Act L of 2013

on the information security of state and municipal bodies[1]

For the sake of the nation, the security of the national electronic data assets forming part of the national assets and the information systems used to manage these as well as the critical information systems and infrastructures are particularly important because of the threats against information society nowadays.

It is a societal demand to ensure the secrecy, integrity and availability of data and information processed in electronic information systems, as well as the closed, full, continuous and risk-proportionate protection of the integrity and availability of their infrastructures, and thereby the protection of cyberspace, which are essential for the State and its citizens.

Considering all this, the National Assembly adopts the following Act:

CHAPTER I

GENERAL PROVISIONS

1. Interpretative provisions

Section 1 (1) For the purposes of this Act:

1. '*data'* means carriers of information, formalized images of facts, definitions and instructions which are proper for communication, visualization and technical processing for persons or automated equipment;

2.[2] '*technical manipulation of data'* means the technical operations involved in data processing, irrespective of the method and instruments employed for such operations and the venue where it takes place, provided that such technical operations are carried out on the data;

3.[3] '*processor'* means a natural or legal person, or an organisation not having legal personality which, within the framework and under the conditions laid down in a contract - including but not limited to a contract concluded under a law provision, too -, technically manipulates personal data;

3a.[4] '*data owner'* means the head of the organizational unit to which the processing of the data is assigned by a law or a public regulatory instrument or where the data is generated;

4.[5] '*data processing*' means any operation or set of operations that is performed upon data, whatever method is used, such as in particular collection, recording, organisation, systematization, storage, adaptation or alteration, use, retrieval, transmission, dissemination, alignment or combination, blocking, erasure and destruction, and blocking them from further use, photographing, sound and video recording, and the recording of physical attributes for identification purposes of a person;

---

[1] Promulgated on 25.04.2013

[2] Declared by Section 8 (1) of the Act CXXX of 2015. Effective from 16.07.2015

[3] Declared by Section 8 (1) of the Act CXXX of 2015. Effective from 16.07.2015

[4] Added by Section 8 (4) of the Act CXXX of 2015. Effective from 16.07.2015

[5] Declared by Section 8 (1) of the Act CXXX of 2015. Effective from 16.07.2015

5.[1] '*controller*' means a natural or legal person, or an organisation having no legal personality, which alone or jointly with others determines the purposes of data processing, makes decisions concerning data processing (including the means used) and implements such decisions or has them implemented by a processor;

6. '*administrative protection'* means organisational, regulatory, control measures for protection, as well as education regarding protection;

6a.[2] '*operator of essential services'* means the service providers designated under Section 2/A of the Act CLXVI of 2012 on identification, designation and protection of critical systems and facilities;

7. '*audit'* means conformity assessment and control regarding compliance with regulations;

7a.[3] *'digital service'* means the service determined in Section 2 *j)* of the Act CVIII of 2001 on certain questions of electronic commerce services and services related to information society;

8. '*secrecy'* means the feature of an electronic information system that the data and information stored therein can be accessed, used or dispose of use only by the people entitled thereto and only according to their level of authorization;

9. *'security incident*' means any unwanted or unexpected unique event or series of events causing an actual adverse effect or a previously unknown situation on the security of electronic information systems, and as a result of which the secrecy, integrity, authenticity, functionality or availability of the information contained in the electronic information system is lost or damaged;

10. *'incident response'* means all planned activity for documenting security incidents occurred in an electronic information system, eliminating their consequences, determining the causes of occurrence and the people responsible therefor, as well as for preventing the future occurrence of similar incidents;

11. *'security class'* means the expected strength of the protection of the electronic information system;

12. *'security classification'* means the determination of the expected strength of protection of electronic information systems based on the risks;

13. *'level of security'* means the preparedness of the bodies in handling security duties laid down in this Act and the implementing laws thereof;

14. *'determination of security level*' means the determination of the preparedness of the bodies in handling security duties laid down in this Act and the implementing laws thereof;

14a.[4] '*EEA State'* means the state determined in the act on the right to informational self-determination and on the freedom of information;

14b.[5] '*electronic information system'* means

a) an electronic communication network within the meaning of the act on electronic communications,

b) any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of digital data, or

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

---

[1] Declared by Section 8 (1) of the Act CXXX of 2015. Effective from 16.07.2015

[2] Added by Section 111 (1) of the Act CXXI of 2018. Effective from 01.01.2019

[3] Added by Section 111 (2) of the Act CXXI of 2018. Effective from 01.01.2019

[4] Added by Section 8 (41) of the Act CXXX of 2015. Amended by Section 123 a) of the Act XXXIV of 2019

[5] Declared by Section 111 (3) of the Act CXXI of 2018. Effective from 01.01.2019

15. '*security of electronic information systems'* means the state of the electronic information system in which its protection is closed, full, continuous and risk-proportionate in terms of the secrecy, integrity and availability of data and information processed in such electronic information systems, as well as the integrity and availability of electronic information infrastructures;

16. *'lifecycle'* shall mean the time period comprising planning, developing, operating and dissolving electronic information systems;

17. *'detection'* means recognition of a security incident;

18. *'user'* means the range of persons using a certain electronic information system;

19. *'threat'* means any possible act or event which may damage the protection, security of electronic information systems or electronic information infrastructures, moreover any omission which may damage the protection, security of electronic information systems;

20. *'physical protection'* means protection against threats in physical space, the most important parts thereof are protection against natural disasters, mechanical protection, electronic signalling system, manpower protection, access control systems, surveillance systems, power supply, broadcasted and conducted interference protection, air conditioning and fire protection;

21. *'continuous protection'* means uninterrupted protection also under changing circumstances and conditions over time;

22. '*global cyberspace'* means the set of globally interconnected, decentralized, increasing electronic information systems, as well as the societal and economic processes in the form of data and information appearing through these systems;

23.[1] '*electronic information system for national defence purposes'* means the set of closed electronic information systems and other electronic information systems open upon their functions, purposes, tasks of the national defence forces, the multi-purpose vocational training institutions belonging to the maintenance control of the minister responsible for national defence, that are not national defence organisations, the companies under the ownership of the minister responsible for national defence, the companies under Section 3 (2) c) of the Act CVI of 2007 on state assets, as well as the companies engaged in activity related to national defence interest according to laws, which supports the operation within the national defence sector and between sectors in a sector-specific manner;

24.[2]

25. '*information'* means observation, experience or knowledge about certain facts, objects or phenomena in an accessible format which changes, alters, essentially influences somebody's knowledge, set of skills, its order, reduces or eliminates that person's uncertainty;

26. *'cyber security'* means continuous and planned use of the political, legal, economic, educational and awareness-raising, as well as technical measures to handle existing risks in cyberspace which, ensuring the acceptable level of risks in cyberspace, form cyberspace into a reliable environment for smooth operation and functioning of societal and economic processes;

27. *'cyber protection'* means protection against threats from cyberspace, including but not limited to preservation of the own cyberspace capabilities;

28. *'risk'* means the degree of threat which depends on frequency of threats (likelihood of the occurrence) and the extent of the harm caused thereby;

---

[1] Declared by Section 111 (4) of the Act CXXI of 2018. Amended by Section 151 a) of the Act XXXI of 2020

[2] Repealed by Section 8 (40) a) of the Act CXXX of 2015. Ineffective from 16.07.2015

29. *'risk analysis'* means the identification and the assessment of risks through the survey of the value, the vulnerability (weak spots) the threats of electronic information systems, the expected damages and their frequency;

30. *'risk management'* means the development of a system of measures to reduce risks affecting electronic information systems;

31. *'risk-proportionate protection'* means the protection of an electronic information system during which the costs of protection are proportionate to the value of the damages causable by threats;

