Act LXIX of 2024

On Hungary's cybersecurity [1]

Valid: 2025. 05. 31. – 2027. 12. 31.

[1] Due to the threats to today's information society, it is of paramount importance for the nation to mitigate threats to electronic information systems and ensure the continuity of services in key sectors.

[2] It is a social expectation for the state and its citizens to ensure the closed, comprehensive, continuous and risk-proportionate protection of the confidentiality, integrity and availability of data and information managed in electronic information systems, which is essential for the state and its citizens, thereby protecting cyberspace, which contributes to the security, resilience and competitiveness of Hungary and the European Union.

[3] With the rapid digital transformation and interconnection of society, electronic information systems and digital devices have become central to everyday life. This development has also led to an expansion of the range of digital threats, which can disrupt economic activities, cause financial losses and undermine user confidence, thus causing significant damage to economic and social life. In addition, cybersecurity is a key factor for many critical sectors to successfully embrace digital transformation and fully exploit the economic, social and sustainable benefits of digitalisation.

[4] In view of all this, and of the directive on measures ensuring a high uniform level of cybersecurity throughout the European Union, the Parliament hereby enacts the following law:

Chapter I

GENERAL PROVISIONS

1. Scope of the Act

Section 1 (1) The provisions of this Act relating to the obligations of organisations and the regulatory supervision of cybersecurity shall apply to a) the organisations

listed in Annex 1 belonging to the public administration sector, b)

[2] to those economic entities under majority state control which do not fall within the scope of point a) and in respect of which at least one of the following conditions is met:

ba) its total number of employees reaches or exceeds 50 people, or bb) its

annual net sales and balance sheet total exceeds the equivalent of EUR 10 million in forints, c)

organisations identified as essential or important by the national cybersecurity authority referred to in Article 23(1)(a) (hereinafter: national cybersecurity authority) or the national defence cybersecurity authority referred to in Article 23(2)(a) (hereinafter: national defence cybersecurity authority) as per paragraph (6), not falling under points a), b) and d)–f) and Regulation (EU) 2022/2554 of the European Parliament and of the Council, those organisations referred

d)[3] to in Annexes 2 and 3 which qualify as medium-sized enterprises or exceed the thresholds prescribed for medium-sized enterprises under the Act on Small and Medium-sized Enterprises and the Support for Their Development and which do not fall under point a),

[4] e) regardless of their size, to organisations not covered by point a) and listed in Annexes 2 and 3, if the organisation

1The Act was adopted by the National Assembly on its session of December 17, 2024. Date of promulgation: December 20, 2024.
2Section 1(1)(b) in conjunction with Section 53(1) of Act XXXII of 2025 established text.
3Section 1(1)(d) in conjunction with Section 53(2) of Act XXXII of 2025 established text.
4Section 1(1)(e) in conjunction with Section 53(2) of Act XXXII of 2025 established text.

ea) electronic communications service provider,

eb) trust service provider,

ec) DNS service provider,

ed) top-level domain name registrar or ee) domain name

registration service provider, and f) business companies carrying

out activities related to national defense interests.

(2) Critical organizations and critical infrastructures designated under the Act on the Resilience of Critical Organizations (hereinafter referred to as: Critical Organization) and the Act on the Coordination of Defense and Security Activities (hereinafter referred to as: Vbö.) In relation to organisations and infrastructures designated as being significant for the defence and security of the country (hereinafter collectively referred to as: organisations significant for the defence and security of the country), the classification of the organisation in accordance with paragraph (1) shall govern the application of the provisions of this Act, unless the critical organisation or organisation significant 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) [5] The provisions of this Act – with the exception of Section 9 and Sections 13–15 – governing the organisations referred to in Section 1(1)(a) shall apply to any critical organisation or organisation significant for the defence and security of the country which does not qualify as an organisation referred to in Section (1).

(3) Organizations – the importance of the services they provide for the functioning of the state, society and the economy
They are classified as essential or important organizations based on their criticality and, in some cases, the size of the organization.

(4) Among the organizations referred to in paragraph (1), the following organizations shall be considered as essential

organizations: a) organizations referred to in Annex 1, except for the offices of the representative bodies of settlements with a population not exceeding 20,000 people,

b) [6] organizations referred to in paragraph (1) b),

c) organizations that are designated as essential by the national cybersecurity authority or the national defense cybersecurity authority
identified as an organization, d)

critical organizations designated under the Act on the Protection

of Human Rights, e) the Act on the Protection of Human Rights. organizations designated under the Act on Small and

Medium-sized Enterprises and Support for Their Development, which are significant for the protection and security of the country, f) organizations as per Annex 2, which are are classified as medium-sized enterprises or exceed the thresholds prescribed for medium-sized enterprises, and

g) qualified trust service providers and top-level domain name registrars, as well as DNS service providers, regardless of their size. h)

[7] business companies carrying out activities related to national defense interests.

(5) The organizations referred to in paragraph (1) are considered important organizations and the provisions relating to the organizations are as follows:
This Act shall apply, with the exceptions set out in this Act, to the following organisations:

a) offices of the representative bodies of settlements with a population not exceeding 20,000 people, b)

organizations that are considered important by the national cybersecurity authority or the national defense cybersecurity authority
identified as an organization,

c) an organization according to Annex 2 that is not considered a core organization, and d) an organization

according to Annex 3 that is not considered a core organization under points b)–e) of paragraph (4).

(6) The condition for the identification procedure pursuant to point c) of paragraph (1) is that the

organization 1. is the sole provider in Hungary of a service that is essential for the provision of critical social or economic services.
to maintain activities; 2. a disruption

of the service provided by could have a significant impact on public order, public security or public health; 3. a disruption of the service

provided by could have a significant impact on critical social or economic activities; 4. a disruption of the service provided by could create a significant

systemic risk, in particular in sectors where the
said disturbance may have cross-border effects;

5. is of particular importance at national or regional level for the type of sector or service in question, or for other domestic interdependent sectors; 6. is subject to national security protection pursuant to a

government resolution on the scope of bodies and facilities subject to national security protection; or the national cybersecurity authority deems its identification justified for national security reasons, or for national defense or military national security reasons, the national defense cybersecurity authority;

5Section 1(2a) is replaced by Section 53(3) of Act XXXII of 2025 he enrolled.
6Section 1(4)(b) in conjunction with Section 53(4) of Act XXXII of 2025 established text.
7Point h) of Section 1 (4) is replaced by Section 53 (5) of Act XXXII of 2025 he enrolled.

7. provides at least 20,000 persons with services in the sectors listed in Annexes 2 and 3 or those necessary for the operation of the state services;

8. provides services to at least five organizations falling within the scope of this Act; 9. is under majority state control; 10. is a data processor of state registers falling within the scope of national data assets as defined by law; 11. performs data processing for a fundamental or important organization; 12. qualifies as a publicly owned business entity that does not fall within the scope of paragraph (1) b) or 13. develops an electronic information system within the framework of projects supported by budgetary and European Union funds.

(7) The provisions of this Act relating to cybersecurity certification shall be implemented by the Information and Communication Technology (ICT) hereinafter referred to as: ICT) products, ICT services or ICT processes.

(8) The provisions of this Act relating to post-quantum encryption shall apply to the following organisations (hereinafter referred to as: organisations obliged to apply post-quantum encryption) and their activities under their official supervision, as specified in the decree of the President of the Supervisory Authority for Regulated Activities (hereinafter referred to as: SZTFH): a) organisations obliged to use the Government Decree on Government Networks, and b) public utility service providers subject to the following acts and public service providers subject to the following acts and legal acts issued under the authority of the following acts:

ba) the Act on Natural Gas Supply, bb) the Act on the Security Stockpiling of Natural Gas, bc) the Act on Electricity, bd) the Act on District Heating Services, be) the Act on Water Utility Services, and bf) the Act on Waste.

(9) The provisions of this Act relating to vulnerability assessments shall apply: a) b) to [8] the electronic information systems of the organisations referred to in points a)–c) and f) of paragraph (1), and vulnerability assessments concerning electronic information systems specified in the agreement pursuant to Section 61, with the exceptions set out in the agreement.

(10) The provisions of this Act relating to cybersecurity incident management shall apply to: a) the organisations referred to in paragraph (1), and b) the organisations covered by Regulation (EU) 2022/2554 of the European Parliament and of the Council, with the derogations specified in this Act.

to handle cybersecurity incidents affecting its electronic information systems.

(11) In the case of cybersecurity incidents voluntarily reported by organizations or persons other than those specified in paragraph (10), the national cybersecurity incident management center shall act in accordance with the provisions of this Act.

Section 2 (1) The provisions of this Act shall apply to a) organizations referred to in Section 1 established or having a representative established in the territory of Hungary,

b) electronic communications service providers providing services in the territory of Hungary,

c)[9] to those DNS service providers, top-level domain name registrars, organizations providing domain name registration services, cloud service providers, data center service providers, content service network service providers, outsourced (directed) infocommunication service providers, outsourced (directed) infocommunication security service providers, online marketplaces, online search engines and social media service platforms whose principal place of business is located in Hungary.

(2) The principal place of business of an organization referred to in point c) of paragraph (1) is in Hungary if a) decisions related to cybersecurity risk management measures are predominantly made in Hungary, b) cybersecurity operations related to the organization's electronic information systems are carried out in Hungary, or c) the organization's location with the highest number of employees is in Hungary.

Section 3 (1) The scope of this Act does not extend to a) electronic information systems handling classified information, b) electronic information systems for operational purposes,

8Section 1(9)(a) is Section 71(1) of Act XXXII of 2025 Text amended accordingly.
9A Section 2(1)(c) of Act XXXII of 2025, Section 54. Text established by §.

c) on physical protection in the application of nuclear energy and the related licensing, reporting and inspection system programmable systems falling within the scope of the Government Decree, and d)

cybersecurity services provided by the body designated in the Government Decree.

(2) The Government shall determine in its decree the scope of cybersecurity services referred to in paragraph (1) point d) and the the range of organizations obliged or entitled to use it.

(3) The provisions of this Act with regard to electronic information systems for national defense purposes are set out in this Act. shall be applied with certain exceptions.

2. Interpretative provisions

Section 4 For the purposes of

this Act, 1. ***data:*** the carrier of information, the formalized representation of facts, concepts or instructions, which is used by people or suitable for communication, display or processing by automatic means;

2. ***data processing:*** the concept under the Act on Informational Self-Determination and Freedom of Information; 3. ***data processor:*** the concept under the Act on Informational Self-Determination and Freedom of Information; 4. ***data management:*** the concept under the Act on Informational Self-Determination and Freedom of Information; 5. ***data controller:*** the concept under the Act on Informational Self-Determination and Freedom of Information; 6. ***data exchange service:*** the concept under the Act on Electronic Communications; 7. ***data center service:*** a service that provides centralized placement, connection and operation of information technology and network equipment for data storage, processing and transmission, including facilities and infrastructure for energy supply and environmental monitoring;

8. ***data classification:*** the security classification of data and information managed by the organization in the electronic information system in terms of their confidentiality, integrity and availability;

9. ***sectoral cybersecurity incident management centre:*** a cybersecurity incident management centre operated by one or more organisations belonging to a sector covered by this Act for the purpose of centralised and uniform management of cybersecurity incidents occurring in a specific area of expertise within the sector;

10. ***auditor:*** an independent economic entity authorized to conduct cybersecurity audit activities pursuant to this Act; 11. ***penetration testing:*** a vulnerability assessment method that identifies weaknesses in the ICT system and electronic information system and checks their exploitability by simulating malicious attacks against security measures;

12. ***internal IT security assessment:*** a vulnerability assessment method in which the vulnerability assessment of the IT system is carried out directly from the internal network endpoint, or the device or system component used in the internal network is examined; 13. ***confidentiality:*** the property of an electronic

information system that the data and information stored in it can only be accessed by those authorized to do so. are authorized and can only access, use, and dispose of it according to their level of authorization;

14. ***trust service:*** a concept under the Act on the Digital State and Certain Rules for the Provision of Digital Services; 15. ***trust service provider:***

a concept under the Act on the Digital State and Certain Rules for the Provision of Digital Services; 16. ***security class:*** the expected strength

of the protection of an electronic information system; 17. ***security classification:*** the

determination of the expected strength of the protection of an electronic information system based on the risks; 18. ***digital service:*** a concept under

the Act on the Digital State and Certain Rules for the Provision of Digital Services; 19. ***DNS:*** a hierarchical naming system, also known as the

domain name system, which enables the identification of Internet services and resources, enabling end-user devices to use Internet routing and connection services in order to access these services and resources; 20. ***DNS service provider:*** an organization that provides one of the following services to an organization other than the organization:

or for a person: a) ***authoritative DNS service:*** a service that directly enables the querying of domain name data – managed by the domain name registration service provider – and is part of the top-level domain name registry service, b) ***recursive DNS service:*** a DNS service that forwards users' domain name queries to the appropriate authoritative DNS service providers in the hierarchically structured domain name system and forwards the responses to the query by the authoritative DNS service provider to the user,

c) ***DNS caching:*** temporary storage of responses to domain name queries and serving user queries based on the stored domain name data,

21. ***domain name:*** the alphanumeric equivalent of an IP address used for Internet communication, 22. ***domain name registration service provider:*** a service provider authorized by the top-level domain name registrar, which is eligible to register a domain;

23. ***electronic communications service provider:*** the concept defined in the Electronic Communications Act; 24. ***electronic information system:***

a) an electronic communications network defined in the Electronic Communications Act, b) any device or group of devices connected or related to each other, one or more of which performs automated processing of digital data based on a program, including cyber-physical systems, or c) digital data stored, processed, retrieved or transmitted by the elements listed in subparagraphs a) and b) for the purpose of their operation, use, protection and maintenance; 25. ***electronic information system security:*** the ability of

electronic information systems to withstand, with a given degree of certainty, any event that may endanger the availability, integrity or confidentiality of the data stored, transmitted or processed on them or the services offered by or accessible through the aforementioned network and information systems; 26. ***life cycle:*** the period of time encompassing the design, development, operation and termination of an electronic information system; 27.

event: change of state in the electronic information system; 28. ***European cybersecurity certification scheme:*** point (9) of Article 2 of Regulation (EU) 2019/881 of the European Parliament and of the Council concept according to;

29. ***user organisation:*** an organisation using a central system or a central service; 30. ***cloud service:*** a digital service that enables self-service network access to a flexible pool of shared physical or virtual resources that can be scaled on demand; 31. cloud ***service provider:*** an organisation providing cloud computing services; 32. ***manufacturer:*** a manufacturer of an ICT product, a provider of an ICT service, and a manufacturer or provider of an ICT process; 33.

deployment: the act of populating an electronic information system with data and putting it into use for its intended purpose

34. ***electronic information system for national defense purposes:***

a) the set of electronic information systems of national defence organisations, multi-purpose vocational training institutions not classified as national defence organisations under the management of the minister responsible for national defence, business associations under the ownership of the minister responsible for national defence, and business associations carrying out activities related to national defence interests according to law, which support the operation within and between sectors in a sector-specific manner, b) the electronic information systems of organisations and infrastructure within the national defence sector that are significant for the defence and security of the country, c) their electronic information

[10] organization and infrastructure not affected by dual designation that is significant for the defense and security of the country systems, and d) the electronic information system of an organisation identified as a fundamental or important organisation by the national defence cybersecurity authority; 35. ***national defence cybersecurity incident management centre:*** an organisation designated pursuant to Section 63(2); 36.

temporary inaccessibility: temporary prevention of access to electronic data; 37. ***ICT process:*** as defined in point (14) of Article 2 of Regulation (EU) 2019/881 of the European Parliament and of the Council; 38. ***ICT service:*** as defined in point (13) of Article 2 of Regulation (EU) 2019/881 of the European Parliament and of the Council; 39. ***ICT product:*** as defined in point (12) of Article 2 of Regulation (EU) 2019/881 of the European Parliament and of the Council; 40. ***major cybersecurity incident:***

a) a cybersecurity incident as defined in a directly applicable European Union legal act, b) in the absence of a directly applicable European Union legal act, a cybersecurity incident that ba) results in or threatens to result in a reduction of at least 5% of the business service of the organisation or of the service provided by the organisation or a loss of at least 5% of the annual revenue of the organisation; bb) causes or is likely to cause a serious disruption of services or causes or is likely to cause financial or reputational loss to the organisation or person affected by the cybersecurity incident; or bc) affects or is likely to affect other natural or legal persons by causing significant material or non-material damage;

10A Section 4, point 34, subparagraph c) of Act XXXII of 2025, section 55. Text established by §.

41. ***significant cyber threat:*** a cyber threat that, based on its technical characteristics, can be assumed to have a serious impact on an organisation's electronic information systems or on the users of the organisation's services, causing significant material or non-material disadvantage or damage;

42. ***representative:*** any natural or legal person established in Hungary who has been specifically designated to act on behalf of an organization not established in Hungary and to whom the cybersecurity authority or the cybersecurity incident management center may address on behalf of the given organization;

43. ***cybersecurity:*** the term defined in point 1 of Article 2 of Regulation (EU) 2019/881 of the European Parliament and of the Council; 44. ***cybersecurity audit:*** the classification of electronic information systems into security classes and the verification of the adequacy of the protection measures in accordance with the security classification;

45. ***cybersecurity authority:*** the authority referred to in points a) and b) and (2) of Section 23 (1); 46. ***cybersecurity incident:*** an event that endangers the availability, integrity or confidentiality of data stored, transmitted or processed on electronic information systems or the services offered by or accessible through these systems; 47. ***cybersecurity incident management:*** all activities and procedures aimed at preventing, detecting, analysing and containing a cybersecurity incident or at responding to a cybersecurity incident and restoring operations following a cybersecurity incident; 48. ***cybersecurity incident management centre:*** the body referred to in Section 63 (1) and (2); 49. ***cybersecurity near-incident:*** an event that could have compromised the availability, integrity or confidentiality of data stored, transmitted or processed on electronic information systems or the services offered by or accessible through these systems, but the occurrence of which was prevented or which did not occur;

50. ***cyber threat:*** the term defined in point 8 of Article 2 of Regulation (EU) 2019/881 of the European Parliament and of the Council; 51. ***cyber-physical system:*** programmable electronic information systems that interact with the physical environment or manage devices that interact with the physical environment. These electronic information systems directly sense or cause physical change by monitoring or controlling devices, processes and events; 52. ***outsourced (managed) infocommunication security service provider:*** an outsourced (managed) infocommunication service provider that manages cybersecurity risks or provides a service related thereto;

53. ***outsourced (directed) information and communication service provider:*** an organization that provides services related to the installation, management, operation or maintenance of an ICT product, network, infrastructure, application or any other electronic information system at the premises of the service user or remotely;

54. ***risk:*** the degree of threat, which is the frequency and probability of occurrence of a threat and the extent of the damage caused by it;

55. ***risk analysis:*** the assessment of the value, vulnerability, threats, and expected damage of the electronic information system and identifying and assessing risks by assessing their frequency;

56. ***risk management:*** the development of a system of measures to reduce the risks affecting an electronic information system and the implementation of those measures; 57. ***risk management framework:*** a set of structured yet flexible approaches and organisational processes that integrate cybersecurity risk management activities throughout the system development life cycle through the identification, implementation, assessment, operation and monitoring of risk-proportionate protective measures in order to continuously detect threats to new and existing systems and to effectively manage their risks; 58. ***public administration body:*** an organisation referred to in points 1 to 13 of Annex 1; 59. ***social media service platform:*** a platform that enables end-users to use multiple devices to connect, share content, discover and communicate with each other through;

60. ***central system:*** an electronic information system developed or operated centrally for a closed client group, assisting in the performance of certain state and local government tasks, through which functions implemented are used by user organizations in a given institutional circle, either mandatory or optional;

61. ***central service:*** a service to be provided by a central service provider on a mandatory basis or based on individual requests; 62. ***central service provider:*** an organization that, based on legal provisions, provides services to organizations performing state and local government tasks provides IT and electronic communications services with exclusive rights;

63. ***research site:*** a research site within the meaning of the Act on Scientific Research, Development and Innovation – with the exception of educational institutions – the primary purpose of which is to conduct applied research or experimental development with the aim of exploiting the results of the research for commercial purposes;

64. ***top-level domain name registrar:*** an organization to which a specific top-level domain has been entrusted and which is responsible for the management of the top-level domain, including the registration of domain names under the top-level domain, and for the –, technical operation of the top-level domain, including the operation of its name servers, the maintenance of its databases and the distribution of top-level domain zone files between the name servers, regardless of whether any of these operational activities are performed by the organization itself or outsourced, except in cases where the top-level domain names are used exclusively by the registry for its own use;

65. ***conformity assessment:*** the assessment procedure demonstrating that specified requirements relating to an ICT product, ICT process or ICT service have been fulfilled; 66. ***conformity assessment body:*** the concept defined as such 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 making available on the market of products and repealing Regulation (EEC) No 339/93;

67. ***declaration of conformity:*** a document issued by the manufacturer or service provider attesting that a given ICT product, ICT service or ICT process has been assessed for compliance with the security requirements of a national cybersecurity certification scheme;

68. ***'self-assessment of conformity' means*** the concept defined as such in Regulation (EU) 2019/881 of the European Parliament and of the Council; ***Milestone*** 69 : in the case of the development of a central system financed by European Union funds, the concept defined in Article 2(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(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 laying down financial rules for the former and for the Asylum, Migration and Integration Fund, the Internal Security Fund and the instrument for financial support for border management and visa, and in the case of other projects aimed at development, the concept defined in the project;

70. ***qualified trust service:*** Act on the Digital State and Certain Rules for the Provision of Digital Services concept according to;

71. ***qualified trust service provider:*** Act on the Digital State and Certain Rules for the Provision of Digital Services concept according to;

Technical specification 72 : ***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, 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 referred to as Regulation (EU) No 1025/2012) in Article 2(4) defined concept;

73. ***electronic information system for operational purposes:***

a) an electronic information system used by law enforcement agencies and national security services to perform public security and national security tasks specified by law, and

b) an electronic information system used by defence organisations to perform military operational tasks specified in the law, in particular direct operational support, planning, leadership and situation monitoring;

