Government Decree 187/2015 (VII.13.)

on the functions and powers of the authorities responsible for electronic information security and the information security supervisor, as well as the determination of closed electronic information systems

The Government, acting on the basis of authorization given by Section 24 (1) *a)* to *c), h)* and *i)* of the Act L of 2013 on the electronic information security of state and municipal bodies, acting within its function laid down in Article 15 (1) of the Fundamental Law, orders as follows:

1. Interpretative provisions

Section 1 For the purpose of this Decree:

1.[1]

2.[2]

3.[3]

4.[4] '*electronic form'* means the electronic form specified in point 2 of Section 2 of the Government Decree 451/2016 (XII.19.) on the detailed rules of electronic administration, provided and published by the authority;

5.[5] *'official record'* means the record kept by the authority, containing the data under Section 15 (1) of the Hungarian Cyber Security Act;

6.[6] *'body'* means the body determined in Section 2 (1) and (2) of the Hungarian Cyber Security Act, with the exception of the body operating an information system under Section 2 (3) and (5) of the Hungarian Cyber Security Act.

2.[7] The authority responsible for electronic information security

Section 2[8] (1) As the authority responsible for electronic information security (hereinafter referred to as 'Authority'), the Government designates the Special Service for National Security under the Act L of 2013 on the electronic information security of state and municipal bodies (hereinafter referred to as 'Hungarian Cyber Security Act').

---

[1] Repealed by Section 54 of the Government Decree 323/2018 (XII.28.) Ineffective from 01.01.2019

[2] Repealed by Section 73 a) of the Government Decree 375/2020 (VII.30.) Ineffective from 31.07.2020

[3] Repealed by Section 54 of the Government Decree 323/2018 (XII.28.) Ineffective from 01.01.2019

[4] Added by Section 537 (1) of the Government Decree 457/2017 (XII.28.) Effective from 01.01.2018. It shall be applied in the proceedings initiated and repeated after its entry into force.

[5] Added by Section 537 (1) of the Government Decree 457/2017 (XII.28.) Effective from 01.01.2018. It shall be applied in the proceedings initiated and repeated after its entry into force.

[6] Added by Section 537 (1) of the Government Decree 457/2017 (XII.28.) Amended by Section 72 a) of the Government Decree 375/2020 (VII.30.)

[7] Declared by Section 44 of the Government Decree 323/2018 (XII.28.) Effective from 01.01.2019

[8] Declared by Section 44 of the Government Decree 323/2018 (XII.28.) Effective from 01.01.2019

(2) The Authority shall be subject only to the laws acting within its administrative authority competence, and shall not be bound by any instructions during its administrative authority procedures and in relation to the content of the decisions of the Authority, with the exception of the instructions to perform the duties or remedy the omission.

3. General provisions on administrative authority procedures

Section 3[1] (1) In the procedure of the Authority, submission of the application to the government window is excluded.

(2) There is an opportunity for call for remedy of deficiencies two times in a procedure.

Section 4 The Authority shall consult with the body concerned before making the decision on closing its procedure, unless an immediate threat or a security incident or the repeated unlawful conduct of the body concerned precludes it.

Section 5 (1) In order to carry out its tasks, the Authority is entitled to - with the least possible disturbance to the operation and management of the body concerned with the measure -

a) enter the premises related to the information technology activities of the body concerned,

b) carry out investigations at the sites concerned that provide data processing to the body concerned, perform technical data manipulation or are affected by information technology, and during that it is entitled to be familiarized with and check any instruments, documents, contracts, active or passive devices, information systems, security measures related to electronic information security as well as make copies of instruments, documents, contracts related to electronic information security, and

c) carry out information technology technical investigation, if necessary, with individual access right to the information technology system

in the course of its proceedings through an on-site investigation on its own or together with another authority.

(1a)[2] The Information Office shall ensure that the data stored in the electronic information system shall not be available to the investigation authority during the on-site investigation under paragraph (1).

(2) In case of the ordering of an on-site investigation, the Authority shall issue credentials for the colleagues of the Authority performing the on-site investigation. The credential shall contain the purpose, the subject of the on-site investigation, the circumstances giving rise to its ordering, the legal reference, the expected duration of the on-site investigation, the method of the on-site investigation and the name of the persons carrying out on-site investigation.

(3) The on-site investigation shall not result in learning the data regarding interception and the persons cooperating therein, moreover the means and methods of the interception.

(4) The head of the body concerned shall be notified about the ordering of the on-site investigation in writing in advance, and the information security officer of the body concerned shall be notified of the same electronically, ten days before the commencement of the on-site investigation. The credential of the person carrying out on-site investigation shall be attached to the notification.

