Act LXIX of 2024

on the cybersecurity of Hungary

[1] In the interest of the nation, it is of particular importance, in view of the threats affecting today's information society, to mitigate threats to electronic information systems and to ensure the continuity of services in key sectors.

[2] There is a societal expectation that the confidentiality, integrity and availability of the data and information processed in electronic information systems indispensable to the State and its citizens should be ensured through closed, comprehensive, continuous and risk-proportionate protection, thereby protecting cyberspace, which contributes to the security of Hungary and the European Union and to strengthening their resilience and competitiveness.

[3] Electronic information systems and digital devices have become a central element of everyday life amidst the rapid digital transformation and interconnectedness of society. This development has also led to an expansion of the digital threat landscape, which can impede the pursuit of economic activities, cause financial loss and undermine users' confidence, thereby causing significant damage to economic and social life. Moreover, cybersecurity is a key enabler for many critical sectors to successfully embrace digital transformation and to fully harness the economic, social and sustainability benefits of digitalisation.

[4] In view of the above and of the 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 listed in Annex 1 belonging to the public administration sector,

b) economic operators under majority State control that do not fall within the scope of point a) and 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 or annual budget revenue appropriation exceeds the forint equivalent of EUR 10 million and, where the entity is required to prepare financial statements pursuant to section 8 (2) of Act C of 2000 on accounting, the balance sheet total exceeds the forint equivalent of EUR 10 million;

c) entities that do not fall within 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, and 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 by the national defence cybersecurity authority referred to in section 23 (2) (hereinafter the "national defence cybersecurity authority");

d) entities listed in Annex 2 or 3 that do not fall within the scope of point a) and qualify as medium-sized undertakings within the meaning of the Act on small and medium-sized undertakings and the support of their development, and entities listed in Annex 2 or 3 that do not fall within the scope of point a) and meet at least one of the following conditions:

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

db) the annual net turnover or annual budget revenue appropriation exceeds the forint equivalent of EUR 10 million and, where the entity is required to prepare financial statements pursuant to section 8 (2) of Act C of 2000 on accounting, the balance sheet total exceeds the forint equivalent of EUR 10 million;

e) entities that do not fall within the scope of point a) and are listed in Annex 2 or 3, regardless of size, 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.

(1a) For the purpose of converting the amounts specified in euro in paragraph (1) into forints, the official foreign exchange rate published by the Hungarian National Bank applicable on the date of closure of the entity’s financial year or, in the case of a budgetary organ, on the date of closure of the fiscal year, shall be applied. In the case of a newly established entity, the official foreign exchange rate published by the Hungarian National Bank applicable on the last day of the year preceding the reference year shall be applied.

(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 of significance 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 of significance 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 of significance 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 and entities of significance 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 functioning of the State, 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 of significance 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, within the meaning of the Act on small and medium-sized undertakings and the support of their development, qualify as medium-sized undertakings 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 that do not qualify as an essential entity; and

d) entities listed in Annex 3 that do not qualify as an essential entity under paragraph (4) b) to e).

(6) The identification procedure under paragraph (1) c) shall be subject to the following conditions:

1. the entity shall is the sole provider in Hungary of a service that is essential for the maintenance of critical social or economic activities;

2. disruption of services provided by the entity could have a significant impact on public order, public security or public health;

3. disruption of services provided by the entity could have a significant impact on critical social or economic activities;

4. disruption of the services provided by the entity could give rise to significant systemic risk, particularly in sectors where such disruption may have cross-border effects;

5. the entity is of particular importance at national or regional level for the relevant sector or type of service, or for other domestically interdependent sectors;

6. the entity is subject to national security protection pursuant to a government decision on the scope of organs and facilities under national security protection, or is considered, for national security reasons, by the national cybersecurity authority, or, for national defence or military reasons, by the national defence cybersecurity authority, to require identification;

7. the entity provides services to at least 20 000 persons in sectors listed in Annexes 2 and 3 or services necessary for the functioning of the State;

8. the entity provides services to at least 5 entities falling within the scope of this Act;

9. the entity is under majority State control;

10. the entity acts as a data processor of state registers falling within the scope of national data assets as defined by law;

11. the entity processes data for essential or important entities;

12. the entity qualifies as a publicly owned company not falling within the scope of paragraph (1)(b); or

13. the entity develops electronic information systems within projects financed from the budget or 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 (hereinafter "entity required to apply post-quantum cryptography") and to the supervisory activities concerning them, as determined in a decree of the president of the Supervisory Authority for Regulatory Affairs (hereinafter "SARA"):

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

b) a public utility service provider falling within the scope of any of the following Acts and an entity providing a public service falling 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 the security 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 assessment of this Act shall apply to vulnerability assessments 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 falling 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 of the Government.

(2) The Government shall determine, by decree, the scope of the cybersecurity services referred to in paragraph (1) d) and the category of entities obliged or 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 security classification of data and information processed by the entity in an electronic information system based on their confidentiality, integrity and availability;

9. *sectoral cybersecurity incident handling centre* means a cybersecurity incident handling centre operated by one or more entities related to a single sector falling 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 assessment method whereby weaknesses of an ICT system or an electronic information system are identified and their exploitability is assessed by simulating malicious attacks against security measures;

12. *internal IT security assessment* means a vulnerability assessment method whereby the security testing of an information system is carried out directly from an internal network endpoint, or whereby devices or system components used within the internal network are tested;

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 by the top-level domain name registry to register domain names;

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;

31a. *economic operator* means the term as defined by the Act on the Code of Civil Procedure;

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. *commissioning* means the population of an electronic information system with data and the commencement of its intended use;

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

a) the aggregate of the electronic information systems of national defence entities, multi-purpose vocational training institutions under the maintainer's direction of the Minister responsible for national defence that do not qualify as national defence entities, companies in respect of which the Minister responsible for national defence exercises ownership rights, and companies carrying out activities relating to national defence interests under the law, providing sector-specific support for operations within the national defence sector and across sectors;

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

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

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

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 the verification of the compliance of the security classification of electronic information systems and the protective measures corresponding to that security classification;

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 aimed at preventing, detecting, analysing and containing cybersecurity incidents, or responding to and recovering from cybersecurity incidents;

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 the system development lifecycle through the identification, introduction, assessment, operation and monitoring of risk-proportionate protective measures, for the purpose of the continuous detection of threats to, and the effective management of risks relating to, 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 register only for its own use;

65. *conformity assessment* means, except in Chapter IX/A, the assessment process for demonstrating whether specified requirements relating to an ICT product, ICT process or ICT service have been complied with;

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. *declaration 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* means 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 drawn up pursuant to Directive (EU) 2022/2555 of the European Parliament and of the Council for addressing large-scale cybersecurity incidents and crises, which sets out the objectives 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 privilege* means a user privilege specifically created for the person conducting a security scan for the purpose of carrying out a vulnerability assessment;

84. *availability* means ensuring that electronic information systems are accessible to authorised persons and that the data processed therein are usable;

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

86. *integrity* means the attribute of data whereby its content and characteristics correspond to what is expected, including assurance that it originates from the expected source, i.e. is authentic, as well as its traceability and assurance of origin, i.e. non-repudiation, and also the attribute of elements of an electronic information system whereby such elements can be used for their intended purpose;

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

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

89. *vulnerability assessment* means a vulnerability management process or method consisting of the security examination of information systems, hardware and software, carried out using automated tools and direct expert assessment;

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 assessment* means a vulnerability assessment 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-related 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 operational electronic information system concerned to an extent that involves substantial change to its functionality or affects the expected level of its protection;

96a. *economic operator under majority State control* means an economic operator

a) which is under the majority control of the Hungarian State as defined in the Act on the Civil Code, or

b) which is subject to the proprietary, control or supervisory rights of the Government, any of its members or the Speaker of the National Assembly, exercised directly or through a budgetary organ under their control;

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) which is implemented without interruption even under changing circumstances and conditions over time;

b) which covers all elements of the electronic information system;

c) which takes into consideration all foreseeable threats and risks; and

d) the costs of which are proportionate to the value of potential damage caused by such 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 be ensured:

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)

used by the entity exercising control over the electronic information system, the controller and the processor for a specific objective.

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

c) the national cybersecurity incident handling centre and 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 under the control of an entity shall be regarded as the electronic information system of that entity.

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

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

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

a) electronic information systems under the control 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 under the control of or used by the entity;

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

3. shall, in the case of 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. shall 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. shall classify the electronic information systems referred to in point 1 a) into security classes in accordance with the law;

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

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

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

9. shall ensure, where applicable, the assessment of the compliance of the protective measures selected in accordance with the provisions of a legal act of the European Union and the decree of the Minister responsible for information technology, during the initial security classification;

10. shall regularly ensure the periodic assessment of the 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. shall ensure that deficiencies discovered in the course of the assessment of protective measures relating to security class are remedied;

12. shall decide, within the entity, on the commissioning or further use of an electronic information systems; and

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

(4) The head of the entity shall carry out the tasks set out in paragraph (3) 10 at least every two years, in conjunction with the review of the information security policy and, where the head is required to implement it, the review of the security classification.

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

a) shall ensure training on the protective tasks relating to electronic information systems and the related responsibilities, as well as cybersecurity training and further training for himself and the staff members of the entity as laid down in a decree of the Minister responsible for information technology;

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

c) shall ensure the traceability of the events of the electronic information system;

d) shall, where the entity engages a contributor for the establishment, operation, auditing, maintenance or repair of the electronic information system, for the handling of cybersecurity incidents, or for the performance of data processing or technical processing tasks relating to the electronic information system, ensure that the cybersecurity requirements necessary in connection with the activities performed by that contributor in relation to the electronic information system are complied with as contractual obligations in accordance with this Act;

e) shall, in the event of a cyber threat, a cybersecurity near miss or a cybersecurity incident affecting the electronic information system, ensure, by using all necessary and available resources, rapid and effective response, reporting to the competent cybersecurity incident handling centre, the handling of cybersecurity incidents and recovery;

f) shall ensure that the persons concerned are informed without delay of any cybersecurity incidents and potential threats;

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

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

i) shall, for an entity referred to in section 1 (1) a) to c), ensure that, in the given year, the entity spends on cybersecurity development an amount corresponding to at least 5 per cent of its IT development costs for that year; and

j) shall take any other measures necessary 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 in the case referred to in paragraph (5) d), except, to the extent of the services used, where the entity is required to use a central service provider or a central system.

