevent is further spread and to organise the coordinated performance of the tasks of state organs, throughout and in connection with the cybersecurity crisis, the Operational Corps

a) may request data provision from any organ, legal person or organisation without legal personality, which shall immediately comply with such a data provision request free of charge;

b) shall process personal data accessed in the course of cybersecurity incident handling.

(7) The Operational Corps shall hand over data processed pursuant to paragraph (6) other than information relating to national security activities to the national event handling centre.

(8) The Operational Corps may hand over data processed pursuant to paragraph (6) to the national cybersecurity incident handling centre for the examination of circumstances giving rise to the cybersecurity crisis.

(9) In a cybersecurity crisis, with a view to the handling of the event giving rise to the cybersecurity crisis, the head of the Operational Corps may

a) prescribe an obligation to take an immediate measure for a member of the Operational Corps as regards the entity represented by him;

b) decide whether to involve the national cybersecurity incident handling centre or the national defence incident handling centre in the handling of the cybersecurity incident.

(10) An entity falling within the scope of section 1 (10) other than an entity referred to under section 1 (1) d) or e) shall prepare a cybersecurity plan for the purpose of preparing for and handling a cybersecurity crisis as part of which it shall assess possible risks from cyberspace and, on the basis thereof, develop the procedural elements for crisis management to be taken within its field of operation.

(11) At a request by the national cybersecurity incident handling centre and the central organ of defence and security administration, entities affected by the cybersecurity crisis other than those referred to in paragraph (12) shall compile, hand over electronically or make otherwise accessible, data and information relating to the plan referred to in paragraph (10) and the measures introduced to handle the cybersecurity crisis.

(12) For electronic information systems for national defence purposes, data specified in paragraph (11) shall be made accessible to the national defence cybersecurity incident handling centre and the central organ of defence and security administration, upon request.

(13) The designation of organs and entities involved in cybersecurity crisis management, their functions and powers, the applicable procedure and the organs representing Hungary in EU-CyCLONE shall be provided for by the Government in a decree.

47. The national coordination centre

Section 75 (1) The tasks of the national coordination centre serving as point of contact for the Cybersecurity Competence Community under Regulation (EU) 2021/887 of the European Parliament and of the Council (hereinafter the “national coordination centre”) shall be carried out by the organ designated in a decree by the Government in compliance with the decree.

(2) For the purpose of carrying out its tasks set out in Regulation (EU) 2021/887 of the European Parliament and of the Council, the national coordination centre shall register and process the following as regards an entity seeking to be registered as a member of the Cybersecurity Competence Community within the meaning of Regulation (EU) 2021/887 of the European Parliament and of the Council:

a) identification data;

b) seat, establishment and branch;

c) contact details, including electronic contact details;

d) name or company name, mailing address, phone number and electronic mailing address of the representative operating within the territory of Hungary of an entity registered outside Hungary;

e) name, contact details, including electronic contact details, and position held within the entity of the contact person; and

f) further data prescribed in a government decree, other than personal data.

(3) Unless otherwise provided by the law, data from the register referred to in paragraph (2) may be transferred exclusively to

a) the European Cybersecurity Industrial, Technology and Research Competence Centre within the meaning of Regulation (EU) 2021/887 of the European Parliament and of the Council;

b) the cybersecurity authority;

c) a public authority within the meaning of Regulation (EU) 2022/2554 of the European Parliament and of the Council;

d) the single point of contact under Regulation (EU) 2022/2555 of the European Parliament and of the Council; and

e) the national cybersecurity incident handling centre.

(4) As regards a registered member of the Cybersecurity Competence Community, the national coordination centre shall publish on its website its name, the country where it has its seat, its official website, the type of the entity and its domains of activity in accordance with Article 8 (3) of Regulation (EU) 2021/887 and its data specified in a government decree other than personal data.

(5) Detailed rules on the functions and powers of the national coordination centre, its procedure and the register shall be laid down by the Government in a decree.