74. ***large-scale cybersecurity incident:*** a cybersecurity incident that causes a level of disruption that exceeds Hungary's ability to respond to it, or that has a significant impact on Hungary and at least one other country; 75. ***non-private cloud service:*** a cloud service provided by a service provider that is accessible to anyone by the service provider in a specific way or exclusively for a specific group of organizations;

76. ***national cybersecurity incident response center:*** a unit responding to cybersecurity incidents operating in accordance with the recommendations of the European Network and Information Security Agency, which is a member of international organizations specializing in network security and the protection of critical information infrastructures [in European usage: CSIRT (Computer Security Incident Response Team), in American usage: CERT (Computer Emergency Response Team)]; 77. ***national cybersecurity certification system:*** a comprehensive system of rules, technical requirements, standards and procedures applicable in Hungary for the certification and conformity assessment of ICT products, ICT services and ICT processes, developed on the basis of the principles of European cybersecurity systems and determined by the certification authority;

78. ***National Cybersecurity Strategy:*** sets out the strategic goals and priorities to be pursued in the field of cybersecurity, as well as the a document defining the management measures necessary for their implementation;

79. ***national cybersecurity certificate:*** a document issued by an independent third party that certifies that a given ICT product, ICT service or ICT process has been assessed for compliance with the security requirements of a national cybersecurity certification scheme;

11 80. ***national crisis management plan:*** a national plan for responding to large-scale cybersecurity incidents and crises, based on Directive (EU) 2022/2555 of the European Parliament and of the Council, which sets out the objectives and rules for managing large-scale cybersecurity incidents and crises;

81. ***online search engine:*** the term defined in point (5) of Article 2 of Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fair and transparent conditions for business users of online intermediation services; 82. ***online marketplace:*** a service that uses

software, including a website, part of a website or an application, operated by or on behalf of a trader, and through which consumers can conclude distance contracts with other traders or consumers;

83. ***registered user authorization:*** for the person conducting the security assessment, to perform the vulnerability assessment user rights specifically created for the purpose;

84. ***availability:*** ensuring that electronic information systems are available to the person authorised to do so are accessible and the data managed therein can be used;

85. ***vulnerability:*** weakness, sensitivity or deficiency in an ICT product, service or process, the exploitation of which threatens or compromises the confidentiality, integrity or availability of an ICT product, service or process;

86. ***integrity:*** the property of data that refers to the fact that the content and properties of the data are as expected, including the certainty that it originates from the expected source, i.e. it is authentic, as well as the verifiability and certainty of origin, i.e. its non-repudiation, and the property of the elements of the electronic information system that refers to the fact that the element of the electronic information system can be used in accordance with its intended purpose;

87. ***vulnerability:*** a weakness, sensitivity or deficiency in an electronic information system, the exploitation of which threatens or violates the confidentiality, integrity or availability of an electronic information system;

88. ***vulnerability management plan:*** a plan document aimed at eliminating vulnerabilities; 89.

vulnerability assessment: a vulnerability management tool or method that involves examining IT systems, hardware and software from a security perspective, the verification being carried out using automated tools and direct examinations carried out by an expert;

90. ***standard:*** the term defined in point 1 of Article 2 of Regulation (EU) No 1025/2012; 91.

organisation: a state body or a state organisation, a legal person under the Civil Code, a legal person an organization without personality;

92. ***support system:*** not directly involved in the performance of the basic tasks of the organization referred to in Section 1(1)(a)–(c) receiving electronic information system that is necessary for the operation of systems that perform a basic task;

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

94. ***content delivery network provider:*** a provider of a network of geographically distributed servers ensuring the widespread, seamless and rapid availability of digital content and services; 95. ***remote vulnerability assessment:*** a

vulnerability assessment during which

a) an external vulnerability assessment of the electronic information system from the Internet is carried out, within the framework of which free searching in public databases available on the Internet, targeted information collection, and mapping of the vulnerability of the services of accessible computers are carried out, b) vulnerabilities of web applications are revealed through automated and manual examinations, or c) wireless access and connection points are searched, mapped, encryption procedures are analyzed, and the decryptability of encryption keys is checked using target software and manual examination;

96. ***further development:*** the development of the relevant, already operating electronic information system to such an extent that results in a substantial change in its functionality or affects the expected strength of its protection;

97. ***operational cybersecurity incident:*** a cybersecurity incident that unintentionally reduces or eliminates the availability of data stored, transmitted or processed on electronic information systems or the services offered by or accessible through these systems;

98. ***operator:*** a natural person, legal person, organization without legal personality or sole proprietor who either: which operates the electronic information system or parts thereof and is responsible for its operation;

99. ***closed, comprehensive, continuous and risk-proportionate protection:*** protection of the electronic information system in a way that 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 account all conceivable threats and dangers, and d) whose costs are proportional to the value of the damage that can be caused by the threats.

11A Section 4, point 80, Section 71, point 2, Act XXXII of 2025 Text amended accordingly.

3. General principles

Section 5 (1) Electronic information systems falling within the scope of this Act shall be implemented and maintained throughout their entire life cycle. must be ensured

a) data and information managed in the electronic information system and the services provided by the electronic information systems
the confidentiality, integrity and availability of services available on or through it, and

b) the integrity and availability of the elements of the electronic information system
closed, comprehensive, continuous and risk-proportionate protection.

(2) Within the framework of the protection of the electronic information system, the organization with the authority to dispose of the electronic information system, the data controller or the data processor, for a given purpose, shall: a) the devices used to

process data and information, including the environmental infrastructure, hardware, network and
data carriers

b) the procedures used to handle data and information, including regulations, software and related processes, and c) the persons handling the items specified

in points a) and b)
It is also necessary to ensure the protection of its ensemble.

(3) Adequate budgetary resources shall be provided for the

operation of a) the national cybersecurity authority and the national defense cybersecurity

authority, b) the state body authorized to conduct vulnerability assessments pursuant to Section 57(1) (hereinafter: state body authorized to conduct vulnerability assessments), and c) the national cybersecurity incident

management center and the national defense cybersecurity incident management center pursuant to Section 63.

Chapter II

OBLIGATIONS OF FUNDAMENTAL AND IMPORTANT ORGANIZATIONS

4. General obligations of essential and important organizations

Section 6 (1) The electronic information system of the organization shall be considered to be the electronic system at the disposal of the organization. information system.

(2) The head of the organisation shall establish and operate a risk management framework in order to protect electronic information systems, as set out in the directly applicable European Union legal act, or in the absence thereof and in matters not regulated by the directly applicable European Union legal act, as set out in the regulation of the minister responsible for IT.

(3) Within the framework of the activity specified in paragraph (2), the head of the organization

shall: 1. ensure the assessment of the electronic information systems and central services used by the organization and
on its registration, broken down as follows: a) electronic information
systems at the disposal of the organization, b) central systems used by the
organization, c) services and support systems provided
by the central service provider used by the organization, d) other support systems at the disposal of the organization or used
by the organization;

2. determines the roles, responsibilities, tasks and the necessary powers related to the protection of the electronic information systems at the disposal of the organization and used by the organization, appoints or assigns the person responsible for the security of the electronic information system;

3. in the case of an organization referred to in Annex 1, it shall ensure the assessment and classification of data managed in the electronic information system referred to in point 1, subparagraph a); 4. it

shall carry out impact analysis and risk management activities in accordance with the decree of the minister responsible for IT regarding the electronic information systems referred to in point 1, subparagraph a) and their environment; 5. it shall classify the

electronic information systems referred to in point 1, subparagraph a) into security classes as specified in the legislation; 6. it shall determine the measures

proportionate to the risks with regard to the electronic information systems referred to in point 1, subparagraph a).
protective measures;

7. issues an information security policy regarding users and electronic information security requirements, and ensures its review at least every two years or in cases specified in law;

8. ensures the implementation of the security measures specified for the protection of electronic information systems; 9. ensures – if relevant – that the provisions of the European Union legal act and the decree of the minister responsible for IT are complied with on the assessment of the adequacy of the protective measures selected in accordance with the first security classification,

10. regularly ensures the periodic assessment of security measures, including at least risk analyses, audits, and conducting an internal cybersecurity assessment based on an independent recommendation issued by the cybersecurity authority, to ensure that the security measures defined in accordance with the legislation and risks adequately ensure the security of the organization and its electronic information systems;

11. ensures that deficiencies identified during the assessment of security department-related protection measures are remedied; 12. decides within the organization on the introduction or continued use of electronic information systems; and 13. ensures that cybersecurity regulatory obligations are met. (4)

[12] The tasks specified in point 10 of paragraph (3) shall be carried out by the head of the organization at least every two years, simultaneously with the review of the information security policy or, if he is obliged to implement it, with the review of the security classification.

(5) In order to ensure the protection of the electronic information system, the head of the organization shall: a) ensure the training of the protection tasks of electronic information systems and the responsibilities related to them, and the cybersecurity training and further training of himself and the organization's employees – as specified in the decree of the minister responsible for IT; b) ensure the participation in mandatory domestic cybersecurity exercises and the independent holding of cybersecurity exercises; c) ensure the traceability of events in the electronic information system; d) if the organization uses a collaborator in the creation, operation, auditing, maintenance, repair of the electronic information system, or in the management of cybersecurity incidents, or in the performance of data management and data processing activities related to the organization's electronic information system, he shall ensure that the cybersecurity requirements necessary in connection with the activities performed by the collaborator in connection with the electronic information system are fulfilled as a contractual obligation in accordance with the provisions of this Act;

e) in the event of a cyber threat, near-miss or cyber security incident affecting the electronic information system, it ensures a rapid and effective response, notification to the competent cyber security incident management center, management of cyber security incidents and recovery, using all necessary and available resources;

f) ensure that data subjects are promptly informed of cybersecurity incidents and potential threats;

g) ensures that the recommendations and guidelines of the cybersecurity authority and the competent cybersecurity incident management center are followed taking into account to ensure the protection of the electronic information system;

h) shall strive to carry out the tasks specified in this legislation as soon as possible; i) in the case of organizations referred to in Section 1(1)(a)–(c), shall ensure that the organization spends an amount corresponding to at least 5% of the costs spent by the organization on IT development in the given year on cybersecurity developments during the relevant year and j) shall take other necessary measures to protect the electronic information system.

(6) The head of the organization is also responsible for the tasks specified in paragraphs (3)–(5) in the case specified in paragraph (5) d), except – to the extent of the services used – in those cases where the organization must use a central service provider or a central system.

(7) The fulfillment of the reporting obligation pursuant to paragraph (5) e) shall not affect the reporting obligations existing under other laws. obligations.

(8) In order to demonstrate compliance with certain requirements under paragraphs (1) to (5), European or An ICT product, ICT service or ICT process certified under a national cybersecurity certification system may be used.

(9) [13] The organizations specified in the decree of the Minister responsible for IT – in the decree of the Minister of Defence with regard to electronic information systems for national defence purposes – under Section 1(1)(a)–(c) and (f) and the organizations specified in the decree of the President of the National Security Council under Section 1(1)(d) and (e) are obliged to use an ICT product, ICT service or ICT process certified under a European or national cybersecurity certification scheme – as specified in the decree of the Minister responsible for IT, the Minister of Defence or the President of the National Security Council.

(10) In relation to electronic information systems at the disposal of an important organisation falling within the scope of Section 1(1)(a) and (c) and an organisation falling within the scope of Section 1(1)(b) which is not an organisation as defined in Annexes 2 and 3

12A Section 6(4) in conjunction with Section 56(1) of Act XXXII of 2025 established text.
13Section 6(9) is the text amended by Section 71(3) of Act XXXII of 2025 .

a) it is not necessary to operate the full risk management framework set out in paragraph (2), b) c) at least the
[14] the requirements of points 4–5 and 9 of paragraph (3) do not need to be met, and
requirements for the “basic” security class must be met.

(11) The organization with the authority to dispose of the electronic information system for national defense purposes shall contact the national defense cybersecurity authority in the official procedure regarding the electronic information system for national defense purposes and shall fulfill the notification and other obligations prescribed by this Act towards the national defense cybersecurity authority.

(12) [15] The detailed rules for holding domestic cybersecurity exercises, as well as Section 1(1) a)–c) and f)
Detailed provisions regarding the obligations of organizations falling within its scope are set out in a government decree.

Section 7 (1)[16] For cybersecurity supervision activities – with the exception of budgetary bodies – the organization referred to in Section 1(1)(b) which is also an organization referred to in Annexes 2 and 3, as well as the organization referred to in Section 1(1)(d) and (e) – if the organization is a controlled member of a recognized group of companies pursuant to the Act on the Civil Code (hereinafter referred to as: recognized group of companies), or the dominant member – shall be obliged to pay a cybersecurity supervision fee in the amount specified in the decree of the President of the SZTFH – based on the provisions of Section (2).

(2) The annual cybersecurity supervision fee shall be a maximum of 0.015 percent of the net sales revenue of the organization referred to in paragraph (1) of the previous business year – or, in the absence of sales revenue, the pro rata portion of the sales revenue of the current year projected over the entire year – but not more than 10 million forints. The total amount of the annual cybersecurity supervision fee payable shall not exceed 50 million forints for organizations participating in the same recognized group of companies or in the same actual group of companies pursuant to the Act on the Civil Code, or in a group of companies within a consolidation scope comprising the parent company, subsidiaries and jointly managed companies included in the consolidation pursuant to the Act on Accounting. The organization referred to in paragraph (1) shall prove the fact of operating as an actual group of companies or as a group of companies within a consolidation scope in accordance with the provisions of the decree of the President of the SZTFH.

(3) The cybersecurity supervision fee shall be paid by the person liable under paragraph (1) in accordance with the regulation of the President of the SZTFH. must pay to the SZTFH in the manner and on time.

Section 8 (1) An organization not registered in Hungary operating an electronic information system falling within the scope of this Act shall appoint in writing a representative operating in the territory of Hungary who shall be responsible for the implementation of the provisions of this Act in accordance with the rules applicable to the head of the organization. The appointment of the representative shall not affect the liability of the organization or the head of the organization.

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

(3) During the cooperation, the head of the organization
shall a) ensure that the data, documents and any changes thereto are sent to the cybersecurity authority within fifteen days of the change, for the purpose of registration, as specified in the law and on the authority’s website, and b) ensure the necessary conditions for conducting the inspection. (4) following the avoidance

[17] The organization referred to in Section 1(1)(a)–(c) and (f) shall be subject to the scope of this Act, with the exceptions set out in Subsection 51.

a) within 30 days, notify the national cybersecurity authority of the information referred to in Section 28(1)(1)(a)–(e) and (j)
specific data,

b) within 30 days, notify the national cybersecurity authority responsible for the security of the electronic information system
personal data,

c) within 90 days, assess the electronic systems used by the organization in accordance with Section 6(3)(1).
information systems, d) within
120 days – if relevant – performs the data classification pursuant to Section 9, e)
within 180 days sends the organization's information security policy to the national cybersecurity authority, f)

[18] Within 180 days, together with the establishment of the risk management framework pursuant to Section 6 – if it is obliged to implement it – it shall classify its existing electronic information systems into security classes, assess the protection measures related to the electronic information systems, their adequacy and status, and submit a notification to the national cybersecurity authority in accordance with the content specified in the Government Decree.

14A Section 6(10)(b) in conjunction with Section 56(2) of Act XXXII of 2025 established text.
15A Section 6(12) Section 71(4) of Act XXXII of 2025 Text amended accordingly.
16A Section 7(1) is the text amended by Section 71(5) of Act XXXII of 2025 .
17The opening text of Section 8(4) is the text amended in accordance with Section 71(6) of Act XXXII of 2025.
18A Section 8(4)(f) of Act XXXII of 2025, Section 57. Text established by §.

(5) An organization falling under the scope of Section 1(1)(b) and simultaneously qualifying as an organization under Annexes 2 and 3, as well as an organization under Section 1(1)(d) and (e) shall, within 30 days of commencing its operations or becoming subject to this Act, send the data specified in Section 29(1)(a) – with the exception of the data specified in Section 29(1)(a) and (b) – to the SZTFH for registration.

(6) For the purposes of applying paragraphs (4) and (5), the date of coming under the scope of this

Act shall be: a) the date of establishment of the

organisation in the case of a new organisation, b) the date of establishment of the organisation in the case of a new organisation,
in the case of reaching size limits, the first day of the year following the

occurrence, c) the date of entry into force of the legal act establishing the legal status resulting in the
entry into force.

(7) The organization may conclude cybersecurity information sharing agreements for the purpose of implementing the cooperation specified in the decree of the Minister responsible for IT, with the exception of information relating to electronic information systems for national defence purposes. The organization shall inform the cybersecurity authority of the conclusion of a cybersecurity information sharing agreement, its participation in such an agreement or its termination.

5. Data classification

Section 9 (1) In order to ensure that the protection of data managed by the organization is proportionate to the risks, the organization referred to in Section 1 (1) a) is obliged to classify the data managed by it in the electronic information system according to confidentiality, integrity and availability, as set out in a government decree.

(2) [19] The organization referred to in Section 1(1)(b) and (c) and point f) of paragraph 1 of this Article, with regard to its electronic information systems for national defense purposes, is required to perform data classification when using a non-private cloud service and implementing foreign data processing, in order to assess the risks of data processing using a foreign or non-private cloud service.

(3) During data classification, the collective security needs of electronic data logically managed together as a unit – including databases, data warehouses, individual documents and other data files – must be taken into account.

(4) [20] With regard to Section 1(1)(a)–(c) and its electronic information systems for national defense purposes, the organization referred to in point f) may use non-private cloud services or process data abroad solely on the basis of data classification and taking into account its results, unless other legislation prohibits or restricts the use of cloud services or foreign data processing.

(5) The organization shall review the data classification within the framework of security classification and in the event that:
if there is a change in the data to be processed in the electronic information system.

6. Security classification

Section 10 (1) In order to ensure the protection of the organization's electronic information systems, the data processed therein, and the services provided in a manner proportionate to the risks, the organization shall classify the electronic information systems under the scope of this Act and at the disposal of the organization into "basic", "significant" or "high" security classes based on the integrity and availability of the electronic information system concerned and the risk of confidentiality, integrity and availability of the data processed by it, with increasingly stringent protection requirements.

(2) The head of the organization shall decide on the security classification and shall be responsible for its compliance with the legislation and risks, and for the completeness and timeliness of the data used. The organization shall record the results of the security classification in the register of electronic information systems or in other internal regulations.

(3) The requirements for security classification and the specific rules applicable to each security class
The Minister responsible for IT shall determine the protection measures in a decree.

(4) The organization shall determine and implement the IT security policy based on the security class of the electronic information system.
the protection measures prescribed in the decree of the responsible minister for the given electronic information system.

(5) [21] An organization referred to in Section 1(1)(a) and point f) of Section 1(1) with regard to its electronic information systems for national defense purposes, and an organization referred to in Section 1(1)(b) of Section 1(1) that is not an organization referred to in Annexes 2 and 3, with regard to its electronic information system, must, upon becoming subject to this Act, comply with at least the security measures prescribed in the decree of the minister responsible for IT for the “basic” security class.

19A Section 9(2) is the text amended by Section 71(7) of Act XXXII of 2025 .
20A Section 9(4) is a text amended by Section 71(8) of Act XXXII of 2025 .
21A Section 10(5) Section 71(9) of Act XXXII of 2025 Text amended accordingly.

(6) If, in relation to the electronic information system referred to in paragraph (5), a security class higher than “basic” has been determined based on the security classification, the organization has a maximum of two years after the security classification to implement the security measures assigned to the security class in order to achieve the required level of protection.

(7) The security classification shall be reviewed at least every two years, or as required by law concerning the security of the electronic system. In the event of a specific change, it must be reviewed urgently and in a documented manner.

7. Person responsible for the security of the electronic information system

Section 11 (1) The head of the organization shall designate a person responsible for the security of the electronic information system within the organization or enter into an agreement with a person outside the organization in order to perform tasks related to the protection of the electronic information system, operate the risk management framework, report cybersecurity incidents and maintain contact with the cybersecurity incident management center.

(2) [22] In the case of organisations referred to in Section 1(1)(a)–(c) and (f), the mandatory content elements of the agreement referred to in Section (1) shall be contained in a government decree. Even in the event of an agreement being concluded, the natural person who will perform the duties of the person responsible for the security of the electronic information system must be designated.

(3) The duties of the person responsible for the security of the electronic information system may only be performed by a person who is a) capable of acting, has no criminal record and

b) [23] an organization referred to in Section 1(1)(a)–(c) and (f), an organization designated as a critical organization pursuant to the Act on the Protection of Human Rights and Fundamental Freedoms, and an organization designated as a critical organization pursuant to the Act on the Protection of Human Rights and Fundamental Freedoms. In the case of an organization designated as an organization significant for the protection and security of the country, it has the qualifications required for the performance of its duties as prescribed in the decree of the minister responsible for IT, and has

ba) with a professional qualification published by the national coordination centre referred to in Section 75 (1) – as set out in the decree of the minister responsible for IT – or with an accredited international qualification (hereinafter collectively referred to as: professional qualification), or bb) with professional experience acquired in a field specified in the decree of the minister responsible for IT.

(4) A person performing the economic management duties of the organization or a person performing a job related to IT operation or IT development within the organization, or a person who is directly subordinate to such a person, may not be designated or entrusted as a person responsible for the security of an electronic information system, with the exception of paragraph (5).

(5) Paragraph (4) shall not apply to the following organisations: a) important organisations as defined in Section 1(1)(a)–(c), b) organisations as defined in Section 1(1)(d) and (e).

(6) The head of the organization shall ensure that the person responsible for the security of the electronic information system a) participates in the preparation of all decisions affecting the protection of electronic information systems; b) has the conditions, authorizations, information, human and material resources necessary to ensure the protection of the electronic information system;

c) have access to all systems, data and information that are necessary for the performance of the tasks to be performed by him/her necessary and, if

d) assigned within the organization, to participate in the further training specified in the decree of the minister responsible for IT, necessary to maintain their professional knowledge.

(7) The person responsible for the security of the electronic information system shall be bound by a duty of confidentiality with regard to data and information that he or she has come to know in connection with the performance of his or her duties. The head of the organization may grant exemption from the duty of confidentiality.

