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

On the implementation of the Cybersecurity Act of Hungary

Valid: 2025. 07. 04. – 2025. 07. 18.

The Government

Act LXIX of 2024 on the Cybersecurity of Hungary, Section 81 (1) b)–i) in Section 81, Paragraph (2) 2–6, 8–11., 15–18. and 21–25. Based on the authorization received in point 121,
Section 170 (1) Paragraph 7 of Act LXXXVI of 2007 on Electricity Based on the authorization received in point 122, Act CLV of 2009 on the
Protection of Classified Data, Section 37 c) pursuant to the authorization received in point 123 and 124 of Section 73 (1) of Act XCVII of 1995 on Air Transport, with regard to Sections 123 and 124, Based on the authorization received in point 125, Section 170 (1) of
Act LXXXVI of 2007 on Electricity, Section 24. Based on the authorization received in point 126, Section 131, Section 135 and Section 136 of Act
CXXX of 2010 on Legislation, Section 31 (1) b) based on the authorization received in point 127 of Act CXCV of 2011 on public finances, based on the
authorization received in point 15 of paragraph 1 of Section 109 of Act (1) of 2011 on public finances, in point 290 of paragraph 1 of Act CCXXXVII
of 2013 on credit institutions and financial enterprises, in point c) of Section 290 of Act CCXXXV of 2013 on certain payment service providers, in point 88 of Section a) of Act CCXXXV of 2013 on certain payment service providers in point 437. Section c) of Act LXXXVIII of 2014 on Insurance Activities and Act CXXXVIII of 2007 on investment firms and commodity exchange service providers and the rules on the activities they may carry out, Section 180 (1) a) Based on the authorization received in point 129, Section
110 (1) Paragraph 3 of Act CCIV of 2011 on National Higher Education. Based on the authorization received in point 130, Section 81 (2)
Paragraph 7 of Act LXIX of 2024 on the Cybersecurity of Hungary. Based on the authorization received in point 132, Section 21 (1) b) of Act
LXXXIII of 2014 on the uniform electronic card issuance framework Based on the authorization received in point 133, in accordance with Article 15(3) of the Fundamental
Law within its original legislative competence, with regard to Section 134, Section 12 b) of Act LVII of 2018
on the Control of Foreign Investments Prejudicial to the Security Interests of Hungary Based on the authorization received in point 137, in accordance with Article 15(3) of
the Fundamental Law within the original legislative competence specified in Section 138, Section 139 and
Section 140 of Act LXIX of 2024 on the Cybersecurity of Hungary, Section 81 (2) 19. Based on the authorization received in point 141, Section 206 (3c) a) and b)
of Act CLXXXV of 2010 on Media Services and Mass Communication Based on the authorization received in point 142, in accordance with Article 15(2) of the Fundamental Law
within the original legislative competence specified, with regard to Section 143, Section 110 (1) Paragraph
17 of Act CXL of 2021 on National Defence and the Hungarian Defence Forces. Based on the authorization received in point 10 of Section 81 (2) of Act
LXIX of 2024 on the Cybersecurity of Hungary, with regard to Section 144. Based on the authorization received in point 19 of Section 81 (2) of Act
LXIX of 2024 on the Cybersecurity of Hungary, with regard to Sections 145 and 146. Based on the authorization received in point 13 of Section 81 (2) of Act LXIX
of 2024 on the Cybersecurity of Hungary, with regard to Sections 147–150. Based on the authorization received in point 151, Section 132 , Section 50 of
Act XL of 2008 on Natural Gas Supply. Based on the authorization received in point 13 of Section 113 (1) of Act
CIII of 2023 on the Digital State and Certain Rules for the Provision of Digital Services, with respect to Section 152 . Based on the authorization received in point 11-13 of Section 113 (1)
of Act CIII of 2023 on the Digital State and Certain Rules for the Provision of Digital Services, with respect to Section 153 . pursuant to the authorization granted in paragraph 1 of Article
15 of the Fundamental Law Acting within its specific scope of duties, it orders the following:

Chapter I

GENERAL PROVISIONS

1. Scope

Section 1 (1)[1] The provisions of this Decree relating to the obligations of organisations and the regulatory supervision of cybersecurity – with the exception of paragraph (2) – are governed by Section 1(1)(a)–(c) of Act LXIX of 2024 on the Cybersecurity of Hungary (hereinafter referred to as the Cybersecurity Act). and point f), and Section 1(2a) shall apply to organizations as follows.

(2) The provisions of this Regulation concerning the person responsible for the security of the electronic information system are as follows: shall apply to organizations:

a)[2] Cybersecurity Act, Section 1 (1) a)–c) and f) and Section 1(2a) organizations,

b) to those organizations referred to in Section 1(1) (d) and (e) of the Cybersecurity Act, which are subject to the provisions of Act LXXXIV of 2024 on the Resilience of Critical Organizations (hereinafter referred to as the Act LXXXIV of 2024 on the Resilience of Critical Organizations) are designated as critical organizations under the Act on the Protection of Human Rights , or operate infrastructure designated as critical infrastructure (hereinafter collectively referred to as:

critical organization), and c) to organizations pursuant to Section 1(1)(d) and (e) of the Cybersecurity Act , which are subject to the provisions of Act XCIII of 2021 on the Coordination of Defense and Security Activities (hereinafter referred to as: Act XCIII of 2021 on the Coordination of Defense and Security Activities) have been designated as an organization significant for the protection and security of the country or have been designated by the World Bank. operate an infrastructure designated as significant infrastructure for the defense and security of the country (hereinafter collectively referred to as: an organization significant for the defense and security of the country).

(3) The provisions of this Regulation relating to cybersecurity practices and cybersecurity fines shall be implemented by: Cybersecurity Act, Section 1 (1) shall apply to organizations as follows.

(4) The provisions of this Regulation on cybersecurity certification shall apply to activities related to the certification of information and communication technology (hereinafter referred to as: ICT) products, ICT services or ICT processes (hereinafter referred to together as: ICT product).

(5) The provisions of this Regulation relating to vulnerability assessment a)

[3] Cybersecurity Act, Section 1 (1) a)–c) and f) and Section 1(2a) organizations according to electronic information systems, and b) with the

exceptions set out in the agreement, Article 61 of the Cybersecurity Act. electronic means specified in the agreement pursuant to § information systems

applicable to vulnerability assessments.

(6) The provisions of this regulation on cybersecurity incident management and cybersecurity crisis management are a) Section 1(1) of the Cybersecurity Act and (b) organisations covered by Regulation (EU) 2022/2554 of the European

Parliament and of the Council, with the derogations set out in this Regulation

should be used to handle cybersecurity incidents affecting electronic information systems.

(7) The provisions of this regulation relating to the management of vulnerabilities

a) Section 1(1) of the Cybersecurity Act discovered in connection with the electronic information systems of organizations vulnerabilities, and

b) are applicable to the management and reporting of vulnerabilities discovered in connection with the ICT product.

2. Interpretative provisions

2. § For the purposes of this

Regulation: 1. ***audit with administrator privileges:*** a security audit procedure in which the person conducting the audit has system administrator privileges and the purpose of the procedure is to fully check the status of all elements of the electronic information system concerned based on compliance lists; 2. ***application audit:*** a vulnerability assessment method in which the vulnerabilities of applications – including

desktop, mobile and web applications – are mapped using automated and manual testing methods; 3. ***automated vulnerability detection and analysis:*** a vulnerability assessment method in which the vulnerabilities of the organization's electronic information system are mapped and documented exclusively

using target software;

4. ***CSIRT:*** Computer Security Incident Response Team as defined in Directive (EU) 2022/2555 of the European Parliament and of the Council; 5. ***CSIRT Network:***

CSIRTs designated by the Member States of the European Union as defined in Directive (EU) 2022/2555 of the European Parliament and of the Council network established in accordance with the

directive; 1Section 1 (1) of Government Decree 189/2025. (VII. 3.) Section 16, point 1 Text amended accordingly.
2Point a) of Section 1 (2) of Government Decree 189/2025. (VII. 3.) Section 16, point 2 Text amended accordingly.
3Point a) of Section 1 (5) of Government Decree 189/2025. (VII. 3.) Section 16, point 3 Text amended accordingly.

6. ***single point of contact:*** a body designated by the Member States of the European Union to perform liaison functions pursuant to Directive (EU) 2022/2555 of the European

Parliament and of the Council; 7. ***European vulnerability database:*** a register of publicly known vulnerabilities in ICT products, established and operated by the European Union Agency for Cybersecurity (hereinafter: ENISA) pursuant to Directive (EU) 2022/2555 of the European Parliament and of the Council, containing a) information

describing the vulnerability, b) the ICT

product concerned and the severity of the vulnerability in terms of the circumstances under which the vulnerability could be exploited, c) the

availability of related fixes and, in the absence of a fix available, guidance issued by competent authorities or CSIRTs to users of vulnerable ICT products on how to mitigate the risks arising from the disclosed vulnerability; 8th ***alert:*** the Center has identified

a general threat to Hungarian cyberspace that deserves special attention.
information published on threats, new attack methods and events;

9. ***warning:*** a warning issued by the Center in the event of a threat, in cases where there is no
an ongoing cybersecurity incident or the cybersecurity incident was not critical;

10. ***incident management plan:*** a plan document for managing incidents, which, in parallel with the elimination of deficiencies, contains the tasks to be performed in order to prevent, detect, analyze and isolate incidents or to respond to the incident and restore operations after the incident, the milestones for completing the tasks, the related implementation deadlines, the designation of the person responsible for implementation and the resources required for this;

11. ***action plan:*** a plan document containing the tasks to be carried out in order to eliminate deficiencies, milestones for the completion of the tasks, the related implementation deadlines, the designation of the person responsible for implementation and the resources required for this, in order to fulfil the security measures determined in relation to the security class established for the electronic information system at the disposal of the organisation;

12. ***manual testing:*** a vulnerability testing method in which the vulnerabilities of the organization's electronic information system are mapped using queries individually compiled manually by the person conducting the test;

13. ***cybersecurity practice:*** ensuring the compliance of the organizational and tool system specified in the information security policy and a complex task performed to test its functionality;

14. ***cyber-physical systems security assessment:*** a vulnerability assessment method in which the vulnerabilities of cyber-physical systems are mapped by the person conducting the assessment, primarily using passive techniques and procedures, without negatively affecting the functional operation of the electronic information system, or with active means with continuous system monitoring support;

15. ***Centre:*** the national cybersecurity incident management

centre; 16. ***intermediary service provider:*** the provider of electronic commerce services and information society-related services concept under the Act on Certain Issues of Services;

17. ***external IT security audit:*** a vulnerability assessment method, during which, in relation to the elements of the electronic information system accessible from the Internet, free searches are carried out in public databases available on the Internet, targeted information collection is carried out, and the available services and vulnerabilities of the electronic information system are mapped;

18. ***psychological manipulation audit:*** a

vulnerability assessment method, during which attempts are made to influence people
based on which it is possible to obtain confidential information or to spread and operate malicious programs;

19. ***examination with registered user rights:*** a security examination procedure during which the person performing the examination carries out the examination with a user right created specifically for him/her;

20. ***examination without registered user rights:*** a security examination procedure during which the person performing the examination does not have any prior information about the electronic information system being examined and does not have user rights to the system;

21. ***alert:*** a warning requiring immediate action in widely used systems in order to interrupt an ongoing incident or series of incidents;

22. ***vulnerability risk classification: a risk***

rating determined according to the methodology used by the vulnerability assessor
risk analysis result; 23.

intentional incident: an incident caused by a deliberate unlawful or malicious act;

24. ***service provider register:*** the register of DNS service providers, top-level domain name registrars, organisations providing domain name registration services, cloud service providers, data centre service providers, content delivery network service providers, managed service providers and managed security service providers, as well as online marketplaces, online search engines and social media service platforms, maintained by ENISA pursuant to Directive (EU) 2022/2555 of the European Parliament and of the Council;

25. ***wireless network IT security analysis:*** a vulnerability assessment method in which wireless access and connection points are searched for and mapped, encryption procedures are analyzed, and the decryptability of encryption keys is checked using target software and manual testing.

Chapter II

OBLIGATIONS OF ORGANIZATIONS

3. Data classification

Section 3 (1) of the Cybersecurity Act. 9. An organization obliged to classify data according to § 1 shall classify the data based on the criteria specified in Annex 1.

(2) Prior to the decision of the head of the organization regarding the planned foreign data processing or non-private cloud use, a) Section 1(1)(a) of the Cybersecurity Act the organization has a cost-benefit analysis and an exit plan, b) [4] Section 1(1) (b) and (c) of the Cybersecurity Act, and with regard to its electronic information systems for national defense purposes, the organization referred to in point f) shall at least prepare an exit plan.

(3) Within the framework of the cost-benefit analysis, the organization examines and demonstrates the advantages and disadvantages of using a non-private cloud service compared to the currently used technology, and within the framework of the exit plan, it plans the steps, consequences and cost implications of reverting from the use of the cloud service to the local environment or the use of a private cloud.

(4) Section 1(1)(a) of the Cybersecurity Act The head of the organization may decide to use foreign data processing or non-private cloud services if, based on the results of the cost-benefit analysis and the exit plan, the use of foreign data processing or non-private cloud services provides substantiated benefits to the organization.

(5) The organization shall announce the results of the data classification within the framework of the notification of the results of the security classification. to the national cybersecurity authority (hereinafter referred to as: national cybersecurity authority) pursuant to Section 16(1).

4. Provisions on protective measures

Section 4 (1) When defining and assessing the adequacy of security measures, the organisation shall take into account, where available, the results of coordinated security risk assessments carried out by the European Commission and ENISA in relation to critical supply chains.

(2) If the organization or the auditor identifies a deficiency during the assessment of the security measures related to the security class of the given electronic information system during the cybersecurity audit, the organization shall, within 90 days of receiving the results of the investigation or cybersecurity audit, prepare an action plan to eliminate the deficiency, which shall be submitted to the national cybersecurity authority for approval.

5. Security classification review

Section 5 (1) The organization shall review the security classification without delay if there is a change in the risk environment of the electronic information system or in the data classification.

(2) The organization shall send the results of the security classification review to the national cybersecurity authority within 15 days. for the authority.

6. Review of the information security policy

§ 6. The organization shall review and amend the information security policy without delay.

4A Section 3(2)(b) of Government Decree 189/2025. (VII. 3.) Section 16(4) Text amended accordingly.

a) in the event of a change that affects the security, confidentiality, or availability of the electronic information system,
integrity or the service provided by the organization, b) in order to
manage the newly emerging risk, if the cybersecurity incident or incident-related incident has occurred
the risk associated with the situation was not examined during the risk analysis,
c) based on deficiencies identified during the inspection, cybersecurity audit or cybersecurity exercise, as required by the national cybersecurity authority.

Section 7, Section 8 (7) of the Cybersecurity Act under cybersecurity information sharing agreements under
When sharing information, organizations act in a manner that respects the sensitive nature of the information.

7. Cooperation with the national cybersecurity authority

Section 8 (1) The organization shall comply with its notification and data provision obligations electronically in a format specified and published by the national cybersecurity authority – the national defense cybersecurity authority in the case of electronic information systems for national defense purposes – and shall simultaneously send the documents verifying the notified data.

(2) Section 8(4)(f) of the Cybersecurity Act within the framework of the notification, the organization sends the national cybersecurity authority the result of the
a[5] classification of the electronic information system into the security class, if it is obliged to implement it,
b) the protective measures determined based on the security class, including substitute protective measures, c) the assessment of the
adequacy of the protective measures according to point ab), and d) the current status of the
protective measures according to point ab).

Section 9 (1) In the event of the termination of the organization by legal succession, the legal successor shall be obliged to register within 15 days following the change. to notify the legal succession to the national cybersecurity authority for the purpose of acquisition.

(2) The organization shall notify the national authority of its termination without legal succession – no later than the date of termination.
for the cybersecurity authority.

(3) If the national cybersecurity authority becomes aware of the termination of an organization without legal succession, it shall take steps ex officio to record the fact of termination in the register.

8. Cybersecurity practices

Section 10 (1) Section 1 (1) of the Cybersecurity Act organization pursuant to
a) if the Cybersecurity Act, Section 1 (4) is considered a core organization, conducts a cybersecurity exercise
every two years, b) upon the obligation of
the Center or c) upon the obligation of the national cybersecurity
authority, independently or under the direction of the Center.

(2) The organization shall involve the electronic information system in the conduct of cybersecurity exercises, as necessary.
its collaborators involved in its operation and the provision of related services.

(3) The organization shall conduct the training independently or may use a collaborator for this purpose.
The Center defines a methodology for conducting independently organized internships, which it publishes on its website.

(4) The organization shall submit an evaluation report on the independently conducted exercise to the Center within 30 days of the exercise, based on the methodology published on the Center's website. The report shall include at least the exercise scenario, participants, events that occurred, and an evaluation of the effectiveness of the exercise.

(5) The Centre shall assess the adequacy of the exercise. If the Centre identifies deficiencies during the exercise or based on the report submitted on the exercise conducted independently, the national cybersecurity authority shall notify it based on its indication – Section 1(1)(d) and (e) of the Cybersecurity Act - may oblige the head of the organization to modify the inadequate security measures and the organization to repeat the exercise.

(6) In the case of the obligation under points b) and c) of paragraph (1), the organization's participation in cybersecurity exercises is mandatory.

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

Section 11 (1) The person responsible for the security of the electronic information system shall perform his/her duties in accordance with the needs of the organization and its shall be provided according to its provisions.

(2) The head of the organization shall appoint or delegate the person responsible for the security of the electronic information system.

5A Section 8(2)(a) of Government Decree 189/2025. (VII. 3.) Section 16(5) Text amended accordingly.

a) first verify its compliance with legal requirements, b) subsequently notify the national cybersecurity authority for registration, simultaneously sending documents verifying the notified data.