48. Cooperation and reporting

Section 76 (1) The cybersecurity authorities, the certification authority, the post-quantum cryptography supervision authority, the designating authority within the meaning of the Critical Entity Resilience Act, the public authority within the meaning of Regulation (EU) 2022/2554 of the European Parliament and of the Council, the state organ authorised to perform vulnerability scan, the cybersecurity incident handling centres, the national coordination centre and the single point of contact shall mutually cooperate and inform each other of their findings relating to electronic information security.

(2) The information referred to in paragraph (1) shall be provided immediately if it reveals a source of danger threatening electronic information security or indicates a cybersecurity incident. On the basis of the notification, the entities shall immediately start taking the measure within their competence in cooperation with each other.

(3) Detailed rules on cooperation among the entities referred to in paragraph (1), cooperation with EU-CyCLONE, the CSIRTs network, the CSIRTs, authorities and single points of contact of other EU Member States and third countries, and the procedure for information and data provision for the European Commission and the ENISA shall be laid down by the Government in a decree.

Chapter IX

PROVISIONS ON PROCESSING AND DATA PROTECTION

Section 77 (1) The cybersecurity authority, the organ authorised to perform vulnerability scan, the cybersecurity incident handling centre, the single point of contact, and the national coordination centre shall be entitled to process classified data, personal or protected data, trade secret, bank secret, payment secret, insurance secret, securities secret, fund secret, medical secret and secret related to the exercise of a profession that it accessed during the performance of its tasks relating to the protection of electronic information systems laid down in this Act as well as other data accessed in the course of the performance of its tasks only for the period of the performance of its tasks as specified by the law, observing the purpose limitation principle, and in compliance with the provisions of laws on processing.

(2) Organs referred to in paragraph (1) shall be required to delete data recorded in connection with the performance of their tasks from their electronic information systems and data-storage media, with the exceptions set out in paragraphs (3) to (6), after the completion of the performance of their tasks.

(3) An organ referred to in paragraph (1) shall be entitled to process data referred to in paragraph (1) for five years following the authority decision reaching administrative finality, the closure of vulnerability scan and the completion of the investigation of the cybersecurity incident or the cybersecurity crisis, and it shall delete such data from its electronic information systems and data-storage media upon the expiry of five years.

(4) If an entity no longer performs any activity falling within the scope of this Act, the cybersecurity authority shall delete from the register the data registered as regards the entity five years after the notification of the termination of the activity.

(5) Should the entity notify any change to the data, the cybersecurity authority shall delete from the register the original data five years after the notification of the change to the data concerned.

(6) The cybersecurity incident handling centre shall be entitled to process and preserve data generated in the course of the application of preventive means and services and the cybersecurity incident handling centre and the single point of contact shall be entitled to process and preserve data of received notification for five years from the generation of the data or the receipt of the notification, respectively; after this period, the data shall be deleted from the information systems and the data-storage media.

Section 78 (1) As regards data accessed, employees of the cybersecurity authority, the organ or economic operator authorised to perform vulnerability scan and the cybersecurity incident handling centre shall be subject to an obligation of confidentiality

a) for five years following the termination of the employment-related relationship;

b) for classified data, until the end of their validity period;

c) for personal data, without time limitation.

(2) Data generated in the course of the proceeding of the cybersecurity authority, the organ or economic operator authorised to perform vulnerability scan and the cybersecurity incident handling centre shall not be public, with the exception set out in section 79.

(3) A decision with administrative finality of an organ designated by the Government to perform authority tasks set out in this Act relating to electronic information systems for national defence purposes shall not be accessible to anyone other than the party and the person entitled to inspect the documents in accordance with section 33 (3) of Act CL of 2016 on the Code of General Administrative Procedure.

Section 79 (1) The state organ authorised to perform vulnerability scan may publish anonymised statistics on the findings of vulnerability scans that contain no reference to the vulnerabilities of the systems.

(2) The national cybersecurity incident handling centre may publish anonymised statistics on data, information, trends and conclusions arising in the course of the performance of its tasks, and the technical description of incidents.