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

(8) To demonstrate compliance with the individual 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) The entities referred to in section 1 (1) a) to c) and f) listed in a decree of the Minister responsible for information technology or, for electronic information systems for national defence purposes, the Minister for national defence, as well as the entities referred to in section 1 (1) d) and e) listed in a decree of 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 as specified by a decree of the Minister responsible for information technology, the Minister for national defence, or the president of SARA.

(10) In relation to electronic information systems under the control of an important entity falling within the scope of section 1 (1) a) and c), as well as an entity that does not qualify as an entity listed in Annex 2 or 3 and falls 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) 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 exercising control 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) For cybersecurity supervision activities, with the exception of budgetary organs, the entities referred to in section 1 (1) b) that are also an entity listed in Annex 2 or 3, as well as the entities referred to in section 1 (1) d) or e), or, where such 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"), the controlling member instead, shall pay a cybersecurity supervision fee in an amount determined in a decree of the president of SARA in accordance with paragraph (2).

(2) The annual cybersecurity supervision fee shall amount to not more than 0.015 per cent of the net turnover of the entity referred to in paragraph (1) for the previous business year or, absent such turnover, the current year's turnover projected for the full year on a *pro rata* basis, but 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

a) shall ensure that data, documents and any changes thereto are sent to the cybersecurity authority for registration within 14 days of the change, in accordance with the provisions set out in law or on the website of the authority; and

b) shall ensure the conditions necessary for carrying out checks.

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

a) shall, 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) for registration purposes;

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

c) shall, 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) 1;

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

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

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

(5) An entity falling within the scope of section 1 (1) b) that qualifies as an entity listed in Annex 2 or 3, as well as an entity referred to in section 1 (1) d) or e), shall, within 30 days of commencing its activities or becoming subject to this Act, send the data specified in section 29 (1) a), except for the data specified in section 29 (1) a) ab), to SARA for registration.

(6) For the purpose of applying paragraphs (4) and (5), the date of becoming subject to this Act shall be the following:

a) in the case of a new entity, the day of the establishment of the entity;

b) in the cases referred to in section 1 (1) b) or d):

ba) the first day of the year following the occurrence of the condition giving rise to becoming subject to this Act; or

bb) if the entity so requests in its application for registration submitted prior to the day referred to in subpoint ba), the day on which the decision on the registration of the entity reaches administrative finality;

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

(6a) Where, in the case of an entity referred to in section 1 (1) b) or d), the condition specified in section 1 (1) b) ba) or bb), or in section 1 (1) d) da) or db), which gave rise to becoming subject to this Act, ceases to exist, the date on which the entity ceases to be subject to this Act shall be the end of the second year following the cessation of that condition.

(7) An entity may conclude cybersecurity information-sharing agreements for the implementation of a cooperation specified in a decree of 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 of the electronic information systems of the entity, the data processed therein, and the services provided, the entity shall classify its electronic information systems under its control that fall within the scope of this Act into the security classes “basic”, “significant”, or “high”, based on the risks to the integrity and availability of the relevant electronic information system and to the confidentiality, integrity and availability of the data processed therein, with progressively stricter protection requirements.

(2) The head of the entity shall decide on the security classification and shall be responsible for ensuring that it complies with the law and is proportionate to the risks, as well as for the completeness and up-to-dateness of the data used. The entity shall record the outcome of the security classification in the register of electronic information systems or in other internal regulations.

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

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

(5) As regards the electronic information systems of entities referred to in point a), and, in respect of electronic information systems for national defence purposes, in point f), as well as entities referred to in section 1 (1) b) that do not qualify as an entity listed in Annex 2 or 3, such entities shall, upon becoming subject to this Act, meet at least the protective measures prescribed in the decree of the Minister responsible for information technology for the "basic" security class.

(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 2 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) The security classification shall be reviewed in a documented manner at least every two years or, in the event of a change affecting the security of the electronic information system as specified by law, 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 elements of an agreement under paragraph (1) shall be set out in a government decree. Where an agreement is concluded, the natural person who performs the tasks of the person responsible for electronic information system security shall also be designated.

(3) The tasks of the person responsible for electronic information system security may only be performed by a person who:

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

b) in the case of an entity referred to in section 1 (1) a) to c) or f), an entity designated as a critical entity under the Critical Entity Resilience Act or an entity designated as an entity of significance for the defence and security of the country under the Defence and Security Activities Coordination Act, possesses the qualification required for the performance of the tasks as specified in a decree of the Minister responsible for information technology, and also possesses either:

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

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

(4) With the exception specified in paragraph (5), a person who performs financial management tasks at the entity, 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 entrusted as the 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) is involved in the preparation of all decisions relating to the protection of electronic information systems;

b) is provided with the necessary conditions, authorisations, information, human and financial resources required to ensure the protection of the electronic information system;

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

d) where designated within the entity, participates in further training necessary for maintaining professional competence, as specified in a decree of the Minister responsible for information technology.

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

(8) The person responsible for electronic information system security shall participate in further training specified in a decree of 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 act as a substitute for the person responsible for electronic information system security, who shall perform the tasks of the person responsible for electronic information system security in the event of his prolonged absence or other impediment. The head of the entity shall determine the division of tasks and responsibilities between the person responsible for electronic information system security and his deputy. The provisions applicable to the person responsible for electronic information system security shall apply to the deputy.

(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 of significance 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 the persons suitable to perform the tasks of the person responsible for electronic information system security.

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

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

(16) The national cybersecurity authority may verify compliance of the person responsible for electronic information system security with 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) Relating to its training activities, a higher education institution providing cybersecurity-related training

a)

b) may 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 staff members 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 staff members 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 referred to in section 1 (1) b) that qualifies as an entity listed in 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 electronic information system shall be classified into a security class; the resulting classifications shall be submitted to the national cybersecurity authority for approval in accordance with a government decree as follows:

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, for the security class, in a decree of the Minister responsible for information technology that were approved by the national cybersecurity authority.

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

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

(8) When introducing a new electronic information system or further developing an operational electronic information system, the requirements applicable to the established security class shall be met by the time the system is commissioned.

(9) The decision under section 6 (3) 12 of the head of the entity concerning the commissioning or further use of the electronic information system may be adopted 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 same time as the decision referred to in section 6 (3) 12 is adopted, it shall be ensured that the data of the electronic information system specified in a government decree are 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 exercising control 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 referred to in section 1 (1) b) that does not qualify as an entity listed in Annex 2 or 3; or

b) an important entity referred to in 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) 12 of the head of the entity concerning the commissioning or further use of the electronic information system.

(4) The cybersecurity authority may order a vulnerability assessment where justified.

(5) The requirements applicable to the security class shall be met by the time the electronic information system is commissioned; the decision under section 6 (3) 12 of the head of the entity concerning the commissioning or further use of the electronic information system may be adopted only if the requirements are met.

Section 15 (1) Where the vulnerability assessment 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) 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 classified as "significant" or "high" security class, it shall be mandatory to request a comprehensive vulnerability assessment in accordance with a government decree. Based on a decision of the state organ authorised to perform vulnerability assessments, as specified in a government decree, the entity may be exempted from the obligation to perform vulnerability assessment.

(3) The 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) The entities referred to in section 1 (1) b), which are also entities listed in Annex 2 or 3, as well as the entities referred to in section 1 (1) d), and, except for micro undertakings within the meaning of the Act on small and medium-sized undertakings and the support of their development, the entities 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) The 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 2 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) also exercises control over 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 of significance 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 whose requirements the supporting system meets.

(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 control 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 under its control;

c) shall set out as a contractual obligation or, absent a contract, make available on its website to the user entity, the electronic information security requirements to be met by the user entity as a condition for the use of the central system for 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 5 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) take measures to remedy any error or deficiency affecting the central system, should one be identified in the course of a vulnerability assessment 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, avert 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, when notifying the national cybersecurity authority of its electronic information systems, also notify its use of the central system, indicating the data suitable for the identification of the central system as well as the entity exercising control over the central system;

b) shall meet the electronic information security requirements set out by the entity exercising control over the central system and record them in its information security policy; and

c) shall report the cybersecurity incidents affecting the central system to the competent cybersecurity incident handling centre and the entity exercising control over the central system.

(3) For an entity exercising control 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 the use of which is voluntary, the entity exercising control 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. Where the protective measures ensured by the central service provider correspond to the security class of the electronic information system affected by the service provided by the central service provider, the user organisation shall use the service. Otherwise, the user entity shall not use the service or, where the use of the service is mandatory, it shall ensure that the risk-proportionate alternative measures within its control are implemented.

(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 ensure 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 met by the user entity as a condition for the use for 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 5 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) take measures to remedy any error or deficiency affecting the central service or the supporting system, should one be identified in the course of a vulnerability assessment performed as regards an electronic information system of the user entity;

f) shall report cyber threats, cybersecurity near misses and cybersecurity incidents affecting 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, avert or handle cyber threats, cybersecurity near misses and cybersecurity incidents affecting 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 service or the supporting system provided by the central service provider to the entity, the user entity

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

b) shall meet the electronic information security requirements set out by the central service provider, and record them in its information security policy; 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 register

Section 20 (1) The top-level domain name registry shall keep a central register of domain names registered 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 mail address suitable for communication and phone number of the domain name user; and

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

(3) The purpose of processing the data referred to in paragraph (2) shall be to keep up to date the identification and contact details 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) The auditor shall verify, during the cybersecurity audit, the compliance of the security classification of electronic information systems and of the protective measures corresponding to that security classification.

(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 assessments"). The requirements for an auditor shall be set out in a decree of the president of SARA.

(3) SARA shall, in accordance with the detailed rules laid down in a decree of the president of SARA, enter economic operators authorised to perform audits in the register, provided that they demonstrate compliance with the requirements set out in paragraph (2).

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

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

b) date of registration of the auditor and the identifier of the auditor received upon registration;

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

d) the document containing the findings of the audit.

(4a) The register referred to in paragraph (3) shall constitute a publicly certified official register in respect of the data specified in paragraph (4) b).

(5) By way of derogation from the Act on the general rules on taking up and pursuit of service activities, where SARA has not taken a decision on entry in the register referred to in 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 general rules on omission by the authority as laid down in the Act on the Code of General Administrative Procedure shall apply.

(6) Where the auditor no longer carries out auditing activities, SARA shall delete the data referred to in paragraph (4) from the register after the expiry of 5 years following the notification of the cessation of the activity.

(7) Where the auditor notifies a change in the data referred to in paragraph (4), SARA shall delete from the register the data recorded prior to the registration of the change 5 years after the registration of the change.