(3) The notification of the person responsible for the security of the electronic information system shall include the sending to the authority of a copy of the relevant employment contract, mandate or other agreement in such a way that only the information relevant to the authority and necessary for the performance of its tasks and powers can be obtained from it. A copy of the document certifying the education and training of the given person, or a document certifying the professional practice or declaration shall be attached to the agreement.

(4) The agreement on the person responsible for the security of the electronic information system shall include at least the following: must include:

a) data suitable for identifying the contracting parties, b) for identifying the natural person performing the duties of the person responsible for the security of the electronic information system suitable data, c) the subject of the assignment,

d) the rights and obligations of the parties in accordance with the provisions of the applicable laws.

(5) The head of the organization shall certify the clean record of the person responsible for the security of the electronic information system in the manner determined by the national cybersecurity authority or, in the case of electronic information systems for national defense purposes, by the national defense cybersecurity authority.

(6) The head of the organization may oblige the person responsible for the security of the electronic information system to prove compliance with the requirement of a clean criminal record during the legal relationship with the organization.

Section 12 (1) The person responsible for the security of the electronic information system shall be entitled to proceed before the national cybersecurity authority within the scope of this responsibility after being registered by the national cybersecurity authority, and shall be considered a person entitled to represent until the termination of his/her right of representation is notified or until he/she is removed from office by the national cybersecurity authority.

(2) The person responsible for the security of the electronic information system

a) ensures that activities related to the security of the organization's electronic information systems comply with legal requirements on creating and maintaining harmony between

b) ensures the planning, organization and coordination of activities according to the risk management framework, carrying out and checking,

c) prepares and, after approval by the head of the organization, sends the organization's information security policy to the national cybersecurity authority, d) prepares the classification of the organization's electronic information systems into security classes, e) prepares and, with the consent of the head of the organization, initiates the organization's application to the national cybersecurity authority authorization procedures related to its electronic information systems,

f) holds or organizes further training courses prescribed by law for persons obliged to undergo further training, g) gives an opinion on the organization's electronic systems from the point of view of the security of electronic information systems. its information security policies and contracts,

h) conducts continuous and planned inspections to examine how the requirements of the organization's internal standards for electronic information security are implemented, and records the findings in writing for the organization's manager, i) reviews whether the organization's internal regulations for electronic information security are in accordance with the applicable with laws and the organization's internal regulations,

j) using the experience of inspections and possible incidents – make suggestions for areas for development – prepares a security situation assessment for the organization's leader,

k) the head of the organization shall examine the action plan referred to in Section 4(2) at least annually and prepare a report on progress, highlighting any delays and measures required in the short term, l) maintains contact with the national cybersecurity authority and the cybersecurity incident management center, m) informs the body specified in this regulation about any incident affecting the organization's electronic information system, n) cooperates with the Kszetv. with the manager responsible for the resilience of the critical organization according to the Vbö. resistant according to with a manager responsible for capability.

(3) If the duties of the person responsible for the security of the electronic information system are performed by a person outside the organization, he or she must perform his or her duties in a documented manner, physically present at the organization concerned, at least one day every two months for essential organizations and at least one day every three months for important organizations.

10. Procedure to be followed in the case of development and further development of an electronic information system

Section 13 (1) In contracts for the development and further development of the electronic information system (hereinafter collectively referred to as: development), the organization shall specify the conditions for the developer to repair the vulnerabilities discovered during the vulnerability assessment.

(2) In the case of the development of an electronic information system, the organization shall submit the results and justification of the data classification and classification carried out during the design life cycle to the national cybersecurity authority – the national defense cybersecurity authority in the case of an electronic information system for national defense purposes – on the form and annexes published on its website.

(3) The national cybersecurity authority may override the data classification and security level assignment and, in justified cases, You can also determine a higher or lower level classification.

(4) The head of the organization ensures that the security requirements related to the security class are met during development. be realized.

(5) During development, the organization shall

review a) the data classification, if it is among the data to be managed in the electronic information system, and b) the

security classification, if it is within the risk environment of the electronic information system. change occurs.

(6) The organization shall submit the classification obtained as a result of the review to the national cybersecurity authority for approval. When examining the security classification, the national cybersecurity authority shall proceed in accordance with Section 30.

Section 14 (1) The organization shall apply for approval by the national cybersecurity authority of the decision made by the head of the organization regarding the introduction of an electronic information system or the continued use of an existing electronic information system, using a form published on the website of the national cybersecurity authority – or, in the case of an electronic information system for national defense purposes, the national cybersecurity authority.

(2) The application must include the expected protective measures resulting from the security classification. all documentation prepared for its implementation.

(3) The national cybersecurity authority shall grant its approval if it is satisfied that the electronic information system concerned meets all the required cybersecurity criteria and shall register the electronic information system at the same time. Otherwise, the authority shall call for the deficiencies to be filled, the deficiencies to be corrected and the deficiencies to be filled and may prohibit the use and further use of the electronic information system.

11. Provisions governing central systems and central services

Section 15 (1) If the user organization uses a central service related to the electronic information system at its disposal, it shall send the electronic information system to the central service provider.

a) name,

b) security department,

c) brief description of function, and

d) the following data of the designated contact persons – including the data controller, the person responsible for operations and the person responsible for the security of the

electronic

information

system: da) name, db) position, dc) e-mail address and telephone number suitable for contact.

(2) The organisation exercising the right of disposal over the central system or the central service provider shall consult the national cybersecurity authority in advance in order to determine the qualification as a central system, supporting system or central service. The national cybersecurity authority may involve the user organisations in the consultation.

(3) The service provider shall record in its service catalogue the name of the central service and whether a) the service

provided by it is a central service, central system, support system or other is considered a service,

b) what security class requirements the central service or support system can provide, c) what security class requirements the electronic

information systems implementing the central service meet.

(4) In the case of a central service provided jointly by several service providers, the service providers shall set out in an agreement the limits of liability for the parts of the service provided by them, as well as the protective measures provided by the given part of the service.

Chapter III

AUTHORITY SUPERVISION OF CYBERSECURITY

12. General provisions on the national cybersecurity authority

Section 16 (1) The Government a) Section 23 (1) a) of the Cybersecurity Act as the national cybersecurity authority pursuant to, and b) Act CVIII of 2001 on certain issues of electronic commerce services and services related to the information society (hereinafter: Ekertv.) 15/B. The National Security Service is designated as the authority pursuant to §.

(2) The Government shall, pursuant to Section 23(2) of the Cybersecurity Act as the national defense cybersecurity authority for national defense appoints a responsible minister. 6 (3)

The provisions applicable to the national cybersecurity authority shall apply to the activities of the national defense cybersecurity authority, with the exception of those contained in Section 17(1)(e), Section 18(e), Section 25, Section 30(6), and Section 39(3) and (4).

Section 17 (1) The national cybersecurity authority is entitled to a) verify the security classification, the security measures and the compliance with the related procedural rules, b) determine the minimum required security measures, c) determine additional security requirements in addition to the security measures belonging to the security class determined by the organization, d) request information necessary for the assessment of the cybersecurity risk management measures adopted by the organization – including documented cybersecurity policies – and for the assessment of compliance with the obligation to report information,

e)[7] Section 1(1)(b) of the Cybersecurity Act in the case of an organization that is also a member of the Cybersecurity Act. 2. and Annex 3 organization, to access and request the evidence supporting the audit report produced as a result of the cybersecurity audit, and to review its content,

f) conduct regular, ad hoc and targeted security checks, including on-site inspections, remote monitoring measures and random checks,

g) access and request data, documents and information necessary for the performance of its supervisory duties, and to order a review of the documents sent,

h) to use an independent assessor during its procedure – with the exception of national defence electronic information systems – and to take into account the results of the audit carried out by him, as well as the contents of the independent assessment report commissioned by the organisation or the cybersecurity audit report, i) to take into account the security certificates issued to electronic information systems and devices, organisations on the basis of international conventions or international standards, or on the basis of domestic requirements or recommendations based on these, j) to consider compliance with the cybersecurity requirements specified by a European Union legal act as compliance, in whole or in part, with the security requirements specified in the decree of the minister responsible for IT,

k) to order the necessary measures to eliminate the deficiencies identified during the inspection and to monitor their implementation, l) to issue guidelines for the application of standards, the use of ICT products certified by European or domestic cybersecurity certification systems, and the use of qualified trust services in relation to the organizations under its supervisory authority,

m) the introduction of electronic information systems, the use of existing electronic information systems to conduct an on-site inspection and order a vulnerability assessment when approving its further use,

n) upon request from the Centre, order the necessary measures to eliminate the vulnerability reported in relation to the organisation's electronic information system, monitor their implementation, and order a vulnerability assessment based on individual considerations.

6A Section 16(3) of Government Decree 189/2025 (VII. 3.) Section 16(6) Text amended accordingly.
7A Section 17(1)(e) of Government Decree 189/2025. (VII. 3.) 1. Text established by §.

(2) If the national cybersecurity authority, in the course of its official activities, obtains information a) from the organization, b) from the organization exercising authority, supervision or control over the organization, c) from public registers and d) from the body performing the data processing requests data in the context of clarifying the facts, the requested organization or body will provide it free of charge.

Section 18. In performing its tasks, the national cybersecurity authority shall cooperate in the field of electronic information security with a) the cybersecurity incident management centers, b) the cybersecurity certification authority, c) the National Cybersecurity Act. with the appointing authority and the specialized authority pursuant to the Act, d) with the Act. with the designating authority and the specialist authority pursuant to Regulation (EU) 2022/2554 of the European Parliament and of the Council, f) with the law enforcement agencies, g) with the national security services, h) with the military cyberspace operations forces, i) with the National Media and Communications Authority, j) with the National Data Protection and Freedom of Information Authority, k) with the cybersecurity supervisory authorities of the Member States of the European Union or third countries, and l) with the competent authorities of other Member States.

8 Section 18/A as an organ The Government of the Cybersecurity Act, Section 24 (9) food chain surveillance company providing data according to a) designates the National Food Chain Safety Office and b) the National Trade and Consumer Protection Authority.

§ 19 If the organization notifies the national cybersecurity authority of a significant cybersecurity incident, the national cybersecurity authority shall forward the notification to the Center upon receipt.

Section 20 (1) The national cybersecurity authority and the Cybersecurity Act. (a) exchange information, as necessary, on the designation of critical entities, non-cybersecurity risks, threats and incidents affecting essential entities designated as critical entities, on the measures taken in response to those risks, threats and incidents, and on non-cybersecurity risks, threats and incidents, including cybersecurity and physical measures implemented by critical entities, and on the results of oversight activities carried out with respect to such entities,

b) the national cybersecurity authority informs the competent authority of the Cybersecurity Act. authority under the Act on the Protection of takes an official supervisory measure against a critical organization designated pursuant to Directive (EU) 2022/2555 of the European Parliament and of the Council, c) pursuant to the Act on the Protection of Human Rights and Fundamental Freedoms. The authority may make a request to the national cybersecurity authority in order to exercise its authority powers and take measures pursuant to the Cybersecurity Act. in order to ensure compliance with Directive (EU) 2022/2555 of the European Parliament and of the Council in the case of a critical organisation designated as such.

(2) The national cybersecurity authority and the Vbö. shall act in accordance with paragraph (1) within the framework of the cooperation of the designating authority under regarding organizations important for the defense and security of the country.

(3) The national cybersecurity authority shall, in the framework of cooperation with the authority pursuant to Regulation (EU) 2022/2554 of the European Parliament and of the Council, inform the oversight forum established pursuant to Article 32(1) of Regulation (EU) 2022/2554 of the European Parliament and of the Council when it takes an official supervisory measure in order to ensure compliance with the Cybersecurity Act. essential organisations covered by the Directive and designated as critical third-party ICT service providers pursuant to Article 31 of Regulation (EU) 2022/2554 of the European Parliament and of the Council shall comply with Directive (EU) 2022/2555 of the European Parliament and of the Council.

(4) The National Defense Cybersecurity Authority and the Vbö. within the framework of cooperation with the national defense sectoral designating authority according to (1) shall act in accordance with paragraph.

8A 18/A. §-ta 189/2025. (VII. 3.) Government Decree 2. § was introduced.

Section 21 (1) Where an organisation provides services in more than one Member State of the European Union, or provides services in one or more Member States of the European Union and its network and information systems are located in one or more other Member States of the European Union, the national cybersecurity authority shall cooperate, as necessary, with the competent authority of the other Member State. In the framework of the cooperation, the national cybersecurity authority may: a) inform

the data subject of the supervisory measures it applies, through the single point of contact;

the competent authority of a European Union Member State,

b) may request the competent authority of another European Union Member State to take supervisory measures, c) upon

receipt of a reasoned request from a competent authority of another European Union Member State, it shall provide mutual assistance to the requesting authority, in a manner proportionate to its own resources, in order to ensure that the supervisory measures can be implemented efficiently, effectively and consistently.

(2) The national cybersecurity authority may not refuse a request unless it determines that it does not have the competence to provide the requested assistance, the requested assistance is not proportionate to the supervisory tasks of the national cybersecurity authority, or the request concerns information or involves activities the disclosure or implementation of which would be contrary to the essential interests of national security, public security or defence of Hungary. Before refusing a request, the national cybersecurity authority may consult other competent authorities, as well as the European Commission and ENISA.

(3) The national cybersecurity authority may, by mutual agreement, implement joint supervisory measures with other European

with the competent authorities of EU Member States.

13. Official procedure of the national cybersecurity authority

Section 22 (1) In the procedures of the national cybersecurity

authority, a) the submission of the application at the government

window is excluded, b) a request to remedy deficiencies twice is allowed, with the exception set out in paragraph (2).

(2) The national cybersecurity authority shall refrain from repeated remediation if the remediation would be carried out with regard to the same deficiency in relation to the same organization.

(3) The national cybersecurity authority may consult with the organization before making a decision concluding its procedure.

Section 23 (1) The national cybersecurity authority shall initiate an official procedure in the event of a cybersecurity incident if a) the

cybersecurity incident was reported by the organization independently or pursuant to Section 70 (3) b) of the Cybersecurity Act, based on a report from the Center. point could not resolve it by using a business organization according to

b) the size of the cybersecurity incident and the value of the damage caused by the incident justify this,

c)[9] initiated by the Center.

(2) The national defense cybersecurity authority shall initiate an official procedure to investigate the cybersecurity incident of which it has become aware.

Section 24. The national cybersecurity authority may decide on the deletion of essential or important organizations from the register

a) ex officio or b) at

the request of the organization concerned.

Section 25 (1) The person concerned may request inclusion in the register of persons capable of performing the duties of the person responsible for the security of the electronic information system from the national cybersecurity authority, using a form published on the authority's website, if he or she complies with the Cybersecurity the conditions set out in the Act and this decree.

(2) The application pursuant to paragraph (1) shall contain the following personal identification data of the natural person responsible for the security of the electronic information system: a) his/her identification data, b) his/her electronic

mail address, c)

[10] data and documents used to verify the qualifications required by the decree of the Minister responsible for IT, the professional qualifications published by the national coordination center pursuant to Section 105, accredited international qualifications, or professional experience acquired in the field specified in the decree of the Minister responsible for IT.

(3) If the natural person responsible for the security of the electronic information system is the Cybersecurity does not meet the conditions set out in the Act and this Regulation, the national cybersecurity authority shall reject the application for registration. The applicant may not submit a new application for registration within 90 days after the authority's decision becomes final.

9A Section 23(1)(c) of Government Decree 189/2025. (VII. 3.) Section 16(7) Text amended accordingly.
10A Section 25(2)(c) in conjunction with Section 3(1) of Government Decree No. 189/2025 (VII. 3.) established text.

(4) Following registration, the national cybersecurity authority shall publish on its website the name and electronic mail address of the natural person responsible for the security of the electronic information system.

(5) The natural person responsible for the security of the registered electronic information system must continuously comply with the Cybersecurity Act. Section 11 (3) and (8) in paragraph, and the conditions set out in this Regulation.

(6) The natural person responsible for the security of the electronic information system shall report any change in the reported data to the national cybersecurity authority for registration within 15 days of its occurrence.

(7) The national cybersecurity authority shall delete from the register the person responsible for the security of the electronic information system. a natural person a) at
their request, or b)
in accordance with Section 11 (3) of the Cybersecurity Act in case of non-compliance with specified conditions.

(8) The national cybersecurity authority may remove from the register the person responsible for the security of the electronic information system. a natural person, if
[11] Section 11 (8) of the Cybersecurity Act does not fulfill his/her obligation to undergo further training,
a) b) fails to comply with the obligation under Section 12(3), or c) the
Cybersecurity tv. and this decree.

14. Procedure for identification as an essential or important organization

Section 26 (1) The national cybersecurity authority shall examine the possibility of identification as an essential or important organization if a) the Cybersecurity
Act. the organization was not designated as a critical organization, and the Cybersecurity as defined in the Act
Compliance with identification criteria is likely,
b) the Vbö. Based on this, the organization was not designated as an organization significant for the protection and security of the country, and the Cybersecurity Compliance with the identification criteria specified in the Act is likely,
c) the organization or facility is subject to national security protection, or d) the
identification is based on data from the national cybersecurity authority, vulnerability assessment, incident assessment or the Center
the need arose.

(2) If the Act No. as a critical organization, and the Vbö. based on the procedure for designating an organization as a significant organization for the defense and security of the country, the organization has not been designated as a critical organization or as a significant organization for the defense and security of the country, or the designation is revoked, the Act on the Protection of the Environment, and the Vbö. The designating
authority shall inform the national cybersecurity authority of this decision.

(3) If the conditions for identification are met, the national cybersecurity authority shall initiate a procedure in which it shall inform the organization concerned: the data that it meets the criteria for identification as an essential or important organization.

(4) If the organization agrees with the content of the order initiating the procedure, it shall inform the national cybersecurity authority thereof within 20 days.