32. *'early warning'* means signalling the expected occurrence of any threats long enough before the occurrence of the threat, so that effective protective measures can be adopted;

32a.[1] *'critical data'* means personal data or data protected by any law;

33.[2] *'critical information infrastructure'* means the electronic information facilities, devices or services of critical infrastructures designated as European or national critical infrastructures under the Hungarian Critical Infrastructure Protection Act whose inoperability or destruction would make the infrastructures designated as European or national critical infrastructures, or their parts inaccessible or would significantly reduce their operability;

34. '*logical protection'* means protection established in an electronic information system by information technology tools and procedures (programs, protocols);

35. *'Hungarian cyberspace'* means the part of electronic information systems of global cyberspace which are located in Hungary, as well as the societal and economic processes in the form of data and information through electronic systems of global cyberspace which take place in Hungary, or are directed to Hungary, or Hungary is concerned thereby;

36. *'prevention'* means to avoid the occurrence of the effect of the threat;

37. '*reaction'* means the measure to prevent or delay the spread of a security incident that has occurred, and to mitigate further damage;

38. *'availability'* means to ensure that electronic information systems are available to authorized people and the data processed therein are usable;

39. '*integrity'* means the features of the data regarding that the content and properties of the data are the same as expected, including the certainty that it comes from an expected source (authenticity), and also its traceability, certainty of origin (non-repudiation), as well as the features of electronic information infrastructures that the electronic information infrastructure can be used for its intended purpose;

40. *'vulnerability'* means a part or a feature of electronic information systems through which a threat may materialize;

41. *'vulnerability testing'* means the detection of weak spots (security gaps) of electronic information systems and incidents threatening through them;

41a.[3] '*serious security incident'* means the IT incidents that, if it occurs, secrecy, integrity or availability of the data critical to the operation of the State may be harmed, human lives may be in immediate danger, personal injuries may occur in large numbers, severe loss of confidence may occur against the State or the bodies concerned, fundamental human rights or rights prioritized from the perspective of the operation of society may be infringed;

---

[1] Added by Section 8 (43) of the Act CXXX of 2015. Amended by Section 123 b) of the Act XXXIV of 2019
[2] Declared by Section 119 (1) of the Act CCXXII of 2015. Effective from 01.01.2016
[3] Added by Section 8 (44) of the Act CXXX of 2015. Effective from 16.07.2015

42.[1] *'computer incident response centre'* means the computer emergency response teams operating under the recommendations of the European Network and Information Security Agency which have membership and accreditation in organization specialized in protection of international network security as well as critical information infrastructures [(in European use: CSIRT (Computer Security Incident Response Team), in American use: CERT (Computer Emergency Response Team)];

43.[2] *'bodies'* means the legal entity or the sole proprietor carrying out or having data processing or technical manipulation of data carried out, as well as the operator;

44. *'full protection'* means the protection covering all parts of electronic information systems;

45.[3] *'operator'* means a natural person, a legal entity or a sole proprietor, who or which operates the electronic information system or their parts and is responsible for operation;

46. *'security duties'* means prevention and early warning, detection, reaction, incident management;

47.[4] '*closed electronic information system'* means an electronic information system separated as intended, ensuring to perform national security, national defence, law enforcement, diplomatic information tasks which only meets the special needs, and supports the operation of organization and technology created for this purpose;

48. *'closed protection'* means protection covering all possible threats.

(2)[5]

(3)[6] For the purposes of this Act, the tools (environmental infrastructure, hardware, network and data carriers), and the procedures (regulation, software and related processes) used to process data, information for certain purposes by the data owner, as well as all the persons processing them.

2. Scope of the Act

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

a) central public administration bodies, except for the Government and government committees,

b) the Office of the President of the Republic,

c) the Office of the National Assembly,

d) the Office of the Constitutional Court,

e) the National Office for the Judiciary and the courts,

f) the prosecution services,

g) the Office of the Commissioner for Fundamental Rights,

h) the State Audit Office of Hungary,

i) the Magyar Nemzeti Bank (Central Bank of Hungary),

j) capital and county government offices,

k) offices of the representative body of local and national minority municipalities, official administrative associations,

l) the Hungarian Defence Forces.

---

[1] Amended by Section 8 (39) a) of the Act CXXX of 2015

[2] Declared by Section 8 (2) of the Act CXXX of 2015. Effective from 16.07.2015

[3] Amended by Section 84 a) of the Act XV of 2014

[4] Declared by Section 8 (3) of the Act CXXX of 2015. Effective from 16.07.2015

[5] Repealed by Section 8 (40) b) of the Act CXXX of 2015. Effective from 16.07.2015

[6] Declared by Section 8 (5) of the Act CXXX of 2015. Effective from 16.07.2015

(2) The provisions of this Act shall apply to the protection of the electronic information systems of:

a) the bodies determined in paragraph (1) and the bodies processing data for them,

b) the processors of state records laid down in laws, within the scope of national data assets,

c)[1] the infrastructures designated as European or national critical infrastructures under the Hungarian Critical Infrastructure Protection Act,

d)[2] the contributors in providing essential services to the operators of essential services,

e)[3] the bodies under national security protection.

(3)[4] In case of closed electronic information systems of the bodies under the leadership and control of the minister responsible for national defence determined in a governmental decree, the body designated by the Government shall carry out the administrative authority duties laid down in this Act and the security surveillance as set out in governmental decrees.

(4)[5]

(5)[6] In case of electronic information systems for national defence purposes, the body operating within the defence sector, designated by the Government shall carry out the administrative authority duties laid down in this Act and the security surveillance as set out in governmental decrees.

(6)[7]

(7)[8] The provisions of this Act shall apply with certain derogations set out in

a) the act on classified data protection regarding electronic information systems processing classified data,

b) the act on electronic communication and the act on media services and mass communication regarding media service activities and electronic communications activities.

Section 3 (1)[9] The data processed by the bodies indicated in Section 2 (1) *a)-h)* and *j)-l)* and by the body indicated in Section 2 (1) *i)* - with the exception of data processed in the context of risk assessment and portfolio management activities related to the conduct of monetary policy and the management of foreign exchange reserves -, as well as the data within the scope of national data assets, processed by the bodies indicated in Section 2 (2) *b)* shall be processed in electronic information systems operated and stored in Hungary and in closed electronic information systems used for national defence, diplomatic information purposes.

(2)[10] The electronic information systems indicated in Section 2 (2) *c)* and *d)* may be operated in the territories of the Member States of the European Union, with the exception defined in paragraph (1).

---

[1] Declared by Section 119 (2) of the Act CCXXII of 2015. Effective from 01.01.2016
[2] Added by Section 143 (1) of the Act XXXI of 2020. Effective from 01.07.2020
[3] Added by Section 143 (1) of the Act XXXI of 2020. Effective from 01.07.2020
[4] Declared by Section 143 (2) of the Act XXXI of 2020. Effective from 01.07.2020
[5] Repealed by Section 152 a) of the Act XXXI of 2020. Ineffective from 01.07.2020
[6] Declared by Section 8 (6) of the Act CXXX of 2015. Effective from 16.07.2015
[7] Repealed by Section 152 a) of the Act XXXI of 2020. Ineffective from 01.07.2020
[8] Added by Section 8 (7) of the Act CXXX of 2015. Effective from 16.07.2015
[9] Declared by Section 112 (1) of the Act CXXI of 2018. Effective from 01.01.2019
[10] Amended by Section 151 b) of the Act XXXI of 2020

(3)[1] The data processed by the bodies indicated in Section 2 (1) a)-h) and j)-k) and by the body indicated in Section 2 (1) i) - with the exception of data processed in the context of risk assessment and portfolio management activities related to the conduct of monetary policy and the management of foreign exchange reserves - may also be processed in the electronic information systems operated within the territories of the EEA States with the permission of the authority supervising the security of electronic information systems (hereinafter referred to as 'Authority') or based on an international treaty.