(8) The purpose of processing the data referred to in paragraph (4) shall be to ensure that information relating to auditors is kept up to date and to enable SARA to carry out monitoring activities.

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

Section 22 (1) For the purpose of verifying compliance pursuant to section 21 (1), the auditor shall be entitled, in a manner ensuring the traceability of the activities, to carry out the following tests:

a) internal IT security testing and remote vulnerability assessment, and, in the case of ’significant’ or ‘high’ security classes, penetration testing;

b) cryptographic conformity assessment; and

c) in the case of ‘significant’ or ‘high’ security classes, security source code analysis of custom-developed software implementing critical security functions.

(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, in relation to the electronic information system of the entity,

a) it finds facts that seriously endanger the continued operation of the entity; or

b) it detects circumstances indicating the commission of a criminal offence, a breach of law or a serious breach of the internal regulations of the entity, or a 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* in the case of an entity under section 1 (1) b);

b) at the request of the national cybersecurity authority in the case of an entity under section 1 (1) d) or e).

(5) The auditor shall process the documents under the control of, and received from, the auditee, including also personal data and data qualifying as trade secrets, necessary for carrying out the audit, for the purpose of verifying compliance with the requirements subject to audit, to the extent necessary for, and for the duration 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 by decree of 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 cybersecurity supervision of electronic information systems falling within the scope of this Act shall be performed as follows:

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

b) for electronic information systems of entities referred to in section 1 (1) d) and e) which do not fall within the scope of point a), by SARA.

(2) For electronic information systems for national defence purposes, the national defence cybersecurity authority performing cybersecurity supervision under this Act shall be designated, from within the national defence sector, in a decree of the Government. The provisions on the national 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 verify compliance of the person responsible for electronic information system security and his deputy with the requirements set out in law, and if so, shall enter them in the register;

2. shall assess whether the security classification is justified and, based on its findings, shall decide on its entry in the register;

3. shall enter the 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 on the correspondence between protective measures set out in European Union legal acts and in the decree of the Minister responsible for information technology;

6. may, for the purpose of demonstrating compliance with electronic information security requirements, require the application of relevant European and international standards and technical specifications relating to the security of electronic information systems, without prescribing or favouring any particular type of technology;

7. shall verify compliance with the requirements for the classification of electronic information systems set out in law or by the national cybersecurity authority itself;

8. shall order the security deficiencies identified during an inspection or otherwise coming to its knowledge to be remedied, and the measures necessary to remedy such deficiencies to be taken, and shall verify the effectiveness of those measures;

9. may take and monitor any measures relating to the protection of electronic information systems by means of which threats posing a risk to the electronic information system concerned can be addressed;

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 met during the development of electronic information systems;

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

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 of significance 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 carrying out its inspection tasks, the national cybersecurity authority shall prepare an annual inspection plan on the basis of a risk analysis, after seeking the proposals of the 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) 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) 10 applies, the national defence cybersecurity authority shall inform the national defence cybersecurity incident handling centre.

(4) The functions and powers of the national cybersecurity authority and the national defence cybersecurity authority, as well as the detailed rules governing their proceedings shall be laid down in a government decree.

(5) SARA

a) shall proceed in accordance with paragraph (1) 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 any measures relating to the protection of electronic information systems by means of which threats posing a risk to the electronic information system concerned can be addressed;

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 evidencing the compliance of security classification and security measures;

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

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

(6) The detailed rules for carrying out an administrative compliance check by SARA shall be determined by a decree of 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) For the purpose of performing its tasks set out in law, the cybersecurity authority shall be entitled to prioritise the conduct of supervisory tasks on the basis of risk assessment.

(9) For the purpose of carrying out the tasks relating to cybersecurity supervision under section 23 (1), by 1 February each year, the food-chain supervisory organs specified in a decree of the Government shall inform SARA and the national cybersecurity authority of the name, seat and tax number of the 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 shall be excluded in proceedings conducted by the cybersecurity authority.

(2) In the case of inspections aimed at verifying compliance with protective measures and authority proceedings aimed at investigating cybersecurity incidents, the administrative time limit for authority proceedings and administrative compliance checks conducted by the national cybersecurity authority shall be 120 days.

(3) The administrative time limit for administrative compliance checks conducted by SARA shall be 120 days; in the case of proceedings relating to the official registration of auditors, economic operators authorised to carry out vulnerability assessments or incident investigations, as well as the supervision of entities certifying the application of post-quantum cryptography and of entities authorised to provide post-quantum cryptography applications, the administrative time limit shall be 90 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 procedure"), provided that it does not fall within the scope of section 1 (1) and was not designated as a critical entity under the Critical Entity Resilience Act or an entity of significance 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 procedure, the national cybersecurity authority shall act in accordance with the provisions of section 2.

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

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

(3) For the purposes of conducting an identification procedure, 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 register and process the following:

1. for an entity,

a) the data required for the identification of the entity, the date of its registration, and the date of any modification to the register;

b) the contact details of the entity, including electronic contact details; as well as the public IP addresses and IP ranges used by the entity; and, except for the entities listed in Annex 1, the entity's seat, establishment and branch;

c) the qualification of the entity as essential or important;

d) the sector, subsector and type of entity to which it belongs, as specified in Annexes 2 and 3;

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

f) the designation of the entity's electronic information systems, their brief description, their security classification, the security class achieved at the time of registration and at review, the date of registration, and the date of any modification to the register;

g) data related to the classification of data processed in the electronic information system, including the location of data processing, specifying the country or the type of cloud service;

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

i) the protective measures related to the electronic information system and their status, as well as the date of their registration and the date of any modification to the register;

j) the name or company name, mailing address, phone number and electronic mail address of the representative of an entity not registered in Hungary operating within the territory of Hungary;

k) data suitable for the identification of a person or entity performing the tasks of the person responsible for electronic information system security, and the personal identification data, direct contact phone number, electronic contact details, education, professional qualification and professional experience of the natural person actually performing the task, as well as the date of their registration and the date of any modification to the register;

l) the entity's information security policy, the date of registration thereof, and the date of any modification to the register;

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

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

o) information relating to administrative compliance checks;

p) the outcome of vulnerability assessments and the vulnerability management plan for addressing vulnerabilities;

q) the entity's status as a critical entity or as an entity of significance for the defence and security of the country;

2. for an entity connected to a central system:

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

b) the name of the entity exercising control over the central system;

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

a) the unique identification number of the central system;

b) the name of the user entities;

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

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

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

c) the name of the user entities;

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

6. the personal identification data and contact details, including electronic contact details and data relating to expertise, of the natural persons suitable to perform the tasks of the person responsible for electronic information system security, as well as the date of registration of these data and the date of any modification to the register;

7. further data, not qualifying as personal data, prescribed in a government decree.

(1a) The register referred to in paragraph (1) maintained by the national cybersecurity authority shall constitute a non-public publicly certified official register, except for the publicly certified data contained in the register of personal data and addresses and the company register, as well as paragraph (1) 1 b), e), g), h), j), m) to q), paragraph (1) 2, paragraph (1) 3 b), and paragraph (1) 4, 5 and 7.

(2) For the purpose of performing its tasks under this Act, the national defence cybersecurity authority shall register the data referred to in paragraph (1) 1 a) to m), o) and p), in the case of entities falling within its competence the data referred to in paragraph (1) 1 q), and the data referred to in paragraph (1) 2 to 5 and 7.

(2a) The registers referred to in paragraphs (1) and (2) maintained by the national defence cybersecurity authority shall constitute publicly certified official registers, except for the publicly certified data contained in the register of personal data and addresses and the company register, as well as the data under paragraph (1) 1 b), e), g), h), j), m), o) to q), paragraph (1) 2, paragraph (1) 3 b), and paragraph (1) 4, 5 and 7.

(2b) Publicly certified data contained in the register referred to in paragraph (2a) maintained by the national defence cybersecurity authority shall not be public for thirty years from the date of their creation on grounds of national defence and national security.

(2c) The head of the national defence cybersecurity authority may authorise access to the publicly certified data referred to in paragraph (2a), after weighing the above grounds.

(3) The national cybersecurity authority and the national cybersecurity incident handling centre may access the data referred to in paragraph (1) 1 a) to c), j) to k) and p) in 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 registers 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 the information security policy submitted by the critical entity and the entity of significance for the defence and the Defence and Security Activities Coordination Act, respectively.

(7) The national cybersecurity authority shall publish on its website a list of natural persons suitable to perform 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 of the president of SARA, register and process the following:

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

aa) the data required for the identification of the entity;

ab) the entity's seat, establishment and branch

ac) if the entity is not established in the European Union but offers services in Hungary and designates a representative established in Hungary, the name or company name, mailing address, phone number and electronic mail address of the representative;

ad) the date of registration and deregistration of the entity;

ae) the natural identification data, phone number and electronic mail address of the person responsible for electronic information system security;

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

ag) further data, not qualifying as personal data, prescribed in a decree of the president of SARA, other than personal data;

b) for the entity authorised to perform vulnerability assessments:

ba) the data required for the identification of the entity;

bb) the contact details, including electronic contact details; and

b) the date of its registration and its identifier received upon registration;

c) for the natural person authorised to perform vulnerability assessments:

ca) the natural identification data required for the identification of the natural person;

cb) the contact details, including electronic contact details;

cc) data relating to expertise; and

cd) the date of registration and the identifier received upon registration;

d) the data of economic operators authorised to handle cybersecurity incidents as referred to in section 70 (5).

(1a) The register referred to in paragraph (1) a) shall constitute a publicly certified official register in respect of the data specified in paragraph (1) a) ad); the register referred to in paragraph (1) b) shall constitute a publicly certified official register in respect of the data specified in paragraph (1) b) bc); and the register referred to in paragraph (1) c) shall constitute a publicly certified official register in respect of the data specified in paragraph (1) c) cd).

(2) SARA shall compile, 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 compilation 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 from the register referred to in paragraph (1) may be transferred 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 the data relating to the entity contained in the register maintained by SARA.

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

21. Legal consequences

Section 30 (1) Should an entity fail to meet the security requirements laid down by the law or observe the related procedural rules, to address 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 law and the related procedural rules and, setting an appropriate time limit, call upon it to address security deficiencies relating to the requirements, identified during an inspection or an audit or otherwise coming to its knowledge, to take the measures necessary to ensure 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 the security requirements set out in the law or does not observe the related procedural rules, does not address 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 threat potentially affecting them as well as of any preventive, protective or remedial measures that are necessary or can be taken in response to that threat, and of 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 meet 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), (5) and (6) may be applied jointly 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 take measures to lift the 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 meet the cybersecurity requirements set out in the law or does not observe 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 of 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 in a decree of the president of SARA.