(5) If the organization disagrees with the content of the order initiating the procedure, it shall send its detailed reasoned opinion to the national cybersecurity authority within 20 days. The detailed reasoned opinion shall include:
organization

a) a detailed description of the service provided by,
b) a list of electronic information systems contributing to the provision of the service, their role and importance in the provision of the service, c) their
contribution to the provision of other services, and d) the Cybersecurity data
relevant to the determination of the criteria specified in the Act on the identification of an essential or important organization.

(6) The national cybersecurity authority shall process the information sent by the relevant organization in accordance with Section 1(6) of the Cybersecurity Act. In its substantive decision concluding the official procedure, the competent authority, considering the criteria set out in the text, shall decide on the identification or non-identification as an essential or important organization.

Section 27 (1) The national cybersecurity
authority shall: a) at least
every three years, b) at the request of the essential or important organization
upon its termination, or c) in view of a change notified by the essential or important organization
review the circumstances giving rise to the identification.

11A Section 25(8)(a) of Government Decree 189/2025. (VII. 3.) Section 17(a) Text amended accordingly.

(2) Depending on the outcome of the review, it shall maintain or withdraw its decision on identification.

Section 28. The identified essential or important organization shall promptly notify the national cybersecurity authority if there is a change in its operating conditions that affects or may affect its essential or important organization status.

15. Data classification analysis

Section 29 (1) The national cybersecurity authority shall evaluate the result of the data classification within the framework of a procedure aimed at examining the justification of the security classification in order to determine the legality of the use of non-private cloud services and the processing of data abroad.

(2) If the classification according to the data classification is not clear based on the results of the investigation, the national cybersecurity authority shall clarify within the framework of the procedure what kind of data the organization processes or plans to process in the electronic information system and what amount of data it processes.

(3) If the national cybersecurity authority does not agree with the result of the data classification, it may oblige the organization to:
for reviewing and repeating data classification.

(4) If, based on the results of the investigation, the scope of the data managed or planned to be managed in the electronic information system indicates that their management abroad or the use of non-private cloud services in relation to them is not possible as set out in Annex 1, the national cybersecurity authority shall not approve the use of the electronic information system.

16. Security classification examination

Section 30 (1) The examination of the security classification of electronic information systems shall be carried out by the national cybersecurity is carried out based on information sent to the authority, according to criteria specified in law.

(2) If the declared security classification of an electronic information system – including the action plan to eliminate the deficiencies identified in determining the security classification of the given electronic information system – is approved by the national cybersecurity authority, the decision to this effect shall not preclude a subsequent independent review of the security classification or a review of the security classification during an inspection of the organisation or organisational unit concerned.

(3) The national cybersecurity authority may override the security class determined by the organization and, with justification, may also determine a higher security class.

(4) If, during its procedure, the national cybersecurity authority determines a security class for the electronic information system that is higher than the security class determined and declared by the head of the organization, the class corresponding to the decision of the national cybersecurity authority shall be taken as the basis for applying the deadline for achieving the requirements of the next security class.

(5) If the national cybersecurity authority sees the possibility of applying a lower class than the declared security class for the electronic information system, it shall make a proposal to the organization.

(6) [12] The national cybersecurity authority may oblige the Cybersecurity Act. Section 1 (1) b) organization, which is also the Cybersecurity TV. Annex 2 or 3 is subject to the review and modification of the security class of the electronic information system if, during the conduct of the cybersecurity audit, the auditor recorded an “inadequate” assessment as a result of examining the adequacy of the security class established by the organization.

17. Annual audit plan of the national cybersecurity authority

Section 31 (1) The annual audit plan shall be compiled by the national cybersecurity authority by 30 November of the year preceding the year in question, following a preliminary risk assessment, and may involve the National Cybersecurity Authority in its compilation. the appointing authority and the Vbö. appointing authority.

(2) The national cybersecurity authority shall evaluate the implementation of the annual audit plan by 1 March of the year following the year in question.

(3) The national cybersecurity authority shall review the annual audit plan during its implementation and amend it as necessary. (4)
[13] The national cybersecurity authority may deviate from the provisions of the audit plan if it needs to conduct immediate audits or procedures that serve to prevent serious cybersecurity incidents threatening Hungarian cyberspace, national electronic data assets, and electronic information systems of paramount importance to the state and citizens.

12 Section 30(6) is amended by Government Decree 189/2025. (VII. 3.) 4. § was introduced.

13A Section 31(4) of Government Decree 189/2025. (VII. 3.) Section 16, point 8 Text amended accordingly.

(5) The national defense cybersecurity authority requests data from the Vbö to compile its annual audit plan . from the national defence sectoral designating authority pursuant to paragraph 1. The annual audit plan of the national defence cybersecurity authority, as well as the amendment pursuant to paragraph 3, shall be approved by the minister responsible for national defence.

18. General rules of official control

Section 32 (1) The national cybersecurity authority shall conduct
inspections a) based on the annual inspection
plan, or b) on an
ad hoc basis.

(2) The national cybersecurity authority may conduct an extraordinary inspection if it is justified by the occurrence of a significant cybersecurity incident, the threat thereof, or the violation of legal requirements by the organization, and if it becomes aware of a fact or circumstance that justifies it.

Section 33 (1) The national cybersecurity authority shall notify the head of the relevant organisation of the order for an inspection by electronic means at least ten days before the commencement of the inspection. The notification shall include the purpose and subject of the inspection, the circumstances giving rise to the order, the reference to the legal provisions on which the order is based, the expected duration of the inspection and the method of the inspection.

(2) The notification referred to in paragraph (1) may be
omitted if a) there is a serious threat,
b) a significant cybersecurity incident has
occurred, c) the occurrence of the circumstances referred to in points a) or b) is likely, or
d) the relevant organisation would likely, based on the available data, frustrate the successful conduct of the inspection.

(3) The national cybersecurity authority shall issue a letter of authorization to its employee performing the inspection.

Section 34 (1) In the course of its proceedings, in order to perform its duties, the national cybersecurity authority shall be entitled, independently or together with another authority, to:

a) enter the premises of the organization concerned related to its information technology activities, b) provide
data management for the organization concerned, perform data processing or are involved in information technology matters
to monitor the locations,

c) during the inspection, to examine and inspect any document, contract, active or passive device, information system, or security measure related to electronic information security, to make copies of the documents, contracts, or security measures related to electronic information security, and

d) perform information technology technical inspections, with individually granted access rights to the information technology system.

(2) In the interest of the security of electronic information systems and the data processed therein, the national cybersecurity authority is entitled to monitor all measures relating to the protection of electronic information systems that can address threats to the electronic information system concerned.

(3) The inspection may not result in the discovery of data relating to the secret information gathering work, the use of covert means and the persons cooperating in it, as well as the means and methods of secret information gathering and the use of covert means.

Section 35 (1) The head, staff member, employee of the organization affected by the inspection, or any other person involved in electronic information security based on a contractual relationship and responsible for the security of the electronic information system, shall be obliged to cooperate with the national cybersecurity authority.

(2) The person responsible for the security of the electronic information system shall be required to participate in the inspection.

(3) The organization is obliged to submit the documents requested by the national cybersecurity authority in an orderly and transparent form.

Section 36. The national cybersecurity authority shall prepare a report on the inspection, which shall be sent to the organization for comments in writing within 15 days of the conclusion of the inspection. The organization may make written comments in this regard within 15 days – the authority is not bound by them. In order to clarify the comments, the national cybersecurity authority may initiate a consultation with the organization.

19. Legal consequences

Section 37 (1) In order to meet the information security requirements, the national cybersecurity authority shall – while setting an appropriate deadline – call on the head of the organization to eliminate any deficiencies, omissions or violations of security requirements that endanger electronic information security, to fulfill the obligations specified in law, and to take the required measures.

(2) The national cybersecurity authority shall oblige the relevant organisation to take immediate measures if the deficiency or omission endangering electronic information security or the breach of a security requirement threatens to result in a serious cybersecurity incident. In this context, it may propose disciplinary action against the person exercising the employer's authority.

(3) Upon notification of the incident management center, the national cybersecurity authority shall, while setting an appropriate deadline, call on the organization or intermediary service provider to cease the unlawful activity or unlawful state, and in this context, to fulfill its obligation to report, provide data and cooperate.

(4) Until the expiry of the time limit for filing an action to challenge the official decision, or in the case of filing an administrative lawsuit, the Until a final court decision is made, the data affected by the disputed legal violations cannot be deleted or destroyed.

Section 38 (1) When applying legal consequences, the national cybersecurity authority shall take into account the following aspects: a) the severity of the deficiency or omission that endangers electronic information security, the breached security requirement, b) the duration of the breach, c) whether a significant cybersecurity incident or large-scale cybersecurity incident has occurred, or whether such an event has existed the risk of its occurrence, d) the impact or potential impact of the incident on the affected organisation or other organisations, e) any material or non-material damage caused, including any financial or economic loss, the impact on other services and the number of users affected, f) the unique or repeated nature of the event, g) any relevant infringements committed by the affected organisation in the past, h) any intent or negligence of the perpetrator of the infringement, i) the conduct of the affected organisation, the measures taken by the organisation to prevent or mitigate the material or non-material damage any measures, j) whether approved codes of conduct or approved certification mechanisms have been complied with, k) the level of cooperation with the competent authorities of the natural or legal persons held responsible, and l) the effectiveness, proportionality and dissuasiveness of the legal consequence envisaged.

(2) The following shall be considered serious infringements: a) repeated infringements; b) failure to report or remedy significant incidents; c) failure to remedy deficiencies following binding instructions from the competent authorities; d) obstruction of inspections or control activities ordered by the competent authority after the infringement has been established; e) communication of false or seriously inaccurate information.

Section 39 (1) Section 1 (1) b) of the Cybersecurity Act and at the same time the Cybersecurity Act. 2. and Annex 3 In the case of an organization that qualifies as an organization under the Cybersecurity Act. 7. §, § 8. Subsection (5) and 16. In case of non-fulfillment or non-fulfillment of the provisions pursuant to §, the SZTFH may contact the national cybersecurity authority in order to take supervisory measures.

(2) The national cybersecurity authority shall inform a) the Cybersecurity Act. or b) the appointing authority under the Vbö. the designating authority, if measures are taken or legal consequences are applied to an organization within their supervisory authority beer.

(3) The national cybersecurity authority shall inform the National Authority for Data Protection and Freedom of Information without undue delay if, in the course of performing its tasks, it becomes aware of a breach by the organisation which has or may result in the infringement of personal data, as defined in Article 4(12) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [hereinafter: Regulation (EU) 2016/679 of the European Parliament and of the Council] and the organisation has not reported the data protection incident to the National Authority for Data Protection and Freedom of Information.

(4) If the supervisory authority competent under Regulation (EU) 2016/679 of the European Parliament and of the Council is located in another EU Member State, the national cybersecurity authority shall inform the National Data Protection and Freedom of Information Authority of the potential personal data breach referred to in paragraph (3).

(5) If the National Data Protection and Freedom of Information Authority imposes a fine for a violation, the national cybersecurity authority shall not impose a fine for a violation resulting from the same conduct, but may apply a different legal consequence in justified cases.

20. The Information Security Supervisor

Section 40 (1) The national cybersecurity authority shall appoint an information security officer assigned to the organization in an impartial, selected through an objective process.

(2) The information security supervisor may be assigned to several relevant organizations simultaneously, if the reasons for the assignment allow it.

(3) In the case of a fixed-term secondment, the secondment may be extended no more than once before the expiry of the secondment period, until the completion of the ongoing measures. When determining the duration of the secondment, the seriousness of the breach of obligations by the organisation concerned and the protective measures necessary to avert the threat shall be taken into account.

(4) The decision on secondment shall contain the purpose and subject of the secondment, the data necessary for the personal identification of the information security supervisor, the circumstances giving rise to the secondment, the legal reference, the duration of the secondment, data on the method and regularity of the performance of the activity, and the amount of the information security supervisor's fee.

(5) The information security supervisor, with the involvement of the national cybersecurity authority and the relevant organization, shall prepare an action plan within the deadline set by the national cybersecurity authority to eliminate the deficiencies identified by the national cybersecurity authority. The information security supervisor shall act on the basis of the action plan approved by the authority.

(6) A person may not be assigned as an information security supervisor if: a) he/she is in
a legal relationship with the relevant organization, b) he/she was in a legal
relationship with the relevant organization in the three years preceding the assignment, c) at the time of assignment or in the
three years preceding the assignment, he/she has a regular and permanent assignment or
is or was in a business relationship,
d) a relative of the manager, economic manager or employee of the relevant organization during the period of his/her capacity and for three years after its termination,
e) a representative of the organization concerned, during the existence of this capacity and for three years after its termination, and f) a person from
whom an objective assessment of the given situation cannot be expected due to business interests or other reasons (bias).

Section 41 (1) The information security supervisor is entitled to monitor the security requirements set out in the legislation and the
in connection with compliance with and fulfillment of related procedural rules
a) request written and oral information and data from the managers and any employee of the organization concerned, b) inspect all
documents and records related to information technology of the organization concerned,
to have a copy or extract made,
c) enter all information technology-related premises of the organization concerned, d) propose immediate
measures to the head of the organization concerned to eliminate the direct threat (restriction, termination of operations), e) propose measures to establish or restore
legal operations, and within this framework, initiate a review of the relevant regulations, f) provide a preliminary opinion on measures related to operations that also affect electronic information security, and g)
object to measures and decisions taken or omitted by the organization concerned.

(2) The information security officer is not authorized to make financial commitments.

(3) The information security supervisor shall a) present
his/her letter of mandate to the relevant organization, b) monitor
the implementation of the security requirements and procedures set out in the legislation and the performance of the tasks prescribed in the legislation at the relevant organization from the date of his/her mandate, c) identify the reasons that led to the failure to
fulfil the obligation or the emergence of the threat, d) implement the necessary measures based on the measures set out in points c) and
c) and the known conditions of the operation of the relevant organization
to prepare an action plan,

e) initiate immediate measures so that their implementation does not make it impossible to perform the core activity, and immediately notify the national cybersecurity authority thereof, f) comply with the rules on the obligation of

confidentiality, g) report to the authority – after prior consultation with the

organization – at the frequency specified in the action plan, and provide an account in the report of the measures taken, the fulfillment of security requirements, and the further measures necessary for the development of electronic information security, and

h) upon termination of its mandate, prepare a summary report on its operations, including the measures taken and their results
the results of the investigation and the proposed further measures, the approval of which will be decided by the national cybersecurity authority.

(4) The head of the organization, the person responsible for the security of the electronic information system, and the organization's employees are obliged to cooperate with the information security supervisor, provide him with the necessary information, and hand over documents.

(5) The national cybersecurity authority may review the justification for the appointment of an information security officer.

(6) The information security supervisor's assignment may be terminated before the expiry of the period specified in the mandate.
can happen if

a) the reason for the secondment has been resolved and the summary report of the information security supervisor has been submitted to the national cybersecurity authority approved, or

b) the information security officer is recalled by the national cybersecurity authority.

(7) The information security officer shall be recalled by the national cybersecurity authority if a) it establishes

that the security requirements of the organization concerned are not being met for reasons attributable to the information security officer.
requirements, or

b) a circumstance giving rise to exclusion has arisen, or the circumstance giving rise to exclusion existing at the time of the secondment has been removed from the national comes to the attention of the cybersecurity authority.

(8) In the case specified in paragraph (7), the national cybersecurity authority is entitled to appoint a new information security supervisor.

(9) The national cybersecurity authority shall immediately notify the termination of the assignment of the information security supervisor in writing.
informs the head of the relevant organization.

(10) The information security supervisor is entitled to remuneration for the performance of his/her activities – based on a monthly remuneration of seven times the current minimum wage – in proportion to the period specified in the assignment, and to reimbursement of his/her justified expenses.

(11) The fee and proven costs of the information security officer shall be borne by the organization concerned.

21. Cybersecurity fine

Section 42 (1) Section 30 (2) of the Cybersecurity Act a) the national

cybersecurity authority against the organization referred to in Section 1 (1) a)–c) of the Cybersecurity Act, as set out in Annex 2, b) the Regulatory Activities Supervisory

Authority (hereinafter referred to as: SZTFH) against the organization referred to in Section 1 (1) d) and e) of the Cybersecurity Act point may impose a cybersecurity fine in the amount specified in
Annex 3 against the organization.

(2) The maximum amount of the fine that may be imposed pursuant to paragraph (1)

shall be: a) if the organization qualifies as a basic organization, the amount in forints corresponding to EUR 10 million or, if this is higher, the organization
an amount equivalent to 2% of its total global annual turnover in the previous financial year,

b) if the organization is considered an important organization, an amount equivalent to EUR 7 million or, if higher, the organization's previous
an amount equivalent to 1.4% of its total global annual turnover for the financial year.

(3) When determining the maximum amount of the fine in forint that can be imposed pursuant to paragraphs (1) and (2), the provisions on the imposition of fines shall be applied.
The euro exchange rate published by the Hungarian National Bank on the day of the decision shall be used as a basis.

(4) If the head of the organization fails to comply with his/her statutory obligations, the national cybersecurity authority shall impose a fine of 15 million
may be fined up to HUF 100,000, or in the case of a repeated violation.

Section 43. Paragraph (4) of Section 15/B of the Agricultural Act Based on this, the national cybersecurity authority may impose a cybersecurity fine of up to 15 million forints on the intermediary service provider in the event of failure to fulfill its tasks specified in this regulation regarding the management and investigation of cybersecurity incidents.

Section 44 (1) The fine must be paid within 8 days of the decision of the cybersecurity authority becoming final.
to the account kept at the Hungarian State Treasury, specified in a decision of the cybersecurity authority.

(2) During the payment, the text “cybersecurity fine” and the fine must be indicated in the transfer notification section.
number of the decision establishing the

(3) In the event of multiple violations, the maximum fine that can be imposed for each violation is
the amount of the maximum fines that can be imposed.

(4) Payment of the fine does not exempt from criminal and civil liability, nor from the act giving rise to the imposition of the fine.
from the obligation to eliminate the circumstance.