Section 80 (1) When fulfilling their information and data provision obligations, the organs referred to in section 77 (1) shall proceed observing the provision of laws on classified data protection and general data protection. Information and data provision shall not entail the provision of information the publication of which would be contrary to the national security, public safety or essential defence interests of Hungary.

(2) Confidential information, such as rules on business confidentiality, shall be exchanged with the European Commission and other relevant authorities only where the information exchange is necessary for the application of Directive (EU) 2022/2555 of the European Parliament and of the Council. The information exchanged shall be limited to that which is relevant and proportionate to the purpose of that exchange. The exchange of information shall preserve the confidentiality of that information and protect the security and commercial interests of entities concerned.

Chapter X

FINAL PROVISIONS

49. Authorising provisions

Section 81 (1) Authorisation shall be given to the Government to designate in a decree

a) the organ authorised to provide cybersecurity services;

b) the national cybersecurity authority;

c) the supervision authority for electronic information systems for national defence purposes;

d) the certification authority referred to in section 45 (1) b);

e) the state organ authorised to perform vulnerability scan;

f) the organ operating the national cybersecurity incident handling centre;

g) the organ operating the national defence cybersecurity incident handling centre;

h) the organs and entities involved in the management of cybersecurity crises, the organs representing Hungary in EU-CyCLONE;

i) the national coordination centre; and

j) the food-chain supervision organ providing data in accordance with section 24 (9).

(2) Authorisation shall be given to the Government to determine in a decree

1. the detailed rules on cybersecurity services, the scope of cybersecurity services, the entities obliged and entitled to use them and the terms for using the services;

2. the detailed provisions on the obligations of the entities referred to in section 1 (1) a) to c) and f);

3. the detailed rules on the classification of data processed in electronic information systems;

4. the minimum content of an agreement referred to in section 11 (1);

5. the detailed duties and powers of the person responsible for electronic information system security and the procedure for registration and deregistration in the register of persons responsible for electronic information system security;

6. the detailed rules applicable in the course of the development of the electronic information systems of an entity referred to in section 1 (1) a) to c) or f);

7. the detailed rules on IT and electronic communications service tasks the central service provider provides with exclusive right on the basis of a law to an entity carrying out a state and local government task;

8. the functions and powers of the national cybersecurity authority and the authority exercising cybersecurity supervision over electronic information systems for national defence purposes, and the detailed rules on their procedure and the register;

9. for entities referred to in section 1 (1) a) to c) and f), the requirements for an information security officer and the detailed rules on his designation, rights and tasks;

10. the amount of the fine that the cybersecurity 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;

11. the amount 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;

12. the detailed rules on the task of the certification authority under section 45 (1) b), the procedure governing the certification authority activity, the authorisation procedure, the administrative audit and the record-keeping, as well as the data content excluding personal data of the records, and the rules for affixing the conformity mark;

13. the detailed rules on conformity self-assessment and the certification procedure with respect to defence industry research, development, manufacturing and trade; on the requirements for conformity assessment bodies with respect to the national cybersecurity certification scheme; on the conditions for the registration of conformity assessment bodies with respect to the European cybersecurity certification scheme; and on the obligations and activities of conformity assessment bodies;

14. the certification schemes with respect to defence industry research, development, manufacturing and trade, taking account of the national cybersecurity certification schemes;

15. the detailed rules on the performance of vulnerability scan, the specific vulnerability scanning methods and the content of the position statement;

16. the functions and powers of the national cybersecurity incident handling centre and the national defence cybersecurity incident handling centre and the detailed rules on the performance of their tasks;

17. the detailed rules on the establishment of the sector-related cybersecurity incident handling centre;

18. the detailed rules on the detection and reporting of ICT vulnerabilities and other vulnerabilities and the coordination and other tasks of the national cybersecurity incident handling centre as regards reported ICT vulnerabilities and other vulnerabilities;