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 the cybersecurity requirements set out in the law or does not observe 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 identified deficiencies to be remedied or the measures necessary for compliance to be taken; or

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

(2) If, despite the application of the measures referred to in paragraph (1), the auditor does not meet the requirements set out in the law or does not observe 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, by a conclusive decision, order that data published via an electronic communications network be rendered temporarily inaccessible where such data poses a threat to the security of Hungarian cyberspace and is subject to cybersecurity incident handling by the national cybersecurity incident handling centre.

(2) Where data published via an electronic communications network infringes or jeopardises national defence interests or poses a threat to the security of an electronic information system for national defence purposes, the power to order that such data be rendered temporarily inaccessible shall lie with the national defence cybersecurity authority.

(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 90 days; this period may be extended by 90 days where 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 72 hours.

(2) If rendering data temporarily inaccessible is ordered with immediate effect, it shall be implemented in the shortest possible time, taking into account 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 obligation set out in this Subtitle. If the time limit set for compliance with the obligation expires without result, the fine may be imposed repeatedly, with a new time limit being specified.

(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 obligation to temporarily remove electronic data shall apply to the hosting service provider or an intermediary service provider providing hosting services within the meaning of the Act on certain issues of electronic commerce services and information society services, where such provider 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 1 working day from the communication of the conclusive decision.

(2) The 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 activities of conformity assessment bodies shall not apply to the cybersecurity certification regulated in this Chapter and the activities 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 ICT-related 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-related 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-related 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 declarations 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 for individual requirements or groups of requirements;

b) the critical security functions for which internal IT security or remote vulnerability assessment 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’, ‘significant’ 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 ‘significant’ 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 ‘significant’:

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 ICT-related 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 ICT-related 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 certificates and declarations of conformity

Section 41 (1) The national cybersecurity certificate and the national declaration of conformity shall specify the following:

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

b) the assurance level; and

c) the relevant technical specifications, standards and procedures.

(2) The national cybersecurity certificate and the national declaration 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 declaration of conformity has been issued shall without delay inform the certification authority of any ICT-related 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 of 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 declaration 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 declaration 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 declaration of conformity stating that compliance with the requirements set out in the national cybersecurity certification scheme has been checked. As part of the check, compliance with 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 declaration 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 declaration 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 of 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) of the president of SARA, except for defence industry research, development, manufacturing and trade;

b) of 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 has not taken a decision on entry in the register referred to in 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 general 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 in a decree of the president of SARA. As regards defence industry research, development, manufacturing and trade, the certification schemes shall be established in a decree of the Government, 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 areas not covered by a European cybersecurity certification scheme where there is a need to strengthen 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, upon the adoption of a European cybersecurity certification scheme, without delay take the necessary measures to review and subsequently repeal any national cybersecurity certification scheme covering the same subject matter

(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 be excluded in proceedings conducted by the certification authority.

(2) The administrative time limit for the certification authority shall be 120 days.

(3) In relation to a European cybersecurity certification scheme, the certification authority shall notify the European Commission of the conformity assessment body accredited by the national accreditation body within 15 days of the conclusive decision on its registration in the official register reaching administrative finality. The applicant body shall provide evidence of its accreditation status by attaching the conclusive decision of the national accreditation body.

(4) The certification authority shall conduct an authorisation procedure in respect of a conformity assessment body if the national or European cybersecurity certification scheme applicable to the ICT product, ICT service or ICT process

a) sets out additional requirements and, as a result, an authorisation procedure is required; or

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

(5) If paragraph (4) b) applies, authorisation shall be granted on 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 the authorisation procedure under paragraph (4) shall not extend beyond the expiry of the accredited status.

(7) In relation to a European cybersecurity certification scheme, if the certification authority conducts an authorisation procedure under paragraph (4), it shall notify the European Commission of the conformity assessment body within 15 days of the conclusive decision granting the authorisation reaching 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 declarations of conformity to provide any information and data necessary for the performance of the tasks of the authority; and

b) to conduct administrative compliance checks at conformity assessment bodies and issuers of declarations of conformity.

(9) The certification authority shall take action against any entity that carries out conformity assessment activities without authorisation and that does not comply with the requirements under section 44.

(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 register and process the following:

1. the data of the declarations of conformity made available by the manufacturer of ICT products, ICT services or ICT processes;

2. the technical documentation attached to declarations of conformity, and other information relating to the conformity of the ICT products, ICT services or ICT processes with the certification scheme;

3. 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 evidencing compliance with the requirements laid down in the decree of the president of SARA;

4. 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;

5. the application, data and documents connected to the authorisation procedure under section 47 (4) if such a procedure is to be conducted;

6. 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;

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

8. the identifier assigned to the conformity assessment body upon registration by the European Commission;

9. the data required for the identification of any contributor engaged by the conformity assessment body, and of its designated contact point;

10. the date of registration of the conformity assessment body;

11. the data of the certificate issued by the conformity assessment body;

12. the data required for the identification of the manufacturer and the designated contact point;

13. information related to the refusal of issuance, restriction, suspension, and withdrawal, of certificates;

14. information related to any ICT-related vulnerabilities and irregularities referred to in section 41 (3);

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

16. data and documents relating to complaints lodged.

(2) The register referred to in paragraph (1) shall constitute a publicly certified official register in respect of the data specified in paragraph (1) 6, 7 and 10.

(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-related 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 referred to in paragraph (1) may be performed to the following entities:

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

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

c) the cybersecurity incident handling centres referred to in section 63, for the performance of the activities relating to ICT-related vulnerabilities and irregularities referred to in section 41 (3).

(5) The conformity assessment body and the manufacturer shall, for the purposes of registration, send the data referred to in paragraph (1) to the certification authority within 8 days of the data becoming available, and in the event of any change, within 8 days of the occurrence of such change.

Section 49 (1) If the certification authority becomes aware, or establishes in the course of its inspection, that the conformity assessment body or the manufacturer does not meet the security requirements set out in the applicable European Union or Hungarian legislation or does not observe the related procedural rules, it shall, by a decision containing a warning and setting a time limit, call upon the conformity assessment body or the manufacturer to comply with the security requirements set out in the applicable European Union and Hungarian legislation and the related procedural rules.

(2) If, notwithstanding paragraph (1), the conformity assessment body or the manufacturer does not meet the security requirements set out in the legislation or does not observe the related procedural rules, the certification authority may impose a fine of such amount as specified in a government decree, taking into account all the circumstances of the case, and the fine may be imposed repeatedly in the event of continued non-compliance.

(3) The certification authority may impose an administrative fine of such amount as specified in a decree of the Government on any person carrying out conformity assessment activities without authorisation. 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 imposed as an administrative sanction.

Section 50 (1) The certification authority shall process classified data, personal data or sensitive data, as well as other legally protected data qualifying as trade secrets, bank secrets, payment secrets, insurance secrets, securities secrets, pension fund secrets, medical secrets and other secrets linked to the exercise of a profession, obtained in the course of performing its tasks, only for the period of performing its tasks and in accordance with the principle of purpose limitation. The certification authority shall record the data supporting the conclusions drawn from the administrative compliance check, 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 declaration 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 declaration 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 subject to an obligation of confidentiality with regard 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 activities, the administrative compliance checks and its tasks relating to register keeping in accordance with a decree of the president of SARA or, in the case of a certification authority under section 45 (1) b), of the Government.

(5) The manufacturer in carrying out conformity self-assessment and the conformity assessment body in the course of a certification procedure, shall act in accordance with a decree of 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 application of post-quantum cryptography

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

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

b) the integrity and availability of the electronic information system and its components, including in particular in communications conducted over government networks between physically separated sites of entities required to apply post-quantum cryptography; and in communications conducted over public internet interfaces, including where services provided by providers within the meaning of the Electronic Communications Act or information society services are used or provided; through the use of post-quantum cryptography providing a level of security beyond that of conventional cryptographic applications.

30. Protection of entities required to apply post-quantum cryptography

Section 52 An entity required to apply post-quantum cryptography shall, in the performance of its tasks set out by law, procure, for deployment, a post-quantum cryptography application from a registered entity authorised to provide such applications for communications conducted over government networks between its physically separated sites and over public internet interfaces, including where services provided by providers within the meaning of the Electronic Communications Act or other information society services are used, and shall establish the necessary protection on the networks under its control in order to ensure that the electronic flow of information is protected against cyberattacks caused by quantum computers.

31. Requirements for entities providing post-quantum cryptography applications

Section 53 (1) Only an entity that meets the following requirements may provide post-quantum cryptography applications (hereinafter: entity providing post-quantum cryptography applications) to an entity required to apply post-quantum cryptography:

a) does not pose a national security risk; and

b) complies with the requirements set out in paragraph (3).

(2) On the basis of paragraph (1), only an entity may carry out activities relating to the provision of post-quantum cryptography applications

a) which holds a facility security clearance as defined in the Act on the protection of classified data; and

b) whose employees and subcontractors hold personnel security clearances as defined in the Act on the protection of classified data.

(3) Activities relating to the provision of post-quantum cryptography applications may be carried out only by an entity whose electronic information system ensures the closed operation of system components, and prevents unauthorised access to, and undetected modification of, the information system. The electronic information system of an entity providing post-quantum cryptography applications shall comply with the requirements laid down in this Act.

32. Certification of compliance with post-quantum cryptography requirements

Section 54 (1) Compliance with the requirements set out in section 53 (3) shall be demonstrated by the entity intending to provide post-quantum cryptography applications by means of a system integrity certificate relating to the information system, issued by a certification body entered in the register referred to in section 56 (3) b) (hereinafter "certification body").

(2) The certification body shall issue an expert opinion to the entity intending to provide post-quantum cryptography applications confirming that its end-to-end application is suitable for post-quantum cryptography that provides a level of security beyond that of a cryptography applications.

(3) Where a certification body identifies, in relation to the information system of a certified entity, any fact that adversely affects the continuous operation of the entity, or becomes aware of circumstances indicating the commission of a criminal offence, a breach of law or the risk thereof, it shall notify SARA without delay.

33. Provisions on the certification bodies

Section 55 (1) A certification body may only be an entity that does not pose a national security risk and complies with the requirements set out in section 53 (2).