(5) The fine shall be imposed by the court imposing the fine, with the exception of violations of the law that can be terminated immediately, in the same circumstances.
may be imposed again two months after the final decision has been communicated.

Chapter IV

CYBERSECURITY CERTIFICATION

22. Certain provisions relating to cybersecurity certification authority activities

Section 45. The Government shall designate the Minister responsible for National Defence as the certifying authority pursuant to Section 45(1)(b) of the Cybersecurity Act with regard to cybersecurity certification authority tasks related to military research, development, production and trade.

Section 46 (1) The tasks of the cybersecurity certification authority are defined in Section 45 (1) a) of the Cybersecurity Act. SZTFH performing cybersecurity certification authority tasks related to military research, development, production and trade, Section 45 (1) b) of the Cybersecurity Act authority designated pursuant to Section 49 (2) of the Cybersecurity Act (hereinafter collectively referred to as: certification authority) shall impose a fine in the amount specified in Annex 4 for violation of European Union legal acts and Hungarian legislation (hereinafter referred to as: irregularity).

(2) The fine imposed must be paid by the certifying authority within 8 days after the decision of the certifying authority becomes final.
to the account kept at the Hungarian State Treasury, specified in the authority's decision.

(3) In the event of multiple violations, the maximum fine that can be imposed for each violation is
the amount of the maximum fines that can be imposed.

(4) The certification authority shall impose a fine under the same circumstances as provided for in Section 49(1) of the Cybersecurity Act. determined based on
may impose it again after the expiry of the deadline without result.

Section 47. The certification authority shall forward information on vulnerabilities or irregularities affecting the security of the ICT product to the
For the center.

Chapter V

VULNERABILITY TEST

23. General provisions regarding vulnerability assessment

Section 48 (1) The Government designates the National Security Service as the state body referred to in Section 57(1)(a) of the Cybersecurity Act (hereinafter referred to as: state body authorized to conduct vulnerability assessments) .

(2) The Military Security Service shall be responsible for conducting vulnerability assessments regarding electronic information systems for national defense purposes.
National Security Service is authorized.

(3) The Military National Security Service is authorized to conduct vulnerability assessment activities.
The provisions applicable to state bodies shall apply.

(4) Section 57(1)(c) of the Cybersecurity Act During the vulnerability assessment carried out by the economic entity according to
the provisions of this chapter shall apply.

Section 49 (1) The purpose of vulnerability assessment is to identify the weaknesses of the organization's electronic information system and system components, and to develop solution proposals for addressing the identified vulnerabilities in order to strengthen the protection and security of electronic information systems and system components.

(2) The subject of the vulnerability assessment is the examination of electronic information systems, system elements, tools, procedures and related processes used to manage data and information, as well as the examination of the general IT preparedness of the persons handling them and the organization.

24. Test methods

Section 50 (1) During a comprehensive vulnerability assessment, the following assessments shall be carried out, as specified in the basic document establishing the vulnerability assessment procedure: a) external IT security assessment, b) internal IT security assessment, c) application assessment, d) wireless network IT security assessment, or e) cyber-physical systems security assessment.

(2) The vulnerability assessment may include three types of eligibility phases with regard to the orientations specified in paragraph (1):

a) scan without registered user rights, b) scan with registered user rights and c) scan with administrator rights.

Section 51 (1) Vulnerability testing methods that are not considered comprehensive are: a) automated vulnerability detection and analysis, b) psychological manipulation testing, c) penetration testing, d) cryptographic compliance testing and e) source code testing.

(2) The vulnerability assessment methods referred to in paragraph (1) may form part of a comprehensive vulnerability assessment, However, their use does not replace a full vulnerability assessment.

Section 52 (1) The deadline for a vulnerability assessment carried out by a state body authorised to carry out vulnerability assessments shall be a maximum of 90 days from the date specified in the vulnerability assessment basic document or in the resolution of the national cybersecurity authority.

(2) If the organization's electronic information system or system component deviates significantly from the average and is therefore unique A vulnerability assessment procedure is required, and the vulnerability assessment deadline can be a maximum of 120 days.

(3) The state body authorized to conduct the vulnerability assessment may extend the deadline for the vulnerability assessment once, by a maximum of 30 days, before its expiration, and shall notify the organization and the national cybersecurity authority thereof.

(4) The electronic information system of the organization deviates significantly from the average if a) the electronic information system has aa) more than 10 IP addresses in the external Internet domain, b) more than 10 web services, or ac) more than 50 servers in the internal network, or ad) more than 500 workstations, or ae) more than 5 wireless networks, or af) more than 500 users, b) the organization has the electronic information system affected by the investigation at more than three locations, or c) the organization declares this in the basic document initiating the vulnerability investigation and thereby The state body authorized to conduct vulnerability assessments agrees.

25. Conducting a vulnerability assessment

Section 53 (1) During the preparation of the vulnerability assessment, the state body authorized to conduct the vulnerability assessment and the economic organization authorized to conduct the vulnerability assessment pursuant to Section 57(1)(c) of the Cybersecurity Act (hereinafter collectively referred to as: the body conducting the vulnerability assessment) shall prepare a vulnerability assessment basic document.

(2) The vulnerability assessment basic document must record at least 1. the name of the organization performing the vulnerability assessment, 2. in the case of a business organization, the name of the person performing the vulnerability assessment, 3. the organization with the right of disposal over the affected electronic information system, 4. the name of the affected electronic information system, as well as the affected system components and applications,

5. the data controller of the electronic information system, 6. the subject of the test, 7. the test tasks and objectives, 8. the vulnerability test method, 9. the authorization phase of the vulnerability test, 10. the vulnerability test and risk assessment methodology, 11. the conditions necessary for conducting the vulnerability test and the method of ensuring them, 14 11a.

in the case of a business entity – in the case of a vulnerability assessment covering an electronic information system classified as "significant" or "high" security class – the name of the testing laboratory registered for a "significant" or "high" reliability level in accordance with the Decree of the President of the SZTFH on cybersecurity certification of information and communication technologies and the scope of activities to be performed by the testing laboratory during the vulnerability assessment,

12. the duration of the vulnerability assessment, the schedule for its implementation, 13. the circumstances giving rise to the suspension or termination of the vulnerability assessment, and 15 14. the signature of the head of the organization or the manager authorized by him or her and authorized to replace the head of the organization in an organizational manner.

(3) If the vulnerability assessment is ordered by the national cybersecurity authority, the vulnerability assessment basic document shall also include the assessment tasks set out in the authority decision, and the items set out in point 14 of paragraph (2) shall not be included.

(4) If the vulnerability assessment is initiated by a state body authorized to conduct vulnerability assessments, the provisions of paragraph (2), point 14, do not need to be indicated.

Section 54 (1) In the event of an organization initiating a vulnerability assessment, the organization may make proposals for the assessment tasks, which is decided by the body conducting the vulnerability assessment.

(2) The vulnerability assessment basic document shall be sent to the affected organisation by the body carrying out the vulnerability assessment – at least 8 days before the start of the vulnerability assessment. The affected organisation may make comments on the content of the vulnerability assessment basic document within 5 days of receipt. The comments may not affect the examinations ordered by the national cybersecurity authority. The body carrying out the vulnerability assessment shall decide on the comments.

Section 55 (1) If, after the signing of the vulnerability assessment basic document, a change occurs in the information recorded in the vulnerability assessment basic document, the body conducting the vulnerability assessment, taking into account the significance and weight of the change, shall, based on consultation with the organization having the right of disposal over the electronic information system concerned,

a) initiate the modification of the vulnerability assessment basic document, b) modify the closing date of the vulnerability assessment, c) suspend the execution of the vulnerability assessment, d) terminate the vulnerability assessment or e) close the vulnerability assessment by issuing a resolution.

(2) After signing the vulnerability assessment basic document, in the event of a request for modification in the vulnerability assessment method or methodology, the body performing the vulnerability assessment shall terminate or close the vulnerability assessment as set out in the signed vulnerability assessment basic document.

(3) If the conditions set out in the vulnerability assessment basic document and this regulation are not fully met available, the vulnerability assessment cannot be performed or its execution must be suspended.

Section 56 (1) The body performing the vulnerability assessment shall exercise due diligence during the vulnerability assessment to limit the services provided by the electronic information system under assessment to a level no greater than absolutely necessary and to conduct the vulnerability assessment during a period that is not critical to the service. The body performing the vulnerability assessment shall inform the affected organization in advance of the expected extent and duration of the limitation.

(2) The body performing the vulnerability assessment shall inform the organization affected by the vulnerability assessment of the IP address or other unique technical identifier used by it for the assessment, which the organization may not prohibit from accessing the service during the assessment period, and shall ensure that the body performing the vulnerability assessment can access the service.

(3) The body conducting the vulnerability assessment shall, as far as possible, ensure that the vulnerability assessment is carried out without gaining access to the data stored on the electronic information systems of the national security service carrying out civilian intelligence activities.

14 Section 53, paragraph (2), point 11a. is replaced by Section 5, paragraph (1) of Government Decree 189/2025. (VII. 3.) he enrolled.

15Section 53(2)(14) in conjunction with Section 5(2) of Government Decree No. 189/2025 (VII. 3.) established text.

Section 57. The organization shall notify the vulnerability assessment to be carried out by the business organization in the vulnerability assessment to a state body authorized to carry out the procedure.

Section 58 (1) The organization is obliged – in accordance with the basic vulnerability assessment document or, in the case of an order by a state body authorized to conduct a vulnerability assessment, in the order – to provide the body conducting the vulnerability assessment with the data, documents, tools and other information necessary for conducting the vulnerability assessment, and to tolerate any reduction or loss of service on the electronic information system under assessment resulting from the vulnerability assessment.

(2) In the case of an inspection without registered user rights, the relevant organization shall: a) send the data relating to the access points of the electronic information system or service to be inspected to the body conducting the vulnerability assessment, and ensure – even in the case of a system with limited access – the possibility of physical and logical access to the access points,

b) provides the body conducting the vulnerability assessment with the electronic information system or service to be assessed monitoring.

(3) In the case of an examination with registered user rights, in addition to what is specified in paragraph (1), the relevant organization shall send a) the user rights matrix and b) the user documentation to the body performing the vulnerability assessment.

(4) In the case of an audit with administrator privileges, the organization shall send the system plan to the body conducting the vulnerability assessment, in addition to the provisions of paragraphs (2) and (3).

(5) The organization shall notify the vulnerability assessment body of the periods that are unsuitable for performing the vulnerability assessment in terms of the services provided or its operation by the organization at least 8 days before the preparation of the vulnerability assessment basic document. The indicated periods shall not be included in the duration of the vulnerability assessment specified in this Regulation.

(6) In the event of a change in the availability of services during the vulnerability assessment, the notification must be made immediately, must be done within 3 days at the latest.

(7) If the organization does not provide or incorrectly provides the data necessary for performing the vulnerability assessment, the state body authorized to perform the vulnerability assessment shall not perform the assessment or – in the case of a vulnerability assessment ordered by the state body authorized to perform the vulnerability assessment or the national cybersecurity authority – shall initiate with the national cybersecurity authority the obligation of the organization to cooperate and provide data.

(8) In the case of electronic information systems for national defense purposes, the data specified in paragraphs (2)–(6) shall be must be reported to the cybersecurity incident management center.

Section 59 (1) The organization is obliged to inform all organizations involved in the operation of the electronic information system affected by the vulnerability assessment in writing about the planned vulnerability assessment and about any changes in the information provided.

(2) The information must include a) the fact that the vulnerability assessment has been carried out, b) the electronic information system concerned, c) if known, the planned start and duration of the vulnerability assessment, d) the fact that a service outage or reduction in the service provided by the electronic information system concerned is expected, e) with regard to the data controller of the electronic information system, the data stored in the electronic information system concerned or a request for consent to access the processed data and to perform a vulnerability assessment, or f) vulnerability assessment for the organization involved in the operation of the electronic information system request for acknowledgement of its completion.

(3) The a) data controller of the electronic information system affected by the vulnerability assessment shall declare in writing that it consents to the vulnerability assessment, and b) the organization involved in its operation shall declare that it acknowledges the information.

(4) Upon request by the national cybersecurity authority, the organization shall present the information and the consent or a statement of acknowledgement.

Section 60 (1) The organization involved in the operation of the electronic information system affected by the vulnerability assessment may not obstruct the vulnerability assessment and is obliged to provide the appropriate access necessary for conducting the vulnerability assessment.

(2) If an organization involved in the operation of the electronic information system affected by the vulnerability assessment impedes the performance of the vulnerability assessment, the organization exercising the right of disposal over the electronic information system affected by the vulnerability assessment shall notify the national cybersecurity authority – in the case of an electronic information system for national defense purposes, the national defense cybersecurity authority – which may, in justified cases, oblige the obstructing organization to acknowledge the vulnerability assessment and eliminate the obstructive circumstance. In the absence of jurisdiction, the national cybersecurity authority may initiate action by the authorized authority in order to oblige.

§ 61. Vulnerability assessment may be conducted in accordance with internationally accepted vulnerability assessment and risk assessment methodologies. During vulnerability assessment, only a risk assessment methodology may be used that takes into account at least the extent of the impact of the vulnerability and the complexity of its exploitation.

Section 62 (1) Upon completion of the vulnerability assessment, the body conducting the vulnerability assessment shall send the position statement it has prepared within 8 days – or within 21 days if the electronic information system of the affected organization deviates significantly from the average – to the affected organization and the national cybersecurity authority – the national defense cybersecurity authority in the case of electronic information systems for national defense purposes.

(2) The position statement shall include at least the following: 1. the name
of the body performing the vulnerability assessment, 2. the name of
the organization with the right of disposal over the electronic information system concerned, 3. the name of the electronic information
system concerned, as well as the system components and applications concerned, 4. the date and duration of the vulnerability assessment, 5.
the subject of the vulnerability assessment, 6. the assessment
tasks and objectives, 7. the applied
vulnerability assessment method, 8. the
vulnerability assessment and risk assessment methodology
used, 9. a description of the assessment results, 10. if applicable to the applied
vulnerability assessment methodology, all
risks assessed,
regardless of whether a given system contains the vulnerability or not, 11. the name of the vulnerability, 12. a description of the
vulnerability, 13. the risk classification of the vulnerability,
14. the classification and description of the
impact, 15. the classification and description of the complexity of
exploiting the vulnerability, 16. if possible, a detailed
description of the vulnerability discovery, 17. a proposal for improving the vulnerability, 18. proposals for measures
regarding short, medium and long-term measures, 19. a proposal for the need to conduct a follow-up test, 20.
in the case of a business organization, the name of the person performing
the vulnerability test, and 21. the signature of the body performing the vulnerability test. 16 (3)

Unless otherwise provided in the vulnerability assessment basic document, the body conducting the vulnerability assessment shall send the draft position statement to the organization for comment, on which the head of the organization may make comments once, within 8 days. In this, he may make a proposal for reviewing the risk and may modify the risk classification by up to one level. The body conducting the vulnerability assessment shall decide on the acceptance of the opinion.

(4) The national cybersecurity authority shall accept the contents of the cybersecurity audit report as equivalent to the vulnerability assessment statement referred to in paragraph (2) if it contains the aspects and information specified in paragraph (2).

(5) Statement on the vulnerability assessment conducted with regard to electronic information systems for national defense purposes
The relevant organization also shares its draft with the body providing its professional management or the owner's legal practitioner.

Section 63 (1) If a vulnerability classified as critical or high according to the methodology used during the vulnerability assessment is discovered, the organization is obliged to take measures to correct, address or mitigate the discovered vulnerabilities.

a) in the case of a new electronic information system, until the system is put into use, b) in other
cases, immediately after receipt of the position statement, but no later than within 30 days.

16A Section 62. (3) of Government Decree 189/2025. (VII. 3.) 6. Text established by §.

(2) In the case of point b) of paragraph (1), the organization shall, after consultation with the organization conducting the vulnerability assessment and the national cybersecurity authority, consider the need to suspend the use of the electronic information system.

(3) Vulnerabilities classified as low-level according to the methodology used during vulnerability assessment may be accepted without any obligation to provide justification.

(4) The affected organization shall prepare a vulnerability management plan within 30 days of receiving the resolution and submit it to the to the national cybersecurity authority, which will forward it to the state body authorized to conduct the vulnerability assessment.

(5) The vulnerability management plan includes the vulnerability identified during the vulnerability assessment, the vulnerability management measures and tasks, the milestones for completing the tasks, the related implementation deadlines, the technical details of the fix and their impact on the system, and the resources required for this.

26. The follow-up examination

Section 64 (1) If the body conducting the vulnerability assessment proposes in the position statement to conduct a follow-up assessment, the national cybersecurity authority shall state in its decision on the vulnerability management plan for eliminating the vulnerabilities whether it obliges the organization to conduct a follow-up assessment.

(2) If the resolution identifies a critical or high-level vulnerability, a follow-up investigation is mandatory.

(3) In the event of a mandatory follow-up inspection, the organization shall be subject to a procedure approved by the national cybersecurity authority. initiates the follow-up inspection after the last deadline specified in the vulnerability management plan has passed.

(4) The organization may also initiate the follow-up investigation itself, in which case it shall simultaneously with the initiative – if this has not been done before the initiative – send the vulnerability management plan to the national cybersecurity authority.

(5) A follow-up review may be conducted after the vulnerability management plan has been approved by the cybersecurity authority or if justified. In some cases, this may take place after obtaining permission from the national cybersecurity authority.

(6) The body conducting the follow-up investigation shall prepare a follow-up investigation statement, which shall be communicated to the person concerned. organization and the national cybersecurity authority.

(7) The general provisions on vulnerability assessment shall apply to the follow-up examination.

(8) The post-investigation resolution conducted with regard to electronic information systems for national defense purposes shall be submitted to the relevant The organization also shares it with the body providing its professional management or with the owner's legal practitioner.