19. the detailed rules on and the system of early warnings, the provisions on the designation of the operator of the system, and the procedure for using the related early warning service;

20. the detailed rules on and the system of early warnings relating to electronic information systems for national defence purposes, the provisions on the designation of the operator of the system, and the procedure for using the related early warning system;

21. the procedure for reporting threats, cybersecurity near misses and cybersecurity incidents, and the detailed rules on handling and investigating cybersecurity incidents and cybersecurity near misses;

22. the detailed rules on the conduct of national cybersecurity exercises;

23. the functions and powers of organs and entities involved in handling cybersecurity crises and the applicable procedure;

24. the rules relating to the establishment and operation of the National Cybersecurity Task Force and the bodies supporting its operation as well as their functions and powers; and

25. the detailed rules on the cooperation among the organs referred to in section 76 (1) and with the entities referred to in section 76 (3) and on the procedure for information and data provision to the European Commission and the ENISA;

26. the detailed ruled rules on the functions and powers and procedure of the national coordination centre and on the register.

(3) Authorisation shall be given to the Minister responsible for information technology to determine in a decree

a) the requirements for security classification and the specific protective measures to be applied for each security class;

b) the provisions on the training and further training of the head of an entity and the further training of persons responsible for electronic information system security;

c) as regards entities referred to in section 11 (3) b), the education required for the performance of the tasks of a person responsible for electronic information system security; the procedure for the publication of professional qualifications by the national coordination centre referred to in section 75 (1) and any acceptable professional experience; as well as, as regards entities referred to in section 1 (1) a) to c), the qualification, further training obligation and professional experience required for the performance of the tasks of an information security officer, and the procedure for the publication of professional qualifications by the national coordination centre referred to in section 75 (1);

d) ICT products, ICT services and ICT services certified under a national or European cybersecurity certification scheme the use of which is mandatory, and the entities referred to in section 1 (1) a) to c) and f) obliged to use them.

(4) The Minister responsible for information technology shall issue the decree referred to in paragraph (3) a) after seeking the opinion of the president of SARA.

(5) Authorisation shall be given to the Minister responsible for national defence to determine in a decree, in agreement with the Minister responsible for taxation policy, the amount of the administrative service fee payable for proceedings by the certification authority under section 45 (1) b) and the detailed rules concerning the collection, distribution, management, registration and reimbursement of this fee.

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

a) the amount of the cybersecurity supervision fee and the provisions on its payment;

b) the procedure for the registration of auditors and the requirements for auditors;

c) the procedure for carrying out a cybersecurity audit and the maximum cybersecurity audit fee, excluding value added tax;

d) as regards entities referred to in section 1 (1) d) and e) and auditors, the detailed rules on cybersecurity supervision and the performance of cybersecurity tasks, and on the conduct of administrative audit;

e) the procedure for the registration of entities referred to in section 1 (1) b), d) and e) in the cybersecurity supervision official register under section 29 (1) a), and the detailed rules on the data content of the register not qualifying as personal data;

f) for entities referred to in section 1 (1) d) and e), the requirements for an information security officer and the detailed rules on his designation, rights and tasks;

g) the entities required to use post-quantum cryptography;

h) the detailed rules on the registration of post-quantum cryptography application providers and the data content of the register excluding personal data, as well as the supervision of the post-quantum cryptography application providers;

i) the detailed rules on certifying that the computer system components of a post-quantum cryptography application provider are closed;

j) the detailed rules on the registration of the certifying entity, the data content of the register excluding personal data, and the supervision of the certifying entity;

k) the detailed rules on the procedure governing the certification authority activity, the authorisation procedure, the administrative audit and the record-keeping, and the data content of the register excluding personal data, as well as the rules for affixing the conformity mark, except for the certification authority activity under section 45 (1) b);

l) except for defence industry research, development, manufacturing and trade, the detailed rules on conformity self-assessment and the certification procedure; on the requirements for conformity assessment bodies with respect to the national cybersecurity certification scheme; on the conditions for the registration of conformity assessment bodies with respect to the European cybersecurity certification scheme; and on the obligations and activities of conformity assessment bodies;

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

n) ICT products, ICT services and ICT services certified under a national or European cybersecurity certification scheme the use of which is mandatory, and the entities referred to in section 1 (1) d) and e) obliged to use them.