(2) A certification body shall be entitled to process data under the control of the entity intending to provide post-quantum cryptography applications or of the certified entity, which are necessary for conducting the certification, including classified data, personal data or sensitive data, trade secrets, bank secrets, payment secrets, insurance secrets, securities secrets, pension fund secrets and other secrets linked to the exercise of a profession obtained, exclusively for the purpose of verifying compliance with the requirements to be certified, to the extent necessary for, and until the conclusion of, the certification procedure; such data shall not be transmitted to third parties.

(3) The certification body shall specify in its regulations the positions the holders of which may have access to trade secrets and may become acquainted with their content in the course of the certification procedure. Staff members participating in the procedure shall be subject to an obligation of confidentiality with regard to any trade secret that come to their knowledge in the course of the certification procedure, including after the termination of their legal relationship with the body certifying post-quantum cryptography applications.

34. Supervision of post-quantum cryptography

Section 56 (1) Acting within its supervisory powers, SARA, in respect of certification bodies and entities authorised to provide post-quantum cryptography applications:

a) may carry out an administrative compliance checks;

b) conduct extraordinary checks where there is a suspicion of non-compliance with the requirements set out in this Chapter.

(2) SARA shall monitor compliance by certification bodies and entities authorised to provide post-quantum cryptography applications with their obligations, applying section 25 (1) and (3), in accordance with the detailed rules set out in a decree of the president of SARA.

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

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

b) certification bodies carrying out certification in accordance with section 54.

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

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

b) the date of registration of the entity and its identifier received upon registration;

c) further data, not qualifying as personal data, prescribed in a decree of the president of SARA.

(4a) The register referred to in paragraph (3) shall constitute a publicly certified official register in respect of the data specified in paragraph (4) b).

(5) If an entity entered in the register referred to in paragraph (3) no longer carries out activities relating to the provision of post-quantum cryptography applications or certification activities, SARA shall delete the data referred to in paragraph (3) from the register after the expiry of 5 years following the notification of the cessation of such activities.

(6) If the entity authorised to provide post-quantum cryptography applications or a certification body notifies any change in the data referred to in paragraph (3), SARA shall delete from the register the data recorded prior to the registration of the change after the expiry of 5 years following the registration of that change.

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

Chapter VI

VULNERABILITY ASSESSMENT

35. Entities authorised to carry out vulnerability assessments

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

a) state organ designated in a decree of 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 registered in the register of economic operators authorised to perform vulnerability assessments maintained by SARA, which holds a facility security clearance, meets the infrastructural requirements and possesses the necessary expertise for the performance of the task.

(2) A person may carry out the assessment on behalf of an economic operator authorised to perform vulnerability assessments only if that person

a)

b) possesses the necessary expertise for the performance of the vulnerability assessment;

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

d) is registered in the register of persons authorised to carry out vulnerability assessments maintained by SARA.

(3) Registration under paragraph (1) c) shall be conditional upon the economic operator authorised to carry out vulnerability assessments employing at least 2 experts who meet the requirements set out in paragraph (2). The detailed rules on registration under paragraph (1) c) and (2) d), as well as the infrastructural requirements and the necessary expertise for the performance of the activities, shall be laid down in a decree issued by the president of SARA after seeking the opinion of the Minister responsible for information technology.

(4) In the course of the procedure for entry in the registers referred to in paragraphs (1) and (2), SARA shall involve the state organ authorised to perform vulnerability assessments for the purpose of verifying compliance with the expertise and infrastructural requirements required for the performance of the task.

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

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

b) of the electronic information systems 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 assessments not have sufficient human resources to carry out a vulnerability assessment, it may consent to the entity referred to in paragraph (5) having the vulnerability assessment carried out by an economic operator authorised to perform vulnerability assessments, selected by the entity.

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

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

(9) The organ referred to in paragraph (1) to which a request for a vulnerability assessment has been submitted shall verify whether it is authorised to carry out the vulnerability assessment and, if it determines that another organ referred to in paragraph (1) is exclusively authorised, shall forward the request to the competent organ without delay.

36. Initiating vulnerability assessments

Section 58 (1) The national cybersecurity authority may require an entity to undergo a vulnerability assessment. Should the entity fail to fulfil the obligation imposed by the authority, the national cybersecurity authority may impose a fine.

(2) When imposing an obligation referred to in paragraph (1), the national cybersecurity authority shall take account of the importance of the electronic information system for the functioning of the State.

(3) When imposing an obligation referred to in paragraph (1), the national cybersecurity authority shall specify the electronic information system to which the vulnerability assessment is to apply, and may also determine the vulnerability assessment tool or method to be used.

Section 59 The state organ authorised to perform vulnerability assessments may also launch and carry out a vulnerability assessment at its own initiative if it holds registered user privilege or, in the absence thereof, in relation to the electronic information systems of entities referred to in section 57 (5).

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 that a vulnerability assessment be carried out on an electronic information system even where it is not required by an authority, provided that the system has been classified into a security class and registered with the cybersecurity authority.

(2) The head of the entity shall request the commencement of the vulnerability assessment referred to in paragraph (1) at least 60 days prior to its planned commencement, for the purposes of its planning and preparation. When determining the planned commencement date of the vulnerability assessment, the entity shall also take into account the time required for the vulnerability assessment method as specified in a government decree, while also considering the planned commissioning date of the electronic information system.

(3) The state organ authorised to perform vulnerability assessments may, after assessing the requests received, establish a priority order and, taking that priority order into account, set the commencement date of the vulnerability assessment no later than 15 days after the date previously determined.

(4) The state organ authorised to perform vulnerability assessments shall prioritise vulnerability assessments ordered by the cybersecurity authority or launched *ex officio* over those requested by an entity. In establishing the order, the organ shall take into account the available resources and, applying a risk-based approach, the significance of the electronic information system for the functioning of the State. Where the fulfilment of a request by an entity does not interfere with the performance of its mandatory tasks, the state organ authorised to perform vulnerability assessments shall carry out the vulnerability assessment, subject to 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 assessments may carry out a vulnerability assessment under an agreement entered into with the entity exercising control over the electronic information system.

37. General provisions on vulnerability assessments

Section 62 (1) A vulnerability assessment may also be carried out in respect of a specific part of an electronic information system.

(2) By its nature, a vulnerability assessment may result in a service disruption or degradation; the entity carrying out the vulnerability assessment shall not be liable for any damage arising therefrom, except in cases of damage caused intentionally.

(3) The methods of vulnerability assessment and the detailed rules governing the conduct of vulnerability assessments shall be laid down in a government decree.

(4) The entity carrying out the scan shall issue a position statement on the outcome of the vulnerability assessment, which shall also include the classification of vulnerabilities identified. The detailed requirements as to content of the position statement shall be set out in a government decree.

Chapter VII

PROVISIONS RELATED TO CYBERSECURITY INCIDENTS

38. Cybersecurity incident handling centres

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

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

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

Section 64 (1) The national cybersecurity incident handling centre shall carry out the tasks relating to:

a) threats affecting cyberspace, early warning and cybersecurity incident prevention;

b) cybersecurity incident handling;

c) cybersecurity crisis management;

d) vulnerabilities;

e) information and awareness-raising activities in the field of cybersecurity; and

f) the representation of Hungary in European Union and international cooperation,

as specified in a government decree.

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

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

b) shall direct preparedness for threats originating from cyberspace and the 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, and detect threats and attacks originating from cyberspace;

d) shall implement, or initiate, the measures necessary to interrupt attacks originating from cyberspace and to determine their 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 in relation to ICT-related 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. The detailed rules for the detection and reporting of ICT-related vulnerabilities and other vulnerabilities shall be laid down in a decree of the Government. In the case of CT-related vulnerabilities and other vulnerabilities reported in relation to electronic information systems of entities not listed in section 1 (10), or to ICT products or ICT services not falling within the scope of this Act, the national cybersecurity incident handling centre shall carry out the tasks set out in a government decree subject to the resources available to it and taking into account the level of risk. In respect of such reports, the national cybersecurity incident handling centre shall be obliged to act only where this does not impose a disproportionate or unjustified burden on it or where the report concerns an electronic information system of an entity falling within the scope of this Act.

(4) The national cybersecurity incident handling centre may take over, or support, the handling and investigation of cybersecurity incidents that seriously endanger Hungarian cyberspace.

(5) The defence cybersecurity incident handling centre shall, in respect of the national defence sector, carry out the tasks referred to in paragraph (1).

(6) A sectoral cybersecurity incident handling centre shall carry out the tasks set out in a cooperation agreement concluded with the national cybersecurity incident handling centre.

(7) The functions and powers of the national cybersecurity incident handling centre and of the national defence cybersecurity incident handling centre, the detailed rules on the performance of their tasks, as well as the detailed rules on early warning, including its system, the provisions on the designation of the operator of that system, and the conditions 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 originating from cyberspace, and may provide services in this regard (hereinafter jointly "preventive means") to the 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 entity's own expense; the national cybersecurity incident handling centre shall decide on the application of preventive means subject to the resources available to it and taking into account the level of risk.

(3) An entity referred to in section 1 (1) a) to c) may also be required by the national cybersecurity authority, on a proposal from the national cybersecurity incident handling centre, to apply preventive means, and the national cybersecurity incident handling centre may itself decide, on the basis of a risk assessment, on the application of preventive means following prior information of 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 the 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 connect to the system operated by the national cybersecurity incident handling centre for the sharing of threat information; the entity may also itself request connection to that system. The national cybersecurity incident handling centre shall require the connection of an entity referred to in section 1 (1) a) to c), or consent to such connection, taking into account the level of risk and subject to the resources available to it.

(6) The national cybersecurity incident handling centre shall be entitled, in relation to all internet addresses used or geolocated in Hungary and the services hosted thereon, to collect information intended solely for general cybersecurity purposes from which threats and cybersecurity incidents can be clearly identified.

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

(8) Data identified during vulnerability assessments may be used and processed by the national cybersecurity incident handling centre solely in anonymised form for the purpose of assessing the state of cyberspace.

40. Reporting and handling of cybersecurity incidents

Section 66 (1) Entities referred to in section 1 (1) a to c) and f) shall without delay report, in accordance with the provisions laid down in a government decree, to the national cybersecurity incident handling centre any threats, cybersecurity near misses and cybersecurity incidents, including operational cybersecurity incidents, occurring in, or coming to their knowledge in connection with, their electronic information systems.

(2) Entities referred to in section 1 (1) d) and e) shall report, in accordance with the provisions laid down in a government decree, to the national cybersecurity incident handling centre any threats, cybersecurity near misses and cybersecurity incidents, including operational cybersecurity incidents, occurring in, or coming to their knowledge in connection with, their electronic information systems, which cause a serious disruption or a pecuniary loss to the operation of the entity or to the provision of services by the entity, or cause significant material or non-material damage to other natural or legal persons.