Chapter VI

PROVISIONS RELATED TO CYBERSECURITY INCIDENTS

27. Cybersecurity Incident Response Centers

Section 65 (1) The Government shall, pursuant to Section 63 (1) of the Cybersecurity Act, as the national cybersecurity incident management center according to It designates a National Security Service.

(2) The Government shall, pursuant to Section 63(2) of the Cybersecurity Act designates the Military National Security Service as the national defense cybersecurity incident management center. The Military National Security Service handles cybersecurity incidents and threats together with incident management centers operating under its professional management and coordination, separated by task, at the body or organization under the direction and leadership of the minister responsible for national defense.

Section 66 (1) An organization may operate as a cybersecurity incident management center within a sector if, upon examination by the Center or another independent organization and approval by the Center, it meets the conditions based on international or European Union standards determined by the Center.

(2) Based on the investigation, the cybersecurity incident management center within the sector and the Center shall conclude a cooperation agreement, which shall record the incident management capabilities of the cybersecurity incident management center within the sector and the rules for the division of tasks and cooperation between the two organizations.

(3) In the performance of its tasks specified in the cooperation agreement concluded with the Centre, the cybersecurity incident management centre within the sector shall – unless otherwise provided by law or the cooperation agreement – have the rights granted to the Centre in relation to the given task.

Section 67 (1) The Centre shall perform the following tasks: 1.
in its scope of tasks related to threats affecting cyberspace and the prevention of cybersecurity incidents:

a) conducts regular security situation assessments of the Hungarian cyberspace while continuously collecting data, and also prepares dynamic risk and event analysis according to a unified
methodology, b) monitors and analyzes cyber threats, vulnerabilities, risks and cybersecurity incidents, c) receives
domestic and international reports on cyber threats and cybersecurity incidents, processes data on threats and cybersecurity incidents coming from its own and other available sources and notifies the affected parties within its customer base or notifies and transfers the data to the competent incident management center, d) continuously operates its cybersecurity-related services, e) operates the early warning system in accordance with the government decree, f) operates
the distributed government trap system, g) publishes immediate warnings on
critical network security threats, ensures their display in
Hungarian, h) can exchange information with essential and important organizations and their sectoral or inter-sectoral groups;

2. in its responsibilities related to cybersecurity incident management:
a) receives, manages and coordinates reports, information and alerts on cybersecurity incidents, threats and near-misses affecting electronic information systems, b) receives and manages international reports affecting Hungarian
cyberspace, c) monitors cybersecurity incidents at the national level, d)
raises awareness, issues alerts, issues warnings and provides information
to stakeholders regarding risks and cybersecurity incidents, e) may issue warnings to users, cybersecurity incident management centres, authorities, authorities
supervising the security of electronic information systems and the single point of contact, f) maintains contact with organisations and service providers in order to manage reported cybersecurity incidents and takes and
coordinates the necessary measures to manage them, g) immediately notifies the data subjects and the competent authority of cybersecurity incidents that have come to its attention, h)
provides assistance to the organisations concerned in the management of cybersecurity incidents during its management, i)
records the reports received, the measures taken and their results, j) investigates and supports
the investigation of cybersecurity incidents, threats, and near-misses, k) determines the procedures
for managing cybersecurity incidents and risks, as well as the procedures and rules for classifying cybersecurity incidents, risks and information, l) approves the operation and operating rules of the incident management center within the sector, m) ensures continuous availability; 3. in its scope of tasks related to the management of cybersecurity
crises:

a) performs – unless otherwise provided by law – the coordination of tasks related to the cybersecurity and restoration of electronic information systems during the management of cybersecurity crises, b) represents Hungary
in the European Network of Cyber Crisis Contact Points (hereinafter: EU-CyCLONe) as defined in Section 106, c) participates
in the development of Hungary's Cyber Crisis Management
Plan, d) participates in the EU political-level integrated crisis response
mechanism (hereinafter: IPCR) system; e) maintains continuous contact with the national incident management
center in order to effectively manage cybersecurity crises; 4. in its scope of tasks concerning vulnerabilities and vulnerabilities:

a) receives and coordinates notifications, information, early warnings, alerts and information to stakeholders regarding
vulnerabilities affecting electronic information systems and vulnerabilities affecting ICT products, b) publishes internationally published
vulnerabilities on its website, c) performs the CSIRT coordinator tasks
specified in the European Union legal act, d) informs stakeholders about information
related to vulnerabilities, e) registers reported vulnerabilities and informs ENISA
about them as necessary, f) participates in the implementation of vulnerability-related tasks pursuant
to Regulation (EU) 2019/881 of the European Parliament and of the Council;

5. within the framework of its information and awareness-raising activities:
a) prepares analyses and reports on domestic and international information security trends,
b) prepares an annual report on its activities for the minister responsible for IT and in abstract form for the public,

c) develops educational materials and holds training sessions in order to promote security-conscious user behavior, and organizes awareness-raising and awareness-raising campaigns for both organizations under its jurisdiction and citizens, d) participates in domestic and international information security and cyber protection exercises, and may plan, organize such exercises and oblige the organization to participate in the exercise, e) informs the persons responsible for the security of electronic information systems, the competent authorities and the cybersecurity incident management centers in connection with vulnerabilities and threats threatening electronic information systems, f) provides regular information on its website about vulnerabilities and threats, as well as the proposed security measures, g) participates in the awareness-raising program of institutions responsible for raising awareness of information security, and may perform expert-training activities; 6. within the framework of European Union and international cooperation: a) receives and handles international reports affecting Hungarian cyberspace, b) represents Hungary in international incident management cooperation, c) participates in the activities of the CSIRT network, d) provides assistance, in accordance with their capacities and powers, to other members of the CSIRT network at their request within the framework of mutual assistance pursuant to Article 11(3)(f) of Directive (EU) 2022/2555 of the European Parliament and of the Council, e) cooperates with national computer security incident response teams of third countries or equivalent third-country bodies, f) participates in mutual assistance to other members of the CSIRT network, upon their request, g) operates an exchange programme involving CSIRT officers from other EU Member States, h) participates in peer review pursuant to Article 19 of Directive (EU) 2022/2555 of the European Parliament and of the Council and may initiate peer review, i) may join European Union and international cooperation related to cyber defense and may conclude cooperation agreements;

7. additional responsibilities:

a) for the purpose of creating a picture of the Hungarian cybersecurity situation, it shall carry out proactive, non-intrusive scanning of electronic information systems accessible from the open internet in a manner that does not harm the operation of the organizations' services, in order to detect vulnerabilities or insecurely configured electronic information systems, b) it may also carry out the activity referred to in point a) at the request of the organization in relation to the organization's electronic information systems, c) it shall determine the procedures for handling cybersecurity incidents and risks, as well as the procedures and rules for classifying cybersecurity incidents, risks and information; in doing so, it cooperates with the relevant organizations, d) may operate a government information technology and cybersecurity incident management cooperation forum, e) may participate in the preparation of strategies and regulations related to cybersecurity, f) may require the adoption and application of common or standardized practices, classification systems and taxonomies, may issue binding and non-binding resolutions and recommendations regarding procedures for preventing and handling cybersecurity incidents, handling cybersecurity crises, and coordinated disclosure of vulnerabilities.

(2) For the purpose of managing cybersecurity incidents and threats, the Centre shall cooperate with a) cybersecurity authorities, b) the national defence cybersecurity incident management centre, c) cybersecurity incident management centres within the sector, d) essential and important organisations and their sectoral or inter-sectoral groups, e) organisations involved in the management of cybersecurity incidents, f) law enforcement agencies, g) national security services, h) the National Media and Communications Authority and the National Informatics and Communications Directorate operated by it, i) electronic communications service providers, centralised IT and electronic communications service providers, j) the Kszetv. with critical organizations and authorities, as well as the Vbö. with organizations and authorities that are significant for the protection and security of the country, k) the National Data Protection and Freedom of Information Authority, and

l) military cyberspace operations forces.

(3) The Centre may, subject to its resources, prioritise the implementation of its tasks on the basis of a risk-based approach.

Section 68 (1)[17] The National Defence Cybersecurity Incident Management Centre shall perform the tasks set out in Section 67 with regard to the electronic information systems within its jurisdiction, with the exception of Section 67(1)(1)(f), Section 67(1)(2)(l), Section 67(1)(3)(a), Section 67(1)(4)(b), (c), (f) and (g), Section 67(1)(5)(f) and Section 67(1)(6)(a)–(i).

(2) The National Defence Cybersecurity Incident Management Centre shall send the report referred to in Section 67(1)(5)(b) to the Minister responsible for National Defence.

(3) The National Defense Cybersecurity Incident Management Center shall be responsible for the electronic information systems under its jurisdiction. keeps a record of the contact details necessary for communicating with the bodies under its jurisdiction.

(4) The National Defense Cybersecurity Incident Management Center shall, at the request of the Center, provide the Cybersecurity Act, Section 66 (5) data related to the handling and investigation of threats, near-miss situations and cybersecurity incidents transmitted in accordance with

(5) The activities of the National Defense Cybersecurity Incident Management Center – in paragraph (1), Section 81 and Section 89 except as otherwise provided – the provisions applicable to the Centre shall apply.

§ 69 The Centre must meet the following requirements: a) it must publish contact details suitable for reporting to the Centre on its website and must ensure continuous availability,

b) its office premises and supporting information systems must be located in a secure location, c) it must have an appropriate system for handling and forwarding reports, d) it must ensure the confidentiality and reliability of its activities, e) it must have sufficient and qualified human resources to properly perform its tasks, f) it must have redundant systems and a backup workspace to ensure the continuity of its services, g) it must develop cooperative relationships with relevant private sector actors.

28. Threat analysis and prevention activities

Section 70 (1) The Centre shall analyse and evaluate, on the basis of information and data requested and mandatorily provided by the bodies operating the electronic information system and the cybersecurity incident management centres within its jurisdiction, signs indicating a cybersecurity incident or threat affecting electronic information systems. It shall notify the person responsible for the security of the electronic information system of the organisation exercising the right of disposal over the electronic information system of the risk or existence of a cybersecurity incident and of the proposed measures.

(2) The Centre may conduct an assessment by continuously monitoring the technical data and information received from the centralized IT and electronic communications service provider and may search for signs of a cybersecurity incident or threat affecting the operation of networks or services.

(3) The Centre shall investigate activities indicating a cybersecurity incident or threat and may issue warnings to organisations, users, cybersecurity incident response centres, competent authorities, the single point of contact and relevant bodies.

Section 71 (1) Within the framework of the threat information sharing system operated by the Centre, information collection may only concern the types of ports and services accessible from the open internet and basic metadata of the organisation's electronic systems.

(2) Section 65 (6) of the Cybersecurity Act for the activity listed below, only once a day per internet address
The Center will retain the generated data for five years.

Section 72 (1) When applying preventive measures and providing services in this regard (hereinafter referred to as preventive measures), the Centre shall exercise due diligence to limit the services provided by the electronic information system concerned to a level no greater than absolutely necessary and to apply preventive measures during periods that are not critical to the service.

(2) The relevant organization is obliged to provide the Centre with the data, documents, tools and other information necessary for the application of the prevention tools and to tolerate any reduction or loss of service on the relevant electronic information system resulting from the application of the prevention tools.

17A Section 68(1) is the text amended in accordance with Section 16(10) of Government Decree 189/2025 (VII. 3.) .

29. Vulnerability Management

Section 73 (1) If a European Union legal act issuing a European cybersecurity certification scheme contains rules on the manner of reporting and handling cybersecurity vulnerabilities detected in relation to an ICT product, the provisions therein shall be followed.

(2) The person reporting the vulnerability (hereinafter referred to as: the reporter) or the manufacturer or service provider of the ICT product affected by the discovered vulnerability (hereinafter jointly referred to as: the manufacturer) shall also, in the case referred to in paragraph (1), inform the Centre about the discovered vulnerability and the affected ICT product, as well as about the information requested by the Centre.

Section 74 (1) In the absence of a European cybersecurity certification scheme, the procedure established by the manufacturer for the receipt and management of information on vulnerabilities from third parties, the correction of the reported vulnerability and the coordinated publication of the vulnerability shall apply to the ICT product.

(2) The notifier or the manufacturer of the ICT products affected by the discovered vulnerability shall also be obliged in the case referred to in paragraph (1) to: inform the Centre about the discovered vulnerability and the ICT product concerned, as well as any information requested by the Centre.

Section 75 (1) With the exception of electronic information systems for national defense purposes, the organization with the right to dispose of the electronic information system, as well as the manufacturer of the ICT product, may provide the opportunity for anyone to search for information on the vulnerability of its electronic information systems, system components, or ICT products, by adhering to the procedures determined by it.

(2) The organization or manufacturer that wishes to use the option set out in paragraph (1) shall develop and publish on its website a procedure for identifying vulnerabilities in its electronic information systems, system components and ICT products, receiving their reports, coordinating the reporting entity and the organization, and correcting and sharing the vulnerabilities identified, and shall inform the Center thereof.

(3) The organization or the manufacturer may, at its discretion, provide financial compensation to the notifier.

(4) The procedure to be developed by the organization shall specify at least the following: a) which electronic information
systems, system elements and ICT products are subject to vulnerability detection capabilities
affected group, and what techniques are permitted or prohibited to use,
b) the communication channel through which the organization expects vulnerability reports, c) whether the organization
accepts anonymous reports, d) the contact information of the
organizational unit or person responsible for receiving reports, e) the process of coordinating with the
reporter and the method of informing about the process and current status of the bug fix, f) the procedure for implementing bug fixes to be carried out as a
result of the reports, g) the timeframe within which the vulnerability will be fixed.

(5) A person undertaking vulnerability research shall accept the terms and conditions published on the organization's website and/or the organization's
and may act on the basis of an agreement between the person.

(6) In the agreement referred to in paragraph (5), the parties shall specify at least the following elements: a)
the interface provided by the organization, on which the person undertaking the vulnerability research may conduct the research, b) the method of making the report, c)
the information to be provided by the reporter,
d) whether the reporter requests anonymity, e) if the
organization provides financial compensation for the report,
the amount and conditions thereof, f) the time available to the organization to investigate and correct the reported
vulnerability, g) if the organization fails to investigate or correct the error within the deadline set in the agreement, the reporter

the possibility of notifying the Center,
h) the fact that the provision of information about the vulnerability to other affected organizations is
Center is eligible.

(7) The organization applying paragraph (1), if a vulnerability is reported regarding its electronic information system, system component or ICT product, is obliged to a) examine the reported vulnerability within
the deadline set in the agreement or published on its website, or failing that, within the shortest possible time, but not more than 30 days, and prepare an action plan for eliminating the vulnerability, b) send feedback to the notifier, consult with the notifier regarding the discovered vulnerability, c) correct the discovered
vulnerability within the deadline set in the agreement, or failing that, within the shortest possible time,

but depending on the severity of the vulnerability, take action within a maximum of 90 days from the date of notification,

d) notify the notifier of the measures taken, e) inform the
Centre of the action plan for eliminating the vulnerability and the measures taken,
(8) If, after notification, the relevant organisation – in the agreement or in the procedure it has issued, or in these
in the absence of a response within 30 days – does not take action to correct the vulnerability, the notifier is entitled to notify the Center.
(9) If the vulnerability discovered by the reporter affects another organization's electronic information system, system component, or ICT
If the vulnerability also affects its product, the Center will inform the affected organization about the vulnerability based on the organization's notification.
(10) The notifier is obliged
to a) act in accordance with the agreement concluded for the purpose of revealing the vulnerability or as specified in the law, b)
notify the relevant organization of the discovered deficiency or vulnerability through the channel specified by the organization within the deadline specified in the agreement, or in the absence of an agreement to this effect, immediately, and provide the organization with the information necessary for identifying the vulnerability and fixing the error, as well as any possible solution suggestions,
(11) The Centre
shall a) assess the reported vulnerability,
b) identify any additional organisations that may be affected, c)
take measures to contact those affected, d) may inform the competent
authority about any organisation that fails to comply with the notification, information or cooperation obligation.
cybersecurity authority.

Section 76 (1) If the conditions set out in Sections 73–75 are not met, a vulnerability discovered by a natural or legal person in relation to an electronic information system or ICT product shall be reported to the Centre. The report shall be made in the manner specified on the Centre's website.
(2) The Center may issue recommendations to determine the framework and conditions for lawful detection of vulnerabilities.
(3) When reporting under paragraph (1), the reporter a) may
request to remain anonymous, b) must
provide his/her contact information if he/she does not request to remain anonymous, c) must
maintain the confidentiality of the report, d) must
provide the information at his/her disposal and any possible solution proposals to the Center, e) must keep the information
regarding the vulnerability confidential and may only notify the Center and the relevant organization, f) may not notify the vulnerability and the related
information to the relevant organization
dependent on the provision of compensation,
g) is only entitled to take measures necessary to prove the vulnerability, h) is obliged to refrain
from the following harmful behaviors: ha) installing malicious
code, hb) copying, deleting,
changing data, hc) making modifications to the
system, hd) repeated logins to the system,
he) sharing the vulnerability and the knowledge
acquired in connection with it with a third party, hf) deeper penetration or attempted penetration using other
methods.
(4) Based on the notification, the
Centre shall a) take measures to identify the affected organisations and contact them, b) provide
assistance to the vulnerability reporter, c) act as an
intermediary between the reporter, the organisation with the right to dispose of the electronic information system or the manufacturer of the ICT product and other stakeholders in order to conduct negotiations on the disclosure of the vulnerability and to address the vulnerabilities,

d) coordinate the coordination of vulnerability disclosure, e) ensure
the follow-up of actions related to reported vulnerabilities, and f) liaise with ENISA regarding the
reporting of reports to the European Vulnerability Database and the
for querying from the database.

(5) Based on the Center's notification, the manufacturer or the organization with the right to dispose of the electronic information system shall declare within 10 days whether it considers the contents of the notification to be a vulnerability, and shall also declare the repair.
The manufacturer is obliged to fix the vulnerability within 30 days or, in the case of an unfixable vulnerability, to implement a replacement protection measure. After the declaration or action deadline has expired without success, the Center may take action to publish the vulnerability.