(4) The enterprises operating electronic information systems subject to this Act that are not registered in Hungary shall designate a representative acting in Hungary who shall be responsible for the implementation of the provisions of this Act according to the rules for the head of the body.

Section 4[2] The Authority shall take the security certificates issued for electronic information systems, devices, bodies under international agreements or international standards, domestic requirements or recommendations based on them, as well as the inspection reports drawn up by an independent qualified inspector into account during its procedure.

CHAPTER II

ELECTRONIC INFORMATION SECURITY REQUIREMENTS

3. Essential electronic information security requirements

Section 5 In the whole lifecycle of the electronic information systems subject to this Act, the closed, full, continuous and risk-proportionate protection of

a) secrecy, integrity and availability of the data and information processed in electronic information systems, and

b) the integrity and availability of electronic information systems and its elements

shall be implemented and ensured.

Section 6 Within the framework of the electronic information systems' protection under the conditions determined in Section 5, bodies shall lay down logical, physical and administrative security measures prescribed in special laws which shall support:

a) prevention and early warning,

b) detection,

c) reaction,

d) security incident management.

4. Security classification of electronic information systems

Section 7 (1) For the purpose of ensuring that the electronic information systems subject to this Act and the data processed therein can be protected in proportion to the risks, electronic information systems shall be classified into security classes in terms of secrecy, integrity and availability.

---

[1] Declared by Section 112 (2) of the Act CXXI of 2018. Effective from 01.01.2019

[2] Declared by Section 113 of the Act CXXI of 2018. Effective from 01.01.2019

(2) On the occasion of security classification, grades number 1 to 5 shall be applied based on the risk of secrecy, integrity and availability of the electronic information systems concerned and the data processed thereby, along with stricter security standards in concert with higher numbering.

(3) Security classification shall be approved by the head of the body, being responsible for its compliance with laws and risks, the completeness and actuality of data used. Security classification shall be set out in the body's information security policies and rules.

(4) Based on the security classes under secrecy, integrity and availability of electronic information systems, security measures laid down in Sections 5 and 6 shall be implemented for the given electronic information system.

(5)[1] The head of a body may establish a higher security class relevant to the electronic information system than stipulated in the conditions laid down in this Act, or a lower security class regarding the electronic information system in exceptional cases with the prior permission of the Authority and with a justification covering the risks.

(6)[2] Regarding the electronic information systems of infrastructures designated as European or national critical infrastructures under the Hungarian Critical Infrastructure Protection Act, a higher security class relevant to the electronic information system may be established than stipulated in the conditions laid down in this Act, or also a lower security class regarding the electronic information system may be established with the prior permission of the Authority and with a justification covering the risks.

Section 8 (1) Security classification shall be reviewed at least every three years or, if necessary, out of turn, in a documented manner.

(2) The out of turn security classification shall be carried out in case of a legislative change related to the security of an electronic information system or in case of the introduction of a new electronic information system. The out of turn review shall be carried out also in the case if there is a change in the status of the body or regarding the data processed or technically manipulated thereby.

(3) The body has the opportunity to gradually implement security measures to achieve the expected strength of protection set out in compliance with Section 7 (2), regarding electronic information systems. In this context based on the security class established at the first test, security measures assigned to every further, higher security class shall be implemented within a two-year period.

(4)[3]

(5) If the body identifies deficiencies at the establishment of the security class regarding its certain electronic information system, an action plan shall be prepared to repair the deficiency within 90 days after the test.

(6)[4] The Authority may revise the security class established by the body with the exception of electronic information systems determined in Section 2 (5), and may establish higher, or in justified cases lower security classes, too.

---

[1] Declared by Section 119 (4) of the Act CCXXII of 2015. Effective from 01.01.2016

[2] Added by Section 119 (5) of the Act CCXXII of 2015. Effective from 01.01.2016

[3] Repealed by Section 8 (40) c) of the Act CXXX of 2015. Ineffective from 16.07.2015

[4] Declared by Section 8 (10) of the Act CXXX of 2015. Amended by Section 151 c) of the Act XXXI of 2020

(7)[1] Requirements belonging to a security class established during the introduction of a new electronic information system or the development of an operating electronic information system shall be implemented prior to use.

5. Security levels of the bodies having an electronic information system

Section 9 (1) According to the criteria set out in the legislation, the bodies shall classify their bodies into security levels based on preparedness to the protection of electronic information systems for the form of risk-proportionate, cost-efficient protection.

(2)[2] According to the criteria set out in the legislation, the organizational units

a) developing electronic information systems,

b) operating electronic information systems,

c) responsible for operation of electronic information systems or

d) responsible for information security of electronic information systems

shall be classified into different security levels expected from the body, based on preparedness to the protection of electronic information systems.

(3)[3] The bodies' preparedness for protection shall determine the security levels of the bodies and organizational units.

(4)[4] The method of the use of electronic information systems shall determine the security levels of bodies and organizational units according to the criteria set out in the legislation.

(5)[5] The bodies or organizational units may establish a higher security level relevant to the given bodies than stipulated in the conditions laid down in this Act, as well.

(6)[6] Regarding the bodies of infrastructures designated as European or national critical infrastructures under the Hungarian Critical Infrastructure Protection Act, a higher security level relevant to the given bodies than stipulated in the conditions laid down in this Act, or also a lower security level regarding the bodies - with a justification - may be established.

Section 10 (1)[7] Based on criteria set out in the legislation, bodies and organizational units shall establish which security level they meet when conducting the test.

(2)[8] If the security level is lower on the basis of test than the security level set out in laws for the certain body and organizational unit, the body shall prepare an action plan to achieve the security level provided therefor within 90 days after the test.

(3)[9] The security level of the bodies or the organizational units under Section 9 (2) shall be achieved according to the schedule in the action plan. If the security level does not achieve level 1 on the basis of the test, the measures necessary for achieving level 1 shall be implemented within 8 years after the test, carried out under the criteria set out in paragraph (1).

---

[1] Added by Section 8 (11) of the Act CXXX of 2015. Effective from 16.07.2015
[2] Declared by Section 8 (12) of the Act CXXX of 2015. Effective from 16.07.2015
[3] Declared by Section 8 (12) of the Act CXXX of 2015. Effective from 16.07.2015
[4] Declared by Section 8 (12) of the Act CXXX of 2015. Effective from 16.07.2015
[5] Added by Section 8 (13) of the Act CXXX of 2015. Effective from 16.07.2015
[6] Added by Section 119 (6) of the Act CCXXII of 2015. Amended by Section 21 a) of the Act LV of 2019
[7] Declared by Section 8 (14) of the Act CXXX of 2015. Effective from 16.07.2015
[8] Declared by Section 8 (14) of the Act CXXX of 2015. Effective from 16.07.2015
[9] Declared by Section 8 (14) of the Act CXXX of 2015. Amended by Section 136 of the Act LXVII of 2016, Section 91 of the Act LXXII of 2017, Section 126 of the Act XL of 2018, Section 114 of the Act LXVI of 2019

(4) During implementing the security level provided for in Section 9 (2), the bodies have the opportunity to gradually achieve the security level set out. In this context, a higher security level shall be achieved within a two-year period regarding every level to move to the subsequent higher level.

(5)[1] After achieving the security level provided for in Section 9 (1), the determination of security levels shall be reviewed at least every 3 years or, if necessary, out of turn, in a documented manner.

(6)[2] The determination of security levels of bodies and organizational units shall be, out of turn, renewed in case of a change related to the security of an electronic information system or in case of the introduction of a new electronic information system.