(8) [25] The person responsible for the security of the electronic information system participates in the Minister responsible for IT. in the further training specified in the decree.

(9) The person responsible for the security of the electronic information system is entitled to request information from those involved in the performance of the organization's electronic information security obligations and tasks regarding the fulfillment of security requirements. In this context, he is entitled to learn about the data related to the activities of the contributors necessary to support compliance with the requirements, as well as all documents generated regarding the security of electronic information systems.

22A Section 11(2) Section 71(10) of Act XXXII of 2025 Text amended accordingly.
23A Section 11(3)(b) in conjunction with Section 58(1) of Act XXXII of 2025 established text.
24A Section 11(6)(d) in conjunction with Section 58(3) of Act XXXII of 2025 established text.
25A Section 11(8) in conjunction with Section 58(4) of Act XXXII of 2025 established text.

(10) In justified cases, the organization may appoint or entrust a person authorized to replace the person responsible for the security of the electronic information system, who shall perform the duties of the person responsible for the security of the electronic information system in the event of the person responsible for the security of the electronic information system being permanently absent or prevented from performing the duties of the person responsible for the security of the electronic information system. The head of the organization shall decide on the division of duties and responsibilities between the person responsible for the security of the electronic information system and his/her deputy. The provisions concerning the person responsible for the security of the electronic information system shall apply to the deputy.

(11) If justified by the number, size or security needs of the organization's electronic information systems, an electronic information security organizational unit may be established within the organization, led by a person responsible for the security of the electronic information system.

(12) [26] An organization referred to in Section 1(1)(a)–(c) and (f), an organization designated as a critical organization pursuant to the Act on the Protection of Human Rights and Fundamental Freedoms, and an organization designated as a critical organization pursuant to the Act on the Protection of Human Rights and Fundamental Freedoms. In the case of an organization designated as significant for the protection and security of the country, detailed rules regarding the duties and powers of the person responsible for the security of the electronic information system shall be determined by government decree.

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

(14) The purpose of the register of persons responsible for the security of the electronic information system is to enable organizations to select a person responsible for the security of the electronic information system who is suitable for performing the task from among the persons included in the register.

(15) Entry into and deletion from the register of persons responsible for the security of the electronic information system
Its procedure is determined by government decree.

(16) [27] The national cybersecurity authority may examine whether the person responsible for the security of the electronic information system meets the requirement of no criminal record set out in point (a) of paragraph (3). In order to establish this, it may request data from the criminal record system.

8. Education and training related to the security of electronic information systems

Section 12 (1) A higher education institution providing training related to cybersecurity shall, in connection with the provision of training activities: in context
[28]

a) b) may contribute to the complex resilience of information security, cyber defense, and critical organizations
on skills exercises.

(2) The organization conducting cybersecurity training shall be a)

managed by the managers of essential and important organizations, persons responsible for the security of the electronic information system training for employees of organizational units,

b) may organize further training for the managers of essential and important organizations, persons responsible for the security of electronic information systems, and employees of organizational units managed by persons responsible for the security of electronic information systems.

9. Development and further development of the electronic information system

Section 13 (1) The provisions of this subtitle shall apply to the following organizations that qualify as essential organizations in relation to the development of new electronic information systems or the further development of existing electronic information systems (hereinafter collectively referred to as: development):

a) an organization referred to in Section 1(1)(a) and (c), and b)
[29] an organization that qualifies as an organization under Section 1(1)(b) and also under Annexes 2 and 3.

(2) In the case of the development of an electronic information system, the organization shall act in accordance with the provisions of the government decree in order to ensure the fulfillment of information security requirements and to obtain approval of the operation of the electronic information system by the national cybersecurity authority.

26A Section 11(12) is a text amended by Section 71(11) of Act XXXII of 2025 .
27A Section 11(16) in conjunction with Section 58(5) of Act XXXII of 2025 established text.
28A Section 12(1)(a) is replaced by Section 72(a) of Act XXXII of 2025 repealed.
29A Section 13(1)(b) of Act XXXII of 2025, Section 59. Text established by §.

(3) During the development, the classification of the data planned to be managed in the system and the security classification of the electronic information system shall be carried out in the design life cycle of the electronic information system – where the data classification obligation is prescribed by this Act – and shall be submitted to the national cybersecurity authority for approval in the manner specified in the government decree.

a) in the case of internal development, prior to the allocation of resources, b)
in the case of external development, prior to the conclusion of the contract for this purpose – taking into account the legal provisions on public procurement – in such a way that the information security requirements are recorded in the contract for the development of the electronic information system.

(4) The organization shall record in the development contract the requirements related to the classification approved by the national cybersecurity authority and shall take measures towards the organization performing the development to ensure their implementation during the development.

(5) The development shall be carried out by a team of IT specialists approved by the national cybersecurity authority, with regard to the security department. must be implemented in accordance with the protection requirements specified in the regulation of the responsible minister.

(6) If, during the development, the organization becomes aware of a circumstance that affects the electronic information system concerned system security, then the tasks specified in paragraphs (2)–(4) must be performed repeatedly.

(7) The national cybersecurity authority may order a vulnerability assessment during the procedure. (8)
Introduction of a new electronic information system or further development of an existing electronic information system
The requirements for the established safety class must be met until the system is put into use.

(9) The decision of the head of the organization to put into use and continue to use the electronic information system pursuant to Section 6(3)(12) may be made if the requirements resulting from the security classification approved by the national cybersecurity authority have been met in accordance with Subsection (8).

(10) At the same time as the decision pursuant to Section 6(3)(12), the electronic information system shall be on the notification of data specified in a government decree to the national cybersecurity authority.

(11) In the case of the development of a central system – in addition to the provisions of paragraphs (1) to (10) – the organization with the authority to dispose of the electronic information system is obliged to inform the national cybersecurity authority on issues affecting the security of the central system for the first time during the planning phase and thereafter upon reaching each milestone.

Section 13/A[30] The provisions of this subtitle shall also apply to the development of electronic information systems for national defense purposes of the organization referred to in Section 1(1)(f).

Section 14 (1)[31] If the development of the electronic information system is
carried out by a) a fundamental organisation as defined in Section 1(1)(b) which is not an organisation as defined in Annex 2 or 3 or b) an important organisation as defined in Section 1(1)(a) and (c),
The provisions of this section shall prevail instead of those of Section 13.

(2) The organization referred to in paragraph (1) shall take measures towards the organization carrying out the development to ensure that the protection requirements are met.

(3) The organization referred to in paragraph (1) shall notify the cybersecurity authority a) of the electronic information system during the design life cycle, prior to the commencement of development, and b) following the decision of the head of the organization to put the electronic information system into use or continue to use it, pursuant to point 12 of paragraph (3) of Section 6.

(4) In justified cases, the cybersecurity authority may order a vulnerability assessment.

(5) The requirements of the security class must be met until the system is put into use, and the decision of the head of the organization to put into use and continue to use the electronic information system, pursuant to Section 6, Subsection (3), Point 12, may be made only if these requirements are met.

Section 15 (1) If the vulnerability assessment of the electronic information system of the organization referred to in Section 1(1)(a)–(c) is mandatory by law or by decision of the national cybersecurity authority, the decision referred to in Section 6(3)(12) shall be subject to the approval by the national cybersecurity authority of the vulnerability management plan prepared in relation to the identified vulnerabilities.

(2) In the case of an electronic information system classified as “significant” or “high” in the security class referred to in paragraph (1), it is mandatory to initiate a full vulnerability assessment in accordance with the government decree. The organization may be exempted from the obligation to conduct a vulnerability assessment based on the decision of a state body authorized to conduct vulnerability assessments specified in a government decree.

30A 13/A. §-ta Act XXXII of 2025. 60. § was introduced.
31A Section 14(1) is replaced by Section 61 of Act XXXII of 2025. Text established by §.

(3) The detailed guidelines governing the development of the electronic information systems of the organization referred to in Section 1(1)(a)–(c) shall be as follows: The rules are contained in a government decree.

10. Cybersecurity audit

Section 16 (1) An organization referred to in Section 1(1)(b) which is also an organization referred to in Annexes 2 and 3, as well as an organization referred to in Section 1(1)(d) and – with the exception of microenterprises pursuant to the Act on Small and Medium-sized Enterprises and the Support of Their Development – an organization referred to in Section 1(1)(e) shall be required to have a cybersecurity audit conducted every two years or upon order of the competent cybersecurity authority pursuant to Section 23(1) in order to demonstrate compliance with the cybersecurity requirements pursuant to this Act.

(2) The organization is

obliged to a) conduct a cybersecurity audit within 120 days of its registration pursuant to Section 21(3);
to enter into an agreement with a registered auditor, and

b) have the cybersecurity audit carried out for the first time within two years of registration.

(3) Cybersecurity audits may not be conducted for electronic information systems for national defense purposes.

(4) If the organization referred to in paragraph (1) also has the authority to dispose of an electronic information system for national defense purposes has, the head of the organization is responsible for compliance with the provisions of paragraph (3).

(5) [32] The National Defense Cybersecurity Authority shall inform the SZTFH about the registration as an electronic information system for national defense purposes in the case of business entities conducting activities related to national defense interests and organizations and national defense infrastructures that are not subject to double designation and are significant for the defense and security of the country, in accordance with the law.

11. Special provisions for support systems

Section 17 (1) The organisation shall ensure that the supporting system is also protected at a level appropriate to the electronic information system it supports, in accordance with the provisions of the decree of the Minister responsible for IT, if the given protection measures can be applied in a risk-proportionate manner to the relevant supporting system. The organisation shall assess the protection measures used in the supporting system.

(2) If the organization provides the support system as a service, it shall inform the organization using the support system that:
the requirements of which safety class the supporting system meets.

(3) Only a support system that is compatible with the electronic information system it supports may be used.
protection needs.

12. Special provisions for central systems

Section 18 (1) The organization exercising the right to dispose of the central system shall, in relation to the central system provided by it to the user organization, a) perform the

tasks specified in Subheading 4; b) notify the

national cybersecurity authority to which organization the central system at its disposal is provided; c) specify as a contractual requirement or, in the

absence of a contract, make available on its website to the user organization the electronic information security requirements to be complied with by the user organization as a condition for using the central system in order to protect the central system;

d) may monitor the implementation of the tasks specified in point c); e)

shall call on the user organization to remedy the deficiencies and correct the errors identified during the inspection pursuant to point d), setting a deadline; in the event of this being unsuccessful, it shall inform the national cybersecurity authority in order to take further measures; f) shall

cooperate with the user organization, within the framework of

which fa) it shall notify the user organization of pre-planned events affecting the central system at least five days before the event, fb) shall

inform it of cybersecurity incidents affecting the central system as a matter of urgency, fc)

shall inform the user organization of any cyber threat, near-incident cybersecurity situation or cybersecurity situation affecting the electronic informat
in the event of an incident, informs about possible preventive, recovery or other measures,

fd) if the vulnerability assessment carried out with regard to the electronic information system of the user organisation is not carried out by the central
reveals errors and deficiencies affecting the system and takes measures to correct

them, 32A Section 16 (5) Act XXXII of 2025 Section 71, point 12 Text amended accordingly.

g) reports cyber threats affecting the central system to the competent cybersecurity incident management center, cybersecurity incident-prone situations, and

h) take the measures prescribed by the competent cybersecurity incident management center in order to prevent, respond to, and manage cyber threats, near-misses, and cybersecurity incidents affecting the central system, and to reduce the consequences, and if the service it uses is affected, take action towards the service provider to take the necessary measures.

(2) With regard to the central system used by the user organisation, the user organisation shall: a) report the

use of the central system when reporting its electronic information systems to the national cybersecurity authority, including data suitable for identifying the central system and the organisation exercising the right of disposal over the central system; b) comply with the electronic information security requirements specified by

the organisation exercising the right of disposal over the central system.
meets the requirements, records these in its information security policy and

c) reports cybersecurity incidents affecting the central system to the competent cybersecurity incident management center and the organization exercising control over the central system.

(3)[33] In the case of an organization exercising the right to dispose of a central system that is used mandatorily under a law, the division of tasks and responsibilities between the central system service provider and the user organization is set out in the law applicable to the given central system. In the absence of this, and in the case of a central system that is used voluntarily, the organization exercising the right to dispose of the central system and the user organization conclude a service contract.

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

(5) The national cybersecurity authority is entitled to request information regarding the central system from both the central system service provider and to verify compliance with electronic information security requirements at both the user organization and the user organization.

13. Special provisions for systems provided by central service providers

Section 19 (1) The central service provider shall inform the user organisation of the security class requirements of the service it provides, or of the security class requirements of the systems implementing the central services. If the security class of the electronic information system affected by the service provided by the central service provider is met by the protection measures provided by the central service provider, the user organisation shall use the service. Otherwise, the user organisation shall not use the service, or in the case of mandatory use, the user organisation shall ensure the application of risk-proportionate alternative measures that are feasible within the scope of the user organisation.

(2) The central service

provider shall a) maintain continuous contact with the national cybersecurity authority,

b) notify the national cybersecurity authority of which organization provides the central service or support system.
provides for,

c) ensures the implementation of risk-proportionate protection measures for the central service or support system, d) defines and

makes available to the user organization the electronic information security requirements to be complied with by the user organization as a condition of use in order to protect the central service or support system, e) cooperates with the user organization, within the framework of

which ea) notifies about pre-planned events affecting the central

service or support system at least five days before the event, eb) informs without delay about cybersecurity incidents affecting the central

service or support system, ec) informs about possible preventive, recovery or other measures in the event of a cyber

threat, a near-cyber security incident or a cybersecurity incident, ed) if a vulnerability assessment carried out in relation to the electronic information system of the user organization is carried out by the central

reveals errors or deficiencies affecting the service or the support system and takes measures to correct them,

f) reports to the competent cybersecurity incident management center any incident affecting the central service or the supporting system cyber threats, cybersecurity near-incident situations, cybersecurity incidents, and

g) take the measures prescribed by the competent cybersecurity incident management center in order to prevent, respond to, and manage cyber threats, near-misses, and cybersecurity incidents affecting the central service or the supporting system, and to reduce the consequences, and if the service it uses is affected, take action towards the service provider to take the necessary measures.

33A Section 18(3) Section 71(13) of Act XXXII of 2025 Text amended accordingly.

(3) The central service or support system provided by the central service provider to the user organization
regarding the user organization

a) notifies the national cybersecurity authority of the use of the central service or the supporting system in the central
by designating the service

provider, b) meets the electronic information security requirements specified by the central service provider, records these in its information security policy, and c) reports cybersecurity incidents

affecting the central service or the supporting system to the cybersecurity
for the incident management center and the central service provider.

(4) In the case of a central service or support system that is used mandatorily under a law, the division of tasks and responsibilities between the central service provider and the user organization shall be determined by the law applicable to the given central service or support system. In the absence of such a law, and in the case of a central service or support system that is used voluntarily, the central service provider and the user organization shall conclude a direct financing contract.

(5) The detailed rules relating to the IT and electronic communications service tasks provided by the central service provider to organizations performing state and local government tasks with exclusive rights pursuant to law shall be determined by government decree.

(6) The national cybersecurity authority shall be responsible for the central services and support systems provided by the central service provider. keeps records.

(7) The national cybersecurity authority is entitled to ensure compliance with electronic information security requirements both in the central Check with both the service provider and the user organization.

14. Top-level domain name registry

Section 20 (1) The central top-level domain name registry shall be responsible for the domain names registered under the top-level domain. keeps records.

(2) The central domain name registry shall contain: a) the

domain name concerned, b)

the date of domain name registration, c)

the name of the domain name user, his/her e-mail address and telephone number where he/she can be contacted,

and d) the name, e-mail address and telephone number of the administrative contact person managing the domain name, if they differ from c)
from the data according to point.

(3) The purpose of the processing of data pursuant to paragraph (2) is to keep the identification and contact details of the administrative contact person managing the domain name and the natural or legal person using the domain name up to date.

(4) In order to verify the authenticity and ensure the integrity of the data in the central domain name registry, the top-level domain name registrar is obliged to publicly publish the procedure for verification, previously approved by the SZTFH.

(5) The top-level domain name registry shall make the data contained in the central domain name registry, with the exception of personal data, publicly accessible.

(6) The top-level domain name registry shall provide direct access to the data included in the central domain name registry to the prosecutor's office, the national security services, the investigative authorities and the organizations conducting preparatory proceedings under the Criminal Procedure Act, the cybersecurity authority and the cybersecurity incident management center.

Chapter III

CYBERSECURITY OVERSIGHT

15. Provisions on cybersecurity audit

Section 21 (1) The auditor shall verify the security classification of electronic information systems and the adequacy of the protection measures according to the security classification during the implementation of the cybersecurity audit.

(2) A cybersecurity audit may be conducted by an auditor who has the expertise and infrastructure conditions necessary to perform the task and who qualifies as an economic entity pursuant to Section 57(1)(c) (hereinafter referred to as: an economic entity authorized to conduct vulnerability assessments). The requirements imposed on the auditor shall be determined by decree of the President of the SZTFH.

(3) The SZTFH shall register economic entities authorized to perform the audit, subject to verified compliance with the requirements set out in paragraph (2), in accordance with the detailed rules set out in the decree of the SZTFH President.

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

a) the auditor's data and the personal identification data necessary to identify his designated contact person,
your telephone number and email address,

b) the auditor's identification number – received upon registration –, c) the

data of the collaborators used by the auditor, and the natural person necessary to identify the designated contact person
your personal identification data, telephone number, e-mail address, and

d) a document containing the results of the audit.

(5) Contrary to the Act on the General Rules for Commencing and Continuing Service Activities, if the SZTFH has not decided on the inclusion in the register pursuant to paragraph (3) within the administrative deadline applicable to it, the applicant shall not be entitled to commence or continue the activity specified in his application, and the general rules of the Act on General Administrative Procedure concerning the failure of the authority shall apply.

(6) If the auditor no longer performs auditing activities, the data referred to in paragraph (4) shall be transferred to the SZTFH of the activity. must be deleted from the register five years after the notification of its completion.

(7) If the auditor reports a change in the data referred to in paragraph (4), prior to the entry of the change in the register:
The SZTFH will delete the data from the register five years after the registration of the change in the data.

(8) The purpose of processing the data pursuant to paragraph (4) is to keep information on auditors up to date and to carry out the audit activities of the SZTFH.

(9) Data from the register referred to in paragraph (4) may be transferred exclusively to cybersecurity authorities and cybersecurity incident management centers, unless otherwise provided by law.

Section 22 (1) To verify compliance pursuant to Section 21 (1), the auditor is entitled to monitor the activity
carry out the following tests in an appropriate manner:

a) internal IT security and remote vulnerability assessment, and in the case of a “significant” or “high” security class
penetration testing, b)

cryptographic compliance testing, and c) in the case of

a “significant” or “high” security class, custom-developed software performing critical security functions
security source code review.

(2) The auditor shall send the results of the audit to the SZTFH and the organization immediately after the completion of the audit.

(3) The auditor shall immediately inform the SZTFH in writing if he establishes a fact related to the electronic information system of the organization that a) seriously endangers the

continuous operation of the organization, or b) leads to the commission

of a crime, violation of the law, serious violation of the organization's internal regulations or their
detects circumstances indicating danger.

(4) The results of the audit and the information referred to in paragraph (3) shall be sent by

the SZTFH a) ex officio in the case of the organization referred to in Section 1(1)(b), b) in

the case of the organization referred to in Section 1(1)(d) and (e), at the request of the national cybersecurity authority.

(5) The auditor shall handle the documents received from the audited organization, including personal data and data considered as business secrets, in the management of the audited organization, necessary for conducting the audit, for the purpose of examining the fulfillment of the requirements verified during the audit, to the extent necessary for conducting the audit, until its completion, and may not forward them to a third party.

(6) The auditor shall specify in the regulations the positions held by the persons who may have access to trade secrets and their contents during the audit. The persons participating in the audit shall be bound by a confidentiality obligation with regard to personal data and trade secrets that they have come to know during the audit, which shall remain in force for 5 years after the termination of the employment relationship, and without time limit with regard to personal data.

(7) The cybersecurity audit under this subtitle does not affect the certification obligation prescribed by other legislation.

(8) The SZTFH shall monitor the auditor's compliance with his obligations by applying Section 25, Subsections (1) and (3).

(9) The President of the SZTFH shall determine in a decree the maximum audit fee, calculated without VAT,
and the procedure for conducting a cybersecurity audit.

16. General provisions concerning the cybersecurity authority

Section 23 (1) The cybersecurity supervision of electronic information systems falling within the scope of this Act – for national defense purposes except electronic information systems –

a) in the case of electronic information systems of organizations referred to in Section 1(1)(a)–(c), in the Government Decree designated national cybersecurity authority,

b) electronic information systems of organizations not covered by point a) of Section 1(1)(d) and (e) In the case of its systems, it is provided by the SZTFH.

(2) In the case of electronic information systems for national defense purposes, the national defense cybersecurity authority performing cybersecurity supervision pursuant to this Act shall be designated by the Government in a decree within the national defense sector. The provisions applicable to the national cybersecurity authority shall apply to the activities of the national defense cybersecurity authority.

(3) The national cybersecurity authority is a body with independent tasks and official powers, which is subject exclusively to the law during its official activities, is independent of all other bodies and cannot be instructed regarding official matters within its scope of responsibility – except for instructions to perform a task or to remedy an omission.