(5) The notification under paragraph (4) may be omitted, if

---

[1] Declared by Section 537 (2) of the Government Decree 457/2017 (XII.28.) Effective from 01.01.2018. It shall be applied in the proceedings initiated and repeated after its entry into force.

[2] Added by Section 64 of the Government Decree 375/2020 (VII.30.) Effective from 31.07.2020

a) there is a serious threat,

b) a serious security incident has occurred,

c) the circumstance under points *a)* or *b)* is likely to occur, or

d) the body concerned would presumably frustrate the effective conduct of the on-site investigation, on the basis of the available data.

(6) The head of the body concerned with the on-site investigation, the colleagues, employees thereof and other contributors concerned in relation with the electronic information security based on a contractual relationship, as well as the information security officer shall cooperate with the Authority.

(7) The Authority shall record the on-site investigation in minutes, which shall be sent in writing to the body concerned within eight days after the end of the on-site investigation to provide observations. The body concerned may make observations being non-binding for the Authority in that regard within eight days in writing. In order to clarify the observations, the Authority may initiate a consultation with the body concerned.

Section 5/A[1] (1) For the protection of the electronic information systems and the data processed therein, the Authority is entitled to investigate all measures related to the protection of the electronic information systems with which the threats endangering the electronic information systems may be handled.

(1a)[2] The Information Office shall ensure that the data stored in the electronic information systems are not accessible to the investigating authority during the investigation under paragraph (1).

(2) In the course of its procedure, the Authority is entitled to take into consideration the result of an investigation carried out by an independent qualified inspector.

4. Duties of the Authority

Section 6 (1) The Authority

a) shall give authorization to operate electronic information systems in the European Economic Area (hereinafter referred to as 'EEA') Member States by the body concerned,

b) shall investigate the operation of the electronic information systems outside EEA Member States by the bodies concerned,

c) shall inspect compliance with information security requirements in information technology development projects,

d) shall keep a record of the names of the electronic information systems of the body, the security classes of electronic information systems, as well as the data of the physical, logical and administrative security measures specified in law, necessary for the classification of electronic information systems,

e)[3] if necessary, shall consult and cooperate with law enforcement agencies and the Hungarian National Authority for Data Protection and Freedom of Information,

f)[4] shall conduct the physical, logical and administrative security investigations within the framework of an administrative audit according to the requirements specified in law,

---

[1] Added by Section 45 of the Government Decree 323/2018 (XII.28.) Effective from 01.01.2019
[2] Added by Section 65 of the Government Decree 375/2020 (VII.30.) Effective from 31.07.2020
[3] Declared by Section 46 of the Government Decree 323/2018 (XII.28.) Effective from 01.01.2019
[4] Declared by Section 46 of the Government Decree 323/2018 (XII.28.) Effective from 01.01.2019

g)[1] shall represent Hungary in international organizations responsible for the security of electronic information systems,

h)[2] shall keep a record about and publish the notifications received from the incident response center under Section 19 (1) of the Hungarian Cyber Security Act in relation to security incidents on its website.

i) to *n)*[3]

(1a)[4] In case of occurrence of the security incident regarding the electronic information systems of the operators of essential services and specified in the Hungarian Cyber Security Act, the Authority may inform the public on its website and may oblige the service providers in a conclusive decision to provide information, if it is, at its discretion, necessary to prevent a certain security incident or for responding to an already ongoing security incident.

(2) Regarding the operation of the electronic information systems in EEA Member States, the Authority shall carry out an authorization procedure with the exception of Section 7 (3). During the procedure, the Authority shall investigate

a) the reason for data processing in EEA Member States,

b) the description of data and databases processed in EEA Member States,

c) whether the data processing system and its operator is identified by name and whether the name, position, contact data of the person responsible for the legal compliance of data processing is known,

d) the technical and technological description of data processing systems, including the hardware and software components, as well,

e) the information security description of the data processing systems, the internal regulations and instructions related to the systems and regarding the operator,

f) the result of the mandatory security system review,

g) the operator's declaration on the compliance with Hungarian information security rules and

h) whether the authorities competent at the site of the operation are entitled to access to the data processed.

(3) The descriptions under paragraph (2) *e)* to *g)* shall not be investigated, if the valid security certificate issued upon international agreements or international standards, as well as upon the domestic requirements or recommendations based thereon is available at the date of the submission of the request and is presented to the Authority.

Section 7 (1) The request for authorization shall contain the data under Section 6 (2) and (3). The request shall be submitted to the Authority within ninety days before the start of data processing abroad. The documentation and instruments under Sections 6 (2) *b)*, *e)* and *f),* as well as 6 (3) shall be attached as an exact copy of the original and in a certified translation into Hungarian as the Annex of the request.

(2) Without the authorization of the Authority, the operation of an electronic information system in EEA Member States and technical data manipulation or data processing in such a system may not be commenced. The expiry of the authorization shall be adjusted to the period of validity of the certificates submitted.