(7)[3] If the security level is lower on the basis of out of turn review than the security level set out in laws for the certain body or organizational unit, the body or the organizational unit shall prepare an action plan to achieve the security level provided therefor within 90 days after the examination.

(8)[4] The determination of the security levels of bodies and the responsible organizational units shall be approved by the head of the bodies, being responsible for the compliance with laws and risks, the completeness and actuality of data used. The result of the determination of security levels shall be set out in the body's information security policies and rules or in the rules related to the organizational unit.

6. Bodies' duties ensuring the protection of their electronic information systems

Section 11 (1) The head of bodies shall ensure the protection of electronic information systems as follows:

a) shall ensure compliance with requirements in laws regarding the security classes relevant to electronic information systems,

b) shall ensure compliance with requirements in laws regarding the security level relevant to the body,

c)[5] shall appoint or entrust an information security officer,

d) to *e)*[6]

f) shall lay down rules on persons responsible for the protection of electronic information systems of the body, their duties and the competence necessary thereto, as well as on users, and shall issue the information security policies and rules,

g) shall ensure the education about the security duties of electronic information systems and their scope of responsibilities, and shall maintain the own information security knowledge and also that of the colleagues of the body,

h) shall ascertain through regular security risk analysis, monitoring, audits whether the security of electronic information systems of the body is in compliance with laws and risks,

i) shall ensure the traceability of events of electronic information systems,

---

[1] Declared by Section 8 (15) of the Act CXXX of 2015. Effective from 16.07.2015
[2] Declared by Section 8 (15) of the Act CXXX of 2015. Effective from 16.07.2015
[3] Declared by Section 8 (15) of the Act CXXX of 2015. Effective from 16.07.2015
[4] Declared by Section 8 (15) of the Act CXXX of 2015. Effective from 16.07.2015
[5] Declared by Section 8 (16) of the Act CXXX of 2015. Effective from 16.07.2015
[6] Repealed by Section 8 (40) d) of the Act CXXX of 2015. Ineffective from 16.07.2015

j) shall react quickly and efficiently to security incidents by using all necessary and available resources upon the occurrence of a security incident, and after that shall respond to security incidents,

k) shall ensure to fulfil the requirements set out in this Act as contractual obligations, if a contributor is involved in the creation, operation, audit, maintenance or repair of electronic information systems,

l) shall ensure to fulfil the requirements set out in this Act as contractual obligations, if a contributor is involved in data processing or technical manipulation by the body,

m) shall be responsible for immediately notifying the people concerned about security incidents and possible threats,

n) shall take other measures necessary for the protection of electronic information systems.

(2) The head of the bodies shall be responsible for the duties set out in paragraph (1) also in the case provided for in paragraph (1) *k)* and *l),* except for the cases if a centralized IT and electronic communications provider or a central data controller and processor service provider designated by laws shall be involved by the body.

(3)[1] Involving a centralized IT and electronic communications provider or a central data controller or processor designated by laws, the centralized IT and electronic communications provider or the central data controller or processor designated by laws shall fulfil the requirements provided for in paragraphs (1) and (2) that it shall contribute to the duties of the body and the information security officer regarding the activities falling within its competence. The task sharing between the two bodies is ensured by bilateral service contracts, which come into effect with the signature of the minister supervising the central service provider or its representative. In context of duties set out in paragraph (1) *a)* and *b)*, the preparation of IT security rules on organizational level belongs to the responsibility of the head of the body also in the case, if a centralized IT and electronic communications provider designated by laws is involved therein.

(4)[2]

(5)[3] In case of public bodies under national security protection, the incident response centre exercises the right of prior opinion regarding the appointment of the information security officer.

(6)[4] A person taking part in investigation of security incidents can only be someone who has a mandate issued by the head of the body with the prior opinion of the incident response centre. The mandate shall be in writing. The person taking part in investigations of incidents shall take part in an information session held by the incident response centre about security incident response procedures before the mandate.

(7)[5] In case of electronic information systems for defence purposes, the provisions of paragraphs (5) and (6) shall not be applied.

Section 12 The head of the bodies shall cooperate with the Authority. During this, it shall

a) provide information about the information security officer determined in Section 11 (1) *c)*,

b) send the IT security policy and rules of the body for information purposes,

c) ensure the conditions necessary to conduct the investigation

---

[1] Declared by Section 8 (17) of the Act CXXX of 2015. Effective from 16.07.2015

[2] Repealed by Section 8 (40) e) of the Act CXXX of 2015. Ineffective from 16.07.2015

[3] Added by Section 8 (18) of the Act CXXX of 2015. Amended by Section 119 a) of the Act CXXI of 2018

[4] Added by Section 8 (18) of the Act CXXX of 2015. Amended by Section 119 a), b) of the Act CXXI of 2018

[5] Added by Section 8 (18) of the Act CXXX of 2015. Amended by Section 152 b) of the Act XXXI of 2020

to the Authority.

Section 13 (1) The information security officer may provide information, report directly to the head of the body in the course of conducting the tasks of the information security officer.

(2) The information security officer shall be responsible for fulfilling all tasks occurring at the body, related to the security of electronic information systems. In this context, the information security officer shall

a) ensure to establish and maintain consistency of the activities related to security of electronic information systems of the body with legislation,

b) carry out and manage planning, organization, coordination and control of activities under point *a)*,

c) prepare the information security policy and rules regarding the electronic information systems of the body,

d) prepare the security classification of electronic information systems of the body and the determination of the security level of the body,

e) give opinion regarding the security of electronic information systems, the body's regulations and contracts in this subject matter,

f)[1] keep in touch with the Authority and the incident response centre.

(3) The information security officer shall inform the organization set out in laws about any security incident subject to this Act concerning the electronic information systems, that belong to the information security officer, according to legislation.

(4) If the size or the security needs of the electronic information systems of the body justify, an electronic information security organizational unit may be established within the body which is led by the information security officer.

(5) The information security officer shall ensure the fulfilment of the requirements set out in this Act in case of the security related activities concerning the electronic information systems subject to this Act of

a) the contributors in planning, developing, creating, operating, auditing, examining, risk analysis and risk management, maintenance or repair of all electronic information systems of the body,

b) the contributors, if the body involves contributors to data processing or technical manipulation.

(6) The duties and responsibilities of the information security officer under this Act may not be assigned to a third party in the cases set out in paragraph (5).

(7) The information security officer is entitled to request information about the fulfilment of security requirements from the contributors under paragraph (5). In this context, data related to contributors' activity and all documents related to the subject matter of the security of electronic information systems shall be requested to support compliance with the requirements.

(8) Only such person may carry out the tasks of the information security officer at the body who has no prior record, has higher education and professional qualifications required for the performance of the duties.

(9) The information security officer shall justify the compliance with the requirement of clean record prior the establishment of its relationship with the body. The body may require that the information security officer justifies compliance with the requirement of clean record during the existence of the relationship with the body.

---

[1] Amended by Section 119 a) of the Act CXXI of 2018

(10) The person shall not obtain the qualifications under paragraph (8) who has accredited international qualifications determined in special laws or five-year professional experience in this field.

(11) The information security officer and the persons taking part in performing the duties related to the security of electronic information systems shall take part in regular professional training and further trainings determined in ministerial decrees.

CHAPTER III

SECURITY SURVEILLANCE OF ELECTRONIC INFORMATION SYSTEMS

7. Surveillance of the security of electronic information systems

Section 14 (1)[1] The Authority designated by the Government conducts security surveillance of the electronic information systems subject to this Act, with the exception of the electronic information systems for national defence purposes, the critical infrastructures for national defence and the bodies under national security protection falling under the competence of national defence sector.