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

a) the detailed rules on the registration of entities and persons authorised to perform vulnerability scan, and the infrastructural conditions and professional expertise required for performing the activity; and

b) the detailed rules on the registration of economic operators authorised to handle cybersecurity incidents, the data content of the register excluding personal data, as well as the infrastructural conditions and professional expertise required for performing the activity.

(8) The president of SARA shall issue the decree referred to in paragraph (7) after seeking the opinion of the Minister responsible for information technology.

50. Provisions on entry into force

Section 82 (1) With the exception specified in paragraph (2), this Act shall enter into force on 1 January 2025.

(2) Section 120 (1) shall enter into force on 2 January 2025.

51. Transitional provisions

Section 83 (1) Data referred to in section 8 (4) that are included in the register under Act L of 2013 on the electronic information security of state and local government organs (hereinafter the "Electronic Information Security Act") as of 31 December 2024 need not be reported again; the national cybersecurity authority shall process such data as part of the register referred to in section 28 (1).

(2) An entity referred to in section 1 (1) a) or b) shall perform its data provision obligation under section 8 (4) towards the national cybersecurity authority within the time limit set out in section 8 (4) if

a) it fell within the scope of the Electronic Information Security Act before the entry into force of this Act and did not yet fulfil its obligation under section 8 (4); or

b) it did not fall within the scope of the Electronic Information Security Act before the entry into force of this Act.

(3) If an entity referred to in section 1 (1) a) or b) already reported to the national cybersecurity authority the data of the person responsible for electronic information system security in accordance with the Electronic Information Security Act, it shall not be required to report such data again.

(4) If the person responsible for electronic information system security at an entity referred to in section 1 (1) a) or b) does not meet the requirements set out in section 11 (4) at the time of entry into force of the Act, the ground for incompatibility shall be eliminated within 2 years.

(5) If an entity referred to in section 1 (1) a) or b) should already have carried out the initial security classification of its already operating electronic information systems by the entry into force of this Act in accordance with the Electronic Information Security Act, the initial security classification shall be carried out within 120 days following the entry into force of this Act, together with the establishment of the risk management framework referred to in section 6.

(6) If the cybersecurity authority made an authority decision on the security classification of the electronic information systems of an entity referred to in section 1 (1) a) or b) in accordance with the Electronic Information Security Act before the entry into force of this Act, the security classification shall be reviewed in accordance with this Act within two years following the authority decision on security classification reaching administrative finality. If, in accordance with this provision, the review became due before the entry into force or becomes due within 180 days from the entry into force of this Act, the time limit for the review of the security classification shall be extended in such a manner that the available period shall be 180 days.

Section 84 Security classes 1 and 2 under the Electronic Information Security Act shall correspond to ‘basic’ security class, security classes 3 and 4 under the Electronic Information Security Act shall correspond to ‘substantial’ security class, and security class 5 under the Electronic Information Security Act shall correspond to ‘high’ security class.

Section 85 (1) If an entity referred to in section 1 (1) a) or an entity falling within the scope of section 1 (1) b) other than an entity listed in Annex 2 or 3 fell within the scope of the Electronic Information Security Act before the entry into force of this Act and already fulfilled the requirements prescribed therein for the security class of its electronic information systems, 1 year from the entry into force of this Act shall be available for that entity to implement the new protective measures prescribed by the Minister responsible for information technology in a decree.

(2) If an entity referred to in section 1 (1) a) or an entity falling within the scope of section 1 (1) b) other than an entity listed in Annex 2 or 3 fell within the scope of the Electronic Information Security Act before the entry into force of this Act and was not yet required to fulfil the requirements prescribed therein for the security class of its electronic information systems, that entity may implement the protective measures prescribed by the Minister responsible for information technology in a decree gradually in accordance with section 10 (6). The calculation of the time limit ensuring gradual approach shall be based on the security class determined in accordance with section 84 the requirements corresponding to which should have already been fulfilled. The period available for the implementation of the protective measures shall not be shorter than 1 year.