17. Duties of the cybersecurity authority

Section 24 (1) The national cybersecurity authority shall: 1. examine the person responsible for the security of the electronic information system and his/her deputy as provided for in the law. compliance with the requirements, and in case of compliance, it records it,

2. examines the validity of the security classification and decides on its registration based on the results of the examination, 3. registers and keeps records of the data referred to in Section 28 (1), 4. determines the guidelines, recommendations and requirements relating to the security of electronic information systems, 5. may issue guidelines in accordance with the provisions of European Union law and the decree of the Minister responsible for IT. regarding the compatibility of protection measures with each other,

6. may require the application of European and international standards and technical specifications relevant to the security of electronic information systems in order to demonstrate compliance with electronic information security requirements – without requiring or preferring the use of a particular type of technology,

7. checks the classification of electronic information systems, as defined by law or by the fulfillment of requirements,

8. orders the elimination of security deficiencies discovered or brought to its attention during its inspection, and the measures necessary to eliminate them, and monitors their effectiveness, 9. may take and monitor all measures relating to the protection of electronic information systems, with which the threats to the affected electronic information system can be managed,

10. in the event of a cybersecurity incident – in cases specified in a government decree – initiates an official procedure and immediately informs the national cybersecurity incident management center about the reports of cybersecurity incidents received, 11. may participate in information security and cybersecurity-related exercises, and represents Hungary upon request in international information security and cybersecurity exercises,

12. represents Hungary at domestic and international information security and cybersecurity events, 13. may participate in the expert assessment pursuant to Article 19 of Directive (EU) 2022/2555 of the European Parliament and of the Council, and may initiate an assessment,

14. monitors the domestic implementation of Directive (EU) 2022/2555 of the European Parliament and of the Council, 15. participates in awareness-raising activities serving the protection of Hungarian cyberspace, 16. checks that information security requirements are met during the development of electronic information systems, 17. approves the use of electronic information systems in accordance with government decree, may prohibit or restrict the use of the electronic information system, data processing abroad and the use of cloud services until the identified deficiencies are remedied,

18. may identify an organization as a fundamental or important organization as specified in a government decree, 19. may make a proposal to the designating authority under the Act on Critical Organizations and the Act on Critical Organizations to designate an organization as a critical organization. for the appointing authority according to to designate an organization that is significant for the defense and security of the country,

20. may organize domestic information security and cybersecurity exercises and may order the organization's participation in the exercise, and may issue guidelines regarding the exercises organized by the organization,

21. acts as a specialist authority in accordance with the provisions of the Act on the designation of specialist authorities acting on certain compelling reasons based on public interest. in technical matters specified in government decree,

22. in European Union and international organizations and committees responsible for the security of electronic information systems represents Hungary and

23. performs the functions of the single point of contact pursuant to Directive (EU) 2022/2555 of the European Parliament and of the Council.

(2) The national cybersecurity authority shall, within the scope of its control tasks, comply with the provisions of the Act on Cybersecurity and the Act on Cybersecurity. prepares an annual audit plan based on a risk analysis, after prior consultation with the designating authority.

(3) The national defence cybersecurity authority shall perform the tasks set out in points 1–11, 15–21 of paragraph (1), and the provisions of paragraph (13) of Section 11 and paragraphs (4) and (7) of Section 28 shall not apply to its activities. The national defence cybersecurity authority shall inform the national defence cybersecurity incident management centre in the case of point 10 of paragraph (1).

(4) The tasks and powers of the national cybersecurity authority and the national defense cybersecurity authority, as well as the detailed rules governing their procedures, shall be contained in a government decree.

(5) The SZTFH

a) shall act in accordance with the provisions of paragraphs 4, 5, 7, 8 and 11–15 of paragraph (1), as well as paragraphs (3) and (4), and the decree of the President of the SZTFH,

b) may order and control all measures relating to the protection of electronic information systems, with which the threats to the electronic information system concerned can be managed, c) records the data referred to in Section 29(1), d)

[34] in the event of a significant cybersecurity incident or suspicion of non-compliance with security requirements, it may carry out an extraordinary inspection or order an extraordinary audit, e) by specifying the purpose, it is entitled to request from the organization and become familiar with: ea) documents supporting the security classification and the adequacy of security measures, eb) a document on the implementation of the internal IT security audit, and ec) other data, information and documents supporting legal compliance for the purpose of performing supervisory tasks.

(6) The detailed rules for conducting the official inspection of the SZTFH are determined by the decree of the President of the SZTFH.

(7) The cybersecurity authority is entitled to take supervisory measures or apply legal consequences a) in relation to organisations that provide services in the territory of Hungary or whose network and information systems are located in the territory of Hungary and for this purpose a request for mutual assistance is received from the cybersecurity authority of a European Union Member State, and

b) organizations that do not have a designated representative in any of the European Union Member States but provide services in Hungary regarding.

(8) In order to perform its tasks specified in law, the cybersecurity authority is entitled, based on a risk analysis, to: Prioritize the execution of supervisory tasks.

(9) [35] The food chain supervision bodies specified in the Government Decree shall inform the SZTFH by 1 February of each year – for the purpose of performing tasks related to cybersecurity supervision pursuant to Section 23 (1) b) – of the name, registered office and tax number of the organizations referred to in line 3 of the table in Annex 3.

18. General rules of administrative procedure

Section 25 (1) The use of summary proceedings is excluded during the proceedings of the cybersecurity authority.

(2) The administrative deadline for the official procedure conducted by the national cybersecurity authority for the verification of the implementation of protective measures and for the official procedure for the investigation of cybersecurity incidents is one hundred and twenty days. day.

(3) The administrative deadline for the official inspection conducted by the SZTFH is one hundred and twenty days, and ninety days for procedures related to the official registration of auditors, business organizations authorized to conduct vulnerability assessments, incident investigations, and the inspection of organizations certifying the application of post-quantum encryption, or organizations authorized to provide post-quantum encryption applications.

(4) The procedure pursuant to paragraph (3) may be suspended for the period until the completion of the company audit.

19. Identification procedure

Section 26 (1) The national cybersecurity authority may identify an organization as an essential or important organization (hereinafter referred to as the identification procedure) if it does not fall under Section 1(1) or has not been designated as a critical organization under the Cybersecurity Act or the Cybersecurity Act. is designated as an organization significant for the defense and security of the country and at least one of the conditions specified in Section 1 (6) is met.

34A Section 24(5)(d) is the text amended by Section 71(14) of Act XXXII of 2025 .
35A Section 24(9) is replaced by Section 62 of Act XXXII of 2025. Text established by §.

(2) If the conditions set out in Section 1(6)(6) to (9) are met, the national cybersecurity authority shall:
identifies the organization as an organization.

(3) The national cybersecurity authority shall act in accordance with the provisions of Section 2 during the identification procedure.

Section 27 (1) The national cybersecurity authority shall act ex officio during the identification procedure.

(2) The national cybersecurity authority shall decide in a decision on the inclusion of the organization in the register of essential or important organizations, in the framework of which it shall determine the tasks to be performed by the organization under this Act and inform the organization.

(3) In order to conduct the identification procedure, the national cybersecurity authority is entitled to request data – with the exception of personal data – from a) the
organization, b) the organization exercising authority, supervision or control over the organization and c)
from public registers.

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

20. The official register

Section 28 (1) For the purpose of carrying out its tasks specified in this Act, the national cybersecurity authority shall register and manage 1. in relation to the
organisation: a) the data necessary
for the identification of the organisation, b) the organisation's
contact details, including electronic contact details, and the public IP addresses or IP domains used by the organisation, and, with the exception of organisations listed in Annex 1, the organisation's registered office, site, branch, c) the organisation's classification as a core or important organisation, d) its affiliation to the sector, sub-sector, or type of
organisation listed in Annexes 2 and 3, e) if relevant, the list of the European Union Member
States in which the organisation provides services, f) the name, brief description, security class classification of the
organisation's electronic information systems, the definition of the security class achieved at the time of registration and review, g) data related to the classification of data processed in the electronic information system, the location of their data processing, including
the name of the country or the type of cloud, h) the electronic data relating to cloud services used in connection with the information system, i) the security measures related to the electronic information system and their
status, j) the name or company name, mailing address, telephone number and electronic mail address of the representative of an organization not registered in Hungary operating in the territory of Hungary, k) data suitable for identifying the person
or organization performing the tasks of the person responsible for the security of the electronic information system, as well as the personal identification data, telephone number providing direct contact, electronic
contact, education, professional qualifications and professional experience of the natural person actually performing the task, l) the organization's information security regulations, m) data relating to the further training of the head of the organization and the person responsible for the security of the electronic information system, n) the results of the audit, except for electronic information systems for national
defense purposes, o) information related to official
inspections, p) the results of the vulnerability assessment and the vulnerability management plan for eliminating vulnerabilities;

2. in the case of an organization connected to a central system:
a) the name and unique identification number of the central system used by the user organization, b) the name of the
organization exercising the right of disposal over the central system;

3. in the case of a central system, in addition to the provisions of point
1: a) the unique identification number of the central
system, b) the name of the user organizations; 4. in
the case of a central service provider, in addition to the provisions of point 1:
a) the unique identification number of the electronic information system participating in the service provided by the central service provider, b) data suitable for identifying the supporting system provided by the central service provider,

c) the name of the user organisations;

5. notifications received from the Cybersecurity Incident Management Center regarding cybersecurity incidents, including the data relating to the persons involved;

6. natural persons suitable for performing the duties of the person responsible for the security of the electronic information system personal identification data, contact details, including electronic contact details, and data relating to expertise; 7. additional data not considered personal data as required by government decree.

(2) For the purpose of carrying out its tasks specified in this Act, the National Defence Cybersecurity Authority shall keep records of (1) the data specified in subparagraphs a)–m), o) and p) of paragraph 1, as well as in subparagraphs 2–5 and 7.

(3) The national cybersecurity authority and the national cybersecurity incident management center are responsible for national defense cybersecurity. You can view the data specified in subparagraphs a)–c), j)–k) and p) of paragraph (1) from the authority's register.

(4) The national cybersecurity authority, taking into account the data provided by the SZTFH, shall compile the basic and important organizations list and reviews it every two years.

(5) Data from the register referred to in paragraphs (1) and (2) shall be transmitted – unless otherwise provided by law – exclusively to a) the SZTFH, b) the national cybersecurity incident management center, c) the single point of contact pursuant to Directive (EU) 2022/2555 of the European Parliament and of the Council, d) the National Data Protection and Freedom of Information Authority, e) the designating and registering authority pursuant to the Kszetv., f) the Vbö. the designating and registering authority pursuant to Regulation (EU) 2022/2554 of the European Parliament and of the Council, h) the national defence cybersecurity authority, i) the cyberspace operations forces of the Hungarian Defence Forces, j) the national defence cybersecurity incident management centre and k) the national cybersecurity authority can be done for.

(6) The national cybersecurity authority is a critical organization and an organization significant for the defense and security of the country. The information security policy sent by the Kszetv. and Vbö. to the registration authority.

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

Section 29 (1) The SZTFH – for the purpose of implementing its tasks specified in this Act – shall, by decree of the President of the SZTFH: records and manages, as provided for in the following: a) in relation to the organization referred to in Section 1(1)(b), (d) and (e): aa) the data necessary for the identification of the organization, ab) the registered office, registered office, branch office of the organization, ac) if the organization is not an organization established in the European Union, but offers services within Hungary and appoints a representative established in Hungary, the name or company name, mailing address, telephone number and electronic mail address of the representative, ad) the personal identification data, telephone number and address of the person responsible for the security of the electronic information system your email address, ae) the list of the European Union Member States in which the organisation provides services, af) additional data not considered personal data as prescribed by the decree of the President of the SZTFH; b) the data necessary to identify the organisation authorised to carry out the vulnerability assessment, including the organisation's contact details electronic contact details;

c) the personal identification data and contact details necessary for the identification of the natural person authorised to conduct the vulnerability assessment, including electronic contact details, as well as data relating to the expertise of the natural person authorised to conduct the vulnerability assessment; and

d) the data necessary for the identification of economic entities authorized to handle cybersecurity incidents, the organization contact details, including electronic contact details.

(2) The SZTFH shall compile a list of essential and important organisations and organisations providing domain name registration services falling within the scope of Section 1(1)(d) and (e) and shall review it every two years. After compiling and reviewing the list, the SZTFH shall inform the national cybersecurity authority of the data specified in the government decree.

(3) [36] Data from the register referred to in paragraph (1) may be transferred exclusively to cybersecurity authorities, cybersecurity incident management centers, and organizations referred to in paragraph (9) of Section 24, unless otherwise provided by law.

(4) The SZTFH provides direct access to the national cybersecurity authority and the national cybersecurity
for the incident management center to the organization's registration data managed by the SZTFH.

(5) If an organization included in the register pursuant to paragraph (1) a) announces that it no longer qualifies as an organization pursuant to paragraph (1) b), d) or e) of Section 1, then the SZTFH shall delete the data pursuant to paragraph (1) a) from the register five years after the notification.

21. Legal consequences

Section 30 (1) If the organization fails to meet or comply with the security requirements set out in the legislation and the related procedural rules, fails to remedy security deficiencies, fails to take the measures necessary for compliance, or fails to cease its activities, the cybersecurity authority shall:

a) warns against compliance with the security requirements set out in the legislation and the procedural rules related to them, and calls upon the organisation to eliminate the security deficiencies discovered or brought to its attention during the requirements, inspection or audit, or to take the necessary measures for compliance, and to fulfil reporting and data provision obligations, b) may oblige it to cease the unlawful conduct and to refrain from committing the unlawful conduct again, c) – if the organisation has
the authority to do so – to the body supervising the organisation or to the body established under the National Assets Act

You can contact a property rights practitioner and request their assistance, and

d) authorized by a government decree or – in the case of organizations referred to in Section 1(1)(d) and (e) – by the President of the SZTFH
to assign an information security supervisor at the organization's expense, as specified in the regulation issued by.

(2) If, despite the application of the measures referred to in paragraph (1), the relevant organisation fails to meet or comply with the security requirements set out in the legislation or the related procedural rules, fails to remedy the security deficiencies, fails to take the measures necessary for compliance, or fails to cease its activities, the cybersecurity authority may impose a fine of an amount specified in a government decree, taking into account all the circumstances of the case.

(3) If the head of the organization fails to comply with his/her obligations prescribed by law, the national cybersecurity authority may, after considering all the circumstances of the case, impose a fine in the amount specified in a government decree, and in the event of a repeated violation, it shall impose a fine.

(4) The amount of the fine that may be imposed by the cybersecurity authority, the criteria for determining it, and the amount of the fine
The detailed procedural rules for the payment method are determined by government decree.

(5) The cybersecurity authority
may a) oblige the organization to disclose the fact and circumstances of the violation of the law to a body specified by the cybersecurity authority;
discloses it in a manner that takes into account the rules on data protection and business secrets,

b) may order that users of the services provided by the organization be informed of the potential threat affecting them, as well as of the preventive, protective or remedial measures necessary or possible to eliminate such a threat, and of their expected effects, 37

c) In the event of a cybersecurity incident, it may inform the public on its website or may oblige organizations to provide information in a resolution if this is necessary to prevent a given cybersecurity incident or to manage an ongoing cybersecurity incident and

d) may oblige the organization to inform the cybersecurity authority if it is necessary to take crisis management or emergency management measures.

(6) If the essential organization that is not a public administration body does not comply with the deadline set by the cybersecurity authority
complies with the official obligation, the cybersecurity authority

a) may initiate a complaint with the competent authority regarding the essential services provided by the essential organization affected by the infringement or temporary suspension of a certification or permit for all or part of the activities and

b) may initiate a complaint with the court of registration against the head of the basic organization and the senior officials of the given organization temporary suspension from performing his/her duties.

(7) The legal consequences set out in paragraphs (1), (2), and (5) and (6) may be applied jointly and repeatedly.

36A Section 29(3) is replaced by Section 64 of Act XXXII of 2025. Text established by §.
37A Section 30(5)(c) of Act XXXII of 2025 Section 71(15) Text amended accordingly.

(8) If the organization takes the necessary measures to remedy the deficiencies or complies with the official obligation fulfils the requirements, the cybersecurity authority shall take measures to terminate the temporary measures pursuant to paragraph (6).

(9) The cybersecurity authority shall take into account the aspects of proportionality and gradualness when applying legal consequences. acts taking into account the effectiveness and deterrent effect of the legal consequence.

(10) [38] If the organization referred to in Section 1(1)(a)–(c) and (f) ignores the official obligation or fails to comply with the protective measures recommended by the national cybersecurity authority through its own fault, resulting in a cybersecurity incident or near-incident situation, the national cybersecurity authority may oblige the organization to reimburse the costs incurred in preventing the occurrence of the cybersecurity incident or near-incident situation.

(11) If the organization referred to in Section 1(1)(d) and (e) fails to comply with the cybersecurity requirements set out in the legislation or the does not comply with or does not comply with the related procedural rules, the SZTFH, in addition to the provisions of paragraphs (1) to (5),

a) is entitled to prohibit the person concerned, taking into account the opinion of the authority licensing or supervising the activities of the organisation organization from activities that directly endanger the fulfillment of safety requirements,

b) in the event of a fine being imposed, inform the authority licensing or supervising the organization's activities about the imposition of the fine and the on the facts underlying the imposition.

Section 31 (1) The cybersecurity authority shall appoint the information security supervisor referred to in Section 30 (1) d) for a fixed period of time or until a specific condition is met. The information security supervisor shall supervise the fulfilment of the security requirements set out in the legislation and the compliance with the related procedural rules within the organisation. The cybersecurity authority shall provide professional guidance to the information security supervisor's activities.

(2) Section 1(1) 39 a)

In the case of organizations referred to in points a)–c), the requirements for the person of the information security supervisor, the detailed rules regarding his/her assignment, authorizations and tasks shall be laid down by a government decree, the requirements regarding his/her qualifications, further training obligations and professional experience, as well as the procedure for publishing professional qualifications by the national coordination center pursuant to Section 75 (1) shall be laid down by a decree of the minister responsible for IT,

b) in the case of organizations referred to in points d) and e), the requirements for the information security officer, The detailed rules regarding his/her assignment, powers and duties shall be determined by decree of the President of the SZTFH.

Section 32 (1) If the SZTFH detects or becomes aware – even based on a report from the national cybersecurity authority – that the auditor does not meet or comply with the cybersecurity requirements set out in the legislation or the related procedural rules, the SZTFH is entitled to

a) to warn about the compliance with the requirements set out in the legislation or the related procedural rules, b) to order the elimination of the identified deficiencies or the measures necessary for compliance by setting a deadline the adoption, or

c) temporarily suspend the auditor from auditing activities, informing the national cybersecurity authority.

(2) If, despite the application of the measures referred to in paragraph (1), the auditor fails to comply with or comply with the requirements set out in the legislation or the related procedural rules, fails to remedy the identified deficiencies, fails to take the measures necessary for compliance, or fails to cease the activity, the SZTFH may, after considering all the circumstances of the case, impose a fine as specified in a government decree, which may be repeated in the event of further non-compliance.

(3) If the SZTFH detects a breach of law pursuant to paragraph (1) that affects the entity audited by the auditor, the SZTFH shall immediately notify the person responsible for the security of the electronic information system designated at the entity audited by the auditor and provide information on the circumstances of the possible cybersecurity incident or data leak.

22. Temporary unavailability

Section 33 (1) The cybersecurity authority may order in a resolution the temporary inaccessibility of data published via electronic communications networks that pose a threat to the security of Hungarian cyberspace and in relation to which the national cybersecurity incident management center is conducting cybersecurity incident management.

(2) The national defense cybersecurity authority shall order the temporary inaccessibility of data published via the electronic communications network that violates or endangers national defense interests or poses a threat to the security of an electronic information system for national defense purposes.

38A Section 30(10) is a text amended by Section 71(16) of Act XXXII of 2025 .
39A Section 31(2)(a) is replaced by Section 65 of Act XXXII of 2025. Text established by §.

(3) The temporary inaccessibility of electronic data shall be ordered by the cybersecurity authority in a decision declared immediately enforceable. The cybersecurity authority shall order the temporary inaccessibility of electronic data for a maximum of ninety days, which period may be extended by a further ninety days in justified cases.

(4) The decision ordering the temporary inaccessibility of electronic data shall be published by the cybersecurity authority by means of an announcement. and sends it to the National Media and Communications Authority (hereinafter: NMHH).

(5) The announcement must be published on the website of the cybersecurity authority for 3 days. The announcement is the date of publication of the decision. day following its publication.

(6) The NMHH shall send the decision via the delivery system pursuant to the Act on Electronic Communications to the
for the decision obligor.

(7) The person liable for the decision pursuant to paragraph (3) shall – without its being specified in the decision –
telecommunications service provider.

(8) The implementation of temporary inaccessibility is organized and monitored by the NMHH on the basis of the Act on Electronic Communications.

(9) The obligation to temporarily disable access shall cease upon expiry of the deadline specified in the decision.

(10) The cybersecurity authority shall terminate the temporary inaccessibility before its termination if a) the reason for the order has
ceased to exist, b) based on
information from the court, prosecutor's office or investigative authority acting in the criminal case, or the NMHH, a coercive measure to temporarily inaccessibly make electronic data inaccessible or a measure to permanently inaccessibly make electronic data inaccessible is being ordered or implemented in relation to the electronic data, or

c) the implementation of the provision by electronic communications service providers with the given data content may be questionable.

(11) If the cybersecurity authority has ordered the disabling of electronic data pursuant to paragraph (1) or (2) and, after the decision becomes final, establishes that the unlawful activity carried out by the publication of the electronic data included in the decision is also carried out by the making accessible or publishing of other electronic data with the same content as the determination of the unlawfulness – in particular another IP address, domain or domain subdomain – then, without a repeated official procedure and decision-making – pursuant to paragraph (3), it shall notify the NMHH by sending the data necessary for the disabling electronically, via a secure delivery service (hereinafter: simplified follow-up), which shall communicate this data exclusively electronically to the electronic communications service providers providing access.

Electronic communications service providers are obliged to ensure the disabling of electronic data sent in accordance with the data required for disabling, with a view to simplified follow-up, until the relevant decision made pursuant to paragraph (3) remains enforceable.

Section 34 (1) In order to prevent a significant cyber threat or interrupt an ongoing series of cybersecurity incidents, the head of the national cybersecurity incident management center may order temporary inaccessibility with immediate effect until the decision of the cybersecurity authority or for a maximum period of seventy-two hours.

(2) Temporary inaccessibility with immediate effect shall be implemented within the shortest possible time according to the state of the art.

Section 35 (1) The cybersecurity authority may impose a fine of HUF 1 million to HUF 5 million on an electronic communications service provider that fails to comply with its obligations under this sub-title. The fine may be imposed repeatedly after the deadline for compliance with the obligation has expired without result, with a new deadline being set.