(2) The duties of the Authority are the followings:

a) the monitoring of security classification and of determination of security levels, as well as making decision based on the result of the monitoring,

b) the monitoring of fulfilment of the requirements determined in laws regarding the security classification of electronic information systems and the security levels of the bodies,

c) the order to repair the security deficiencies detected or learnt during the monitoring, and the monitoring of its effectiveness,

d) preparation of a risk analysis based on available information,

e)[2] initiation of authority proceedings to examine the incoming notifications related to security incidents,

f) proposal ensuring the security regulation of critical systems and facilities, for the designation of national critical infrastructures to the sectoral designating authority under the Hungarian Critical Infrastructure Protection Act, which,

g)[3]

h)[4] cooperation in monitoring the fulfilment of the security requirements related to regulated electronic administration service providers with the electronic administration supervision authority set out in the act on general rules for electronic administration and trust services,

i) keep in touch with national security services in the field of electronic information security,

j)[5] keep in touch with the incident response centres determined in Section 19 (1)-(4),

k) to *n)*[6]

---

[1] Declared by Section 144 (1) of the Act XXXI of 2020. Effective from 01.07.2020

[2] Declared by Section 8 (20) of the Act CXXX of 2015. Effective from 16.07.2015

[3] Repealed by Section 8 (40) f) of the Act CXXX of 2015. Ineffective from 16.07.2015

[4] Amended by Section 442 a) of the Act L of 2017

[5] Declared by Section 8 (21) of the Act CXXX of 2015. Effective from 16.07.2015

[6] Repealed by Section 8 (40) f) of the Act CXXX of 2015. Ineffective from 16.07.2015

(2a)[1] The Authority perform its duties under paragraph (2) regarding the electronic information systems of national security service for civilian intelligence - without learning the data stored thereon - according to governmental decrees.

(3)[2] The general administrative time limit of procedures of the Authority is - with the exception set out in paragraph (3a) - 30 days.

(3a)[3] The administrative time limit of procedures of the Authority is 120 days in case of examination of fulfilment of the logical protection obligation.

(3b)[4] In the procedures of the Authority,

a) the clients' notification about the initiation of a proceeding may be omitted,

b) the body shall take part in expert's procedure.

(4)[5] In the context of performing the duties set out in paragraph (2) *a)* and *b),* on a proposal from the Authority, the minister responsible for e-government shall prepare an annual audit plan (hereinafter referred to as 'annual audit plan') in agreement with the minister responsible for IT, taking into account the proposals of the minister responsible for the professional supervision of the protection of classified data and the minister responsible for disaster management.

Section 15 (1) The Authority shall keep records and processes

a) the data necessary to identify the body,

b) the name of electronic information systems of the body, the security classification of electronic information systems and the determination of the security level of the body, the electronic information systems' technical data set out in special laws,

c) the natural identification data, the phone number, the fax number, the e-mail address and the qualifications set out in Section 13 (8) of the information security officer of the body,

d) the information security policy and rules of the body,

e)[6] notifications received from the incident response centre related to security incidents.

(2) The purpose of processing data determined in paragraph (1) is to fulfil the obligations related to protection of electronic information systems and to ensure its authority monitoring.

(3)[7] The body shall send the data set out in paragraph (1) *a)-c)* and their changes, as well as the regulation under paragraph (1) *d)* to the Authority for registration.

(4)[8] Unless otherwise provided by law, data transfer from the record determined in paragraph (1) may be carried out only to the incident response centres determined in Section 19 (1)-(4).

(5) If the body no longer carries out any activity subject to this Act, the data set out in paragraph (1) shall be deleted by the Authority from the record five years after notification of the termination of the activity.

---

[1] Added by Section 144 (2) of the Act XXXI of 2020. Effective from 01.07.2020

[2] Declared by Section 190 of the Act CLXXXVI of 2015. Effective from 01.01.2016. Its provisions shall be applied in the procedures started after the entry into force.

[3] Added by Section 190 of the Act CLXXXVI of 2015. Effective from 01.01.2016. Its provisions shall be applied in the procedures started after the entry into force.

[4] Added by Section 441 (1) of the Act L of 2017. Effective from 01.01.2018

[5] Amended by Section 44 (2) of the Act XCIII of 2014. Amended under Section 44 (4) of the Act XCIII of 2014.

[6] Declared by Section 8 (22) of the Act CXXX of 2015. Amended by Section 119 a) of the Act CXXI of 2018

[7] Declared by Section 8 (23) of the Act CXXX of 2015. Effective from 16.07.2015

[8] Declared by Section 8 (23) of the Act CXXX of 2015. Effective from 16.07.2015

(6) If the body notifies the change in data set out in paragraph (1), the original data shall be deleted from the record five years after notification of the change in data, by the Authority.

Section 16 (1) The Authority is entitled to take, order, monitor all measures regarding the security of electronic information systems for the security of electronic information systems and data processed therein, by which the threats against electronic information systems concerned may be handled. To this end, the Authority is entitled to:

a) monitor security requirements set out in laws and the conduct of procedural rules related thereto at the bodies concerned,

b) request the documents necessary to support compliance with the requirements, and review the documentation sent under Section 12 *b)*,

c) control the security classification under Sections 7 to 8, the determination of security level under Sections 9 to 10, or the security measures, the Authority is entitled order the measures necessary to repair the deficiencies detected, monitor their fulfilment,

d) control the compliance with the information security requirements in the planning phase of development projects from central and EU funds,

e)[1] organize domestic information security and cyber defence exercises,

f)[2] represent Hungary upon request in international information security and cyber defence exercises,

g)[3] exercise the right of opinion in relation with incident response centres' draft on rules and responsibilities to be followed in case of intersectoral security incidents,

h)[4] involve independent, qualified auditors during its procedure, and take the result of the audit conducted by them into account,

i)[5] determine minimum expected security requirements.

(1a)[6] The body under Section 2 (5) shall perform the duties under paragraph (1) *a)*, *b)*, *c)*, *d)* and *i)* regarding sector it supervises.

(2) With the exception set out in paragraph (3), if the body does not perform or does not comply with the security requirements set out in laws and the related procedural rules, the Authority

a) shall call upon the body to perform the security requirements set out in laws and the related procedural rules,

b) is entitled to impose a fine considering all the circumstances of the case, if, notwithstanding point *a),* the body does not perform the security requirements set out in laws and the related procedural rules, and it may be repeated in case of further non-performance.

(3) If the body is a budgetary entity, and it does not perform or does not comply with the security requirements set out in laws and the related procedural rules, the Authority

a) shall call upon the body to perform the security requirements set out in laws and the related procedural rules,

b) is entitled to have a recourse to the organization supervising the body, if the body has such, and to ask its contribution, if, notwithstanding point *a),* the body does not perform the security requirements set out in laws and the related procedural rules,

---

[1] Declared by Section 8 (24) of the Act CXXX of 2015. Effective from 16.07.2015
[2] Declared by Section 8 (24) of the Act CXXX of 2015. Effective from 16.07.2015
[3] Amended by Section 119 a) of the Act CXXI of 2018
[4] Added by Section 114 (1) of the Act CXXI of 2018. Effective from 01.01.2019
[5] Added by Section 145 (1) of the Act XXXI of 2020. Effective from 01.07.2020
[6] Added by Section 145 (2) of the Act XXXI of 2020. Effective from 01.07.2020

c) may initiate the secondment of an information security supervisor, if, notwithstanding points *a)* and *b),* the body does not perform the security requirements set out in laws and the related procedural rules,

d)[1] is entitled to impose a fine as defined in a separate government decree.