Section 86 (1) For an entity referred to in section 1 (1) a) or an entity falling within the scope of section 1 (1) b) other than an entity listed in Annex 2 or 3, the provisions of this Act on the development of a new system shall apply to

a) an in-house developed system under development that was not yet put into use at the time of the entry into force of this Act, provided that the resource requirements have not yet been approved;

b) a system under external development that was not yet put into use at the time of the entry into force of this Act, provided that the call for application for the procurement proceeding for the development has not yet been announced or the contract for the development has not yet been concluded.

(2) If the developed system of an entity referred to in section 1 (1) a) or an entity falling within the scope of section 1 (1) b) other than an entity listed in Annex 2 or 3 has already completed the steps of the development of an electronic information system under paragraph (1) at the time of the entry into force of this Act,

a) the entity shall carry out the security classification of the electronic information system within 180 days, provided that it has not yet done so;

b) the entity may implement the protective measures prescribed by the Minister responsible for information technology in a decree gradually in accordance with section 10 (6), with the proviso that the relevant time limit shall be calculated from the day of entry into force of this Act.

Section 87 If an entity referred to in section 1 (1) a) or an entity falling within the scope of section 1 (1) b) other than an entity listed in Annex 2 or 3 fell within the scope of the Electronic Information Security Act before the entry into force of this Act, the cybersecurity authority, when examining compliance with electronic information security requirements, shall examine compliance with the provisions of the decree on technology security requirements laid down in Act L of 2013 on the electronic information security of state and local government organs and requirements relating to secure information tools, and products as well as security classification and assignment to security levels until the expiry of the time limits set out in this Act, except where the entity declared that it fulfilled the protective measures prescribed in a decree by the Minister responsible for information technology.

Section 88 (1) Administrative cases pending in accordance with the provisions of the Electronic Information Security Act shall be closed by the cybersecurity authority in accordance with the Electronic Information Security Act.

(2) The operator of a critical system element designated in accordance with Act CLXVI of 2012 on the protection, designation and protection of critical systems and facilities shall be considered a critical entity for the purposes of this Act until the decision made in a designation proceeding under the Critical Entity Resilience Act or the Defence and Security Activities Coordination Act reaches administrative finality.

Section 89 (1) An entity referred to in section 1 (1) b), d) or e) that is recorded as a supervised entity in the register kept by SARA in accordance with section 26 (1) of Act XXIII of 2023 on cybersecurity certification and cybersecurity supervision on 31 December 2024 shall not be required to make the report referred to in section 8 (5); SARA shall process its data recorded in the register referred to in section 26 (1) of Act XXIII of 2023 on cybersecurity certification and cybersecurity supervision as part of the register referred to in section 29 (1) a). Data referred to in section 29 (1) a) ae) shall be reported to SARA by 15 February 2025.

(1a) An entity referred to in section 1 (1) b) that is listed also in Annex 2 or 3, as well as an entity referred to in section 1 (1) d) and an entity referred to in section 1 (1) e) other than a micro undertaking within the meaning of the Act on small and medium-sized undertakings and the support of their development, that started operating before 1 January 2025 shall fulfil its obligation referred to in section 16 (2) by 31 August 2025 at the latest.

(2) An entity referred to in paragraph (1a) shall have the initial cybersecurity audit under section 16 (1) carried out by 30 June 2026.

(3) An economic operator recorded as a supervised entity in the register kept in accordance with section 26 (1) of Act XXIII of 2023 on cybersecurity certification and cybersecurity supervision that carried out the security classification of its electronic information systems and the data stored, transferred or technically processed therein in accordance with section 20 (1) of Act XXIII of 2023 on cybersecurity certification and cybersecurity supervision by 31 December 2024 shall not be required to carry out the security classification again in accordance with section 10 (1).