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

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

(5) The national defence cybersecurity incident handling centre and the sectoral cybersecurity incident handling centre shall without delay forward to the national cybersecurity incident handling centre the data relating to threats, cybersecurity near misses and cybersecurity incidents coming to their knowledge.

(6) Should the national cybersecurity incident handling centre, the national defence cybersecurity incident handling centre or the sectoral cybersecurity incident handling centre establish that it lacks competence, it shall without delay transmit the report to the competent cybersecurity incident handling centre.

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

(2) The national cybersecurity incident handling centre may give priority to reports from entities falling within the scope of this Act over voluntary reports. The national cybersecurity incident handling centre shall handle voluntary reports subject to the resources available to it and shall act taking into account the level of risk.

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

(4) No obligation may be imposed on the reporting person as a result of a voluntary report that would not have applied to that person had the report not been made.

Section 68 (1) Where an electronic information system is affected by, or directly threatened by the occurrence of, a significant cybersecurity incident resulting in the compromise of essential information or personal data necessary for the operation of the entity exercising control over the system or of the user entity, the national cybersecurity incident handling centre may, for the purpose of performing its protective tasks, require the entity exercising control over the system to take the measures necessary to eliminate the significant cybersecurity incident or avert the threat.

(2) If an information security officer has been designated for the entity, the officer 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 the compromise of information.

41. Measures necessary to interrupt attacks originating from cyberspace

Section 69 (1) The measures necessary to interrupt an attack originating from cyberspace referred to in section 64 (2) d) may be implemented on the basis of a decision to that effect of the person designated by the Government. After the interruption of the attack, the range of possible further measures necessary to strengthen protection, as well as the need for further decisions relating to the protection of the country, shall be examined.

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

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

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 originating from abroad, the Minister responsible for foreign policy shall be informed of the measures taken and the reasons therefor, with a view to taking further measures.

42. Handling of cybersecurity incidents

Section 70 (1) If a cybersecurity incident occurs, the entity shall take measures to handle 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 the employees it employs have the appropriate expertise;

b) an economic operator engaged by the entity, possessing a facility security clearance and the expertise and infrastructural conditions necessary for the performance of the task, as specified in a decree of the president of SARA, and included in the register referred to in paragraph (4) maintained by SARA;

c) the sectoral 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 cybersecurity incidents in accordance with the detailed rules laid down in a decree of the president of SARA.

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

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

b) the date of registration of the entity and its identifier received upon registration;

c) further data, not qualifying as personal data, prescribed in a decree of the president of SARA.

(5a) The register referred to in paragraph (4) shall constitute a publicly certified official register in respect of the data specified in paragraph (5) b).

(6) In the course of the procedure for entry in the register referred to in paragraph (4), SARA shall involve the national cybersecurity incident handling centre for the purpose of verifying compliance with the expertise and infrastructural requirements required for the performance of the task, as specified in a decree of the president of SARA.

(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 sectoral 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 in the register referred to in paragraph (4) or contact the sectoral cybersecurity incident handling centre or the national cybersecurity incident handling centre for the purpose of handling the cybersecurity incident.

(9)

(10) The national cybersecurity incident handling centre shall handle the cybersecurity incident concerned subject to the resources available to it, taking into account the level of risk.

(11) The cybersecurity incident concerned shall be handled by the national cybersecurity incident handling centre where, in relation to the electronic information system of a critical entity within the meaning of the Critical Entity Resilience Act or the entities designated pursuant to the Defence and Security Activities Coordination Act as being of significance for the defence and security of the country, there is no economic operator meeting the conditions laid down by law for handling cybersecurity incidents, or no such economic operator has sufficient capacity.

(12)

(13) The national cybersecurity incident handling centre may inform the head of the Operational Corps referred to in section 73 (3) of cybersecurity incidents coming to its knowledge where the cybersecurity incident also affects an entity represented by another member of the Operational Corps.

(14) The 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 also apply to the handling of cybersecurity near misses.

43. The provisions on the handling of cybersecurity incidents of entities falling within the scope of 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 falling within the scope of Regulation (EU) 2022/2554 of the European Parliament and of the Council.

(2) Where the handling of a cybersecurity incident exceeds the capacities of an entity falling within the scope of Regulation (EU) 2022/2554 of the European Parliament and of the Council or the contributor engaged by it, the entity may contact the sectoral cybersecurity incident handling centre or the national cybersecurity incident handling centre for the purpose of handling the cybersecurity incident.

Chapter VIII

ORGANISATIONAL FRAMEWORK 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 responsible for the preparation of, and coordination with the entities concerned in relation to, the following under the Directive on measures for a high common level of cybersecurity across the Union:

a) the national cybersecurity strategy; and

b) the national crisis management plan.

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

45. National Cybersecurity Task Force

Section 73 (1) The National Cybersecurity Task Force shall serve as the Government’s body for making proposals and delivering opinions on cybersecurity matters.

(2) The National Cybersecurity Task Force shall ensure the coordination of the activities set out in this Act and its implementing decrees.

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

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

(5) The rules governing 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 framework for 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 a cybersecurity crisis.

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

(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 coordinated defence activities ordered on that basis, the Government may introduce the following measures:

1. increasing the readiness and preventive activities of organs or entities involved in the management of the cybersecurity crisis;

2. providing and strengthening the operational or physical security of the organs and entities referred to in point 1;

3. enhancing the reconnaissance, counterintelligence and cyberspace operations forces activities of national defence organisations, law enforcement organs and national security services, in order to prevent the spillover of threats into Hungary, to repel attacks, and to prevent their consequences;

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

5. ordering the immediate identification of essential services necessary for maintaining critical social or economic activities and of any provider which exclusively ensures such service but has not yet been identified as an essential or important entity;

6. the suspension, restriction and monitoring of electronic communications services, rendering access thereto impossible, and the free-of-charge use, provision for use, suspension of use, and rendering inaccessible of electronic information technology networks and devices and electronic communications equipment;

7. the free-of-charge use and provision for use of operational premises, technical equipment, electronic information systems and facilities of service providers necessary for cybersecurity crisis management;

8. for ensuring continuous operation of the information and communication systems of state organs or entities, as well as organs or entities involved in cybersecurity crisis management, the free-of-charge use or restriction of repair capacities and spare parts stocks, as well as the provision of repair and maintenance services which the owners and employees of companies with repair capacities are obliged to provide;

9. stockpiling and reserve storage of products and devices important for ensuring cybersecurity;

10. mandatory information to the European cyber crisis liaison organisation network (hereinafter the "EU-CyCLONE"), as well as the European Commission and the European Union Agency for Cybersecurity (hereinafter the "ENISA"), and shall determine the content of such information;

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

12. informing Member States of the European Union and allied countries within the North Atlantic Treaty Organization via diplomatic channels of the measures taken by the Government in connection with the cybersecurity crisis.

(5) In providing information under paragraph (4) 10 to 12, the provisions of Union and national rules on the protection of classified data and general data protection legislation shall be duly taken into account.

(6) During a cybersecurity crisis, for the purposes of preventing, identifying, detecting and containing a cybersecurity crisis, as well as for organising the coordinated performance of tasks by state organs, the Operational Corps, in relation to the cybersecurity crisis:

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

b) shall process personal data obtained in the course of the handling of cybersecurity incidents.

(7) The Operational Corps shall hand over data processed under paragraph (6) to the national event handling centre, except for information relating to national security activities.

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

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

a) require a member of the Operational Corps to take immediate measures in respect of the entity the member represents;

b) decide on the involvement of the national cybersecurity incident handling centre or the national defence incident handling centre in the handling of the cybersecurity incident.

(10) Entities falling within the scope of section 1 (10), with the exception of entities referred to in section 1 (1) d) and e), shall prepare a cybersecurity plan for the purpose of preparedness for and management of cybersecurity crisis, in which they shall assess potential risks originating from cyberspace and, on that basis, develop the procedural arrangements for crisis management applicable within their areas of operation.

(11) At the request of the national cybersecurity incident handling centre or the central organ of defence and security administration, an entity affected by a cybersecurity crisis shall, except as provided for in paragraph (12), collect provide electronically or otherwise make accessible data and information relating to the plan referred to in paragraph (10) and to the measures introduced for managing the cybersecurity crisis.

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

(13) The designation of organs and entities involved in cybersecurity crisis management, their functions and powers, the procedures to be followed, and the organs representing Hungary in EU-CyCLONE shall be determined 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 of the Government in accordance with the decree.

(2) For the purpose of performing 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 data of entities applying for membership in the Cybersecurity Competence Community referred to in Regulation (EU) 2021/887 of the European Parliament and of the Council:

a) data necessary for the identification of the entity;

b) seat, establishment and branch;

c) contact details, including electronic contact details;

d) name or company name, mailing address, phone number and electronic mail address of the representative operating within the territory of Hungary of an entity not registered in Hungary;

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

f) further data, not qualifying as personal data, prescribed in a government decree.

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

a) the European Cybersecurity Industrial, Technology and Research Competence Centre pursuant to 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) The national coordination centre shall publish on its website the name, country of seat, official website, entity type and domain pursuant to Article 8 (3) of Regulation (EU) 2021/887 and further data not qualifying as personal data as specified in a government decree, of the registered members of the Cybersecurity Competence Community.

(5) The detailed rules relating to the functions, powers and procedures of the national coordination centre, as well as 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 authority supervising post-quantum cryptography, the designating authority pursuant to the Critical Entity Resilience Act, the designating authority pursuant to the Defence and Security Activities Coordination Act, the public authority pursuant to Regulation (EU) 2022/2554 of the European Parliament and of the Council, the state organ authorised to perform vulnerability assessments, the cybersecurity incident handling centres, the national coordination centre and the single point of contact shall cooperate with one another and inform one another of their findings concerning electronic information security.

(2) The information referred to in paragraph (1) shall be provided without delay 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 measures within their competence in cooperation with one another.

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

(4) Within the framework of cooperation between the cybersecurity authority and the designating authority pursuant to the Critical Entity Resilience Act and the designating authority pursuant to the Defence and Security Activities Coordination Act, the designating authority pursuant to the Critical Entity Resilience Act and the designating authority pursuant to the Defence and Security Activities Coordination Act shall inform the cybersecurity authority of the designation or withdrawal of designation of an entity as a critical entity or as an entity of significance for the defence and security of the country by transmitting its decision thereon.