(4)[2] If the electronic information system

a) is hit by a serious security incident or

b) is threatened by the imminent occurrence of a serious security incident,

which compromises essential information or personal data necessary for the operation of the body operating the system, the incident response centre for the performance of its security duties may obligate the body to take measures necessary to terminate the serious security incident or to eliminate the threat .

(5)[3] If an information security supervisor is seconded to the body, it shall immediately inform the incident response centre about the occurrence of circumstances under paragraph (4). In the case immediate action is required, the incident response centre may apply provisional measures - through the information security supervisor - to the extent necessary to avoid damage to the information.

(6)[4] If the body concerned ignores the notification set out in paragraphs (2) *a)* and (3) *a)*, or does not fulfil the measures proposed by the Authority by its own fault and therefore the security incident under paragraph (4) *a)* and *b)* occurs or may occur, the Authority obligates it to pay the costs of the prevention of occurrence of the security incidents.

8. Information security supervisor

Section 17 (1)[5] The minister responsible for e-government may second the information security supervisor on the proposal of the Authority in case of Section 16 (3).

(2) The information security supervisor may propose measures, procedures determined in a governmental decree to take effective security measures necessary to eliminate threat, and may object to measures of the body. The information security supervisor is not eligible to make a financial commitment.

(3)[6] The minister responsible for e-government decides about the secondment of the information security supervisor for a definite time or about the revocation of the secondment. The minister responsible for e-government professionally manages the activity of the information security supervisor.

(4)[7] The information security supervisor is a government official of the ministry led by the minister responsible for e-government, to whose government service relationship the rules regarding government officials employed in the position of deputy head of ministerial department shall be applied.

---

[1] Added by Section 114 (2) of the Act CXXI of 2018. Effective from 01.01.2019
[2] Added by Section 8 (25) of the Act CXXX of 2015. Amended by Section 119 a) of the Act CXXI of 2018
[3] Added by Section 8 (25) of the Act CXXX of 2015. Amended by Section 119 a) of the Act CXXI of 2018
[4] Added by Section 8 (25) of the Act CXXX of 2015. Effective from 16.07.2015
[5] Amended by Section 44 (2) of the Act XCIII of 2014
[6] Amended by Section 44 (3) of the Act XCIII of 2014
[7] Amended by Section 44 (2) of the Act XCIII of 2014

(5) Such person may be appointed as an information security supervisor who has higher education and professional qualifications required for the fulfilment of the duties and at least three-year leadership experience.

9.[1] Vulnerability testing, investigation of security incidents

Section 18[2] (1) The Authority may oblige the body concerned to have a vulnerability test made and security incidents investigated. If the body concerned does not fulfil the obligation required by the Authority, the Authority shall impose a procedural fine.

(2) The body subject to the Act may initiate vulnerability testing, incident investigation also, without the call of the Authority.

(2a)[3] The body determined in a governmental decree, entitled to conduct vulnerability testing may itself start or conduct vulnerability testing within its own competence having a registered user right, or also without it under the conditions laid down in separate legislation.

(3) Vulnerability testing and investigation of security incidents - with the exception of bodies and electronic information systems set out in paragraph (5) - may be conducted by

a) a state organization determined in a governmental decree, or

b)[4] a business entity having facility security clearance as well as qualifications and infrastructure conditions necessary for the fulfilment of the duties, set out in laws.

(4)[5] Such person may carry out the investigation on behalf of and for the purpose of the business entities under paragraph (3) *b)* whose national security check has been carried out and no national security risk has been determined during such national security check.

(5) Vulnerability testing and investigation of security incidents is carried out regarding

a) closed electronic information systems,

b)[6] state and municipal bodies' electronic information systems of infrastructures designated as European or national critical infrastructures under the Hungarian Critical Infrastructure Protection Act, which are determined in Section 2 (1), and

c)[7] state and municipal bodies in Section 2 (1), under national security protection

- with the exception in paragraph (8) - by a state organ determined in a governmental decree.

(6)[8] The body or business organization carrying out the investigation pursuant to paragraph (1) shall send the result of the investigation to the Authority and the body concerned immediately after the completion of the investigation.

(7) The body concerned shall inform the Authority concerned about the detected deficiencies and the action plan to eliminate vulnerabilities after the conclusion of the investigation.

---

[1] Declared by Section 8 (26) of the Act CXXX of 2015. Effective from 16.07.2015
[2] Declared by Section 8 (26) of the Act CXXX of 2015. Effective from 16.07.2015
[3] Added by Section 115 of the Act CXXI of 2018. 0Effective from 01.01. 2019
[4] Amended by Section 119 (10) a) of the Act CCXXII of 2015
[5] Amended by Section 119 (10) a) of the Act CCXXII of 2015
[6] Declared by Section 119 (7) of the Act CCXXII of 2015. Effective from 2016. I. 1-től.
[7] Declared by Section 119 (7) of the Act CCXXII of 2015. Effective from 2016. I. 1-től.
[8] Amended by Section 119 (10) a) of the Act CCXXII of 2015

(8)[1] The incident response centre under Section 19 (2) shall carry out vulnerability testing and investigation of security incidents regarding the electronic information systems for national defence purposes.

(9)[2] The state body under paragraph (5) shall carry out vulnerability testing and investigation of security incidents, if, in excess of electronic information systems under paragraph (5) *b)*, there is no business organizations meeting conditions laid down by law for vulnerability testing and investigation of security incidents regarding the electronic information systems of infrastructures designated as European or national critical infrastructures under the Hungarian Critical Infrastructure Protection Act.

(10)[3] The state body under paragraph (5) shall carry out vulnerability testing and investigation of security incidents regarding the electronic information systems of national security service for civilian intelligence without learning the data stored thereon according to governmental decrees.

10.[4] Incident response centres

Section 19[5] (1) The Government shall operate incident response centres under the control of the minister responsible for the management of civilian national security services for handling security incidents and threats regarding

a)[6] the operators of essential service and service providers providing digital services, with the exception of electronic information systems under paragraph (2),

b)[7] the ICT infrastructure ensuring the operation of state and municipal electronic information systems, and, with the exception of electronic information systems under paragraph (2), the open electronic information systems of the bodies determined in Section 2,

c) the electronic information systems of critical infrastructures determined in Section 2 (2) *c)*.

(2) By way of derogation from paragraph (1), the Government shall operate incident response centres under the control of the minister responsible for national defence for responding to security incidents and threats set out in this Act regarding the electronic information systems for national defence purposes.

(3)[8]

(4) The bodies determined in Section 2 shall immediately transfer the data of the security incidents learnt to the incident response centre under paragraph (1).

(5)[9] The incident response centre under paragraph (2) shall immediately transfer the data of the security incidents related to security incidents and brought to its attention during cooperation under paragraph (6) to the incident response centre under paragraph (1).

---

[1] Amended by Section 21 b) of the Act LV of 2019, Section 152 c) of the Act XXXI of 2020
[2] Declared by Section 119 (8) of the Act CCXXII of 2015. Effective from 01.01.2016. Amended by Section 119 (10) a) of the Act CCXXII of 2015
[3] Added by Section 147 of the Act XXXI of 2020. Effective from 01.07.2020
[4] Declared by Section 116 of the Act CXXI of 2018. Effective from 01.01.2019
[5] Declared by Section 116 of the Act CXXI of 2018. Effective from 01.01.2019
[6] Amended by Section 151 d) of the Act XXXI of 2020
[7] Amended by Section 151 d) of the Act XXXI of 2020
[8] Repealed by Section 152 d) of the Act XXXI of 2020. Ineffective from 01.07.2020
[9] Declared by Section 148 of the Act XXXI of 2020. Effective from 01.07.2020

(6)[1] The incident response centre under paragraph (2) may take part in international cooperation in the professional field and may be accredited for this purpose.