(4) An economic operator recorded as auditor in the register referred to in section 23 (6) of Act XXIII of 2023 on cybersecurity certification and cybersecurity supervision as of 31 December 2024 shall not be required to request its registration again; SARA shall process its data recorded in the register referred to in section 23 (6) of Act XXIII of 2023 on cybersecurity certification and cybersecurity supervision as part of the register referred to in section 21 (3).

(5) An entity recorded as a conformity assessment body in the register referred to in section 14 (1) of Act XXIII of 2023 on cybersecurity certification and cybersecurity supervision as of 31 December 2024 shall not be required to request registration again; SARA shall process its data referred to in section 14 (1) c) to e), g) to j) and l) of Act XXIII of 2023 on cybersecurity certification and cybersecurity supervision as part of the register referred to in section 48 (1).

(6) Data, other than data referred to in paragraph (7), recorded in the register referred to in section 14 (1) of Act XXIII of 2023 on cybersecurity certification and cybersecurity supervision as of 31 December 2024 need not be reported again; SARA shall process such data as part of the register referred to in section 48 (1).

(7) SARA shall conduct authority proceedings that are pending in accordance with section XXIII of 2023 on cybersecurity certification and cybersecurity supervision on the day of entry into force of this Act applying the provisions of Act XXIII of 2023 on cybersecurity certification and cybersecurity supervision, with the proviso that SARA shall be entitled to arrange for remedying deficiencies within 30 days of the entry into force of this Act. As a result of the proceeding, SARA shall record data to be registered under this Act in the registers under this Act.

(8) An entity recorded in the register of economic operators authorised to perform vulnerability scan under the government decree laying down the rules for vulnerability scanning as of 31 December 2024 shall not be required to request registration again; SARA shall process its registered data as part of the register referred to in section 57 (1) c) on the basis of data provision by the Constitution Protection Office.

(9) An entity recorded in the register referred to in section 57 (1) c) in accordance with paragraph (8) shall provide SARA with proof of compliance with requirements set by this Act and the law issued for the implementation of this Act as a condition for registration by 31 July 2025. If no such proof is provided, SARA shall deregister the entity.

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

Section 90 (1) Section 93 qualifies as cardinal on the basis of Article 46 (6) of the Fundamental Law.

(2) Section 97 qualifies as cardinal on the basis of Article IX (6) of the Fundamental Law.

(3) Sections 118 to 121 and section 123 qualify as cardinal on the basis of Article 23 (4) of the Fundamental Law.

53. Compliance with the law of the European Union

Section 91 (1) This Act serves the purpose of compliance with the following legal acts of the European Union:

a) 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);

b) Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC; and

c) Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market.

(2) This Act contains provisions for the implementation of the following acts of the European Union:

a) 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);

b) 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; and

c) Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

Section 92 The prior notification of the draft of section 70 of this Act was performed in accordance with Article 15 (7) of Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market.

54. Amending and repealing provisions

Section 93

Section 94

Section 95

Section 96

Section 97

Section 98

Section 124

Section 125

Section 126

Section 127

Section 128

Section 129

Section 130

Section 131

Annex 1 to Act LXIX of 2024

Entities within the administrative sector
For the purposes of this Act, the following entities shall be regarded as entities within the administrative sector:

1. a central state administration organ, except for the Government;

2. the Sándor Palace;

3. the Office of the National Assembly;

4. the Office of the Constitutional Court;

5. the National Office for the Judiciary and the courts;

6. the prosecution offices;

7. the Office of the Commissioner for Fundamental Rights;

8. the State Audit Office;

9. the Hungarian National Bank;

10. the Hungarian Defence Forces;

11. capital and county government offices and offices of county general assemblies;

12. offices of representative bodies of towns with county rights and capital district local governments;

13. offices of representative bodies of settlements;

14. the central service provider;

15. the entity exercising the right of disposal over a central system.