(2) The cybersecurity authority, the NMHH and the electronic communications service provider shall not be liable for any damage resulting from the fact that the electronic data made inaccessible, in addition to the content set out in Section 33(1) and (2), also includes other content for which technical separation is not possible or is not expected during the implementation of the making inaccessible.

23. Temporary removal of electronic data

Section 36 (1) The hosting service provider specified in the Act on Certain Issues of Electronic Commerce Services and Information Society Services, or the intermediary service provider also providing hosting services (hereinafter collectively referred to as the party obliged to remove) that manages the electronic data concerned shall be obliged to temporarily remove the electronic data. The party obliged to remove shall be obliged to temporarily remove the electronic data within one working day following the notification of the decision.

(2) The decision specified in paragraph (1) shall be served on the person entitled to dispose of the electronic data if:
Based on the information provided so far in the proceedings, his identity and contact details are known.

(3) Section 33, paragraphs (1) to (5) and (9) to (11), and Sections 34 and 35 shall apply mutatis mutandis 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 to the activities of the national cybersecurity certification authority (hereinafter referred to as: certification authority) pursuant to Regulation (EU) 2019/881 of the European Parliament and of the Council.

24. Requirements for national cybersecurity certification systems

§ 38. The national cybersecurity certification system must meet the following security objectives: a)
protecting stored, transmitted or otherwise processed data against accidental or unauthorized storage, handling, access and disclosure during the entire life cycle of the ICT product, ICT service and ICT process, b) protecting
stored, transmitted or otherwise processed data against accidental or unauthorized destruction, loss, alteration or inaccessibility during the entire life cycle of the ICT product, ICT service and ICT process, c) ensuring that authorized persons, programs or

machines only access the data that is the subject of their access rights.
access data, services or functions,
d) identification and documentation of known dependencies and vulnerabilities,
e) recording at what time and which data and services to be protected were accessed by the authorized person, program or machine or functions accessed, used or otherwise handled,
f) making it possible to verify at what time and what data the authorized person, program or machine,
accessed, used or otherwise handled services or features,
g) verifying that ICT products, ICT services and ICT processes do not contain known
vulnerabilities,
h) the availability of data, services and functions in the event of a physical or technical security incident,
and restoring access to data, services and functions as soon as possible,
(i) ensuring that ICT products, ICT services and ICT processes are risk-proportionate, by default
and be safe by design,
(j) ensuring that the software and hardware of ICT products, ICT services and ICT processes are up to date, and (k) ensuring that there are no defects in ICT

products, ICT services and ICT processes.
known vulnerabilities, and mechanisms are available to securely update them.

Section 39 (1) The national cybersecurity certification scheme shall include:
a) the subject matter and scope of the certification scheme, the type or categories of ICT products, ICT services and ICT
processes, b) a clear definition of the purpose of the certification scheme and the fact that the selected standards, assessment methods and reliability levels meet the needs of the system's target users,
c) a reference to the international, European or national standards used in the assessment or, where such standards are not available or are not adequate, to the technical specifications meeting the requirements set out in Annex II to Regulation (EU) No 1025/2012 or, where such specifications are not available, to the technical specification or other cybersecurity requirements set out in the European cybersecurity certification scheme, d) the level or levels of assurance, e)
the exclusion or permissive provision for
the self-assessment of conformity, f) the additional requirements applicable to
persons and organisations carrying out the conformity assessment, g) the specific assessment criteria
and methods to be applied, including the types of assessment, h) the conditions for use of markings
or labels, i) the content and format of the
national cybersecurity certificate or declaration of conformity to be issued, and j) the issue, validity period
and maintenance of national cybersecurity certificates issued under the scheme,
the conditions for its extension, renewal, and expansion or narrowing of its scope.
(2) If the national cybersecurity certification system applies to multiple assurance levels, the requirements shall be
they should include a clear distinction between the expectations for different levels of reliability.
(3) The national cybersecurity certification system shall specify a) the
assessment procedures for each requirement or group of requirements,

b) those critical protection functions for which internal IT security or remote vulnerability or penetration testing, cryptographic assessments, security source code analyses, which are also suitable for subsequent monitoring of the activity, must be performed, and c) requirements for documenting the assessment results.

25. Confidence levels of national cybersecurity certification systems

Section 40 (1) National cybersecurity certification schemes for ICT products, ICT services and ICT processes shall be:
They may specify one or more of the following confidence levels: “basic”, “significant” and “high”.

(2) The level of assurance provides assurance that the given ICT products, ICT services or ICT
processes meet the relevant security requirements, security functions and have undergone an assessment at a level that, at a “basic”
the)[40] confidence level, addresses basic, known risks related to cybersecurity incidents and attacks, and at a “significant” confidence level,
b)[41] addresses known cybersecurity risks and limited expertise and
the risk of cybersecurity incidents and cybersecurity attacks carried out by perpetrators with resources,

c) seeks to minimise the risk of cyberattacks carried out by perpetrators with significant expertise and resources using state-of-the-art technology at a “high” confidence level. 42

(3) The level of confidence should be proportionate to the likelihood and impact of cybersecurity incidents in relation to the ICT infrastructure.
the level of risk associated with the intended use of the product, ICT service or ICT process.

(4) The assessment activities to be carried out shall include at least the following: a) in the case of a “basic”
level of assurance, a review of the technical documentation to ensure that the requirements of the given certification system are met;
in terms of, b) in
the case of a “significant” level of confidence,
ba) a review of the technical documentation in terms of meeting the requirements of the given certification system, bb)
a review of the determination of the absence of known vulnerabilities, and bc) testing
to determine whether the ICT product, ICT service or ICT process operates the necessary security functions properly, c) in the case of a “high”
level of confidence, ca) a review of the technical
documentation in terms of meeting the
requirements of the given certification system, cb) a review of the determination of the absence of known vulnerabilities,
cc) testing to determine whether the ICT product, ICT service or ICT process
operates properly,
whether it operates the necessary security functions according to the most advanced technology, and
cd) assessing, through penetration testing, how resistant it is to attacks carried out by well-trained perpetrators;
against attacks.

26. Expectations regarding cybersecurity certificates and declarations of conformity

Section 41 (1) The national cybersecurity certificate and the national declaration of conformity shall specify: a) the national
cybersecurity certification system on the basis of which the certificate or declaration was issued, b) the level of assurance, and c)
the relevant technical specifications,
standards and procedures.

(2) The national cybersecurity certificate and the national declaration of conformity shall include: a) the name and
address of the issuing organization, b)
the date of issue, c) the
name and address of the
manufacturer, d) the client of the conformity
assessment, e) the areas of application, or if the conformity is subject to conditions in the given areas of application, these conditions, f) the
validity period, g) the
identification of the ICT product, ICT service and ICT process that is the subject of the certification, its version number, if any, and h) the
signature of the issuer.

40A Section 40(2)(a) Section 71(17) of Act XXXII of 2025 Text amended accordingly.
41A Section 40(2)(b) is the text amended by Section 71(18) of Act XXXII of 2025 .
42A Section 40(3) Section 71(19) of Act XXXII of 2025 Text amended accordingly.

(3) The manufacturer of a certified ICT product, ICT service or ICT process or the manufacturer of an ICT product, ICT service or ICT process for which a declaration of conformity has been issued shall immediately inform the certification authority of any vulnerability or irregularity affecting the security of the ICT product, ICT service or ICT process.

Section 42 (1) A conformity marking shall be affixed to an ICT product, ICT service or ICT process that has been certified or for which a declaration of conformity has been issued, in the manner and form specified in a decree of the President of the SZTFH or, in the case referred to in Section 45 (1) b), of the Government.

(2) The unauthorised affixing of the conformity marking referred to in paragraph (1) shall be prohibited, as shall the affixing of a marking which resembles the form of the conformity marking or which creates the impression that the ICT product, ICT service or ICT process has been certified or a declaration of conformity has been issued in respect of it, and which may thus mislead third parties.

27. Conformity self-assessment, conformity assessment

Section 43 (1) A self-assessment of conformity may be carried out if the national cybersecurity certification system allows it for low-risk ICT products, ICT services and ICT processes corresponding to the “basic” level of assurance.

(2) The manufacturer shall issue a national declaration of conformity stating that the requirements of the national cybersecurity certification system have been verified. The verification shall include an assessment of the compliance with the requirements of the national cybersecurity certification system in accordance with the methodology specified in the certification system.

(3) The manufacturer carrying out the self-assessment of conformity shall, within 15 days of issuing the declaration of conformity referred to in paragraph (2), send to the certification authority, for registration purposes – also in an electronically searchable form – a copy of the declaration of conformity, the technical documentation, the assessment report prepared on the basis of the assessment method specified in the national cybersecurity certification system, and all other relevant assessment information related to compliance with the designated certification system.

Section 44 (1) Conformity assessment activities carried out by a third party may only be carried out by an organization: a)

which has been accredited by the accreditation body designated in accordance with the Act on National Accreditation, or in the case of foreign accreditation, which has been recognised, taking into account the requirements specified in the relevant national or European cybersecurity certification scheme, and which – with the exception of the

b) [43] European certification scheme – complies with the requirements specified in the regulation of the President of the SZTFH – the Government in respect of the certification authority referred to in Section 45 (1) b) – for each level of assurance, and c) which has been registered by the certification authority. (2)

[44] Detailed rules on self-assessment of conformity, the certification procedure, the conditions for registration under point (c) of paragraph (1) in the case of a European certification system, and the obligations and activities of conformity assessment bodies

a) the President of the SZTFH, with the exception of military research, development, production and trade,

b) the Government, with regard to military research, development, production and trade

determined in a regulation.

(3) Contrary to the Act on the General Rules for Commencing and Continuing Service Activities, if the certifying authority has not decided on the registration referred to in point c) of paragraph (1) within the administrative deadline applicable to it, the applicant shall not be entitled to commence or continue the activity specified in his application, and the general rules of the Act on General Administrative Procedure concerning the failure of the authority shall apply.

28. Cybersecurity Certification Oversight

Section 45 (1) The tasks of the certification

authority shall

be performed by a) the SZTFH, b) in derogation from point a), the cybersecurity certification body related to military research, development, production and trade In terms of official duties, it is performed by the authority designated by the

Government.

(2) With the exception of military research, development, production and trade, national cybersecurity certification systems shall be determined by decree of the President of the SZTFH. With regard to military research, development, production and trade, the certification systems shall be determined by decree of the Government, taking into account the national cybersecurity certification systems.

43A Section 44(1)(b) in conjunction with Section 66(1) of Act XXXII of 2025 established text.
44A Section 44(2) in conjunction with Section 66(2) of Act XXXII of 2025 established text.

Section 46 (1) The certification authority shall, in relation to European cybersecurity certification
schemes: a) monitor the development of European cybersecurity certification schemes and monitor the related
standardization processes, b)
participate in the activities of the European Cybersecurity Certification Group, c)
collect information on sectors and areas of expertise that are not covered by the European Cybersecurity Certification Scheme and for which cybersecurity needs to be improved,
d) provide information and support to interested parties where necessary, e)
provide information pursuant to Article 57(4) of Regulation (EU) 2019/881 of the European Parliament and of the Council.

(2) In relation to the maintenance of national cybersecurity certification systems, the certification authority
shall: a) assess the national cybersecurity certification systems in force at least every three years, taking into account current security risks; b) take
immediate action to review the national cybersecurity certification system after a reason for review arises.
for the purpose of review,
c) in the event of the issuance of a European cybersecurity certification scheme, take immediate action to implement national cybersecurity certification schemes of the same subject in order to review and repeal the certification system.

(3) The SZTFH shall act as the certifying authority for the tasks referred to in points b) and e) of paragraph (1).

Section 47 (1) Summary proceedings are excluded during the proceedings of the certifying authority.

(2) The administrative deadline for the certifying authority is 120 days.

(3) In the case of a European cybersecurity certification scheme, the certification authority shall notify the conformity assessment body accredited by the national accreditation body to the European Commission within 15 days of the decision on official registration becoming final. The applicant organisation shall prove its accredited status by attaching the decision of the national accreditation body.

(4) The certification authority shall conduct an authorisation procedure for the conformity assessment body if, for the ICT product, National or European cybersecurity certification scheme for an ICT service or ICT process
a) imposes additional requirements and on this basis an authorisation procedure becomes necessary, or b) requires a
"high" level of confidence for the cybersecurity certificate to be issued within the framework of the system and the certification authority delegates the task of issuing such a certificate to the conformity assessment body in relation to certain national or European cybersecurity certificates or in general.

(5) In the case referred to in point b) of paragraph (4), the condition for granting the permit is that the conformity assessment body qualifies as an economic entity referred to in point c) of paragraph (1) of Section 57.

(6) The validity of the permit issued in the permit procedure pursuant to paragraph (4) may not exceed the expiry of the accredited status.

(7) In the case of a European cybersecurity certification scheme, the certification authority shall, in the event of conducting the licensing procedure pursuant to paragraph (4), notify the conformity assessment body to the European Commission within 15 days of the decision to grant the license becoming final.

(8) Within the framework of its cybersecurity certification supervision tasks, the certification
authority is entitled to a) request conformity assessment bodies and issuers of declarations of conformity to provide information and data necessary for the performance of official tasks, and
b) to carry out official inspections of conformity assessment bodies and issuers of declarations of conformity.

(9) The certification authority shall take action against an organization that does not comply with the requirements of Section 44, which: carries out conformity assessment activities without authorization.

(10) An administrative service fee shall be paid for the procedures conducted by the certification authority pursuant to Section 45(1)(b). The amount of the administrative service fee and the detailed rules relating to its collection, distribution, management, registration and refund shall be determined by a decree issued by the Minister responsible for national defence for the implementation of this Act.

Section 48 (1) The certification authority shall record
and manage: a) the conformity assessment documents provided by the manufacturer of ICT products, ICT services or ICT processes; declaration data,
b) the technical documentation submitted for the declaration of conformity and the information on the ICT products, ICT services or ICT information on the compliance of processes with the certification system,
c) the data necessary for the identification of the conformity assessment body and its designated contact person, if the conformity assessment body is also a public body within the meaning of Article 56(5) of Regulation (EU) 2019/881 of the European Parliament and of the Council, the documents supporting this fact and the fulfilment of the requirements specified in the regulation of the President of the SZTFH,

d) in the decision on the accredited status of a conformity assessment body accredited by the national accreditation body reserved, as well as information regarding changes in accredited status,

e) if the licensing procedure pursuant to Section 47(4) is necessary, the related application, data and documents,

f) the suspension, partial or full revocation of a permit issued during the permit procedure relevant data, as well as the fact that the permit has expired,

g) if the certification authority grants the right to issue a “high” level of confidence cybersecurity certificate to a conformity assessment body the data necessary for identifying the delegated authority, h) the identification number given by the European Commission upon registration of the conformity assessment body, i) the data necessary for identifying the intermediary used by the conformity assessment body and its designated contact person, j) the data of the certificate issued by the conformity assessment body, k) the data necessary for identifying the manufacturer and its designated contact person, l) the information related to the refusal to issue, restriction of the scope, suspension and withdrawal of certificates information,

m) information related to the vulnerability or anomaly referred to in Section 41(3), n) data and documents that have come to its attention during the performance of its supervisory activities, and o) data and documents related to the complaints submitted.

(2) The register referred to in paragraph (1) shall be deemed to be a public register with regard to the data referred to in points f) and g) of paragraph (1).

(3) The purpose of the processing of data pursuant to paragraph (1) is to keep information related to the security of an ICT product, ICT service or ICT process up to date, as well as to perform tasks related to vulnerabilities or anomalies affecting them, and to perform the control and supervisory authority activities of the certification authority.

(4) With regard to any data included in the register referred to in paragraph (1), unless otherwise provided by law, the Data may be transferred to the following organizations:

a) compiling and updating the list of notified conformity assessment bodies for the European Commission, b) notifying the conformity assessment bodies for the accreditation body designated in accordance with the National Accreditation Act performing tasks related to the accreditation and supervision of its activities, and

c) to cybersecurity incident response centers under Section 63 with a vulnerability under Section 41(3) or in order to carry out activities related to the disorder.

(5) The conformity assessment body and the manufacturer shall send the data referred to in paragraph (1) to the certification authority for registration within 8 days of the data becoming available and any changes to the data occurring.

Section 49 (1) If the certification authority becomes aware of or establishes during its inspection that the conformity assessment body or the manufacturer does not meet or does not comply with the safety requirements and related procedural rules set out in the relevant European Union or Hungarian legislation, it shall – by setting a deadline in its decision containing the warning – call on the conformity assessment body or the manufacturer to meet the safety requirements and related procedural rules set out in the relevant European Union and Hungarian legislation.

(2) If, despite the provisions of paragraph (1), the conformity assessment body or the manufacturer fails to comply with or observe the safety requirements set out in the law and the related procedural rules, the certification authority may impose a fine, in the amount specified in the government decree, after considering all the circumstances of the case, which may be repeated in the event of further non-compliance.

(3) The certification authority may impose an administrative fine on a person carrying out an unauthorized conformity assessment activity in the amount specified in the Government Decree. When determining the amount of the fine, the Authority shall consider the aspects set out in the Act on Sanctions for Administrative Violations. The administrative sanction of a warning shall not be applied.

Section 50 (1) The certifying authority shall handle classified data, personal data or sensitive data acquired in the course of its tasks, as well as other data that are considered business secrets, bank secrets, payment secrets, insurance secrets, securities secrets, treasury secrets, medical secrets and other secrets related to the practice of a profession and protected by law, exclusively for the duration of the task, taking into account the principle of purpose limitation. The certification authority shall record the data supporting the findings made as a result of the official inspection and shall process the data recorded in this way until the last day of the 10th year following the cessation of the accredited status of the conformity assessment body or until the last day of the 10th year following the cessation of the validity of the declaration of conformity issued by the manufacturer, provided that if a certificate and a self-assessment of conformity issued by a conformity assessment body are available for the ICT product, ICT service or ICT process affected by the inspection, the later date of the cessation of the accredited status or the expiry of the validity of the declaration of conformity shall be taken into account. The certification authority shall then delete the data from its electronic information systems and data carriers.

(2) Data generated during the procedure of the certifying authority shall not be made public, unless otherwise provided by law.

(3) The employees of the certification authority are bound by a confidentiality obligation with regard to the data obtained pursuant to paragraph (1) – with the exceptions specified in the law – which shall remain in force for 5 years after the termination of the employment relationship, for classified data until the end of its validity period, and for personal data without any time limit.

(4) The certifying authority shall carry out its activities as a certifying authority, perform official controls and perform its tasks related to the maintenance of the register in accordance with the provisions of the decree of the President of the SZTFH – the Government in respect of the certifying authority referred to in Section 45(1)(b).

(5) The manufacturer shall, during the self-assessment of conformity, and the conformity assessment body shall, during the certification procedure,
The President of the Government shall act in accordance with the provisions of the Government's decree regarding the certification authority referred to in Section 45 (1) b).

Chapter V

POST-QUANTUM ENCRYPTION

29. General rules for the application of post-quantum encryption

Section 51. The electronic information system of an organization obliged to use post-quantum encryption shall be protected throughout its entire life cycle. must be implemented and ensured

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

b) the integrity and availability of the electronic information system and its elements, the closed, comprehensive, continuous and risk-proportionate protection of the post-quantum encryption application, which provides security beyond traditional cryptographic applications, on the government-purpose network between the physically separate locations of organizations obliged to apply post-quantum encryption, as well as on the public internet, when using a service provider under the Electronic Communications Act or when using their information society-related services.

30. Protection of an organization required to use post-quantum encryption

Section 52. In the performance of its tasks specified in the law, an organization obliged to apply post-quantum encryption is obliged to obtain a post-quantum encryption application from a registered organization authorized to provide the application for the purpose of building it on a government-purpose network between its physically separated locations, as well as on the public internet interface, in the event of using a service provider pursuant to the Electronic Communications Act or using other information society-related services, and to establish protection on the networks under its management in order to ensure that the flow of information via electronic means is secured against cyberattacks caused by quantum computers.

31. Conditions for an organization providing post-quantum encryption applications

Section 53 (1) Only an organization may provide post-quantum encryption applications (hereinafter referred to as: post-quantum encryption) application provider) for the organization required to use post-quantum encryption, which

a) does not pose a national security risk and b) meets

the requirements of paragraph (3).

(2) Pursuant to paragraph (1), the activity of providing post-quantum encryption applications shall be carried out exclusively an organization can do

a) which has a site security certificate as defined in the Act on the Protection of Classified Data, and b) whose employee or subcontractor has a personal security clearance as defined in the Act on the Protection of Classified Data
has a certificate.

(3) The activity of providing post-quantum encryption applications may only be carried out by an organization whose electronic information system ensures the confidentiality of system elements and prevents unauthorized access to the information system and its undetected modification. The electronic information system of the organization providing post-quantum encryption applications must comply with the requirements of this Act.

32. Certification of compliance with post-quantum encryption requirements

Section 54 (1) The organization wishing to provide post-quantum encryption applications must demonstrate compliance with the requirements specified in Section 53 (3) by means of a confidentiality certificate for the IT system issued by a certification body listed in the register pursuant to Section 56 (3) (b) (hereinafter referred to as: certification body).

(2) The certification body shall issue an expert opinion to the organization wishing to provide a post-quantum encryption application stating that its end-to-end application is suitable for post-quantum encryption providing security beyond cryptographic applications.

(3) If a certification body establishes a fact related to the IT system of the certified organization that adversely affects the continuous operation of the organization or detects circumstances indicating the commission of a crime, violation of the law or the threat thereof, it shall immediately notify the SZTFH.

33. Provisions concerning the certification body

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

(2) The certification body is entitled to process the data necessary for the conduct of the certification, including classified data, personal data or special data, business secrets, bank secrets, payment secrets, insurance secrets, securities secrets, treasury secrets, and secrets related to the practice of other professions, managed by the organization wishing to provide post-quantum encryption applications or the certified organization, solely for the purpose of examining the fulfillment of the requirements to be certified by the certification, to the extent necessary for the conduct of the certification procedure, until the completion of the certification procedure, and may not forward them to a third party.