Section 20[2] (1) The incident response centre under Section 19 (1) shall perform the following tasks:

a) the representation of Hungary in international incident response cooperation with the exception set out in Section 19 (6), receiving and handling international notifications regarding the Hungarian cyberspace,

b) keeping in touch with bodies, service providers for receiving notified security incidents, as well as taking and coordinating measures necessary to respond,

c) carrying out regular security situation assessment of the Hungarian cyberspace,

d) operating continuously available 24-hour on-call service,

e) supporting the investigation of security incidents, during which it may carry out the technical examination of the data of security incidents, to which it may request data or electronic access to data,

f) publishing immediate warnings about critical network security threats, displaying them in Hungarian,

g) making available the internationally published vulnerability on its homepage,

h) making analyses and reports about the domestic and international information security trends to the National Cyber Security Coordination Council,

i) may plan, organize domestic and international information security and cyber defence exercises, and may take part therein,

j) cooperate with the Authority, and, if necessary, with bodies concerned with security incident response,

k) may develop educational materials, hold trainings, organize educational and sensitivity campaigns to promote safety-conscious user behaviour.

(2)[3] The incident response centre under Section 19 (2) shall fulfil the duties under paragraph (1) *b), c), d), e), f), i), j)* and *k)* regarding the sectors supported by itself.

(3)[4] The incident response centre under Section 19 (1) shall fulfil its duties under paragraph (1) regarding the electronic information systems of national security service for civilian intelligence - without learning the data stored thereon - according to governmental decrees.

11. Ensuring government coordination

Section 21 (1)[5] The National Cyber Security Coordination Council led by the minister responsible for e-government (hereinafter referred to as 'Council') shall harmonize the activities set out in this Act and the implementing decrees of the bodies determined in Sections 2 (1), (2), (5) and 14 (1) as an advisory, consultative body of the Government.

(2)[6] The activity of the Council is supported by a cyber coordinator delegated by the minister responsible for e-government and the cyber security working groups ensuring the framework of

---

[1] Declared by Section 148 of the Act XXXI of 2020. Effective from 01.07.2020.
[2] Declared by Section 116 of the Act CXXI of 2018. Effective from 01.01.2019
[3] Amended by Section 151 e) of the Act XXXI of 2020
[4] Added by Section 149 of the Act XXXI of 2020. Effective from 01.07.2020
[5] Declared by Section 8 (32) of the Act CXXX of 2015. Amended by Section 151 f) of the Act XXXI of 2020
[6] Declared by Section 211 of the Act LXVII of 2016. Effective from 01.10.2016

cooperation with non-governmental actors and the National Cyber Security Forum (hereinafter referred to as 'Forum').

(3) to (4)[1]

12. Data protection provisions

Section 22[2] (1)[3] The bodies and business organizations under Sections 2 (5) and 18 (3) are entitled to process classified data, personal or sensitive data, trade secret, bank secret, payment secret, insurance secret, securities secret, treasury secret, medical secret and a secret connected with the exercise of another profession which they learn during fulfilling their duties set out in this Act regarding the protection of electronic information systems, only for the duration of the performance of the task, and taking into account the purpose limitation principle, . After performing the tasks, the recorded data related to performance shall be deleted from the electronic information systems and data carriers with the exception determined in paragraph (2).

(2)[4] The Authority, the bodies set out in Section 18 (5) and the incident response centre set out in Section 19 (1), (2) are entitled to process data determined in paragraph (1) for 5 years after the official authority decision becoming final, completing vulnerability testing and the end of the investigation of security incidents, and they shall delete them from their electronic information systems and data carriers after 5 years.

(3)[5] The colleagues of Authority, the organizations set out in Section 2 (5), the bodies or business organizations set out in Section 18 (3), the organizations determined in Section 18 (5) and incident response centre set out in Section 19 (1), (2) are bound in writing by the obligation of secrecy regarding data learnt under paragraph (1), which obliges them for 5 years after termination of employment, regarding classified data until the end of the duration of secrecy, and regarding personal data without a time limit.

(4) The data created during the Authority's procedures are not public.

(5) The final decision of the body appointed by the Government for authority tasks determined in this Act for closed electronic information systems and electronic information systems for national defence purposes shall not be known except by a client and the person entitled to inspect documents under Section 33 (3) of the Act CL of 2016 on the Code of General Administrative Procedure.

12/A.[6] Electronic communication

Section 22/A[7] (1)[8] Regarding the bodies and electronic information systems subject to this Act,

---

[1] Repealed by Section 212 of the Act LXVII of 2016. Ineffective from 01.10.2016
[2] Declared by Section 117 of the Act CXXI of 2018. Effective from 01.01.2019
[3] Amended by Section 151 g) of the Act XXXI of 2020
[4] Amended by 151 h) of the Act XXXI of 2020
[5] Amended by 151 h), i) of the Act XXXI of 2020
[6] Added by Section 8 (34) of the Act CXXX of 2015. Effective from 16.07.2015
[7] Added by Section 8 (34) of the Act CXXX of 2015. Effective from 16.07.2015
[8] Amended by Section 119 a) of the Act CXXI of 2018.

a) the announcement of the result of the security classification under Section 7, the sending of the action plan under Section 8, the data under Section 15 (1) *a)-c)* and the policy under Section 15 (1) *d)* to the Authority,

b) the announcement of the security incident under Section 13 (3) to the incident response centre is performed by electronic means, in the electronic system operated by the Authority and incident response centre.

(2) Announcement of a security incident may be made on any channel, if the electronic information system of the body is damaged so, that the electronic communication has become impossible.

CHAPTER IV

EDUCATION AND TRAINING, RESEARCH AND DEVELOPMENT

Section 23 In connection with the provision of training activities, the University of Public Service

a) shall develop training and further training requirements, educational programs of the leaders and information security officers, and shall present them to the minister responsible for the development of administration in support of the training determined in Sections 11 (1) *g)* and 13 (8),

b) shall develop qualification requirements determined in Section 13 (8) and present them to the minister responsible for the development of administration,

c)[1] shall provide training and annual further training of the leaders, the information security officers and the colleagues of the organizational units headed by them, and shall cooperate with the experts of incident response centres,

d) shall contribute to the information security, cyber security and critical information system security exercises.

CHAPTER V

FINAL PROVISIONS

13. Authorizing provisions

Section 24 (1) The Government shall be authorized to determine in a decree the provisions on

a) the detailed rules for the duties of the Authority, the detailed procedural rules for the performance of official authority monitoring,[2]

b) the amount of the fine that may be imposed by the Authority, the detailed procedural rules for the imposition and payment of a fine,[3]

c) the duties, the rules of the secondment of and the order of procedures of the information security supervisor,[4]

---

[1] Declared by Section 8 (35) of the Act CXXX of 2015. Amended by Section 119 a) of the Act CXXI of 2018.
[2] See Government Decree 301/2013. (29 July), Government Decree 187/2015. (VII.13.)
[3] See Government Decree 301/2013. (29 July), Government Decree 187/2015. (VII.13.)
[4] See Government Decree 301/2013. (29 July), Government Decree 187/2015. (VII.13.)

d)[1] the detailed rules for early warning, in particular its system, the designation of the system operator and the procedure for using the related early warning service,[2]

e)[3] the incident response centre, its functions and responsibilities, the detailed rules for security incident response procedure,[4]

f) the rules for establishment and operation of Council under Section 21, the Forum and the cyber security working groups, their functions and responsibilities,[5]

g)[6] the detailed rules for the duties to be performed under this Act of the centralized IT and electronic communications provider designated by laws,[7]

h)[8] the electronic information systems under Section 2 (3), the bodies performing authority tasks with regard to these systems and the detailed rules for the performance of tasks,[9]

i)[10] the Authority under Section 2 (5) and the detailed rules for the performance of tasks,[11]

j)[12] the state bodies entitled to vulnerability testing, investigation of security incidents, the professional requirements for business organizations under Section 18 (3) *b)*, the procedural rules for vulnerability testing, investigation of security incidents, and[13]

k)[14] the incident response centre under Section 19 (2) to (4), its functions and responsibilities,[15]

l)[16] the order of a procedure for involvement of an independent qualified auditor under Section 16 (1),

m)[17] the detailed rules for early warning regarding electronic information systems for national defence, in particular their system, the designation of the system operator and the procedure for using the related early warning service,

n)[18] the Authority's duties under Sections 14 (2) and 20 (1) regarding electronic information systems of the national security service for civilian intelligence, and the detailed rules for vulnerability testing and investigation of security incidents.