Chapter IX

DATA PROCESSING AND DATA PROTECTION PROVISIONS

Section 77 (1) The cybersecurity authority, the organ or economic operator authorised to perform vulnerability assessments, the cybersecurity incident handling centre, the single point of contact and the national coordination centre shall be entitled to process classified data, personal data or protected data, trade secrets, bank secrets, payment secrets, insurance secrets, securities secrets, pension fund secrets, medical secrets and other secrets linked to the exercise of a profession, as well as other data, obtained in the course of performing their tasks relating to the protection of electronic information systems specified in this Act, exclusively for the period of performing their tasks laid down by law, in accordance with the principle of purpose limitation and in compliance with the provisions of laws governing data processing.

(2) After completion of the performance of their tasks, the organs referred to in paragraph (1) shall, except as provided for in paragraphs (3) to (6), delete the data recorded in connection with the performance of their tasks from their electronic information systems and data-storage media.

(3) An organ referred to in paragraph (1) shall be entitled to process data referred to in paragraph (1) for 5 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 after the expiry of 5 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 after the expiry of 5 years following the notification of the termination of the activity.

(5) If the entity notify any change to the data, the cybersecurity authority shall delete from the register the original data after the expiry of 5 years following 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 5 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) Staff members of the cybersecurity authority, the organ or economic operator authorised to perform vulnerability assessments and the cybersecurity incident handling centre shall be subject to an obligation of confidentiality, set out in writing, with regard to the data obtained; such obligation of confidentiality shall continue to apply

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

b) for classified data, until the end of the 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 assessments 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 the organ designated by the Government to perform the authority tasks set out in this Act in relation 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 assessments may publish anonymised statistics on the results of vulnerability assessments that do not contain any indication of vulnerabilities of systems.

(2) The national cybersecurity incident handling centre may publish, in anonymised form, statistics relating to data, information, trends and conclusions generated in the course of the performance of its tasks, and technical descriptions of incidents.

A request for access to data relating to an electronic information system or central service used or provided by an entity specified in sections 1 and 2 that also qualifies as an organ performing public duties within the meaning of the Act on the right to informational self-determination and on the freedom of information (hereinafter “organ performing public duties”) shall be refused for a period of up to 20 years from the creation of the data if access to the data would jeopardise cybersecurity interests.

(2) The head of the organ performing public duties shall decide whether the request referred to in paragraph (1) may be fulfilled.

Section 80 (1) In fulfilling their information and data provision obligations, the organs referred to in section 77 (1) shall act in compliance with the provisions of laws governing the protection of classified data and general data protection. The provision of information and data may not extend to information the disclosure of which would be contrary to the national security, public safety or essential defence interests of Hungary.

(2) Confidential information, including trade secrecy rules, may be shared with the European Commission and other competent authorities only where such exchange of information is necessary for the application of Directive (EU) 2022/2555 of the European Parliament and of the Council. The information shared shall be limited to what is relevant and proportionate for the purposes of the exchange of information. In the course of the exchange of information, the confidential nature of the information made available shall be preserved, and the security and commercial interests of the entities concerned shall be protected.

Chapter IX/A

RULES GOVERNING THE IMPLEMENTATION OF REGULATION (EU) 2024/2847 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

48/A General rules concerning the implementation of Regulation (EU) 2024/2847 of the European Parliament and of the Council

Section 80/A For the purposes of this Chapter:

1. *notified body* means the term as defined in Article 3 29 of Regulation (EU) 2024/2847 of the European Parliament and of the Council;

2. *notifying authority* means the term as defined in Article 3 26 of Regulation (EU) 2024/2847 of the European Parliament and of the Council;

3. *conformity assessment* means the term as defined in Article 3 27 of Regulation (EU) 2024/2847 of the European Parliament and of the Council;

4. *market surveillance authority* means the term as defined in Article 3 33 of Regulation (EU) 2024/2847 of the European Parliament and of the Council.

Section 80/B SARA shall act as the notifying authority and the market surveillance authority in respect of the provisions of Regulation (EU) 2024/2847 of the European Parliament and of the Council.

48/B. Activities of the notifying authority

Section 80/C (1) Conformity assessment activities under this Chapter may be carried out only by an entity that

a) complies with the requirements laid down in Article 39 (2) to (12) of Regulation (EU) 2024/2847 of the European Parliament and of the Council;

b) has been entered in the register maintained by SARA; and

c) satisfies the condition laid down in Article 43 (5) of Regulation (EU) 2024/2847 of the European Parliament and of the Council.

(2) The provisions of the Act on the activities of conformity assessment bodies shall not apply to conformity assessment activities regulated in this Chapter or to the activities of SARA under this Chapter.

(3) Designation pursuant to Article 36 (1) of Regulation (EU) 2024/2847 of the European Parliament and of the Council shall take place through entry in the register referred to in paragraph (1) b).

(4) The president of SARA shall, by decree, lay down the detailed rules governing the conditions for entry of conformity assessment bodies in the register referred to in paragraph (1) b) and the fulfilment of certain requirements set out in Article 39 (2) to (12) of Regulation (EU) 2024/2847 of the European Parliament and of the Council, the manner of demonstrating such compliance, as well as the procedure for registration.

(5) Summary procedure shall be excluded in proceedings conducted by SARA acting as the notifying authority.

(6) The administrative time limit for SARA acting as the notifying authority shall be 120 days.

Section 80/D (1) Any person may report to SARA any breach of the conflict-of-interest requirements laid down in Article 39 of Regulation (EU) 2024/2847 of the European Parliament and of the Council.

(2) SARA shall investigate any report submitted pursuant to paragraph (1). Where the report is well founded, or where SARA itself identifies a conflict of interest in the exercise of its powers, SARA shall without delay notify the entity subject to the report, which shall, upon receipt of the notification, without delay suspend the activity affected by the conflict of interest.

(3) Where the entity subject to the report itself identifies the existence of a conflict of interest, it shall, upon such identification, without delay notify SARA thereof and suspend the activity affected by the conflict of interest.

(4) The entity subject to the report shall inform SARA of the measures taken or planned to eliminate the conflict of interest within twenty-one days from receipt of SARA's notification in the case referred to in paragraph (2), or, in the case referred to in paragraph (3), from the date of its own notification.

(5) Within eight days of receipt of the information concerning the measures taken to eliminate the conflict of interest, SARA shall decide whether those measures are adequate. Where the elimination of the conflict of interest has been ensured, the entity subject to the report may continue the activity on the basis of the decision of SARA; otherwise, SARA shall suspend the notification referred to in Article 43 of Regulation (EU) 2024/2847 of the European Parliament and of the Council where the conflict of interest is capable of being eliminated, and shall withdraw the notification where the conflict of interest cannot be eliminated.

(6) SARA shall require the designated entity to withdraw the results of conformity assessment activities carried out in breach of the conflict-of-interest requirements and to withdraw any certificates issued on that basis. This paragraph shall not apply where the conflict of interest exists in relation to the employee who carried out the conformity assessment activity, or to another person having a work-related relationship with the entity subject to the report, provided that a conformity assessment carried out within thirty days by another employee or other person having a work-related relationship with the entity subject to the report who was not affected by the conflict of interest reached the same result.

Section 80/E (1) SARA shall register and process:

a) the data necessary for the identification and contact details of the conformity assessment body or notified body and its designated contact person, as well as documents evidencing compliance with the requirements laid down in a decree of the president of SARA;

b) the date of registration and deregistration of the conformity assessment body or notified body, and its registration number;

c) the reason for deregistration;

d) the date of notification pursuant to Article 43 of Regulation (EU) 2024/2847 of the European Parliament and of the Council;

e) the identification number pursuant to Article 44 (1) of Regulation (EU) 2024/2847 of the European Parliament and of the Council;

f) the fact that SARA has restricted, suspended or withdrawn the notification pursuant to Article 43 of Regulation (EU) 2024/2847, as well as the date of such decision;

g) the conformity assessment module or modules in respect of which the notified body is authorised to carry out conformity assessment procedures;

h) the data relating to certificates issued by the notified body;

i) information relating to the refusal to issue, restriction of scope, suspension and withdrawal of certificates;

j) data and documents relating to complaints submitted;

k) further data, not qualifying as personal data, prescribed in a decree of the president of SARA.

(2) The register referred to in paragraph (1) shall be a publicly certified official register in respect of the data specified in paragraph (1) b) and f).

(3) The purpose of processing the data referred to in paragraph (1) shall be to ensure that information relating to conformity assessment bodies and notified bodies is kept up to date and to enable SARA to carry out its monitoring and oversight activities.

(4) The conformity assessment body or notified body shall send the data referred to in paragraph (1), and any changes thereto, to SARA within 8 days of such data becoming available or, in the case of changes, of their occurrence, for the purpose of registration.

(5) SARA shall publish on its website the name, seat, electronic mail address and phone number of the notified body, as well as the data referred to in paragraph (1) b), e) and g).

(6) Where a notified body no longer carries out conformity assessment activities under this Chapter, SARA shall without delay withdraw the notification relating to that body pursuant to Article 43 of Regulation (EU) 2024/2847 of the European Parliament and of the Council.

(7) Where SARA withdraws a notification pursuant to Article 43 of Regulation (EU) 2024/2847 of the European Parliament and of the Council, or where the condition set out in Article 4 (5) of that Regulation (EU) 2024/2847 of the European Parliament and of the Council is no longer fulfilled, SARA shall delete the data referred to in paragraph (1) relating to the notified body or conformity assessment body concerned from the register five years after the occurrence of those circumstances.

(8) Where a notified body or conformity assessment body reports a change in the data referred to in paragraph 1), SARA shall delete from the register the data recorded prior to the registration of that change five years after the registration of the change.

Section 80/F (1) A notified body shall annually prepare a report on its conformity assessment activities under this Chapter and shall submit it to SARA with the content, within the time limit and in the manner specified in a decree of the president of SARA.

(2) The notified body shall participate, either directly or through its authorised representative, in the work of the group referred to in Article 51 (1) of Regulation (EU) 2024/2847 of the European Parliament and of the Council.

Section 80/G A manufacturer within the meaning of Regulation (EU) 2024/2847 of the European Parliament and of the Council may apply to a court having jurisdiction in civil matters against a decision of a conformity assessment body.