---

[1] Declared by Section 46 of the Government Decree 323/2018 (XII.28.) Effective from 01.01.2019
[2] Declared by Section 46 of the Government Decree 323/2018 (XII.28.) Effective from 01.01.2019
[3] Repealed by Section 54 of the Government Decree 323/2018 (XII.28.) Ineffective from 01.01.2019
[4] Declared by Section 66 of the Government Decree 375/2020 (VII.30.) Effective from 31.07.2020

(3) If data processing or system operation abroad is conducted on the basis of an international treaty to which the State is a contracting party, the Authority shall be informed about the data concerned, the person of the data processor or operator and the content of the contractual relationship. The Authority acknowledges the information without conducting any further procedures.

(4) If the Authority becomes aware of that the body concerned conducts the data processing or operation - including also the unidentifiable data processing services or the cloud computing services provided at a site excluded by law - outside Hungary in an unauthorized way, the Authority shall apply the legal consequences under Section 13.

Section 8 (1) While performing the information security requirements of development projects realized from European Union subsidy, central budget support, the project manager shall send the security classification regarding the electronic information systems to be developed and all the documentations to the Authority requesting an opinion in the planning phase of the project based on which the compliance with security requirements may be checked for the whole project lifecycle, including also expectations to be enforced during the use of electronic information systems after receipt or fulfilment.

(2) Taking into account the milestones at project level, the related electronic information security documentation shall be provided to the Authority at least thirty days before the closing of the relevant project phase in order that the observations or objections of the Authority may be reflected and applied on the project plan and the subject of the project.

(3) In case of projects of less than 60 days, the documentation under paragraph (1) shall be provided to the Authority at the closing of the project. While implementing the project, the content of the project shall be consulted with the Authority, if an electronic information system is concerned.

(4) The Authority may request an opinion from another authority regarding the documents under paragraph (1).

Section 9 (1) The security classification of electronic information systems shall be investigated based on information sent to the Authority according to criteria specified in law.

(2) If the notified security classification regarding the electronic information system - including the action plan for remedying the deficiencies identified at the security classification of the relevant electronic information system - is accepted by the Authority, such a decision does not exclude the review of the security classification independently or during the audit of the body or organizational unit concerned, at a later date.

(3) If the Authority overrides the security classification of the electronic information system determined and notified by the head of the body concerned and determines a higher security class during its procedure, the class corresponding to the decision of the Authority shall be taken as a basis with regard to the application of the time limit for achieving the next security class.

(4) If the Authority sees the possibility of applying a class lower than the notified security class regarding the electronic information system, a proposal is made to that effect to the body concerned.

(5) If the head of the body concerned determines a lower class regarding the electronic information system instead of the security class specified in the law on the requirements of security classification, detailed reasoning shall be provided.

Section 10 (1) The determination of security level of the body and organizational unit concerned - including also the action plan for remedying the deficiencies identified at the determination of security level regarding the body and organizational unit - shall be investigated based on the information sent to the Authority according to criteria specified in law.

(2) If the Authority sees the possibility of applying a level lower than the notified security level regarding the body and organizational unit concerned, a proposal is made to that effect to the body or organizational unit concerned.

4/A.[1] Registration procedure of the Authority and official registration

Section 10/A[2] (1) The body shall notify the data set out in law of the body and the information security officer to the Authority by secure electronic delivery, or failing this, by post.

(2) After the registration, the data notification under Sections 10/B and 10/D may be performed on behalf of a registered body only.

Section 10/B[3] (1) The body concerned with the data reporting obligation under Section 15 (3) of the Hungarian Cyber Security Act, shall perform its data reporting obligation by means of the electronic form published by the Authority pursuant to the rules of electronic disclosure of information.

(2) The form under paragraph (1) shall be sent to the Authority by the body by electronic means, via the electronic data reporting interface of the Authority.

Section 10/C[4] (1) The Authority shall examine whether the forms received pursuant to Sections 10/A and 10/B and their annexes substantively comply with the legal requirements.

(2) Following the examination, the Authority shall register the data reported or shall call on the body to remedy of deficiencies.

(3) In case of change in the data reported previously to the Authority, the body shall ensure to submit the changed data to the Authority according to Section 10/B within eight days after the change.

(4) The Authority shall inform the body about the registration of the reporting by electronic means.

---

[1] Added by Section 537 (3) of the Government Decree 457/2017 (XII.28.) Effective from 01.01.2018

[2] Added by Section 537 (3) of the Government Decree 457/2017 (XII.28.) Effective from 01.01.2018. It shall be applied in the proceedings initiated and repeated after its entry into force.