(3) The certification body shall establish in regulations the positions held by persons who may have access to the trade secret and become familiar with its content during the certification procedure. The employees participating in the procedure shall be bound by a confidentiality obligation with regard to the trade secret that they have come to know during the certification procedure, even after the termination of their legal relationship with the organization certifying the application of post-quantum encryption.

34. Supervision of post-quantum encryption

Section 56 (1) Within its scope of supervision, the SZTFH may a) conduct an official inspection of the certification body and the organizations authorized to provide post-quantum
encryption applications, b) conduct
an extraordinary inspection in case of suspicion of non-compliance with the requirements specified in this chapter.

(2) The SZTFH shall verify the fulfillment of the obligations of the certification body and the organization authorized to provide post-quantum encryption applications by applying Section 25 (1) and (3) in accordance with the detailed rules specified in the decree of the President of the SZTFH.

(3) For the purpose of carrying out its inspection tasks under this Act, the SZTFH shall keep a register of a) the
organisations authorised to provide post-quantum encryption applications, and b) the
certification bodies performing certification pursuant to Section 54.

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

a) the name and registered office of the organisation, as well as the personal identification data, telephone number and e-mail address of its designated contact person, b) the organisation's
identification number – received upon registration –, c) additional data not
considered personal data as prescribed by the decree of the President of the SZTFH.

(5) If the organization included in the register pursuant to paragraph (3) no longer performs activities related to the provision of post-quantum encryption applications or certification activities, the SZTFH shall delete the data pursuant to paragraph (3) from the register five years after the notification of the termination of the activity.

(6) If the change in the data referred to in paragraph (3) is reported by the organization authorized to provide post-quantum encryption applications or the certification organization, the data included in the register prior to the registration of the change shall be deleted from the register by the SZTFH five years after the registration of the change in the data.

(7) Data from the register referred to in paragraph (3) may be transferred exclusively to cybersecurity authorities and cybersecurity incident management centers, unless otherwise provided by law.

Chapter VI

VULNERABILITY TEST

35. Authorized to conduct vulnerability assessments

Section 57 (1) The following are authorized to conduct
vulnerability assessments: a) the state body designated by the Government Decree, with the exception of electronic information systems
for national defense purposes; b) the National Defense Cybersecurity Incident Manager, with respect to electronic information systems for national defense purpose
center, and
c) a business organization with a site security certificate, as well as the infrastructure conditions and expertise necessary to perform the task, which is included in the register of business organizations authorized to conduct vulnerability assessments kept by the SZTFH.

(2) On behalf of an economic entity authorized to conduct a vulnerability assessment, the assessment may only be conducted by a person who:
a) has had
a national security audit conducted and has not identified a national security risk during the national security audit;
they found out,
b) who has the expertise necessary to conduct the vulnerability assessment, c) who has at least
two years of professional experience in the field of vulnerability assessment, and d) who is included in the
register of persons authorized to conduct vulnerability assessments kept by the SZTFH.

(3) The condition for registration under point c) of paragraph (1) is that the economic entity authorized to conduct the vulnerability assessment employs at least two experts under paragraph (2). The detailed rules for registration under point c) of paragraph (1) and point d) of paragraph (2), the infrastructural conditions and expertise necessary for carrying out the activity shall be determined by a decree issued by the President of the SZTFH, after seeking the opinion of the Minister responsible for IT.

(4) During the registration procedure pursuant to paragraphs (1) and (2), the SZTFH shall involve the state body authorized to conduct vulnerability assessments in order to determine whether the expertise and infrastructural conditions necessary for the performance of the task are met.

(5) Vulnerability testing shall be carried out – with the exception of electronic information systems for national defense purposes – by means of vulnerability testing.
a) by the organizations referred to in
points 1–9, 11, 14 and 15 of Annex 1, b) by the organization identified
by the national cybersecurity authority as an essential or important organization, in accordance with the national cybersecurity
in relation to the electronic
information system specified by the authority.

(6) If the state body authorized to conduct the vulnerability assessment does not have sufficient human resources to conduct the vulnerability assessment, it may agree to have the vulnerability assessment carried out by an economic entity authorized to conduct vulnerability assessments, at the organization's choice, as defined in paragraph (5).

(7) The vulnerability assessment of an electronic information system of outstanding importance for the operation and security of the state, the economy and society may be undertaken or supported by the state body authorised to conduct vulnerability assessments.

(8) [45] The vulnerability assessment is carried out by a state body authorized to conduct vulnerability assessments if it is a critical organization pursuant to the Act on the Protection of Information and Communications Technology, other than electronic information systems pursuant to paragraph (5) a), and the Act on the Protection of Information and Communications Technology, as well as There is no business entity that meets the conditions specified in this Act and is authorized to conduct a vulnerability assessment with respect to the electronic information system of an organization designated as an organization significant for the defense and security of the country.

45Section 57(8) is replaced by Section 67 of Act XXXII of 2025. Text established by §.

(9) The body referred to in paragraph (1) to which the vulnerability assessment has been initiated shall be obliged to examine its authority to conduct the vulnerability assessment, and if it establishes that another body referred to in paragraph (1) has the exclusive authority, it shall immediately forward the request to the competent body.

36. Initiate a vulnerability scan

Section 58 (1) The national cybersecurity authority may oblige the organization to conduct a vulnerability assessment. If the
If the organization fails to comply with an official obligation, the national cybersecurity authority may impose a fine.

(2) In the event of an official obligation pursuant to paragraph (1), the national cybersecurity authority shall take into account the electronic the importance of the information system for the functioning of the state.

(3) In its obligation pursuant to paragraph (1), the national cybersecurity authority shall specify which electronic information system the vulnerability assessment shall cover and may also specify the vulnerability assessment tool or method to be used.

Section 59. A state body authorized to conduct vulnerability assessments may initiate and conduct vulnerability assessments on its own initiative, with or without registered user authorization, in relation to the electronic information systems of organizations referred to in Section 57. (5).

Section 60 (1) With the exception of the organizations referred to in Section 1(1)(d) and (e), the head of the organization subject to the Act may initiate a vulnerability assessment without an official obligation, exclusively in relation to the electronic information system classified in the security class and registered by the cybersecurity authority.

(2) The head of the organization shall initiate the vulnerability assessment referred to in paragraph (1) at least sixty days before its planned start, in order to plan and prepare for it. When determining the planned start date of the vulnerability assessment, the organization shall also take into account the time requirements of the vulnerability assessment method specified in the government decree, taking into account the planned date of the electronic information system being put into use.

(3) The state body authorized to conduct the vulnerability assessment may, after considering the requests received, establish a priority order, and taking into account this priority order, may set the previously designated starting date of the assessment at a time no later than fifteen days later.

(4) The state body authorized to conduct vulnerability assessments shall give priority to vulnerability assessments ordered by the cybersecurity authority or initiated ex officio over initiatives initiated by the organization. When establishing the order, it shall proceed by considering the available resources and the importance of the electronic information system for the operation of the state based on a risk-based approach. If the fulfillment of the request initiated by the organization does not hinder the performance of its mandatory tasks, the state body authorized to conduct vulnerability assessments shall conduct the vulnerability assessments depending on the available capacities.

Section 61. With regard to electronic information systems not covered by this Act, the state body authorized to conduct vulnerability assessments may conduct vulnerability assessments based on an agreement concluded with the organization that has the authority to dispose of the electronic information system.

37. General provisions on vulnerability assessment

Section 62 (1) Vulnerability testing may also be directed at a specific part of the electronic information system.

(2) Due to the nature of the activity, vulnerability assessment may result in loss or reduction of service, which may include:
The body conducting the vulnerability assessment is not liable for any resulting damage, except in the case of intentional damage.

(3) Vulnerability testing methods and detailed rules for performing vulnerability testing
determined by government decree.

(4) The organization conducting the investigation shall issue a statement on the results of the vulnerability assessment, which shall include the identified
The detailed content of the position statement is determined by government decree.

Chapter VII

PROVISIONS RELATED TO CYBERSECURITY INCIDENTS

38. Cybersecurity Incident Response Centers

Section 63 (1) The Government shall operate a national cybersecurity incident management center through the body designated by it in a decree in order to manage threats, cybersecurity incidents and crises affecting the open electronic information systems of the organizations specified in Section 1(10), with the exception of electronic information systems for national defense purposes.

(2) The Government shall monitor threats, cybersecurity incidents and incidents affecting electronic information systems for national defense purposes. In order to manage crises, it operates a cybersecurity incident management center through the body designated by it in the decree.

(3) With the approval of the National Cybersecurity Incident Management Centre, a sectoral cybersecurity incident management centre (hereinafter referred to as: sectoral cybersecurity incident management centre) may also be established, with the exception of the national defence sector, in accordance with the provisions of the government decree. The National Cybersecurity Incident Management Centre shall carry out or have carried out an assessment and examination of the capabilities of the sectoral cybersecurity incident management centre, on the basis of which a cooperation agreement shall be concluded. During the examination, the conditions specified in the decree of the President of the SZTFH pursuant to Section 70(3)(b) shall also be taken into account.

Section 64 (1) The national cybersecurity incident management center
shall perform the tasks detailed in a government decree related to: a) threats affecting cyberspace, early warning and
prevention of cybersecurity incidents, b)
management of cybersecurity incidents, c) management
of cybersecurity crisis
situations, d) vulnerabilities, e) information and awareness-raising activities related to
cybersecurity and f) representation of Hungary in the European Union and international
cooperation.

(2) The national cybersecurity incident management center – with the exception of activities related to cyber activities and organizations that threaten national defense interests and military cyberspace operations – a) shall provide for the
organizations falling within the scope of this Act with respect to cyberspace in accordance with the rules of competence specified therein:
tasks against incoming threats and attacks,
b) manages the preparation for threats from cyberspace and related security tasks, with the exception of the national defense sector, c) analyzes the traffic of
electronic communications networks, detects
threats and attacks from cyberspace,
d) implements or initiates measures to interrupt an attack coming from cyberspace and to identify the causes and
necessary measures to identify those responsible.

(3) The national cybersecurity incident management center shall perform the coordination and other tasks specified by the government decree in relation to vulnerabilities and vulnerabilities reported by any natural or legal person in relation to the electronic information system of the organizations specified in Section 1 (10) or the ICT product or ICT service covered by this Act. The detailed rules for the detection and reporting of vulnerabilities and vulnerabilities shall be regulated by the government decree. In the case of vulnerabilities and vulnerabilities reported in relation to the electronic information system of the organizations not listed in Section 1 (10) or the ICT product or ICT service not covered by this Act, the national cybersecurity incident management center shall perform the tasks specified in the government decree depending on the resources available to it and by considering the degree of threat. With regard to the latter reports, the national cybersecurity incident management center is only obliged to act if it does not constitute a disproportionate or unreasonable burden for the national cybersecurity incident management center or if the report affects the electronic information system of an organization subject to the scope of this Act.

(4) The national cybersecurity incident management center may assume responsibility for or support the management and investigation of cybersecurity incidents that seriously endanger Hungarian cyberspace.

(5) The National Defense Cybersecurity Incident Management Center shall perform the tasks set out in paragraph (1) with regard to the national defense sector.

(6) The sectoral cybersecurity incident management center shall perform the tasks specified in the cooperation agreement concluded with the national cybersecurity incident management center.

(7) The tasks and powers of the national cybersecurity incident management center and the defense cybersecurity incident management center, the detailed rules for the performance of their tasks, as well as the detailed rules for early warning, its system, the regulations for the designation of the system operator, and the procedure for using the related early warning service shall be determined by government decree.

39. Preventing Cybersecurity Incidents

Section 65 (1) The national cybersecurity incident management center may use protective and preventive tools aimed at detecting threats from cyberspace and may provide services in this regard (hereinafter collectively: preventive tools) to the organizations referred to in Section 1(1).

(2) The application of preventive measures may be initiated by the organization referred to in Section 1(1) at its own expense at the national cybersecurity incident management center, which shall decide on the application of preventive measures depending on the resources available to it and by considering the degree of threat.

(3) The national cybersecurity authority may also oblige the organization referred to in Section 1(1)(a)–(c) to use preventive measures, based on the proposal of the national cybersecurity incident management center, and the national cybersecurity incident management center may also decide on the use of preventive measures itself, based on a risk analysis, after prior informing the organization concerned.

(4) The organization referred to in Section 1(1)(a)–(c) shall be obliged to use preventive measures when contacted by the national cybersecurity incident management center.

(5) The organization referred to in Section 1(1)(a)–(c) shall, upon request from the national cybersecurity incident management center, be obliged to join the threat information sharing system operated by the national cybersecurity incident management center, and may itself initiate joining this system. The national cybersecurity incident management center shall require the organization referred to in Section 1(1)(a)–(c) to join or consent to joining, taking into account the level of threat and the resources available to it.

(6) The national cybersecurity incident management center is entitled to collect information for general cybersecurity purposes only, from which it can clearly identify threats and cybersecurity incidents, regarding all geo-located internet addresses used in Hungary and the services located on them.

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

(8) The data determined during the vulnerability assessment may be utilized and used by the national cybersecurity incident management center exclusively anonymously for the purpose of assessing the state of cyberspace.

40. Reporting and handling cybersecurity incidents

Section 66 (1)[46] The organizations referred to in Section 1(1)(a)–(c) and (f) shall immediately report to the national cybersecurity incident management center any threats, near-misses and cybersecurity incidents that have occurred or become known to them in their electronic information systems, including operational cybersecurity incidents, as specified in the government decree.

(2) The organizations referred to in Section 1(1)(d) and (e) shall be obliged to report to the national cybersecurity incident management center, as specified in the government decree, any threats, near-incident cybersecurity situations and cybersecurity incidents – including operational cybersecurity incidents – that have occurred in their electronic information systems or that have come to their attention, which cause serious disruption or financial disadvantage in the organization's operations or the provision of services, or which cause significant financial or non-financial damage to other natural or legal persons.

(3) The organizations referred to in Section 1(1)(d) and (e) shall not be subject to any cyber security incident not classified as a cyber security incident pursuant to Section (2). They can also report cybersecurity incidents to the national cybersecurity incident management center.

(4) The organization shall report a threat, near-miss or cybersecurity incident affecting an electronic information system for national defense purposes to the national defense cybersecurity incident management center specified in the Government Decree.

(5) The national defense cybersecurity incident management center and the cybersecurity incident management center within the sector shall immediately forward the data on threats, cybersecurity near-incident situations and cybersecurity incidents that they become aware of to the national cybersecurity incident management center.

(6) If the national cybersecurity incident management center, the national defense cybersecurity incident management center, or the cybersecurity incident management center within the sector detects a lack of competence, it shall immediately send the notification to the competent cybersecurity incident management center.

Section 67 (1) Organizations or persons not falling within the scope of Section 1(10) may, on a voluntary basis, report to the national cybersecurity incident management center threats, cybersecurity near-incident situations, or cybersecurity incidents that have or may have a significant impact on the security of Hungarian cyberspace.

46A Section 66(1) Section 71(20) of Act XXXII of 2025 Text amended accordingly.

(2) The national cybersecurity incident management center may give priority to reports from organizations subject to the scope of this Act over voluntary reports. The national cybersecurity incident management center shall handle voluntary reports depending on the resources available to it and shall act by considering the degree of threat.

(3) In connection with voluntary reports, the national cybersecurity incident management center is only obliged to act if it does not pose a disproportionate or unreasonable burden for the national cybersecurity incident management center or if the voluntary report affects the electronic information system of the organization subject to this Act.

(4) As a result of voluntary reporting, no obligation may be imposed on the reporting person that would not have applied to him/her.
even without making the announcement.

Section 68 (1) If the electronic information system is affected by a significant cybersecurity incident or is threatened with imminent occurrence, which results in damage to essential information or personal data necessary for the operation of the organization with authority over the system or the user organization, the national cybersecurity incident management center may, in order to perform its protection tasks, oblige the organization with authority over the system to take the necessary measures to eliminate the significant cybersecurity incident or to avert the threat.

me.

(2) If an information security officer has been assigned to the organization, the national cybersecurity incident management center shall be informed immediately of the occurrence of the circumstances referred to in paragraph (1). In cases requiring immediate intervention, the national cybersecurity incident management center may, through the information security officer, apply interim measures to the extent necessary to avoid damage to the information.

41. Measures required to interrupt an attack from cyberspace

Section 69 (1) The measures required to interrupt an attack originating from cyberspace pursuant to Section 64 (2) d) may be implemented based on a decision by a person designated by the Government. After the interruption of the attack, the possible scope of further measures necessary to enhance protection and the need for further decisions related to the protection of the country shall be examined.

(2) The measure referred to in Section 64(2)(d) shall: a) be
proportionate to the harm caused or the immediate threat and shall be of a necessary extent and shall aim to:
so that it does not lead to any result or harm beyond interrupting the attack,
b) consistency with national security, defense, law enforcement and foreign policy interests and aspirations must be ensured.

(3) In the event of a significant cyberattack originating from abroad, the measures taken and the reasons for them must be informed to the
the Minister responsible for foreign policy to take further measures.

42. Cybersecurity Incident Management

Section 70 (1) In the event of a cybersecurity incident, the organization shall take measures to address the cybersecurity incident concerned.

(2) The cybersecurity authority may oblige the organization to handle the cybersecurity incident concerned. If the organization fails to comply with the authority's obligation, the cybersecurity authority may impose a fine.

(3) The management of the relevant cybersecurity
incident shall be carried out by: a) the organization itself, if employing an employee with appropriate
expertise, b) a business entity entrusted by the organization, which has a site security certificate, and the expertise and infrastructure conditions necessary for the performance of the task – as specified in the decree of the President of the SZTFH – and which is included in the register kept by the SZTFH pursuant to paragraph (4), c) the cybersecurity incident management
center within the sector, d) the national cybersecurity incident
management center, or e) the national defense cybersecurity
incident management center.

(4) The SZTFH keeps a register of economic entities authorized to handle cybersecurity incidents.
according to the detailed rules set out in the decree of its president.

(5) The register referred to in paragraph (4) shall include: a)
the name and registered office of the economic entity and the natural person identification number of its designated contact person
data, telephone number and e-mail address, b) the identification
number of the economic organization – received upon registration –, c) additional data not
considered personal data as prescribed by the decree of the President of the SZTFH.

(6) During the registration procedure pursuant to paragraph (4), the SZTFH shall involve the national cybersecurity incident management center in order to determine whether the expertise and infrastructure conditions required for the performance of the task, as specified in the decree of the President of the SZTFH, are met.

(7) If the organisation referred to in Section 1(1)(d) and (e) does not handle the cybersecurity incident itself, it shall choose from the economic organisations listed in the register referred to in Section (4). If the handling of the cybersecurity incident exceeds the capacities of the economic organisation, the organisation may contact the sectoral cybersecurity incident management centre or the national cybersecurity incident management centre to handle the cybersecurity incident concerned.

(8) If the organization referred to in Section 1(1)(a)–(c) does not handle the cybersecurity incident itself, it shall select or contact the cybersecurity incident management center within the sector or the national cybersecurity incident management center from among the economic entities listed in the register referred to in Section (4) in order to handle the cybersecurity incident.

(9) The organization referred to in Section 1(1)(a)–(c) is classified as a critical organization under the Act on the Protection of Human Rights and Fundamental Freedoms and as a critical organization under the Act on the Protection of Human Rights and Fundamental Freedoms. In the case of an organization designated as an organization significant for the defense and security of the country, only a person who has undergone a national security audit and who has not identified a national security risk during the national security audit may carry out incident management on behalf of and in the employ of the economic organization referred to in paragraph (3) b).

(10) The national cybersecurity incident management center shall handle the cybersecurity incident concerned with the resources available to it. depending on resources, by considering the degree of vulnerability.

(11) The management of the relevant cybersecurity incident shall be carried out by the national cybersecurity incident management center if the electronic information system of a critical organization pursuant to the Cybersecurity Act or the Cybersecurity Act. With regard to organizations designated as significant for the protection and security of the country, there is no economic entity that meets the conditions specified in the law to carry out cybersecurity incident management or it does not have sufficient capacity.

(12) With regard to the electronic information systems of the national security service performing civilian intelligence activities, the handling of a cybersecurity incident may only be carried out by an employee of the national cybersecurity incident management center who has undergone a national security audit and who has not identified a national security risk during the national security audit.

(13) The national cybersecurity incident management center may inform the head of the Operational Team referred to in Section 73 (3) about cybersecurity incidents that it has become aware of, if the cybersecurity incident also affects an organization represented by another member of the Operational Team.

(14) Detailed rules for the management of relevant cybersecurity incidents shall be established by government decree.

(15) The provisions of this Section shall also apply to the management of situations close to cybersecurity incidents.

43. Provisions governing the management of cybersecurity incidents by organisations subject to Regulation (EU) 2022/2554 of the European Parliament and of the Council

Section 71 (1) When handling cybersecurity incidents of organisations falling within the scope of Regulation (EU) 2022/2554 of the European Parliament and of the Council, the provisions of Sections 63–64, Section 67, Section 68(1), Section 69 and Section 70(10), (13) and (14) shall apply.

(2) If the handling of a cybersecurity incident exceeds the capacity of the organisation covered by Regulation (EU) 2022/2554 of the European Parliament and of the Council or of the intermediary it uses, the organisation may contact the sectoral cybersecurity incident response centre or the national cybersecurity incident response centre to handle the cybersecurity incident.

Chapter VIII

ORGANIZATIONAL SYSTEM FOR THE COORDINATION OF CYBERSECURITY-RELATED TASKS

44. Commissioner for Cybersecurity

Section 72 (1) The Commissioner responsible for cybersecurity shall be appointed by the Minister responsible for IT.

(2) The Commissioner for Cybersecurity shall be responsible for ensuring a high level of cybersecurity across the European Union. measures under the Directive

a) for the compilation of a national cybersecurity

strategy, and b) for the national

crisis management plan and its coordination with the relevant organizations.

(3) The Commissioner responsible for cybersecurity shall lead the National Cybersecurity Working Group.

45. The National Cybersecurity Working Group

Section 73 (1) The National Cybersecurity Working Group is the Government's body for proposing and giving opinions on cybersecurity issues.