(1a)[19] The Government shall be authorized to designate the Authority in a decree.

(2) Authorization shall be given to

---

[1] Declared by Section 118 (1) of the Act CXXI of 2018. Effective from 01.01.2019
[2] See Government Decree 214/2020. (18 May)
[3] Declared by Section 8 (36) of the Act CXXX of 2015. Amended by Section 119 a) of the Act CXXI of 2018.
[4] See Government Decree 185/2015. (VII.13.) , Government Decree 271/2018. (XII.20.)
[5] See Government Decree 484/2013. (XII.17.)
[6] Added by Section 8 (37) of the Act CXXX of 2015. Effective from 16.07.2015.
[7] See Government Decree 186/2015. (VII.13.) , Section 16 of the Government Decree 467/2017. (XII.28.)
[8] Added by Section 8 (37) of the Act CXXX of 2015. Effective from 16.07.2015.
[9] See Government Decree 187/2015. (VII.13.)
[10] Added by Section 8 (37) of the Act CXXX of 2015. Amended by Section 151 j) of the Act XXXI of 2020
[11] See Government Decree 187/2015. (VII.13.)
[12] Added by Section 8 (37) of the Act CXXX of 2015. Effective from 16.07.2015. Amended by Section 119 (10) b) of the Act CCXXII of 2015
[13] See Government Decree 185/2015. (VII 13.) , Government Decree 271/2018. (XII.20.)
[14] Added by Section 8 (37) of the Act CXXX of 2015. Effective from 16.07.2015.
[15] See Government Decree 185/2015. (VII.13.) , Government Decree 271/2018. (XII.20.)
[16] Added by Section 118 (2) of the Act CXXI of 2018. Effective from 01.01.2019
[17] Added by Section 118 (2) of the Act CXXI of 2018. Effective from 01.01.2019
[18] Added by Section 150 of the Act XXXI of 2020. Effective from 01.07.2020
[19] Added by Section 43 of the Act XCIII of 2014. Effective from 01.01.2015

a)[1] the minister responsible for e-government to determine the requirements of the technological security and secure information devices and products provided for in Sections 5 and 6, the requirements of the security classification under Sections 7 to 8 and of the bodies' classification to security levels under Sections 9 to 10, in agreement with the minister responsible for IT and the minister responsible for the professional supervision of protection of classified data,[2]

b)[3] the minister responsible for development of administration to determine the content of the training and further training of the leaders determined in this Act and the information security officers, in agreement with the minister responsible for e-government,[4]

c)[5] the minister responsible for e-government to determine the order of procedures for the official registration of bodies [6]

in a decree.

(3)[7]

14. Entry into force

Section 25 This Act shall enter into force on 1 July 2013.

15. Transitional provisions

Section 26 (1) Bodies shall classify - for the first time - their electronic information systems already operating to security classes under Section 7 within a year after the entry into force of this Act.

(2) Bodies shall classify their bodies to security levels under Section 10 within a year after the entry into force of this Act for the first time.

(3) Bodies shall notify the data provided for in Section 15 (1) *a)* and *c)* within 60 days after the entry into force of this Act, the policy determined in Section 15 (1) *d)* within 90 days after the entry into force of this Act, to the Authority for registration.

(4) The persons who perform the duties of the information security officer at the entry into force of this Act shall meet training requirements provided for in Section 13 (8) within 5 years after the entry into force of this Act.

(5)[8] In case of bodies subject to Section 2 (1), established after 1 July 2014 without a predecessor,

a) security classification under Section 9 shall be concluded within a year after the entry into force of the decision on establishment;

b) the deadlines for data provision under paragraph (3) shall be applied from the entry into force of the decision on establishment.

---

[1] Amended by Section 8 (39) c) of the Act CXXX of 2015

[2] See Decree 77/2013. (XII.19.) NFM of the Minister for National Development, Decree 41/2015. (VII.15.) BM of the Interior Minister

[3] Amended by Section 44 (5) of the Act XCIII of 2014

[4] See Decree 26/2013. (X.21.) KIM of the Minister of Public Administration and Justice

[5] Declared by Act 119 (9) od the Act CCXXII of 2015. Effective from 01.01.2016

[6] See Decree 73/2013. (XII.4.) NFM of the Minister for National Development, Decree 42/2015. (VII.15.) BM of the Interior Minister

[7] Repealed by Section 8 (40) j) of the Act CXXX of 2015. Ineffective from 16.07.2015

[8] Added by Section 417 of the Act XCIX of 2014. Effective from 01.01.2015

(6)[1] Regarding the bodies becoming subject to this Act after 1 July 2014 based on Section 2 (2),

a) the condition for data processing activities under Section 2 (2) *a)* is that the controller shall fulfil the security classification under Section 7 of the Act and its notification obligation under paragraph (3) prior to the start of processing activities;

b) in case of Section 2 (2) *b)* the deadlines under paragraph (3) shall be applied from the entry into force of the law establishing the technical manipulation activities, the security classification under Section 7 shall be performed within 3 months after the entry into force of the law establishing the technical manipulation activities;

c)[2] in case of Section 2 (2) *c)* the deadlines under paragraph (3) shall be applied from the date when the decision on designating the critical information infrastructures becomes final, the security classification under Section 7 shall be performed within a year after the decision on designating the critical information infrastructures becomes final.

(7)[3] In case of bodies becoming subject to this Act after 1 July 2014, the deadline for fulfilment of the obligation under paragraph (4) shall be applied[4]

a) from the entry into force of the decision establishing the body with regard to Section 2 (1);

b) from the start of data processing with regard to Section 2 (2) *a)*;

c) from the entry into force of the law establishing technical data manipulation activities with regard to Section 2 (2) *b)*;

d)[5] from the date when the decision on designating the critical information infrastructures becomes final with regard to Section 2 (2) *c)*.

16.[6] Compliance with the law of the European Union

Section 27[7] This Act serves the purpose of compliance with the Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market.

Section 28[8] The draft of this Act was in advance notified under Article 15 (7) of the Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market.

Section 29[9] This Act serves the purpose of compliance with the Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

---

[1] Added by Section 417 of the Act XCIX of 2014. Effective from 01.01.2015
[2] Amended by Section 442 b) of the Act L of 2017
[3] Added by Section 417 of the Act XCIX of 2014. Effective from 01.01.2015
[4] Amended by Section 442 c) of the Act L of 2017
[5] Amended by Section 442 d) of the Act L of 2017
[6] Declared by Section 8 (38) of the Act CXXX of 2015. Effective from 16.07.2015
[7] Declared by Section 8 (38) of the Act CXXX of 2015. Effective from 16.07.2015
[8] Declared by Section 8 (38) of the Act CXXX of 2015. Effective from 16.07.2015
[9] Added by Section 46 of the Act CXXXIV of 2017. Effective from 10.05.2018