Chapter X

FINAL PROVISIONS

49. Authorising provisions

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

a) the organ authorised to provide cybersecurity services;

b) the national cybersecurity authority;

c) the authority performing cybersecurity supervision 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 assessments;

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

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

f) 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 by decree

1. the detailed rules on cybersecurity services, the scope of cybersecurity services, the entities obliged or entitled to use them, as well as the rules governing the use of such 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 suitable to perform the tasks of the person 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 governing the provision of information technology and electronic communications services by the central service provider to entities performing state local government functions under an exclusive right conferred by law;

8. the functions and powers of the national cybersecurity authority and, for electronic information systems for national defence purposes, of the authority performing cybersecurity supervision, as well as the detailed rules governing their procedure and the register;

9. for entities referred to in section 1 (1) a) to c) and f), the requirements for information security officers and the detailed rules governing their designation, rights and tasks;

10. the amount of fines that may be imposed by the cybersecurity authority, the criteria for determining such fines, and the detailed procedural rules governing the payment of fines;

11. the amount of fines that may be imposed by the certification authority, the criteria for determining such fines, and the detailed procedural rules governing the payment of fines;

12. the detailed rules on the task of the certification authority under section 45 (1) b), the procedure governing certification authority activities, the authorisation procedure, the administrative compliance check and the keeping of the register, as well as the data content of the register excluding personal data, and the rules for affixing conformity marks;

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 assessment, the specific vulnerability assessment 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 sectoral cybersecurity incident handling centre;

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

19. the detailed rules on early warnings, their system, the provisions on the designation of the operator of the system, as well as the rules governing the use of the related early warning service;

20. the detailed rules on early warnings relating to electronic information systems for national defence purposes, their system, the provisions on the designation of the operator of the system, as well as the rules governing the use of the related early warning system;

21. the rules governing the reporting of threats, cybersecurity near misses and cybersecurity incidents, and the detailed rules on the handling and investigation of 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 the handling of cybersecurity crises, as well as the applicable procedure;

24. the rules relating to the establishment and operation of the National Cybersecurity Working Group and the bodies supporting its operation, as well as the functions and powers; and

25. the detailed rules governing cooperation between the organs referred to in section 76 (1) and with the entities referred to in section 76 (3), as well as the procedures for the provision of information and data to the European Commission and ENISA;

26. the detailed rules on the functions and powers and procedure of the national coordination centre, as well as on the registration.

(3) Authorisation shall be given to the Minister responsible for information technology to determine by 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 by 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 such fee.

(6) Authorisation shall be given to the president of SARA to determine by decree

a) the amount of the cybersecurity supervision fee and the provisions on its payment;

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

c) the rules for conducting a cybersecurity audit and the maximum amount of the 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 compliance check;

e) the rules governing the registration, in the cybersecurity supervision official register under section 29 (1) a), of entities referred to in section 1 (1) b), d) and e), as well as the detailed rules on the data content of the register that does not constitute 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 apply post-quantum encryption;

h) the detailed rules on the registration of post-quantum cryptographic solutions providers and the data content of the register excluding personal data, as well as the supervision of the post-quantum cryptographic solutions providers;

i) the detailed rules on the certification of the closed operation of the computer system components of post-quantum cryptographic solutions providers;

j) the detailed rules on the registration of the certification body, the data content of the register excluding personal data, and the supervision of the certification body;

k) with the exception of the certification authority activity referred to in section 45 (1) b), the detailed rules on the procedure governing certification authority activities, the authorisation procedure, the administrative compliance check and the keeping of the register, and the data content of the register excluding personal data, as well as the rules for affixing conformity marks;

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.

o) the detailed rules governing the conditions for entry of conformity assessment bodies in the register referred to in section 80/C (1) b) and the fulfilment of certain requirements set out in Article 39 (2) to (12) of Regulation (EU) 2024/2847 of the European Parliament and of the Council, the manner of demonstrating such compliance, as well as the procedure for registration and the data content of the register, not qualifying as personal data and not regulated by law;

p) the content requirements of the report referred to in section 80/F (1), as well as the time and manner of its submission.

(7) Authorisation shall be given to the president of SARA to determine by decree

a) the detailed rules on the registration of economic operators and persons authorised to perform vulnerability assessments, as well as 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) The 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 notified again; such data shall be processed by the national cybersecurity authority as part of the register referred to in section 28 (1).

(2) An entity referred to in section 1 (1) a) or b) shall fulfil 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 has not yet fulfilled 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) has already notified the national cybersecurity authority of 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 notify such data again.

(4) If, at the time of the entry into force of the Act, the person responsible for electronic information system security of an entity referred to in section 1 (1) a) or b) does not comply with the requirements set out in section 11 (4), a period of 2 years shall be available for eliminating the ground for incompatibility.

(5) If an entity referred to in section 1 (1) a) or b) should already have carried out, in accordance with the Electronic Information Security Act, the initial security classification of its operational electronic information systems by the time of the entry into force of this 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 "significant" 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) that does not qualify as 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 has already met the requirements prescribed therein for the security class of its electronic information systems, a period of 1 year from the entry into force of this Act shall be available for that entity to implement the new protective measures prescribed in a decree of the Minister responsible for information technology.

(2) If an entity referred to in section 1 (1) a), or an entity falling within the scope of section 1 (1) b) that does not qualify as 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 meet the requirements prescribed therein for the security class of its electronic information systems, it may, in implementing the protective measures prescribed in a decree of the Minister responsible for information technology, make use of the possibility of phased implementation referred to in section 10 (6). The time limit calculated taking phased implementation into account shall be based on the security class determined in accordance with section 84, the requirements of which shall already have been met. 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), as well as an entity falling within the scope of section 1 (1) b) that does not qualify as an entity listed in Annex 2 or 3, the provisions of this Act on the development of new systems shall apply to

a) an in-house developed system under development 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 not yet put into use at the time of the entry into force of this Act, provided that the procurement procedure for the development has not yet been launched or the contract for the development has not yet been concluded.

(2) If, at the time of the entry into force of this Act, a system of an entity referred to in section 1 (1) a), or of an entity falling within the scope of section 1 (1) b) that does not qualify as an entity listed in Annex 2 or 3, has already progressed beyond the stages of development of the electronic information system specified in paragraph (1),

a) the entity shall classify the electronic information system into a security class within 180 days, if it has not yet done so;

b) the entity may, in complying with the protective measures prescribed in a decree of the Minister responsible for information technology, make use of the possibility of phased implementation referred to in section 10 (6).

Section 87 If an entity referred to in section 1 (1) a), or an entity falling within the scope of section 1 (1) b) that does not qualify as 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 shall, until the expiry of the time limits set out in this Act, examine compliance with the technology security requirements set out in Act L of 2013 on the electronic information security of state and local government organs and with the provisions of the decree on secure information tools, products and on the requirements relating to classification into security classes and security levels when verifying compliance with electronic information security requirements, except where the entity has declared that it complies with the protective measures prescribed in a decree of the Minister responsible for information technology.

Section 88 (1) Administrative cases pending under 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 identification, designation and protection of critical systems and facilities shall be considered a critical entity for the purposes of this Act until the decision adopted in the 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 registered as 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 notification referred to in section 8 (5); SARA shall process its data entered 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). The data referred to in section 29 (1) a) ae) shall be submitted to SARA by 15 February 2025.

(1a) An entity referred to in section 1 (1) b) that is also an entity listed in Annexes 2 and 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 commenced operations before 1 January 2025 shall fulfil its obligation referred to in section 16 (2) no later than 31 August 2025.

(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 registered as supervised entity in the register kept in accordance with section 26 (1) of Act XXIII of 2023 on cybersecurity certification and cybersecurity supervision that classified its electronic information systems and the data stored, transferred or technically processed therein into security classes 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 registered 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 entered 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 registered 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 entered in the register referred to in section 14 (1) of Act XXIII of 2023 on cybersecurity certification and cybersecurity supervision, other than the data referred to in paragraph (7), as of 31 December 2024 need not be notified 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 under Act 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, within 30 days of the entry into force of this Act, to issue a request to remedy deficiencies. As a result of the procedure, SARA shall enter the data to be recorded under this Act in the registers under this Act.

(8) An entity entered in the register of economic operators authorised to perform vulnerability assessments under the government decree laying down the rules for vulnerability assessment as of 31 December 2024 shall not be required to request registration again; SARA shall process its data entered in the register as part of the register referred to in section 57 (1) c) on the basis of data provided by the Constitution Protection Office.

(9) An entity registered in the register referred to in section 57 (1) c) in accordance with paragraph (8) shall provide SARA with proof of compliance with the requirements prescribed by this Act and the legislation 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.

52/A Official abbreviated designation of the law

Section 90/A The abbreviated designation of this Act to be used in other legislation shall be: Cybersecurity Act.

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;

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;

d) Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act);

e) Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC.

Section 92 The prior notification of the draft of section 70 of this Act was submitted 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 99

Section 100

Section 101

Section 102

Section 103

Section 104

Section 105

Section 106

Section 107

Section 108

Section 109

Section 110

Section 111

Section 112

Section 113

Section 114

Section 115

Section 116

Section 117

Section 118

Section 119

Section 120

Section 121

Section 122

Section 123

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 control 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 the security 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;

	A	B	C
1	**Sector**	**Subsector**	**Type of the entity**
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;
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	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;

	A	B	C
1	**Sector**	**Subsector**	**Type of the entity**
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	Food 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,		food business within the meaning of the Act on the food chain and its authority supervision engaged in wholesale activity 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

	A	B	C
1	**Sector**	**Subsector**	**Type of the entity**
			Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH), establishing a European Chemicals Agency, amending Directive 1999/45/EC and repealing Council Regulation (EEC) No 793/93 and Commission Regulation (EC) No 1488/94 as well as Council Directive 76/769/EEC and Commission Directives 91/155/EEC, 93/67/EEC, 93/105/EC and 2000/21/EC;
6	Manufacturing	Manufacture of medical devices and *in vitro* diagnostic medical devices	entities manufacturing medical devices within the meaning of Article 2, point (1) of Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, or *in vitro* diagnostic medical devices within the meaning of Article 2, point (2) of Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on *in vitro* diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU, 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 engaged in 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;

	A	B	C
1	Sector	Subsector	Type of the entity
8		Manufacture of electrical equipment	economic operators engaged in 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 engaged in 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 motor vehicles, trailers and semi-trailers	economic operators engaged in the 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 engaged in 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 engaged in the activity of 'Manufacture of cement, lime and plaster' under Division 23.5 of Commission Delegated Regulation (EU) 2023/137 of 10 October 2022

	A	B	C
1	**Sector**	**Subsector**	**Type of the entity**
			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