(6) If the notifier reports an exploited vulnerability to the Centre, the Centre shall take appropriate action: a) to issue an alert regarding the vulnerability, b) to contact the manufacturer of the ICT product concerned, c) to notify ENISA, in consultation with the manufacturer of the ICT product concerned, of the vulnerability in the European for inclusion in the vulnerability database.

(7) If the reported vulnerability may have a significant impact on organisations in several European Union Member States, the Centre cooperates with the CSIRTs of the relevant European Union Member States designated as coordinators within the CSIRTs network.

(8) The voluntary notification of a publicly known vulnerability to the European Vulnerability Database shall be made by the manufacturer through the Centre in order to enable users of the ICT product to take appropriate mitigation measures.

30. Reporting cybersecurity incidents

Section 77 (1) of the Cybersecurity Act. 66. In the context of the notification pursuant to §, the organization shall submit to the Center: 1. without undue delay and in any case within 24 hours of becoming aware of the cybersecurity incident, an initial notification, which – if the information is available – shall include a) the designation of the electronic information system concerned, b) a brief description of the cybersecurity incident, including an indication of whether the incident qualifies as an operational cybersecurity incident, c) the status of the cybersecurity incident, d) the duration of the cybersecurity incident, e) if it can be estimated, the expected date of restoration of the service, f) the type and nature of the data affected by the cybersecurity incident, g) the number of users affected by the cybersecurity incident, h) the extent of the disruption to the operation of the service, i) the contact details of the contact person and organisation designated by the operator to handle the cybersecurity incident, j) in the event of the use of an intermediary service provider or central service provider, the name and contact details of the intermediary service provider or central service provider, k) the whether the cybersecurity incident is considered an intentional incident, l) the geographical extent of the area affected by the cybersecurity incident, m) whether the cybersecurity incident may have a cross-border impact, n) any information that allows the Centre to determine the cro

2. as soon as they are available, the infection indicators; 3. without undue delay and in any case within 72 hours of becoming aware of the cybersecurity incident, an incident report, updating where appropriate the information referred to in point 1 and containing an initial assessment of the incident, including its severity and impact; 4. at the request of the Centre, an interim status report; 5. a final report, no later than one month after the submission of the incident report pursuant to point 3, containing the following: a) a detailed description of the cybersecurity incident, including its severity and impact; b) the type of threat or trigger that is likely to have triggered the cybersecurity incident; c) mitigation measures applied and ongoing; d) where applicable, the cross-border impact of the cybersecurity incident; 6. if the cybersecurity incident is still ongoing at the time of submission of the final report, a report on the progress made so far report;

7. in the case referred to in point 6, a final report within one month of handling the cybersecurity incident. (2)

[18] When reporting a cyber threat, a cybersecurity near-incident situation, or an operational cybersecurity incident, (1) The provisions of paragraph 1 shall apply in the manner determined by the Center if they can be interpreted in connection with the given event.

(3) The organization does not have to report a cybersecurity near-incident situation and an operational cybersecurity incident that was handled and resolved automatically during the incident management process and did not result in service degradation. The organization shall also report a recurring cybersecurity near-incident situation and an operational cybersecurity incident in this case.

18A Section 77. (2) of Government Decree 189/2025. (VII. 3.) 8. Text established by §.

(4) By way of derogation from point 3 of paragraph (1), the trust service provider shall notify the Centre of any cybersecurity incident affecting the provision of its trust services without undue delay and in any case within 24 hours of becoming aware of the incident.

Section 78 (1) Cyber threats, near-misses and cyber security incidents shall be reported in the manner specified by the Centre – in the case of electronic information systems for national defence purposes, the National Defence Cyber Security Incident Management Centre – electronically – if available, on the electronic interface specified by the Centre.
If the organization's electronic information system is compromised to such an extent that electronic reporting is not possible, reporting may be done in any other manner.

(2) In the event of a significant or large-scale cybersecurity incident, the organization shall report the incident to the Center immediately and within a short period of time. You can do it on the road or by phone.

(3) The cybersecurity authority shall forward the notification received to the Centre.

31. Cybersecurity Incident Management and Investigation

Section 79 (1) The Centre shall respond to the report immediately and, if possible, within 24 hours of receipt of the initial report. This shall include providing feedback on the incident to the reporting organisation and, at the organisation's request, providing guidance or operational advice on the implementation of possible mitigation measures.

(2) The Centre shall provide technical support if requested by the organisation concerned.

Section 80 (1) Organizations shall notify their service users without undue delay and free of charge of any cybersecurity incidents that are likely to adversely affect the provision of their services and require action by their service users.

(2) The organisation shall, without undue delay or as soon as the information becomes available, inform the users of its services potentially affected by a significant cyber threat of the measures and remedial options that the users of the services can take or use themselves in response to the threat.

(3) If public awareness is necessary to prevent a cybersecurity incident or to manage an ongoing cybersecurity incident, or if disclosure of the cybersecurity incident is otherwise in the public interest, the Centre shall, after consulting the relevant organisation as necessary, inform the competent cybersecurity authority in order to inform the public.

Section 81 (1) The Centre shall investigate the cross-border impact of cybersecurity incidents.

(2) Where a major cybersecurity incident affects two or more Member States, the Centre shall immediately inform the other European Union Member States concerned and ENISA of the major incident.

(3) At the request of the Centre or the competent cybersecurity authority, the single point of contact pursuant to Section 77(1) shall:
forwards the received notification to the single point of contact of the European Union Member State affected by the cybersecurity incident.

(4) When providing information, the Centre and the single point of contact shall take into account the security and business interests of the organisation concerned. and the confidentiality of the information submitted.

(5) In the course of carrying out its tasks, the Centre shall maintain contact with and exchange information with national computer security incident response teams of the Member States of the European Union and third countries using appropriate information sharing protocols, including the Traffic Light Protocol (TLP), in accordance with data protection legislation.

Section 82 (1) The purpose of the technical examination of data related to cybersecurity incidents is to a) reveal
the causes and circumstances of the cybersecurity incident and the extent of the damage caused, b) limit the scope of
electronic information systems and system elements affected by the cybersecurity incident, c) make proposals for the prevention of the
damage caused by the cybersecurity incident, and d) inform other bodies affected by the
cybersecurity incident and the public about the lessons that can be drawn from the incident that occurred.
competent cybersecurity authority in order to prevent the incident from occurring in the future.

(2) In the report on the investigation of the cybersecurity incident, the investigator shall record the aspects and recommendations referred to in paragraph (1). The investigator shall send the report to the organization concerned, the Centre and the competent authority immediately after the completion of the investigations.

Section 83 (1) During the management and investigation of a cybersecurity incident, the organization affected by the incident shall cooperate
With the Centre, which cooperation covers a) the
transfer of information related to the notification,

b) the transfer of technical data necessary for the identification of those involved in the incident and the person responsible for the incident, c) the data, documents, tools and other information necessary for the investigation, as well as the information containing them to provide authentic bit-identified copies, d) to share special, sectoral characteristics related to the infrastructure affected by the incident, e) to inform the Center's specialists about the measures taken to address the consequences of the incident, and during incident investigation, about infrastructure-related settings, f) to provide access to the infrastructure affected by the cybersecurity incident for the Center's specialists, and g) to install early warning or trap systems and sensors deemed necessary based on the risk analysis conducted by the Center.

(2) The installation of early warning or trap systems and sensors as referred to in point g) of paragraph (1) shall be subject to the agreement with the organization. may take place after prior consultation and the installation may not hinder or endanger the operation of the organization.

(3) The organization affected by the cybersecurity incident shall, at the request of the Center, provide the technical, to collect technical data and information and to transmit it in electronic form or make it accessible in any other way.

(4) If the organization affected by the cybersecurity incident is unable to collect the data referred to in paragraph (3) for any reason, the representative of the Center shall, within the framework of on-site consulting, make a proposal with the involvement of experts from the organization concerned on the method of collecting and providing the necessary data, or the Center may collect the data. The organization affected by the incident shall ensure that the Center has access to the data.

(5) The service providers concerned are obliged to introduce bans, limit, suspend or terminate user and subscriber access, as necessary, free of charge, at the request of the Centre, in relation to subscribers affected by the cybersecurity incident.

Section 84 (1) The organization affected by the cybersecurity incident shall, with the support of the Center, develop and immediately implement the measures necessary to eliminate the cybersecurity incident.

(2) The organization shall, after the conclusion of the investigations, provide information on the incident management plan for eliminating the identified deficiencies. informs the relevant authority.

(3) The organization affected by the cybersecurity incident shall review the electronic information system after the incident has been resolved. the completeness of its risk analysis and risk management systems and implements the necessary modifications.

Section 85. The organization exercising the right of disposal over the central system and the central service provider shall, during incident management,

a) the technical information necessary to identify the organization involved in the cybersecurity incident and the person responsible for the incident, to transfer technical data to the Center, b) to apply protective measures and technical solutions against known threats, c) to provide data pursuant to Section 83 (1) at the request of the Center indicating signs of interference in network traffic for the purpose of analysis and evaluation, and

d) cooperate in tasks related to cybersecurity incidents as determined by the Center.

Section 86 (1) When handling cybersecurity incidents, the Centre may, as necessary, become familiar with the various service or business continuity regulations and procedures of intermediary service providers, including their business continuity plans and disaster recovery plans.

(2) Within the framework of cooperation with the Center, the intermediary service provider affected by the cybersecurity incident shall, at the request of the Center, provide the incident management center with the data necessary to identify those involved in the incident, the attacker and the attacked, and, as necessary, introduce bans, restrict, suspend or terminate user or subscriber access in relation to the subscribers affected by the incident in order to manage the specific incident.

(3) In the event of the provision of a service deemed dangerous or harmful, the Centre may oblige the intermediary service provider to: to disable the service.

Section 87 (1) The Centre shall take action against any organization or service provider that fails to comply with the notification, information or cooperation obligations. reports to the cybersecurity authority supervising it.

(2) Based on the information it has obtained during the handling and investigation of the cybersecurity incident, the Center may initiate an obligation for the national cybersecurity authority to conduct a vulnerability assessment of the electronic information system affected by the cybersecurity incident.

§ 88. The Center shall keep a closed technological log of the cybersecurity incident, which shall contain the details of the incident. measures taken in support of the investigation and their results.

Section 89 The provisions of this chapter shall also apply to voluntary reports.

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

Section 90 (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 65–67, Sections 73–76, Sections 78, 79, 81, Section 83(1)(a)–f), Section 83(2) and (3), Section 84(1) and Sections 86–89 shall apply, with the exception of Section 67(1)(2)(k) and Section 67(1)(7)(b).

(2) Where this Regulation refers to a cybersecurity authority, it shall be subject to Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to organisations belonging to the European Parliament and of the Council, the authority referred to in Regulation (EU) 2022/2554 of the European Parliament and of the Council shall be understood.

(3) Participation in the cybersecurity exercise is mandatory if ordered by the Centre. The scope of organisations covered by Regulation (EU) 2022/2554 of the European Parliament and of the Council to be covered by the cybersecurity exercise and the planned date of the cybersecurity exercise shall be determined by the Centre in advance of consultation with the authority referred to in Regulation (EU) 2022/2554 of the European Parliament and of the Council.

Chapter VII

ORGANIZATIONAL SYSTEM FOR THE COORDINATION OF CYBERSECURITY-RELATED TASKS

33. Commissioner for Cybersecurity

Section 91 (1) The Commissioner responsible for cybersecurity may appoint a deputy. The deputy shall act within the scope of his mandate.

(2) The Commissioner responsible for cybersecurity shall be involved in the development and implementation of cybersecurity-related legislation. review.

(3) The Commissioner responsible for cybersecurity may, based on the decision of the National Cybersecurity Working Group, initiate the the Minister responsible for IT is reviewing legislation related to cybersecurity.

34. The National Cybersecurity Working Group

Section 92 (1) The President of the National Cybersecurity Working Group – in case of impediment – shall be appointed pursuant to Section 91 (1) person replaces.

(2) The members of the National Cybersecurity Working Group

are: a) the ministers,

b) the Director General of the National Security Service, c) the

President of the National

Security Service, d) the President of the

Hungarian National Bank, e) the head of the central body of defense and security

administration and f) the Prime Minister's Chief National Security Advisor

1-1 person in a managerial position delegated by.

(3) According to paragraph (2) a), the ministers shall be members of the National Cybersecurity Working Group independently and independently of each other. they delegate members.

(4) In addition to the provisions of paragraph (2), the members of the National Cybersecurity Working Group shall be the Commissioner responsible for cybersecurity. persons invited by.

(5) [19] The person delegating the member shall decide on the recall of a member of the National Cybersecurity Working Group on his or her own initiative or based on the proposal of the chair of the National Cybersecurity Working Group.

(6) The Chairman of the National Cybersecurity Working Group shall report on the work of the National Cybersecurity Working Group at least every six months. reports to the Minister responsible for IT.

35. Operational Corps

He/she [20] The Commissioner responsible for cybersecurity, acting as the head of the Operational Team, shall be subject to the provisions of Section 91 (1) in the event of his/her obstruction. shall be replaced by a person appointed pursuant to Section **93** (1).

(2) The members of the Operational

Staff are: a) a senior person performing operational tasks delegated by the bodies or organizations referred to in Section 92(2),

19A Section 92. (5) of Government Decree 189/2025. (VII. 3.) 9. Text established by §.

20A Section 93. Paragraph (1) of Government Decree 189/2025. (VII. 3.) Section 17. Point b) Text amended accordingly.

b) a senior person delegated by the central body of the professional disaster management body, c) a senior person delegated by the body or organization involved in the management of the cybersecurity crisis, d) persons invited by the Commissioner responsible for cybersecurity.

36th Cybersecurity Forum

§ 94. The Cybersecurity Forum (hereinafter referred to as the Forum), consisting of academic, research, professional, economic and other non-governmental actors invited by the National Cybersecurity Working Group, is led by the President of the National Cybersecurity Working Group, and the professional coordination of the Forum's work is carried out by a person appointed by the Commissioner responsible for cybersecurity.

37. Cybersecurity Sub-Working Groups

Section 95 (1)[21] The National Cyberspace Working Group and the International and European Union Cyberspace Working Group (hereinafter collectively referred to as the Cybersecurity Sub-Working Groups) assist the National Cybersecurity Working Group in its professional and coordination activities and in the implementation of its decisions.

(2) The National Cyberspace Working Group shall be led by a member of the National Security Service appointed by the Head of the National Security Service. It is performed by a person from the staff of the specialized service.

(3) The International and European Union Cyberspace Working Group shall be led by the cyberspace coordinator appointed by the minister responsible for foreign policy, in consultation with the minister responsible for IT.

(4) [22] The members of the Cybersecurity Sub-Working Groups are persons delegated by state bodies or organizations and non-governmental experts invited by the leaders of the Cybersecurity Sub-Working Groups, as well as the Commissioner responsible for cybersecurity. The Chairman of the National Cybersecurity Working Group may make proposals to the leaders of the Cybersecurity Sub-Working Groups in connection with the invitation of members of the Cybersecurity Sub-Working Groups.

(5) Upon the proposal of the National Cyberspace Working Group, the National Cybersecurity Working Group may issue non-legally binding recommendations on best practices in the field of cyberattack management and electronic information security. (6)

[23] The National Cyberspace Working Group contributes, as necessary, to the implementation of professional background tasks necessary for the sectoral and governmental management of cybersecurity crises, in the development of professional proposals and mandates related to the classification of cybersecurity incidents as cybersecurity crises and the relevant positions to be represented by Hungary.

(7) The National Cyberspace Working Group is tasked with strengthening national cybersecurity in all sectors.

(8) The task of the International and European Union Cyberspace Working Group is to facilitate the regular exchange of information between state bodies on cybersecurity work taking place in international organizations, the European Union, and bilateral and multilateral cooperation, and to coordinate the development of the relevant position to be represented by Hungary.

(9) At the request of the National Cybersecurity Working Group, thematic working groups may also be established within the framework of the Cybersecurity Sub-Working Groups.

38. Secretariat

Section 96. The administrative tasks related to the operation of the National Cybersecurity Working Group, the Forum and the Cybersecurity Sub-Working Groups shall be carried out by a secretariat (hereinafter referred to as the Secretariat) provided by the Minister responsible for IT, under the direction of the Commissioner responsible for cybersecurity. The Secretariat shall also provide expert support to the Commissioner responsible for cybersecurity.

39. Tasks of government coordination bodies

Section 97 (1) The task of the National Cybersecurity Working Group is to facilitate the coordination of government activities in the areas of action defined in the National Cybersecurity Strategy of Hungary, to monitor implementation, and to provide opinions on legislation related to cybersecurity.

21A Section 95(1) of Government Decree 189/2025. (VII. 3.) Section 16, point 11 Text amended accordingly.

22A Section 95(4) is the text amended in accordance with Section 16(12) of Government Decree 189/2025 (VII. 3.) .

23A Section 95(6) is the text amended in accordance with Section 16(13) of Government Decree 189/2025 (VII. 3.) .

(2) [24] The National Cybersecurity Working Group shall prepare an action plan (hereinafter referred to as the National Cybersecurity Action Plan) containing government measures associated with the areas of action specified in paragraph (1), taking into account the proposals and opinions of the Forum, under the guidance of the Cybersecurity Sub-Working Groups and the Commissioner responsible for cybersecurity. The National Cybersecurity Action Plan shall be reviewed annually by the National Cybersecurity Working Group.

(3) The Secretariat shall coordinate the annual review of the National Cybersecurity Action Plan, involving the Cybersecurity Sub-Working Groups.

Section 98 (1) The National Cybersecurity Working Group, in accordance with the performance of its tasks, shall, as necessary, but at least every three months: holds a meeting convened by the Commissioner responsible for cybersecurity.

(2) The meetings of the National Cyber Security Working Group shall be chaired by the Chairman or Deputy Chairman of the National Cyber Security Working Group. The Secretariat prepares minutes of the meetings.