(2) The National Cybersecurity Working Group shall ensure the coordination of the activities specified in this Act and its implementing regulations.

(3) The activities of the National Cybersecurity Working Group are carried out by the Operational Core, as well as the cybersecurity sub-working groups and the It is supported by the National Cybersecurity Forum, which provides a framework for cooperation with non-governmental actors.

(4) The activities of the Operational Staff shall be managed by the Commissioner responsible for cybersecurity. The Operational Staff, with the involvement of the central body of the defense and security administration, shall classify the defense and security event resulting from a significant or large-scale cybersecurity incident and shall initiate the taking of crisis management or emergency management measures.

(5) By establishing and operating the National Cybersecurity Working Group and the bodies supporting its operation
The related rules, tasks and powers are regulated by government decree.

46. Cybersecurity crisis management organizational system

Section 74 (1) In the event of a significant or large-scale cybersecurity incident, the Operational Staff of the National Cybersecurity Working Group may, on the initiative of the national cybersecurity incident management center, make a proposal to classify the cybersecurity incident as a cybersecurity crisis situation.

(2) A cybersecurity crisis is a defense and security event in which the Government responsible for IT
may order coordinated protection activities based on the proposal of the Minister.

(3) In the event of a cybersecurity crisis – unless otherwise provided by this Act or the government decree issued for its implementation – the World Cup. shall apply.

(4) In the event of a cybersecurity crisis and the coordinated protection activities ordered on that basis, the Government may introduce as a measure:

1. increasing the readiness and preventive activities of the body or organization involved in cybersecurity crisis management; 2. operational or manpower protection of the bodies or organizations referred to in point 1, and its intensification; 3. increasing the activities of the reconnaissance, response and cyberspace operational forces of the national defense organizations, law enforcement agencies and national security services in order to prevent the spread of the threat to Hungary, and to prevent the attack and its consequences;

4. coordinated or joint action by the bodies or organisations referred to in point 3 within the framework of a coordinated defence activity; 5. a service essential for the maintenance of critical social or economic activities, and the provision of such services alone ordering the immediate identification of a service provider not yet identified as an essential or important organization;

6. the suspension, restriction and control of electronic communications services, the making of access to them impossible, as well as the free use, transfer for use, non-use and inaccessibility of electronic IT networks and devices and electronic communications equipment;

7. the service provider's operating premises and technical equipment necessary for cybersecurity crisis management, the free use and transfer of its electronic information system and facilities;

8. in order to ensure the continuous operation of the information and communication systems of the state and the bodies or organizations involved in cybersecurity crisis management, the free use of repair capacities and spare parts, or the restriction of their use, and the performance of repair and operation services charged to the owners and employees of companies with repair capacities; 9. the stockpiling and reserving of products and equipment important for ensuring cybersecurity; 10. the mandatory information of the European Cyber Crisis Contact Points Network (hereinafter: EU-CyCLONE), as well as the European Commission and the European Union Agency for Cybersecurity (hereinafter: ENISA) and deciding on its content, 11. the provision of mandatory official government information to the parties concerned, and 12. the information of the Member States of the European Union and the allied countries within the North Atlantic Treaty Organization

on the measures taken by the Government in connection with the cybersecurity crisis situation, using diplomatic channels.

(5) When providing information pursuant to points 10 to 12 of paragraph (4), the Union and national rules on the protection of classified information shall be observed. must be carried out in accordance with the provisions of the rules and general data protection legislation.

(6) During the cybersecurity crisis, in order to prevent, identify, detect and prevent the spread of the cybersecurity crisis, as well as to organize the coordinated performance of tasks by state bodies, the Operational Staff – in connection with the cybersecurity crisis –

a) may request data from any body, legal entity or organization without legal personality, which is obliged to comply with this data provision immediately and free of charge,

b) processes personal data obtained during the handling of the cybersecurity incident.

(7) The Operational Body shall process the data processed pursuant to paragraph (6) as information relating to national security activities. except for the national incident management center.

(8) The Operational Body shall process the data processed pursuant to paragraph (6) – the circumstances giving rise to the cybersecurity crisis situation for investigation – to the national cybersecurity incident management center.

(9) The Head of the Operational Staff is responsible for managing the event that triggered the cybersecurity crisis. entitled to

a) to impose an obligation on the member of the Operational Staff to take immediate action with regard to the organization he represents, b) to

decide whether the national cybersecurity incident management center or the national defense incident management center should involvement in handling a cybersecurity incident.

(10) An organization falling under the scope of Section 1(10) – with the exception of an organization under Section 1(1)(d) and (e) – shall prepare a cybersecurity plan in order to prepare for and manage a cybersecurity crisis, in which it assesses the potential risks coming from cyberspace and, based on these, develops the crisis management procedural elements to be implemented in its area of operation.

(11) The organization affected by the cybersecurity crisis situation – with the exception set out in paragraph (12) – shall, at the request of the national cybersecurity incident management center and the central body of defense and security administration, collect data and information related to the plan specified in paragraph (10) and the measures introduced to manage the cybersecurity crisis situation, and transmit it in electronic form or make it accessible in another way.

(12) With regard to electronic information systems for national defence purposes, the data specified in paragraph (11) shall be made available to the national defence cybersecurity incident management centre and the central body of defence and security administration upon their request.

(13) The designation, tasks and powers of the bodies or organizations participating in cybersecurity crisis management, the procedures to be followed, and the bodies representing Hungary in EU-CyCLONE shall be determined by the Government in a decree.

47. The National Coordination Centre

§ 75 [47] (1) The tasks of the national coordination centre (hereinafter: national coordination centre) serving as a contact point for the cybersecurity competence community pursuant to Regulation (EU) 2021/887 of the European Parliament and of the Council shall be performed by the body designated in the Government Regulation in accordance with the provisions thereof.

(2) For the purpose of carrying out its tasks specified in Regulation (EU) 2021/887 of the European Parliament and of the Council, the national coordination centre shall register and manage the following data: a) the data necessary for the identification of the organisation applying to the cybersecurity competence community pursuant to Regulation (EU)

2021/887 of the European Parliament and

of the Council, b) its registered office,

location, branch, c) its contact details, including electronic contact

details, d) the name or company name of the representative operating in Hungary of an organisation not registered in Hungary, and its correspondence address address, telephone number and e-mail address,

e) the name and contact details of the contact person, including electronic contact details, their position in the organisation, and

f) additional data not considered personal data as prescribed by government decree.

(3) Data from the register referred to in paragraph (2) shall be transferred – unless otherwise provided by law – exclusively to a) the

European Cybersecurity Industrial, Technology and Research Facility pursuant to Regulation (EU) 2021/887 of the European Parliament and of the Council; Competence Centre, b)

the cybersecurity authority, c) the

authority pursuant to Regulation (EU) 2022/2554 of the European Parliament and of the

Council, d) the single point of contact pursuant to Directive (EU) 2022/2555 of the European Parliament and of the Council,

and e) the national cybersecurity incident management centre

can be done for.

47A Section 75 of Act XXXII of 2025, Section 68. Text established by §.

(4) The national coordination centre shall publish on its website the names of the registered members of the cybersecurity competence community, their country of residence, their official website, their type of organisation and their field of activity pursuant to Article 8(3) of Regulation (EU) 2021/887, as well as their data not qualifying as personal data as specified in a government decree.

(5) The Government shall determine in a decree the detailed rules relating to the tasks, powers, procedures and registration of the national coordination centre.

48. Cooperation and reporting

Section 76 (1) The cybersecurity authorities, the certification authority, the post-quantum encryption supervisory authority, the designating authority pursuant to the Cybersecurity Act, the The designating authority pursuant to Regulation (EU) 2022/2554 of the European Parliament and of the Council, the public body authorised to conduct vulnerability assessments, the cybersecurity incident response centres, the national coordination centre and the single point of contact shall cooperate and inform each other of their findings concerning electronic information security.

(2) The notification referred to in paragraph (1) shall be made immediately if its subject matter reveals a threat to electronic information security or refers to a cybersecurity incident. Based on the notification, the organizations shall immediately initiate the measures within their competence, in cooperation with each other.

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

Chapter IX

DATA PROCESSING AND DATA PROTECTION PROVISIONS

Section 77 (1) The cybersecurity authority, the body or economic entity authorized to conduct vulnerability assessments, the cybersecurity incident management center, the single point of contact, and the national coordination center are entitled to process classified data, personal data or protected data, business secrets, bank secrets, payment secrets, insurance secrets, securities secrets, treasury secrets, medical secrets and other secrets related to the practice of a profession, as well as other data learned during the performance of their tasks, exclusively during the period of performance of their tasks specified in the law, taking into account the principle of purpose limitation, and in accordance with the provisions of the laws on data processing.

(2) After the completion of the performance of the tasks, the bodies referred to in paragraph (1) shall provide the data recorded in connection with the performance of the tasks – with the exception specified in paragraphs (3) to (6) – are obliged to delete it from their electronic information systems and data carriers.

(3) The body referred to in paragraph (1) is entitled to process the data specified in paragraph (1) for five years after the official decision becomes final, the vulnerability assessment is concluded, and the investigation of the cybersecurity incident or cybersecurity crisis situation is conducted, and is obliged to delete it from its electronic information systems and data carriers after five years.

(4) If the organization no longer carries out activities falling within the scope of this Act, the cybersecurity authority shall delete the data registered regarding the organization from the register five years after the notification of the termination of the activity.

(5) If the organization reports a change in the data, the cybersecurity authority is obliged to delete the original data from the register five years after the notification of the change in the data.

(6) The cybersecurity incident management center is entitled to process and retain the data generated during the application of prevention tools and services, as well as the data of the reports received by the cybersecurity incident management center and the single point of contact for five years from the date of generation of the data or receipt of the report; after that, it is obliged to delete it from its electronic information systems and data carriers.

Section 78 (1) The cybersecurity authority, the body or economic entity authorized to conduct vulnerability assessments, and the employees of the cybersecurity incident management center shall be bound by a written confidentiality obligation with respect to the data they have obtained, which shall apply a) for five years

after the termination of the employment relationship, b) for the end of its validity

period with respect to classified data, and c) without time limit with respect to

personal data.

(2) The cybersecurity authority, the body or economic entity authorized to conduct vulnerability assessments, and the Data generated during the procedure of the cybersecurity incident management center – with the exception of those specified in Section 79 – are not public.

(3) The final decision of the body designated by the Government to perform the official tasks of electronic information systems for national defense purposes, as defined in this Act, on the client, and Section 33 (3) of Act CL of 2016 on General Administrative Procedure cannot be accessed by anyone other than a person authorized to view the document.

Section 79 (1) The state body authorized to conduct vulnerability assessments shall be entitled to publish the results of the vulnerability assessments publish anonymized statistics that do not contain any indication of the vulnerability of the systems.

(2) The national cybersecurity incident management center is entitled to access data and information generated in the course of its tasks. publish statistics on trends, conclusions drawn, and technical descriptions of incidents in an anonymized manner.

Section 80 (1) When fulfilling their obligation to provide information and data, the bodies referred to in Section 77 (1) shall act in accordance with the provisions on the protection of classified data and the general data protection legislation. The provision of information and data may not concern the provision of information the publication of which would be contrary to Hungary's national security, public security or fundamental defence interests.

(2) Confidential information, including business confidentiality rules, may only be shared with the European Commission and other relevant authorities if the 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 to the purpose of the exchange of information. The exchange of information shall preserve the confidentiality of the information provided and shall protect the security and commercial interests of the organisations.

Chapter X

FINAL PROVISIONS

49. Empowering provisions

Section 81 (1) The Government is authorized to designate in a decree a) the body authorized to provide cybersecurity services, b) the national cybersecurity authority, c) the authority performing cybersecurity supervision with regard to electronic information systems for[48] national defense purposes, d) the certification authority pursuant to Section 45 (1) b), 51 e) the state body authorized to conduct vulnerability assessments, f) the body operating the national[49] cybersecurity incident management center, g) the body operating the national cybersecurity[50] incident management center, h)[52][53]

[54] the bodies and organizations involved in managing the cybersecurity crisis, the bodies representing Hungary in EU-CyCLONE, the national coordination center, and the[55]

i)[56] food chain supervision body providing data[57]

j)[58] pursuant to Section 24 (9).

(2) The Government is authorized to establish in a decree: 1. the detailed rules of cybersecurity services, the scope of cybersecurity services, the persons obliged to use them, and authorized organizations, as well as the procedure for using the services,

2.[59] detailed provisions on the obligations of the organisations referred to in Section 1(1)(a)–(c) and (f);[60]

48See Government Decree 418/2024. (XII. 23.).

49See Government Decree 418/2024. (XII. 23.).

50See Government Decree 418/2024. (XII. 23.).

51See Government Decree 418/2024. (XII. 23.).

52See Government Decree 418/2024. (XII. 23.).

53See Government Decree 418/2024. (XII. 23.).

54A Section 81(1)(h) is the text amended by Section 71(21) of Act XXXII of 2025 .

55See Government Decree 418/2024. (XII. 23.).

56A Section 81(1)(i) of Act XXXII of 2025 Section 71(22) Text amended accordingly.

57See Government Decree 418/2024. (XII. 23.).

58A Section 81(1)(j) is replaced by Section 69(1) of Act XXXII of 2025 he enrolled.

59A Section 81(2)(2) is a text amended by Section 71(23) of Act XXXII of 2025 .

60See Government Decree 418/2024. (XII. 23.).

3. detailed rules on the classification of data managed in electronic information systems; 4. the minimum content elements of[61] the agreement pursuant to Section 11(1); 5. detailed tasks and powers of the person[62] responsible for the security of the electronic information system, the electronic the procedure for entering and deleting persons responsible for information system security in the register;[63] 6.[64] the detailed rules applicable during the development of the electronic information systems of the organization referred to in Section 1(1)(a)–(c) and (f);[65]

7. by the central service provider to the organization performing state and local government tasks with exclusive rights based on the law detailed rules on the provision of IT and electronic communications services;

8. the tasks and powers of the national cybersecurity authority and the authority performing cybersecurity supervision with regard to electronic information systems for national defence purposes, as well as the detailed rules on its procedure and records; 9. in the case of organisations referred to in Section 1(1)(a)–(c) and (f), the[66] information security supervisor[67] requirements, detailed rules regarding his/her assignment, powers and duties;[68]

10. the amount of the fine that can be imposed by the cybersecurity authority, the criteria for determining it, and the method of determining the fine detailed procedural rules for the method of payment;[69]

11. the amount of the fine that may be imposed by the certifying authority, the criteria for determining it, and the payment of the fine detailed procedural rules of the method;[70]

12. the detailed rules on the tasks of the certification authority pursuant to Section 45(1)(b), the procedures for certification authority activities, the licensing procedure, official control, record-keeping, as well as the data content of the record that does not contain personal data, and the rules on the affixing of the conformity mark;

13.[71] detailed rules on self-assessment of conformity, the certification procedure, the requirements for conformity assessment bodies in the case of a national cybersecurity certification system, the conditions for the registration of conformity assessment bodies in the case of a European cybersecurity certification system, and the obligations and activities of conformity assessment bodies in the case of military research, development, production and trade;

14. national cybersecurity certification systems for military research, development, production and trade with regard to certification systems;

15. the detailed rules for carrying out vulnerability assessment, the individual vulnerability assessment methods, the content elements of the position statement;[72]

16. the tasks and responsibilities of the national cybersecurity incident management center and the defense cybersecurity incident management center its powers and detailed rules for the performance of its duties;[73]

17. detailed rules on the establishment of a cybersecurity incident management center within the sector; 18. detailed rules on the[74] detection and reporting of vulnerabilities, the national cybersecurity coordination and other tasks related to reported vulnerabilities and vulnerabilities by the incident management center;[75]

19. the detailed rules for early warning, its system, and the regulations for the designation of the system operator, and the procedure for using the related early warning service;

20. the detailed rules for early warning of electronic information systems for national defence purposes, its system, the requirements for the designation of the system operator, and the procedure for using the related early warning service;

21. the procedure for reporting threats, near-miss situations and cybersecurity incidents, detailed rules for the management and investigation of cybersecurity incidents and near-incident situations;[76]

---

61 See Government Decree 418/2024. (XII. 23.).
62 See Government Decree 418/2024. (XII. 23.).
63 See Government Decree 418/2024. (XII. 23.).
64 A Section 81(2)(6) is the text amended by Section 71(24) of Act XXXII of 2025 .
65 See Government Decree 418/2024. (XII. 23.).
66 See Government Decree 418/2024. (XII. 23.).
67 A Section 81(2)(9) is the text amended by Section 71(25) of Act XXXII of 2025 .
68 See Government Decree 418/2024. (XII. 23.).
69 See Government Decree 418/2024. (XII. 23.).
70 See Government Decree 418/2024. (XII. 23.).
71 A Section 81(2)(13) in conjunction with Section 69(2) of Act XXXII of 2025 established text.
72 See Government Decree 418/2024. (XII. 23.).
73 See Government Decree 418/2024. (XII. 23.).
74 See Government Decree 418/2024. (XII. 23.).
75 See Government Decree 418/2024. (XII. 23.).
76 See Government Decree 418/2024. (XII. 23.).

22. the detailed rules for holding domestic cybersecurity exercises; 23. the tasks [77]
and powers of the bodies and organizations involved in managing the cybersecurity crisis, and the procedures to be followed; 24. the establishment and operation [78]
of the National Cybersecurity Working Group and the bodies supporting its operation
related rules, tasks and powers, and [79]
25. cooperation between the bodies referred to in Section 76(1) and with the organisations referred to in Section 76(3), and
detailed rules on the procedure for providing information and data to the European Commission and ENISA, [80]
26. [81] detailed rules on the tasks, powers, procedures and registration of the national coordination centre.

(3) The Minister responsible for IT is authorized to specify in a regulation a) the requirements for security
classification and the specific protection measures to be applied to each security class,

b) [82] responsible for the training and further training of the organization's leader, as well as for the security of the electronic information system provisions regarding the further training of a person,

c) [83] a) in relation to the organisations specified in point b) of paragraph (3) of Section 11 – the qualifications required for the performance of the tasks of the persons responsible for the security of the electronic information system, the procedure for publishing qualifications by the national coordination centre pursuant to Section 75 (1), or the acceptable professional experience, and – in relation to the organisations referred to in points a) to c) of paragraph (1) of Section 1 – the qualifications required for the performance of the tasks of the information security supervisor, the obligation to continue training and professional experience and the procedure for publishing qualifications by the national coordination centre pursuant to Section 75 (1),

d) [84] ICT products, ICT services or ICT processes certified under a mandatory national or European cybersecurity certification scheme, as well as the organisations required to apply them, as referred to in Section 1(1)(a)–(c) and (f).

(4) The minister responsible for IT shall issue the decree referred to in paragraph (3) a) after seeking the opinion of the President of the SZTFH. issue it afterwards.

(5) The Minister responsible for national defence is authorised to determine by decree, in agreement with the Minister responsible for tax policy, the amount of the administrative service fee to be paid for the procedure of the certifying authority referred to in Section 45(1)(b), and the detailed rules relating to the collection, distribution, management, registration and refund of the fees.

(6) The President of the SZTFH is authorized to determine in a decree a) the amount
of the cybersecurity supervision fee and the provisions regarding its payment, b) the procedure for [85]
the registration procedure of auditors and the requirements imposed on auditors, c) the procedure for conducting cybersecurity
audits, and the amount of cybersecurity audits – calculated without VAT –
the highest award, [86]

d) [87] with regard to the organizations referred to in Section 1(1)(d) and (e) and auditors, cybersecurity supervision and
the detailed rules for the performance of tasks and the conduct of official inspections, [88]

e) the procedure for registering the organisations referred to in Section 1(1)(b), (d) and (e) in the cybersecurity supervisory authority register referred to in Section 29(1)(a), as well as the detailed rules concerning the data content of the register that does not constitute personal data, f) in the case of organisations referred to in Section
1(1)(d) and (e), the procedure for registering the information security supervisor
requirements, detailed rules regarding his/her assignment, authorizations and tasks, g) organizations obliged to apply post-quantum encryption, [89]

77See Government Decree 418/2024. (XII. 23.)
78See Government Decree 418/2024. (XII. 23.).
79See Government Decree 418/2024. (XII. 23.)
80See Government Decree 418/2024. (XII. 23.).
81A Section 81(2)(26) is replaced by Section 69(3) of Act XXXII of 2025 he enrolled.
82A Section 81(3)(b) in conjunction with Section 69(4) of Act XXXII of 2025 established text.
83A Section 81(3)(c) in conjunction with Section 69(4) of Act XXXII of 2025 established text.
84A Section 81(3)(d) is the text amended by Section 71(26) of Act XXXII of 2025.
85See Decree 2/2025. (I. 31.) of the Hungarian Supreme Court.
86See Decree 1/2025 (I. 31.) of the Supreme Administrative Court.
87A Section 81(6)(d) is the text amended by Section 71(27) of Act XXXII of 2025.
88See Decree 3/2025. (IV. 17.) of the Hungarian Federal Council of State.
89See Decree 3/2025. (IV. 17.) of the Hungarian Federal Council of State.

h) detailed rules on the registration of an organization providing post-quantum encryption applications, the data content of the register that does not contain personal data, and the inspection of the organization providing post-quantum encryption applications, i) detailed rules on the certification

of the closedness of the IT system elements of the organization providing post-quantum encryption applications,

j) detailed rules on the registration of the certification body, the data content of the register that does not contain personal data, and the inspection 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 for certification authority activity, the licensing procedure, the official inspection, the maintenance of the register, the data content of the register that does not contain personal data, and the rules on the affixing of the conformity mark,

l) [90] – with the exception of military research, development, production and trade – detailed rules on conformity self-assessment, the certification procedure, the requirements for conformity assessment bodies in the case of a national cybersecurity certification system, the conditions for the registration of conformity assessment bodies in the case of a European cybersecurity certification system, and the obligations of conformity assessment bodies and their activities,

m) national cybersecurity certification systems, with the exception of military research, development, production and trade, n) ICT products, ICT

services or ICT processes certified on the basis of a mandatory national or European cybersecurity certification system, as well as the organisations required to apply them pursuant to Section 1(1)(d) and (e).