Annex 2 to Act LXIX of 2024

2. **Service providers and entities operating in sectors of high criticality**

	A	B	C
1	**Sector**	**Subsector**	**Type of the entity**
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 crude oil 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	entities 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 railway infrastructure and industrial sidings, railway undertakings, and rail capacity allocation entities within the meaning of the Act on rail transport, except for companies listed in Annex 1 of Act XXXVII of 2009 on forests, the protection of forests and forest management;
10		Road transport	a) service providers operating intelligent road transport systems; b) traffic management entities; within the meaning of the decree issued 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 activities within the meaning of the Act on waterway traffic;

	A	B	C
1	**Sector**	**Subsector**	**Type of the entity**
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; entities 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;
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; b) data exchange service providers; within the meaning of the Act on electronic communications;
16			trust service providers within the meaning of the Act on digital State and laying down certain rules relating to the provision of digital 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 3 to Act LXIX of 2024

3. **Service providers and entities operating in critical sectors**

	A	B	C
1	**Sector**	**Subsector**	**Type of the entity**
2	Postal and courier services		postal service providers within the meaning of the Act on postal services;
3	a) production b) processing within the meaning of Article 2 (1) m) of Regulation (EC) No 852/2004 of the European Parliament and of the Council of 29 April 2004 on the hygiene of foodstuffs; and c) distribution of food;		food business within the meaning of the Act on the food chain and its authority supervision that carries out wholesale activities within the meaning of section 2, point 18 of Act CLXIV of 2005 on trade, industrial production and processing;
4	Waste management		economic operators carrying out an activity under the Act on waste, except for companies listed in Annex 1 of Act XXXVII of 2009 on forests, the protection of forests and forest management;
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

	A	B	C
1	**Sector**	**Subsector**	**Type of the entity**
			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, except for 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 optical products	economic operators carrying out the activity of ‘Manufacture of computer, electronic and optical products’ under Division 26 of Commission Delegated Regulation (EU) 2023/137 of 10 October 2022 amending Regulation (EC) No 1893/2006 of the European Parliament and of the Council establishing the statistical classification of economic activities NACE Revision 2;
8		Manufacture of electrical equipment	economic operators carrying out the activity of ‘Manufacture of electrical equipment’ under Division 27 of Commission Delegated Regulation (EU) 2023/137 of 10 October 2022 amending Regulation (EC) No 1893/2006 of the European Parliament and of the Council establishing the statistical classification of economic activities NACE Revision 2;
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 Commission Delegated Regulation (EU) 2023/137 of 10 October 2022 amending Regulation (EC) No 1893/2006 of the European Parliament and of the Council establishing the statistical classification of economic activities NACE Revision 2;
10		Manufacture of	economic operators carrying out the

	A	B	C
1	**Sector**	**Subsector**	**Type of the entity**
		motor vehicles, trailers and semi-trailers	activity of ‘Manufacture of motor vehicles, trailers and semi-trailers’ under Division 29 of Commission Delegated Regulation (EU) 2023/137 of 10 October 2022 amending Regulation (EC) No 1893/2006 of the European Parliament and of the Council establishing the statistical classification of economic activities NACE Revision 2;
11		Manufacture of other transport equipment	economic operators carrying out the activity of ‘Manufacture of other transport equipment’ under Division 30 of Commission Delegated Regulation (EU) 2023/137 of 10 October 2022 amending Regulation (EC) No 1893/2006 of the European Parliament and of the Council establishing the statistical classification of economic activities NACE Revision 2;
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 Commission Delegated Regulation (EU) 2023/137 of 10 October 2022 amending Regulation (EC) No 1893/2006 of the European Parliament and of the Council establishing the statistical classification of economic activities NACE Revision 2;
13	Digital providers		a) providers of online marketplaces; b) search providers within the meaning of Act CVIII of 2001 on certain issues of electronic commerce services and information society services; c) providers of social networking services platforms; d) domain name registration service providers;
14	Research		research organisations