Section 99 (1) The Operational Body shall meet as necessary, but at least every three months, in order to fulfil its tasks, and shall be convened by: Commissioner responsible for cybersecurity convenes.

(2) The tasks of the Operational Staff

are: a) preventing, responding to and preventing cybersecurity incidents resulting in a cybersecurity crisis,
carrying out tasks related to mitigating the consequences of, and preparing for,

b) exchange, summarize and evaluate information on cybersecurity incidents, c) propose cybersecurity training

and exercises in order to prepare for the prevention and management of cybersecurity crises,

d) monitoring of cybersecurity incidents of which it has become aware, including the continuous analysis of threats and risks, e) proposing the classification of a significant or

large-scale cybersecurity incident as a cybersecurity crisis, f) coordinating reconnaissance and operational measures in a cybersecurity crisis and taking the necessary official measures

initiating measures,

g) in the event of a cybersecurity crisis, with the involvement of the relevant bodies and organizations, the time required for recovery and the examination of the replaceability of failed services,

h) informing the National Cybersecurity Working Group, as necessary, about the common situational awareness and the measures taken.

(3) The obligation of the members of the Operational Staff and other relevant bodies to provide information to the Operational Staff does not affect their information activities and other obligations prescribed by law or other public law regulatory instruments.

(4) The Operational Body shall establish its own rules of procedure, and the permanent members may initiate the inclusion of an agenda for its meetings. The proposal for the agenda shall be submitted to the chairman in writing, with justification.

(5) The Operational Group shall report on its activities to the National Cybersecurity Working Group at least every six months.

Section 100 (1)[25] The Forum shall meet as necessary, but at least every three months, in accordance with the tasks defined in the law or by the Commissioner responsible for cybersecurity, the National Cybersecurity Working Group or the Sub-Working Groups. The meeting shall be convened by the Chairman of the National Cybersecurity Working Group or a member designated by him.

(2) The meetings of the Forum shall be chaired by the Chairman of the National Cybersecurity Working Group or a member designated by him/her. A reminder of the meetings shall be prepared by the Tikarság.

Section 101 (1)[26] The Cybersecurity Sub-Working Groups meet as necessary, but at least every three months, in accordance with the tasks defined in the law and by the Commissioner responsible for cybersecurity, the National Cybersecurity Working Group. The meetings are convened by the heads of the Cybersecurity Sub-Working Groups.

(2) The Secretariat shall prepare a report on the meetings of the Cybersecurity Sub-Working Groups.

§ 102. The procedural rules governing the operation of the National Cybersecurity Working Group, the Forum and the Cybersecurity Sub-Working Groups are contained in the rules of procedure prepared by the members and approved by the chair of the National Cybersecurity Working Group.

24A Section 97(2) of Government Decree 189/2025. (VII. 3.) Section 17(c) Text amended accordingly.
25A Section 100. (1) of Government Decree 189/2025. (VII. 3.) 10. Text established by §.
26A Section 101(1) of Government Decree 189/2025. (VII. 3.) 11. Text established by §.

Section 103. Members of the National Cybersecurity Working Group, the Forum, the Cybersecurity Sub-Working Groups and the Operational Team, as well as state leaders, government officials, public employees, tax and customs authority employees, professional service employees, law enforcement administrative employees, national security service employees, national security employee employees, professional military service employees, national defense employees, and executive officers or employees of exclusively state-owned companies who contribute to their work, shall not receive remuneration.

§ 104. Communication tasks related to the National Cybersecurity Working Group shall be performed and supervised by the Commissioner responsible for cybersecurity or his/her deputy.

Chapter VIII

THE NATIONAL COORDINATION CENTER

Section 105. The Government shall, pursuant to Section 75 of the Cybersecurity Act. The National Security Service is designated as the national coordination center pursuant to §.

Chapter IX

MANAGING CYBERSECURITY EMERGENCIES

40. Organizational system for managing cybersecurity crises

Section 106 (1) The tasks related to the management of a cybersecurity crisis situation shall be performed by the relevant persons, bodies and organizations under the Cybersecurity and this Decree, and are implemented on the basis of the applicable legal provisions and the provisions of the public law organization regulatory instrument.

(2) The Operational Staff shall continuously monitor the existence of the conditions for the cybersecurity crisis situation, and if the conditions for declaring a cybersecurity crisis situation no longer exist, it shall initiate the Minister responsible for IT to submit a proposal to the Government to repeal the government decree declaring a cybersecurity crisis situation.

(3) The administrative and coordination tasks related to the management of the cybersecurity crisis situation are carried out in accordance with Section 52 c) of the Cybersecurity Act. provided by the national incident management centre (hereinafter referred to as the national incident management centre), with the active support of the relevant cybersecurity incident management centre.

(4) The central body of defence and security administration and the Defence Council, upon the proposal of the minister responsible for IT, shall be informed immediately of the sectoral measures taken in relation to the management of the cybersecurity crisis.

(5) Tasks related to international cooperation in the management of cybersecurity crises shall be carried out by the IPCR.
The coordination of information exchange between Member States on the platform is carried out by the central body of the defence and security administration.

(6) The professional tasks related to the management of the cybersecurity crisis situation shall be performed by the EU on behalf of Hungary.
In CyCLONe a) at
the senior official and executive level, the central body of the defense and security administration, b) at the expert
level ba) the National
Security Service, bb) the ministry led by the
minister responsible for IT and, upon request, by the minister responsible for national defense
It is administered by a
ministry led by

41. Cybersecurity planning and preparedness order

Section 107 (1) The national cyber crisis management plan of Hungary (hereinafter referred to as: national cyber crisis management plan) shall be prepared by the Centre, under the coordination of the Commissioner responsible for cybersecurity, based on the proposals of the National Cyber Security Working Group.

(2) The national cyber crisis management plan shall be developed in accordance with and in accordance with the provisions of the National Coordinated Defense Plan. must be prepared.

(3) The national cyber crisis management plan shall specify at least the following: a) the objectives
of national preparedness measures and activities,

b) the tasks and responsibilities of the authorities dealing with cybersecurity crisis management, c) the procedures for handling cybersecurity crisis situations, including their integration into the general national crisis management framework and information exchange channels,

(d) national preparedness measures, including exercises and training activities; (e) identification of relevant public and private stakeholders and infrastructure; (f) national procedures and agreements between relevant national authorities and bodies.

(4) The relevant information referred to in paragraph (3) shall be submitted to the European Commission and EU-CyCLONe within three months of the adoption of the national cyber crisis management plan, which shall not include information that is sensitive from a national security perspective or the disclosure of which would be contrary to or detrimental to the national security, defence, public security or fundamental interests of Hungary.

(5) The information referred to in paragraph (4) shall be sent by the central body of the defence and security administration to the European Commission and the For EU-CyCLONe after consulting the Defence Council.

Section 108 (1) Section 74 (10) of the Cybersecurity Act The cybersecurity plan must be prepared based on professional standards and government guidelines, and the head of the preparing organization ensures its continuous monitoring and review of related measures.

(2) The cybersecurity plan is part of the organization's Defense and Security Action Plan, which contains special measures specific to the operation of the defense and security organization.

Section 109 (1) In order to prepare for cybersecurity crises, the Operational Body shall: a) conduct sectoral or central cybersecurity crisis management exercises, and b) provide education and training to strengthen cybersecurity and cyber awareness.
can initiate its organization.

(2) The practice referred to in paragraph (1) a) shall be carried out by the Operational Body a) in cooperation with the national cybersecurity authority, the central body of the defense and security administration and the central body of the professional disaster management body, as well as the organization representing the relevant sector, and, where justified, the Military
Organized with the involvement of the National Security Service and the Hungarian Defence Forces,

b) is carried out with the involvement, as necessary, of organizations operating critical infrastructures and organizations significant for the defense and security of the country, and

c) in the case of qualification as a central practice, it is carried out under the direction of the central body of the defense and security administration.

(3) The organization concerned by the practice referred to in paragraph (1) a) or the education and training referred to in paragraph (1) b)
is obliged to participate in the internship, education and training, and to ensure the necessary conditions.

Section 110. In order to prepare for and manage cybersecurity crises, the electronic communications service provider, the intermediary service provider, the organization exercising the right of disposal over the central system, and the central service provider shall cooperate with the national incident management center, the Center, and the Operational Headquarters, taking into account the cybersecurity tasks specified in the law.

42. Notification of a major incident, informing the European Commission and the Member States

Section 111 (1) The European Commission and the EU-CyCLONE senior officials shall be responsible for the large-scale cybersecurity
Incidents are reported by the person designated in accordance with Section 106(6)(a).

(2) The content of the information provided to the relevant EU Member States via EU-CyCLONE shall be determined by the Operational Staff on the basis of a proposal from the In order to manage a cybersecurity crisis, the decision is made by the person or head of the organization designated by the Government.

Chapter X

COOPERATION AND REPORTING

43. National cooperation

Section 112 (1) The national cybersecurity authority, the National Cybersecurity Authority, the defence cybersecurity authority, the authority pursuant to Regulation (EU) 2022/2554 of the European Parliament and of the Council, the single point of contact, the Centre, the defence cybersecurity incident management centre and the sectoral cybersecurity incident management centre shall cooperate in order to implement the obligations specified in the law.

(2) The organisations referred to in paragraph (1) shall cooperate and may conclude cooperation agreements.

a) law enforcement authorities, b) the
National Data Protection and Freedom of Information Authority, c) Regulation
(EC) No 2320/2002 of 28 December 2008 on common rules for the security of civil aviation and repealing Regulation (EC) No 2320/2002.
with the authority referred to in Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008,
d) the authority referred to in Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 of the European Parliament and of the Council and Directives 2014/30/EU and 2014/53 of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91, e) on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/
EC with the supervisory authority pursuant to Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on the placing of

f) Regulation (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code
with the national regulatory authority pursuant to Council Directive [hereinafter: Directive (EU) 2018/1972 of the European Parliament and of the Council], g) pursuant
to the Act on the Protection of the Rights of Persons
with Disabilities. with the appointing authority pursuant to the
Act, h) pursuant to the Act. and (i) the competent authority under other sector-specific Union acts.

(3) The organisations referred to in paragraph 1 and the authority referred to in Regulation (EU) No 910/2014 of the European Parliament and of the Council, Regulation (EU) 2022/2554 of the European Parliament and of the Council and Directive (EU) 2018/1972 of the European Parliament and of the Council shall regularly exchange information, including on cybersecurity incidents and cyber threats.

(4) The national cybersecurity authority and the Centre shall, in accordance with Regulation (EU) 2022/2554 of the European Parliament and of the Council
You can learn the following data from the authority's register: a) data
necessary for identifying the organization, b) the organization's
contact details, including electronic contact details.

Section 113 (1) The SZTFH shall inform the single point of contact a) every two years
by 15 March, regarding the organisations referred to in Section 1(1)(d) and (e) of the Cybersecurity Act, broken down by sectors and subsectors referred to in Annex I or II to Directive (EU) 2022/2555 of the European Parliament and of the Council;

(b) the following data in relation to DNS providers, top-level domain name registrars, organisations providing domain name registration services, cloud service providers, data centre providers, content delivery network providers, managed service providers and managed security service providers, as well as online marketplaces, online search engines and social media service platforms:

ba) name of the
organisation, bb) sector, subsector and type of organisation concerned as referred to in Annex I or II to Directive (EU) 2022/2555 of the European Parliament and of the Council, bc)
the organisation's registered office, establishment, branch or, in the case of an organisation not established in the European Union, the designated
the address of the representative,
bd) contact details of the organisation and its designated representative, including e-mail address and telephone number, be)
the European Union Member States in which the organisation provides services; c) any changes to the data
referred to in point ab) within 30 days of the notification of the change.

(2) The authority referred to in Regulation (EU) 2022/2554 of the European Parliament and of the Council shall inform the single point of contact
every two years by March 15th, on the number of organizations in the following sectors:
a) in the case of the banking services sector, credit institutions as defined in Article 4(1) of Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012, b) in the case of the financial market infrastructures sector, ba) operators of trading venues as defined in Article
4(1)(24) of Directive 2014/65/EU of the European Parliament
and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU, and

bb) Act of 4 July 2012 on OTC derivatives, central counterparties and trade repositories
Central counterparties as defined in point (1) of Article 2 of Regulation (EU) No 648/2012 of the European Parliament and of the Council.
(3) The national cybersecurity authority shall inform the single point of contact: a) every two years by 31
March

aa)[27] Cybersecurity Act, Section 1 (1) a)–c) and point f), and Section 1(2a) the number of essential and important organisations, broken down by sector or subsector referred to in Annex I or II to Directive (EU) 2022/2555 of the European Parliament and of the Council, and

ab) the number of identified essential and important organisations, broken down by sector, sub-sector and type of service provided by them as referred to in Annex I or II to Directive (EU) 2022/2555 of the European Parliament and of the Council, and the provision on which their identification is based, b) at the request of the

European Commission, the names of the essential and important organisations referred to in point ab), provided that this does not prejudice national security, defence or other security interests.

(4) The Centre shall inform the single point of contact every three months about reported cybersecurity incidents, cyber threats and near-misses by sending a statistical report on the reports.

44. The single point of contact

Section 114 (1) The single point of contact shall perform liaison functions with

a) the European Commission,

b) ENISA, c) the

single points of contact of other European Union Member States, d) the

Cooperation Group of Directive (EU) 2022/2555 of the European Parliament and of the Council (hereinafter referred to as the NIS Cooperation Group),[28] and

e) with the Hungarian cybersecurity agencies.

(2) Based on the data provided under Section 113, the single point of contact shall send: a) to the European

Commission and the NIS Cooperation Group: every two years, in accordance with Regulation (EU) 2022/2555 of the European Parliament and of the Council the number of essential and important organisations for each sector and subsector referred to in Annex I or II of the Directive;

b) every two years, the European Commission shall provide the number of identified essential and important organisations, their sectors and subsectors referred to in Annex I or II to Directive (EU) 2022/2555 of the European Parliament and of the Council, relevant information on the type of service they provide and the provision on which their identification is based; c) upon request of the European

Commission, the names of the essential and important organisations referred to in point b), provided that this does not prejudice national security, defence or other security interests;

d)[29] ENISA's information pursuant to Section 113(1)(b) and (c) for the service provider register.

(2a)[30] The single point of contact after receiving the data provision pursuant to Section 113(1)(c) immediately inform ENISA of any change in the data submitted to the service provider register.

(3) The single point of contact shall submit a summary report to ENISA every three months on the reported significant incidents, incidents, cyber threats and near-incident situations, based on the data provided by the Centre pursuant to Article 113(4).

Section 115 (1) In the course of fulfilling the data provision and information obligation, sensitive information may only be shared with the European Commission and other European Union bodies 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 must be limited to what is relevant and proportionate to the purpose of the exchange of information.

(2) During the exchange of information, the confidentiality of the information provided shall be preserved and the rights of the data subject shall be protected. organizations' security and business interests.

(3) No data or information may be provided within the framework of data provision and information that would be contrary to or would harm Hungary's national security, national defense or fundamental security interests.

45. European peer review

Section 116 (1) The national cybersecurity authority and the Centre may, with the consent of the National Cybersecurity Working Group, initiate and participate on a voluntary basis in peer reviews pursuant to Directive (EU) 2022/2555 of the European Parliament and of the Council (hereinafter referred to as: European peer review). A European peer review shall consist of at least one of the following:

(a) the level of implementation of cybersecurity risk management measures and reporting obligations referred to in Articles 21 and 23 of Directive (EU) 2022/2555 of the European Parliament and of the Council;

27A Section 113(3)(a)(aa) is the text amended in accordance with Section 16(14) of Government Decree 189/2025 (VII. 3.) .

28A Section 114(1)(d) in conjunction with Section 12(1) of Government Decree No. 189/2025 (VII. 3.) established text.

29A Section 114(2)(d) is the text amended in accordance with Section 16(15) of Government Decree 189/2025 (VII. 3.) .

30A Section 114. Subsection (2a) is replaced by Section 12. Subsection (2) of Government Decree 189/2025. (VII. 3.) he enrolled.

(b) the level of capabilities, including the available financial, technical and human resources, and the effectiveness of the competent authorities in carrying out their tasks; (c) the operational capabilities
of CSIRTs; (d) the level of implementation
of mutual assistance referred to in Article 37 of Directive (EU) 2022/2555 of the European Parliament and of the Council; (e) the level of
cybersecurity information sharing referred to in Article 29 of Directive (EU) 2022/2555 of the European Parliament and of the Council
level of implementation of agreements; f)
specific issues of a cross-border or cross-sectoral nature.

(2) The European peer review shall be carried out by the European Cybersecurity Agency, based on the methodology developed by the NIS Cooperation Group. carried out by experts.

(3) The national cybersecurity authority and the Centre may: a) when initiating the European
peer review, define specific questions for the purpose of the European peer review, b) before its commencement,
notify the participating Member States of the scope of the European peer review, including the specific questions, c) before its commencement,

conduct a self-assessment of the assessed, based on the methodology published by the NIS Cooperation Group.
aspects, and can pass this self-assessment on to designated cybersecurity experts,

d) report the risk of conflict of interest affecting the expert participating in the assessment to the Member State concerned, the NIS Cooperation Group, the
To the European Commission and ENISA,

e) may raise an objection to the expert before or after the commencement of the investigation, providing appropriate justification.
against the appointment of the expert by the appointing Member State, f) may make

comments on the draft report prepared as a result, g) may publish the report prepared on the subject or an extract thereof on its

website. 31 h) during the course of the assessment, without prejudice to national or EU law on the protection of confidential
or
classified data and without prejudice to Hungary's national security, public security or essential defence interests, it shall provide the designated cybersecurity experts with the information necessary for the assessment.

(4) [32] The same aspects as those subject to peer review determined pursuant to paragraph (1) and point (a) of paragraph (3) shall not be subject to further peer review within two years of the conclusion of the peer review, unless requested by the national cybersecurity authority or the Centre or agreed upon on the basis of a proposal by the NIS Cooperation Group.