(7) The President of the SZTFH is authorized to specify in a decree a) the

detailed procedure for registering economic entities and persons authorized to conduct vulnerability assessments rules, the infrastructural conditions and expertise necessary for carrying out the activity, and b) the detailed rules for [91]

registering economic entities authorized to handle cybersecurity incidents, the data content of the register that does not contain personal data, and the infrastructural conditions and expertise necessary for carrying out the activity.

(8) The President of the SZTFH shall issue the decree referred to in paragraph (7) after seeking the opinion of the Minister responsible for IT.

50. Provisions entering into force

Section 82 (1) This Act shall enter into force on 1 January 2025, with the exception of paragraph (2).

(2) Section 120(1) shall enter into force on 2 January 2025.

51. Transitional provisions

Section 83 (1) Act L of 2013 on the electronic information security of state and local government bodies (hereinafter referred to as the Ibtv.) Data included in the register pursuant to Section 8(4) on 31 December 2024 do not need to be reported again, they will be managed by the national cybersecurity authority as part of the register pursuant to Section 28(1).

(2) The data provision obligation pursuant to Section 8(4) shall be fulfilled by the organization referred to in Section 1(1)(a) and (b) pursuant to Section 8(4). to the national cybersecurity authority within the deadline set out in paragraph 1, if

a) prior to the entry into force of this Act, the Ibtv. was subject to the scope of and has not yet fulfilled the requirements set out in Section 8(4) obligation, and

b) prior to the entry into force of this Act, the Ibtv was not due. under its scope.

(3) If the organization referred to in Section 1(1)(a) and (b) is the person responsible for the security of the electronic information system your data according to the Ibtv. has already notified the national cybersecurity authority, he is not obliged to notify it again.

(4) If the person responsible for the security of the electronic information system of the organization referred to in Section 1(1)(a) and (b) does not meet the requirements of Section 11(4) upon the entry into force of this Act, he or she shall have 2 years to eliminate the cause of the conflict of interest.

(5) If the first classification of the already operating electronic information systems of an organization referred to in Section 1(1)(a) and (b) into a security class is carried out in accordance with the provisions of the Ibtv. should have been completed by the entry into force of this Act, the first security classification must be completed within 120 days of the entry into force of this Act - together with the establishment of the risk management framework pursuant to Section 6.

90A Section 81(6)(l) in conjunction with Section 69(6) of Act XXXII of 2025 established text.

91See Decree 5/2025. (VI. 20.) of the Hungarian Supreme Court.

(6) If the cybersecurity authority has classified the electronic information systems of an organization referred to in Section 1(1)(a) and (b) into a security class before the entry into force of this Act, the Cybersecurity Authority has has made an official decision on the basis of, the review of the security classification shall be carried out within two years of the date on which the official decision on the security classification has become final, as provided for in this Act. If, on this basis, the review is due by the date of entry into force of this Act or within 180 days of the date of entry into force of this Act, the deadline for the review of the security classification shall be extended in such a way that the available time is 180 days.

Section 84 of the Civil Procedure Act. According to the 1st and 2nd security classes are “basic”, 3rd and 4th security classes are “significant”, 5th security class is corresponds to a "high" security class.

Section 85 (1) If an organization referred to in Section 1(1)(a) and an organization not classified as an organization referred to in Annexes 2 and 3 and falling within the scope of Section 1(1)(b) before the entry into force of this Act, the Ibtv. and has already fulfilled the requirements set out therein for the security department of its electronic information systems, has 1 year from the entry into force of this Act to implement the new security measures set out in the decree of the Minister responsible for IT.

(2) If an organization referred to in Section 1(1)(a) and an organization not classified as an organization referred to in Annexes 2 and 3 and falling within the scope of Section 1(1)(b) before the entry into force of this Act, the Ibtv. and has not yet had to meet the requirements for the security class of its electronic information systems, may apply the option of gradual implementation pursuant to Section 10(6) when implementing the security measures prescribed in the decree of the Minister responsible for IT. The basis for calculating the deadline taking into account gradual implementation is the security class determined pursuant to Section 84, the requirements of which have already had to be met. The time available for implementing the security measures may not be less than 1 year.

Section 86 (1) In the case of an organization referred to in Section 1(1)(a) and an organization not classified as an organization referred to in Annexes 2 and 3 and falling within the scope of Section 1(1)(b), the provisions of this Act relating to the development of a new system shall apply to the systems not yet in use at the time of the entry into force of this Act,

a) in the case of a system under development that is developed in-house, if the resource requirements have not yet been accepted, b) in the

case of a system under external development, if the procurement procedure for the development has not yet been announced, or
A development contract has not yet been signed.

(2) If the system developed by the organization referred to in Section 1(1)(a) and by the organization not classified as an organization referred to in Annexes 2 and 3 and falling within the scope of Section 1(1)(b) has exceeded the steps of the development of the electronic information system specified in Section (1) at the time of the entry into force of this Act,

a) the organization shall classify the electronic information system into a security class within 180 days, if it has not already done so, b) when fulfilling the security measures

prescribed in the decree of the minister responsible for IT, it has the option of gradual implementation in accordance with Section 10 (6), provided that the date of entry into force of this Act shall be the basis for calculating the relevant deadline.

Section 87. If an organization referred to in Section 1(1)(a) and an organization not classified as an organization referred to in Annexes 2 and 3 and falling within the scope of Section 1(1)(b) prior to the entry into force of this Act, the Ibtv. During the verification of compliance with electronic information security requirements, the cybersecurity authority shall, until the deadlines specified in this Act have expired, carry out the procedures set out in Act L of 2013 on the electronic information security of state and local government bodies. examines compliance with the provisions of the Regulation on the requirements for specific technological security and secure information devices and products, as well as classification into security classes and security levels, unless the organization has declared compliance with the protection measures prescribed in the Regulation of the Minister responsible for IT.

Section 88 (1) The Civil Procedure Act. The cybersecurity authority shall handle ongoing official cases pursuant to the provisions of the Cybersecurity Act. close it accordingly.

(2) Act CLXVI of 2012 on the identification, designation and protection of vital systems and facilities The operator of a vital system element designated on the basis of this Act is considered a critical organization for the purposes of this Act until the decision made in the designation procedure specified in the Kszetv. or the Vbö. becomes final.

Section 89 (1) An organization referred to in Section 1 (1) b), d) or e) which, on 31 December 2024, was registered by the SZTFH in accordance with Section 26 (1) of Act XXIII of 2023 on Cybersecurity Certification and Cybersecurity Supervision is listed as a concerned organization in the register kept pursuant to Section 8(5), Section 26(1) of Act XXIII of 2023 on Cybersecurity Certification and Cybersecurity Supervision The data included in the register pursuant to Section 29 (1) a) shall be managed by the SZTFH as part of the register pursuant to Section 29 (1) a) sub-point e) of Section 29 (1) a) shall be reported to the SZTFH by 15 February 2025.

(1a) [92] An organization referred to in Section 1(1)(b) which is also an organization referred to in Annexes 2 and 3, as well as an organization referred to in Section 1(1)(d) and – with the exception of microenterprises pursuant to the Act on Small and Medium-sized Enterprises and Support for Their Development – an organization referred to in Section 1(1)(e) which commenced operations before 1 January 2025, shall comply with the obligation referred to in Section 16(2)(a) by 31 August 2025 at the latest.

(2) [93] The organization referred to in paragraph (1a) shall conduct the first cybersecurity audit referred to in paragraph (1) of Section 16 by 30 June 2026. to be completed.

(3) The economic entity that is subject to Section 26 (1) of Act XXIII of 2023 on Cybersecurity Certification and Cybersecurity Supervision is listed as a concerned organization in the register kept pursuant to and until 31 December 2024, Section 20 (1) of Act XXIII of 2023 on Cybersecurity Certification and Cybersecurity Supervision has classified its electronic information systems and the data stored, transmitted or processed therein into a security class, it is not obliged to reclassify them pursuant to Section 10(1).

(4) The economic entity that, on 31 December 2024, is a company that complies with Section 23 (6) of Act XXIII of 2023 on Cybersecurity Certification and Cybersecurity Supervision is registered as an auditor in accordance with Section 23 (6) of Act XXIII of 2023 on Cybersecurity Certification and Cybersecurity Supervision. The SZTFH manages the data included in the register pursuant to Section 21 (3) as part of the register.

(5) The organization that, on 31 December 2024, is a member of the Commission of the European Communities, pursuant to Section 14(1) of Act XXIII of 2023 on Cybersecurity Certification and Cybersecurity Supervision is registered as a conformity assessment body in accordance with Article 14(1)(c)–e) of Act XXIII of 2023 on Cybersecurity Certification and Cybersecurity Supervision, g)–j) and point l) The SZTFH processes your data as part of the register pursuant to Section 48 (1).

(6) Section 14(1) of Act XXIII of 2023 on Cybersecurity Certification and Cybersecurity Supervision Data included in the register pursuant to Section 48 (1) on 31 December 2024 – which do not fall within the scope of data pursuant to Section (7) – do not need to be reported again; the SZTFH will manage them as part of the register pursuant to Section 48 (1).

(7) Upon the entry into force of this Act, Act XXIII of 2023 on Cybersecurity Certification and Cybersecurity Supervision The SZTFH shall conduct ongoing official procedures pursuant to Act XXIII of 2023 on Cybersecurity Certification and Cybersecurity Supervision. shall be carried out by applying the provisions of this Act, with the FSA being entitled to issue a deficiency notice within 30 days of the entry into force of this Act. As a result of the procedure, the FSA shall enter the data to be registered in accordance with this Act into the registers in accordance with this Act.

(8) An organization that is included in the register of economic entities authorized to conduct vulnerability assessments as of 31 December 2024, pursuant to the Government Decree on the Rules for Conducting Vulnerability Assessments, is not required to apply for registration again; its data included in the register will be managed by the SZTFH – based on the data provided by the Office for the Protection of the Constitution – as part of the register pursuant to Section 57(1)(c) of the Act.

(9) The organization registered in the register pursuant to Section 57(1)(c) pursuant to Subsection (8) shall certify to the SZTFH that it has fulfilled the requirements specified as conditions for registration in this Act and in the legislation issued for the implementation of this Act by 31 July 2025. In the event of failure to provide certification, the SZTFH shall delete the organization from its register.

52. The Fundamental Law compliance with the requirement of polarity

Section 90 (1) Section 93 is replaced by Article 46(6) of the Fundamental Law. is considered pivotal.

(2) Section 97 is Article IX. Paragraph (6) of the Fundamental Law. is considered pivotal.

(3) Sections 118–121 and Section 123 are part of Article 23(4) of the Fundamental Law. is considered pivotal.

53. Compliance with European Union law

Section 91 (1) This Act

a) Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures to ensure 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) serves to comply with Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical organisations and repealing Council Directive 2008/114/EC and Directive 2006/123/

c) [94] EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market.

92A Section 89(1a) is replaced by Section 70(1) of Act XXXII of 2025 he enrolled.
93A Section 89(2) in conjunction with Section 70(2) of Act XXXII of 2025 established text.
94A Section 91(1)(c) is the text amended by Section 72(b) of Act XXXII of 2025 .

(2) This Act a) repeals

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 communication technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (cybersecurity legislation),

b) the European Cybersecurity Industrial, Technology and Research Competence Centre and the national coordination centres Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing a network of

(c) lays down the necessary provisions for the implementation of Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience of the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) No 2016/1011.

Section 92. The draft of Section 70 is amended by Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market. prior notification pursuant to Article 15(7) of the Directive has been made.

54. Amending and repealing provisions

§ 93 [95]

Section 94 [96]

§ 95 [97]

Section 96 [98]

§ 97 [99]

§ 98 [100]

Section 99 [101]

Section 100 [102]

Section 101 [103]

Section 102 [104]

Section 103 [105]

§ 104 [106]

Section 105 [107]

Section 106 [108]

§ 107 [109]

Section 108 [110]

95A Section 93, Section 12(2) of Act CXXX of 2010 has lost its effect.
96A Section 94, Section 12(2) of Act CXXX of 2010 has lost its effect.
97A Section 95, Section 12(2) of Act CXXX of 2010 has lost its effect.
98A Section 96, Section 12(2) of Act CXXX of 2010 has lost its effect.
99A Section 97, Section 12(2) of Act CXXX of 2010 has lost its effect.
100A Section 98, Section 12(2) of Act CXXX of 2010 has lost its effect.
101A Section 99, Section 12(2) of Act CXXX of 2010 has lost its effect.
102A Section 100, Section 12(2) of Act CXXX of 2010 has lost its effect.
103A Section 101, Section 12(2) of Act CXXX of 2010 has lost its effect.
104A Section 102, Section 12(2) of Act CXXX of 2010 has lost its effect.
105A Section 103, Section 12(2) of Act CXXX of 2010 has lost its effect.
106A Section 104, Section 12(2) of Act CXXX of 2010 has lost its effect.
107A Section 105, Section 12(2) of Act CXXX of 2010 has lost its effect.
108A Section 106, Section 12(2) of Act CXXX of 2010 has lost its effect.
109A Section 107, Section 12(2) of Act CXXX of 2010 has lost its effect.
110A Section 108, Section 12(2) of Act CXXX of 2010 has lost its effect.

Section 109[111]

Section 110[112]

Section 111[113]

Section 112[114]

Section 113[115]

Section 114[116]

§ 115[117]

Section 116[118]

§ 117[119]

§ 118[120]

Section 119[121]

Section 120[122]

§ 121[123]

Section 122[124]

§ 123[125]

Section 124[126]

Section 125[127]

Section 126[128]

§ 127[129]

Section 128[130]

§ 129[131]

Section 130[132]

111A Section 109, Section 12(2) of Act CXXX of 2010 has lost its effect.
112A Section 110, Section 12(2) of Act CXXX of 2010 has lost its effect.
113A Section 111, Section 12(2) of Act CXXX of 2010 has lost its effect.
114A Section 112, Section 12(2) of Act CXXX of 2010 has lost its effect.
115A Section 113, Section 12(2) of Act CXXX of 2010 has lost its effect.
116A Section 114, Section 12(2) of Act CXXX of 2010 has lost its effect.
117A Section 115, Section 12(2) of Act CXXX of 2010 has lost its effect.
118A Section 116, Section 12(2) of Act CXXX of 2010 has lost its effect.
119A Section 117, Section 12(2) of Act CXXX of 2010 has lost its effect.
120A Section 118, Section 12(2) of Act CXXX of 2010 has lost its effect.
121A Section 119, Section 12(2) of Act CXXX of 2010 has lost its effect.
122A Section 120, Section 12(2) of Act CXXX of 2010 has lost its effect.
123A Section 121, Section 12(2) of Act CXXX of 2010 has lost its effect.
124A Section 122, Section 12(2) of Act CXXX of 2010 has lost its effect.
125A Section 123, Section 12(2) of Act CXXX of 2010 has lost its effect.
126A Section 124, Section 12(2) of Act CXXX of 2010 has lost its effect.
127A Section 125, Section 12(2) of Act CXXX of 2010 has lost its effect.
128A Section 126, Section 12(2) of Act CXXX of 2010 has lost its effect.
129A Section 127, Section 12(2) of Act CXXX of 2010 has lost its effect.
130A Section 128, Section 12(2) of Act CXXX of 2010 has lost its effect.
131A Section 129, Section 12(2) of Act CXXX of 2010 has lost its effect.
132A Section 130, Section 12(2) of Act CXXX of 2010 has lost its effect.

Section 131[133]

Annex 1 to Act LXIX of 2024

Organizations belonging to the public administration sector

For the purposes of this Act, the following organizations shall be considered to be organizations belonging to the public administration sector:

1. the central state administrative body, with the exception of the Government,

2. the Alexander Palace,

3. the Office of the Parliament,

4. the Office of the Constitutional Court,

5. the National Judicial Office and the courts,

6. prosecutors' offices,

7. Office of the Commissioner for Fundamental Rights,

8. the State Audit Office,

9. the Hungarian National Bank,

10. the Hungarian Armed Forces,

11. the capital and county government offices, the offices of the county assemblies,

12. offices of the representative bodies of cities with county rights and district municipalities of the capital,

13. offices of the representative bodies of the settlements,

14. the central service provider,

15. the organization exercising control over the central system.

Annex 2 to Act LXIX of 2024

133A Section 131, Section 12(2) of Act CXXX of 2010 has lost its effect.

2. **Service providers and organizations operating in high-risk sectors**

	THE	B	C
1	**Sector**	**Sub-sector**	**Organization type**
2	Energetics	Electricity	electricity industry according to the Electricity Act enterprise, except for the public lighting operating licensee,
3		District heating and cooling	Licensee under the District Heating Service Act,
4		Petroleum	according to the Mining Act a) establishing and operating a hydrocarbon pipeline licensee, b) a facility used in petroleum processing and storage operator,
5			on the safety stockpiling of imported crude oil and petroleum products central stockpiling organization pursuant to the Act,
6		Natural gas	– the one-stop capacity seller, the organized natural gas market except for the licensed and the pipeline LPG service provider – the Licensee under the Natural Gas Supply Act a natural gas industry enterprise,
7		Hydrogen	operator of hydrogen production, storage and transport,
8	Transportation	Air transport	on civil aviation security rules and On the powers, duties and responsibilities of the Aviation Defense Committee according to the government decree on the operation of an organization involved in the protection of aviation,
9		Rail transport	on forests, forest protection and forest management Annex 1 of Act XXXVII of 2009 economic according to except for companies, the Act on Railway Transport railway network operator – the railway network operator for its own purposes track networks, except for industrial sidings – the railway undertaking company, the railway capacity allocation organization,
10		Road transport	under the authority of the Road Traffic Act a) intelligent road traffic system according to the decree issued service provider operating systems, b) traffic control organization,
11		Water transport	shipping activity according to the Water Transport Act legal entity participating in the continuation of the a business entity with
12		Public transport	on public passenger transport services by rail and road, and Council Regulations 1191/69/EEC and 1107/70/EEC are in force 1370/2007/EC of 23 October 2007 on the exclusion of Regulation (EC) No 1072/2009 of the European Parliament and of the Council public service organization,
13	Healthcare		health care according to the Health Care Act service provider, high-security biological laboratories operator, managing medical reserves and blood supplies organization involved in the research and development of medicines organization, basic pharmaceutical products and pharmaceutical manufacturing organization, pharmaceutical wholesaler, public health emergency critical critical equipment on the list of critical assets medical device manufacturing organization,
14	Drinking water, wastewater	Water utility service	water utility service provider pursuant to the Act on Water Utility Services,
15	Information and communication services		a) according to the Electronic Communications Act electronic communications service provider, b) a service provider providing data exchange services,
16			on the digital state and the provision of digital services trust service provider pursuant to the Act on Certain Rules,
17	Digital infrastructure		the cloud provider,
18			data center service provider,
19			top-level domain name registrar,
20			the DNS provider,
21			content delivery network provider,
22	Outsourced ICT services		a) outsourced (directed) infocommunication service provider,

	THE	B	C
1	**Sector**	**Sub-sector**	**Organization type**
			b) outsourced (directed) infocommunication security service provider,
23	Space-based service		ground infrastructure supporting the provision of space-based services operator

Appendix 3 2 0 2 Year 4 LXIX. it's the law

3. **Service providers and organizations operating in risky sectors**

	THE	B	C
1	**Sector**	**Sub-sector**	**Organization type**
2	Postal and courier services		postal service provider pursuant to the Postal Services Act,
3	a) production, b) processing and c) distribution of food in accordance with 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		a food enterprise pursuant to the Act on the Food Chain and its Official Supervision, which is engaged in wholesale trade, industrial production and processing pursuant to Section 2, Point 18, of Act CLXIV of 2005 on Trade ,
4	Waste management		an economic entity carrying out activities pursuant to the Waste Act, Annex 1 to Act XXXVII of 2009 on Forests, Forest Protection and Forest Management except for business companies as defined in
5	Production and distribution of chemicals		manufacturer, distributor within the meaning of Article 3 of Regulation (EC) No 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH), establishing a European Chemicals Agency, amending Directive 1999/45/EC and repealing Council Regulation (EEC) No 793/93, Commission Regulation (EC) No 1488/94, Council Directive 76/769/EEC, Commission Directives 91/155/EEC, 93/67/EEC, 93/105/EC and 2000/21/EC,
6	Production	Manufacturing of medical devices and in vitro diagnostic medical devices	an organisation manufacturing medical devices as defined in point 1 of Article 2 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, and in vitro diagnostic medical devices as defined in point 2 of Article 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, with the exception of critical devices in a public health emergency a manufacturer of critical medical devices listed in the list, an economic entity carrying out the activity “Manufacture of computer, electronic and optical products” within the scope of sector 26 of Commission Delegated
7		Computer, electronic, optical product manufacturing	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 Rev. 2, an economic entity carrying out the activity “Manufacture of electrical equipment” within the scope of sector 27 2. an economic entity carrying out the activity "Manufacture of machinery and equipment" within
8		Electrical equipment manufacturing	the meaning 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 a system of
9		Manufacture of machinery and equipment n.e.c.	
10		Manufacture of motor vehicles, trailers and semi-trailers	an economic entity carrying out the activity "Manufacture of road vehicles" within the meaning of Section 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 on the establishment of the statistical classification of economic activities NACE Rev. 2, an economic entity
11		Manufacture of other transport equipment	carrying out the activity "Manufacture of other vehicles" within the meaning of Section 30 2. amending Regulation (EC) No 1893/2006 of the European Parliament and of the Council establishing a system (EU) of 10 October 2022
12		Cement, lime, gypsum production	

	THE	B	C
1	**Sector**	**Sector**	**Organizational type**
			2 0 2 3 / 1 3 7 with the authorization of the founding commission order 2 3.5 according to subsectlb6Cement, lime and gypsum production active person management organization,
13 Digital service providers			a) online marketplace provider, b) search engine provider pursuant to Act CVII I of 2001 on electronic commerce services and certain issues related to information society services , c) social media service platform provider, d) domain name registration provider,
14 Research			research center