Section 117 (1) In the case of a European peer review initiated by another European Union Member State, the selection of the cybersecurity expert to be delegated by Hungary shall take into account the criteria specified in the methodology developed by the NIS Cooperation Group.

(2) The expert participating in the European
evaluation shall a) act in accordance with the provisions of the code of conduct developed by the NIS Cooperation
Group, b) use the information obtained during the European peer review solely for the purpose of carrying out the evaluation, c) not disclose
sensitive or confidential information obtained during the European peer review to third parties, d) declare any circumstances that may
cause a conflict of interest before or during the appointment.
immediately after the circumstance arises or becomes known,
(e) prepare a report on the results and conclusions of the European peer review, together with the experts carrying out the review.

Chapter XI

FINAL PROVISIONS

46. Provisions entering into force

Section 118 (1) This regulation shall enter into force on 1 January 2025, with the exception of paragraph (2).

(2) Sections 42–44, Section 46, Section 47, Section 144, Annex 2, Annex 3 and Annex 4 shall enter into force on the 16th day following the promulgation of this Regulation. enters into force on the day.

47. Transitional provisions

31A Section 116(3)(h) is replaced by Section 13(1) of Government Decree 189/2025 (VII. 3.) he enrolled.
32 Section 116(4) is replaced by Section 13(2) of Government Decree No. 189/2025 (VII. 3.) he enrolled.

Section 119 (1) The central service provider shall fulfil the obligation set out in Section 15(3) during the year 2025 by making the information set out in Section 15(3) related to the central service available to the user organisation instead of the service catalogue.

(2) The SZTFH shall provide the data pursuant to Section 113(1) for the first time by 31 March 2025, in the sole
towards the contact point.

(3) The authority referred to in Regulation (EU) 2022/2554 of the European Parliament and of the Council shall provide the data referred to in Section 113(2) for the first time by 31 March 2025 towards the single point of contact.

(4) The national cybersecurity authority shall provide the data referred to in Section 113(3)(a) for the first time by March 2025.
It will be delivered to the single point of contact by 31.

(5) The Centre shall provide the data referred to in Section 113(4) for the first time by 15 April 2025, in the sole
towards the contact point.

(6) The single point of contact shall a)
provide the data pursuant to Section 114(2)(a) and (b) for the first time by 17 April 2025, b) provide the data pursuant to
Section 114(2)(d) for the first time by 17 April 2025, c) provide the data pursuant to Section
114(3) for the first time by 30 April 2025.

(7) Act 187/2015 (VII. 13.) on the tasks and powers of the authorities performing security supervision of electronic information systems and the information security supervisor, and on the definition of closed-purpose electronic information systems
Government Decree [hereinafter: Government Decree 187/2015. (VII. 13.)] The national cybersecurity authority shall conduct ongoing official cases pursuant to Government Decree 187/2015. (VII. 13.) close it accordingly.

48. Compliance with European Union law

Section 120 (1) This
Regulation shall be implemented in accordance with 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), and b) Directive (EU) 2022/2555 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.
It serves to comply with Directive (EU) 2022/2557 of the European Parliament and
of the Council of 14 December 2022.

(2) This Regulation
shall: (a) amend 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 Act),

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.

49. Amending provisions

33 Section 121

34 Section 122

35 § 123

36 Section 124

37 § 125

33A Section 121, Section 12(2) of Act CXXX of 2010 has lost its effect.
34A Section 122, Section 12(2) of Act CXXX of 2010 has lost its effect.
35A Section 123, Section 12(2) of Act CXXX of 2010 has lost its effect.
36A Section 124, Section 12(2) of Act CXXX of 2010 has lost its effect.
37A Section 125, Section 12(2) of Act CXXX of 2010 has lost its effect.

38 Section 126

39 § 127

40 Section 128

41 § 129

42 Section 130

43 Section 131

44 Section 132

45 Section 133

46 § 134

47 § 135

48 Section 136

49 Section 137

50 § 138

51 Section 139

52 § 140

53 Section 141

54 Section 142

55 Section 143

56 § 144

57 Section 145

58 § 146

59 § 147

38A Section 126, Section 12(2) of Act CXXX of 2010 has lost its effect.
39A Section 127, Section 12(2) of Act CXXX of 2010 has lost its effect.
40A Section 128, Section 12(2) of Act CXXX of 2010 has lost its effect.
41A Section 129, Section 12(2) of Act CXXX of 2010 has lost its effect.
42A Section 130, Section 12(2) of Act CXXX of 2010 has lost its effect.
43A Section 131, Section 12(2) of Act CXXX of 2010 has lost its effect.
44A Section 132, Section 12(2) of Act CXXX of 2010 has lost its effect.
45A Section 133, Section 12(2) of Act CXXX of 2010 has lost its effect.
46A Section 134, Section 12(2) of Act CXXX of 2010 has lost its effect.
47A Section 135, Section 12(2) of Act CXXX of 2010 has lost its effect.
48A Section 136, Section 12(2) of Act CXXX of 2010 has lost its effect.
49A Section 137, Section 12(2) of Act CXXX of 2010 has lost its effect.
50A Section 138, Section 12(2) of Act CXXX of 2010 has lost its effect.
51A Section 139, Section 12(2) of Act CXXX of 2010 has lost its effect.
52A Section 140, Section 12(2) of Act CXXX of 2010 has lost its effect.
53A Section 141, Section 12(2) of Act CXXX of 2010 has lost its effect.
54A Section 142, Section 12(2) of Act CXXX of 2010 has lost its effect.
55A Section 143, Section 12(2) of Act CXXX of 2010 has lost its effect.
56A Section 144, Section 12(2) of Act CXXX of 2010 has lost its effect.
57A Section 145, Section 12(2) of Act CXXX of 2010 has lost its effect.
58A Section 146, Section 12(2) of Act CXXX of 2010 has lost its effect.
59A Section 147, Section 12(2) of Act CXXX of 2010 has lost its effect.

60
Section 148

61
Section 149

62
Section 150

63
§ 151

64
Section 152

65
Section 153

Annex 1 to Government Decree 418/2024. (XII. 23.)

Considerations for implementing data classification

1. **Basic goal**

The purpose of data classification is to ensure the confidentiality, integrity and availability of data managed in an electronic information system. should be assessed in terms of availability and risk-proportionate protection should be developed in accordance with their security weight. Data classification also contributes to the clear definition of the processing of data managed in the electronic information system abroad or in the cloud. The organization may also take into account additional data classification aspects in addition to the aspects mandatorily specified in points 2 and 3, which it is obliged to document in connection with the data classification.

2. **Classification of data according to confidentiality**

2.1. **B1 level data**

Any breach or loss of the confidentiality of this data would have no or only negligible financial or reputational impact. can cause loss to the organization.

2.2. **B2 level data**

Any breach or loss of the confidentiality of this data may only cause minor financial or reputational loss to the organization.

2.3. **B3 level data**

A breach or loss of the confidentiality of this data could cause significant financial or reputational loss to the organization.

2.4. **B4 level data**

Any breach or loss of the confidentiality of this data could cause critical financial or reputational loss to the organization.

3. **Assessing data integrity and availability**

66 3.1. **SR1:** DATA **INTEGRITY AND AVAILABILITY IS NOT CRITICAL**

Damage to or loss of the integrity and availability of data stored and managed on an electronic information system may not cause, or may not cause, significant financial or reputational loss to the organization or other person.

3.2. **SR2:** INTEGRITY OR AVAILABILITY OF DATA **IS CRITICAL**

60A Section 148, Section 12(2) of Act CXXX of 2010 has lost its effect.
61A Section 149, Section 12(2) of Act CXXX of 2010 has lost its effect.
62A Section 150, Section 12(2) of Act CXXX of 2010 has lost its effect.
63A Section 151, Section 12(2) of Act CXXX of 2010 has lost its effect.
64A Section 152, Section 12(2) of Act CXXX of 2010 has lost its effect.
65A Section 153, Section 12(2) of Act CXXX of 2010 has lost its effect.
66Sub-paragraph 3.1 of Annex 1 is replaced by Section 16 of Government Decree 189/2025 (VII. 3.). and point 17 Text amended accordingly.

Damage to or loss of the integrity or availability of data stored and managed on an electronic information system can cause significant or critical financial or reputational loss to the organization or another person.

67 4. **The result of data classification**

4.1. **Encryption**

For B2 level data: if technologically possible, encryption must be ensured if foreign data processing or the use of non-private cloud services is implemented.

In the case of level B3–4 data: encryption must be ensured in all cases if foreign data processing or non-private cloud services are used.

4.2. **Location of data processing**

4.2.1. In the case of SR2 classified data: Unless otherwise provided by law, the processing of data may be carried out with geographical restrictions. The data may only be stored in the territory of an EEA member state. In the case of foreign data storage, it must be ensured that the data is also available in the territory of Hungary.

4.2.2. In addition to the provisions of subsection 4.2.1., the numerical value of the data category B and SR shall be added to determine the possible location of data processing. Unless otherwise provided by law, based on the result obtained, the data may be classified into the following categories F1–F4, to which the following provisions shall apply:

4.2.2.1. F1: if the total value of B and SR is: 2

F1 rated data

– without geographical restrictions,

– without restrictions when using a non-private cloud service

can be handled and stored.

4.2.2.2. F2: if the total value of B and SR is: 3

Data classified as F2

– in the case of SR1 classified data, without geographical restrictions, in the case of SR2 classified data, exclusively within the territory of an EEA member state,

– if you are not using a private cloud service

– outside the territory of an EEA Member State, exclusively in a non-private cloud with a cybersecurity certification, audit or authorization by a third party in relation to the service used, as listed on the website of the cybersecurity authority (hereinafter referred to as: third-party certified) or

– Even in an uncertified non-private cloud within an EEA member state

can be handled and stored.

4.2.2.3. F3: if the total value of B and SR is: 4

Data classified as F3

– exclusively within the territory of an EEA member state

– if you are not using a private cloud service

– in a third-party certified non-private cloud or

– in case of use of non-certified non-private cloud services only in Hungary

can be handled and stored.

4.2.2.4. F4: if the total value of B and SR is: 5 or 6 67Point

4 of Annex 1 in accordance with Section 15 (1) of Government Decree 189/2025. (VII. 3.) established text.

Data classified as F4

– exclusively in the territory of Hungary,

– when using cloud services

– in a third-party certified private cloud or

– in government cloud

they can be handled.

4.3. **Summary of the results of data classification:**

	THE	B	C
1		SR1	SR2
2	B1	F1	F2
3	B2	F2	F3
4	B3	F3	F4
5	B4	F4	F4

Annex 2 to Government Decree 418/2024. (XII. 23.)

Section 1(1)(a)–(c) of the Cybersecurity Act cybersecurity fines that can be imposed on an organization under extent

	THE	B	C
1	**Name of the violation**	**The minimum fine (in HUF)** is 200,000.	**The maximum fine (in HUF)** is 2,000,000.
2 failure to submit an application for official registration of the person responsible for the security of the electronic information system **3** failure to submit an application for official registration of the information security policy **4** failure to comply with the obligation to classify into a security class **5** failure to submit an application for modification of the data of the person responsible for the security of the electronic information system		200,000	2,000,000
		200,000	4,000,000
		200,000	2,000,000
6 essential cyber hygiene practices and cybersecurity training organization or failure to prove participation in them		400,000	4,000,000
7 failure to cooperate with incident management centers		500,000	50,000,000
8 failure to comply with the obligation to conduct vulnerability assessments or incident investigations ordered by the national cybersecurity authority or a state body authorized to conduct vulnerability assessments		500,000	50,000,000
9 approved by the national cybersecurity authority failure of the organization to implement a vulnerability management plan		200,000	10,000,000
10 Failure to introduce and apply proportionate security measures		200,000	10,000,000
11 failure to report a cybersecurity incident **12** failure to comply with the obligation to provide information to users of the services provided by the organization or other stakeholders		500,000	5,000,000
		2,000,000	20,000,000
13 failure to prepare a final report or its improper completion **14** failure to comply with the obligation set out in the final, enforceable decision of the national cybersecurity authority **15** cooperation with the information security supervisor		500,000	5,000,000
		1,000,000	50,000,000
failure to **16** breach of the obligation of cooperation of an intermediary service provider **17** falling under the scope of Section 1 (1) b) of the Cybersecurity Act and at the same time falling under Section 2 of the Cybersecurity Act. and Annex 3 In the case of an organization that qualifies as an organization under Section 8(5) of the Cybersecurity Act failure to provide data for registration purposes pursuant to		1,000,000	40,000,000
		1,000,000	40,000,000
		Cybersecurity Act , Section 1 Section 1 (1)(b) of the Cybersecurity Act (1) paragraph b) and subject to the scope of the Cybersecurity Act. 2. and 3.	Cybersecurity TV. 2. and Annex 3 annex according to an organization qualifying as
18 of the Cybersecurity Act. Section 1 (1) b) and at the same time Section 2 of the Cybersecurity Act. and Annex 3 In the case of an organization that qualifies as an organization under the Cybersecurity Act, Section 8		50,000 HUF for activities falling under the scope of Section 1 (1)(b) of the Cybersecurity Act and at the same time	

	THE	B	C
1	**Name of the violation**	**Minimum fine (HUF)**	**Maximum fine (HUF)**
	Paragraph (5) Failure to provide data for registration purposes beyond the deadline		Cybersecurity TV. 2. and Annex 3 a maximum of 0.1% of the net sales revenue of the previous business year – in the absence of sales revenue, the pro rata part of the sales revenue of the current year projected over the entire year – or of the budget revenue appropriation of the previous year, but not more than 15,000,000 HUF
19 of	the Cybersecurity Act. Section 1 (1) b) and at the same time Section 2 of the Cybersecurity Act. and Annex 3 In the case of an organization that qualifies as an organization under Section 7(1) of the Cybersecurity Act Failure to pay the supervision fee	HUF 500,000 is a	maximum of ten times the annual cybersecurity supervision fee
pursu	ant to **20** of the Cybersecurity Act. Section 1 (1) b) and simultaneously subject to the provisions of Section 2 of the Cybersecurity Act. and Annex 3 In the case of an organization that qualifies as an organization under Section 8(3) of the Cybersecurity Act Failure to	50,000 HUF	1,000,000 HUF
send	data changes according to **21** of the Cybersecurity Act. Section 1 (1) b) and simultaneously subject to the provisions of Section 2 of the Cybersecurity Act. and Annex 3 In the case of an organization that qualifies as an organization under Section 16 (1) of the Cybersecurity Act failure to conduct a cybersecurity audit within the deadline	1,000,000 HUF	50,000,000 HUF

Annex 3 to Government Decree 418/2024. (XII. 23.)

Section 1 (1) d) of the Cybersecurity Act and the amount of the cybersecurity fine that can be imposed on an organization under point e)

	THE	B	C
1	**Name of the irregularity Minimum amount of the fine Maximum amount of the fine 2** Section 8 (5) of the Cybersecurity Act Section		
1 (1) of the Cybersecurity Act Section 1 (1) of the Cybersecurity Act for registration under points d) and e) of the organization referred to in points d) and e) of the previous points d) and e) failure to provide data in accordance with the previous section of the Cybersecurity Act, Section 1, Paragraph (1) d) and e) of Section 1 a maximum of 0.1% of the net sales revenue of the organization in the previous business year – in the absence of sales revenue, the pro rata portion of the sales revenue of the current year projected over the entire year – or the budget revenue appropriation of the previous year, but a maximum of HUF 15,000,000 HUF 500,000 a maximum of ten times the annual cybersecurity supervision fee			
3 Section 8 (5) of the Cybersecurity Act Failure to provide data for registration purposes beyond the deadline		
4 Section 7 (1) of the Cybersecurity Act Failure to pay the supervision fee pursuant to **5** Section 8 (3)		
of the Cybersecurity Act Failure to send data changes according to **6** Section 6 (2) of the Cybersecurity	50,000 HUF	1,000,000 HUF
Act Failure to comply with the obligation under Section 16 (1) of the Cybersecurity Act failure to	1,000,000 HUF, the amount referred to in Section 42(2)	
7 conduct a cybersecurity audit within the deadline	1,000,000 HUF	50,000,000 HUF

Annex 4 to Government Decree 418/2024. (XII. 23.)

Amount of fine that can be imposed by the certifying authority

Government Decree 418/2024. (XII. 23.)
On the implementation of the Cybersecurity Act of Hungary

Valid: 2025. 07. 04. – 2025. 07. 18. Query time: 2025.07.13 11:37:21

	THE	B	C
1	**Name of the irregularity**	**The fine is the smallest amount in forints determined**	**The maximum fine amount in forints determined**
2	In the case of self-assessment of conformity, the EU conformity assessment declaration in accordance with Regulation (EU) 2019/881 of the European Parliament and of the Council the obligation to send as provided for in Article 53(3) of the Regulation failure to comply with the certification authority and the European Union For Cybersecurity Agency	50,000	100,000
3	In the case of a self-assessment of compliance, Section 43 (3) of the Cybersecurity Act in paragraph regarding the sending of required documents failure to fulfill obligations to the certification authority	50,000	100,000
4	In Section 44 (1) of the Cybersecurity Act to the conditions set conformity assessment activity by an inappropriate body order	1,000,000	50,000,000
5	Conformity marking Cybersecurity Act, Section 42 (2) unauthorized use according to	300,000	50,000,000
6	Section 48 (5) of the Cybersecurity Act data provision according to failure to	50,000	5,000,000
7	In Section 41 (3) of the Cybersecurity Act specified, the to report a vulnerability or anomaly failure to fulfill an obligation	300,000	5,000,000
8	Any information not included in fields A:2–A:7, disclosed by the certifying authority, Section 49 (1) of the Cybersecurity Act deficiencies according to based on the implementation of the necessary modifications, measures failure to do so	200,000	10,000,000