[3] Added by Section 537 (3) of the Government Decree 457/2017 (XII.28.) Effective from 01.01.2018. It shall be applied in the proceedings initiated and repeated after its entry into force.

[4] Added by Section 537 (3) of the Government Decree 457/2017 (XII.28.) Effective from 01.01.2018. It shall be applied in the proceedings initiated and repeated after its entry into force.

Section 10/D[1] (1)[2] For the purpose of the official registration under Section 15 (1) *b)* of the Hungarian Cyber Security Act, the body shall report the following technical data of the electronic information systems by electronic means, via the electronic data reporting interface of the Authority:

a) the public services provided by the electronic information system,

b) the public IP-address used by the electronic information system and the name of the related service,

c) the domain name used by the electronic information system,

d) the legal entity or the business entity without legal personality taking part in or contributing to the operation of the electronic information system and

e) the electronic communication service or intermediary service used for the operation of the electronic information system and the service provider providing such services.

(2) The data reporting under paragraph (1) shall be performed in the form determined and published by the Authority.

(3)[3] The Authority shall transfer the information security policy and rules submitted by the body for registration purposes to the registration authority of the European and national critical infrastructures.

Section 10/E[4] (1) The body shall report its cessation without succession to the Authority according to Section 10/B within eight days before the date of cessation.

(2) In case of cessation of the body with succession, the successor shall act according to Sections 10/B and 10/D.

(3) If the Authority becomes aware of the cessation of the body with succession in the course of its proceedings specified in law, it shall arrange for rectification of the data contained in the record ex officio.

5. Specific obligations of the body concerned

Section 11 (1) The body concerned, if the designation of the information security officer or the body responsible for the security of the electronic information systems or the preparation of the information security policy and rules fails to be fulfilled for a reason not attributable to it within the period prescribed by law, shall inform the Authority by indicating the reason for the impediment and the time limit for performance within the period prescribed by law.

(2) The information security officer - including also the members and employees of the business entity providing information security services - may perform its duties

a) on a part-time basis,

b) for the period specified in the relevant contract or

c) at more bodies concerned

adapted to the needs of the body concerned and according to its mandate.

---

[1] Added by Section 537 (3) of the Government Decree 457/2017 (XII.28.) Effective from 01.01.2018. It shall be applied in the proceedings initiated and repeated after its entry into force.

[2] Declared by Section 67 (1) of the Government Decree 375/2020 (VII.30.) Effective from 31.07.2020

[3] Added by Section 67 (2) of the Government Decree 375/2020 (VII.30.) Effective from 31.07.2020

[4] Added by Section 537 (3) of the Government Decree 457/2017 (XII.28.) Effective from 01.01.2018. It shall be applied in the proceedings initiated and repeated after its entry into force.

(3) The information to be provided on the information security officer, under Section 12 *a)* of the Hungarian Cyber Security Act shall include the transmission of the copy of the related employment, agency or other contracts upon the request of the Authority in a way that only the information relevant to the Authority, necessary for carrying out its functions and powers can be available. The copy of certificates of qualifications and education of the relevant person or of the certificate or statement certifying professional experience shall be attached to the contract.

(4) When involving the centralized IT and electronic communication service provider designated by law and central data controller and data processor service providers, the head of the body concerned - taking into account Section 11 (3) of the Hungarian Cyber Security Act - shall not be exempt from the obligations laid down in law which belong to the scope of the competence of management and control regarding information security regarding the body concerned.

6. Audit plan

Section 12 (1) The annual audit plan shall be drawn up by the Authority until 30 November of the year preceding the reference year.

(2) The Authority shall assess the implementation of the audit plan until 1 March of the year following the reference year.

(3) The Authority may diverge from the audit plan, if immediate investigations or procedures shall be carried out, which serve the prevention of serious security incidents endangering the Hungarian cyberspace, the national electronic data assets, the electronic information systems of special importance to the State and its citizens.

7. Legal consequences

Section 13[1] (1) For the purpose of compliance with the information security requirements, the Authority shall call on the head of the body concerned - setting a deadline - to eliminate deficiencies, omissions that endanger electronic information security or breaches of security requirements, to fulfil an obligation laid down in law and to take the measures expected.

(2) The Authority obliges the body concerned to take immediate measures, if deficiencies, omissions that endanger electronic information security or breaches of security requirements threaten with the occurrence of a serious security incident. In this context, a proposal for disciplinary liability may be made towards the person exercising employer's rights.

(3) In case of the notification of the incident response center under Section 19 (1) of the Hungarian Cyber Security Act, the Authority shall call on the body concerned, setting a deadline, to terminate the activities violating laws or the infringement, in that context particularly to perform notification, data provision, cooperation obligations.

[1] Declared by Section 47 of the Government Decree 323/2018 (XII.28.) Effective from 13.01.2019

(4)[1] In case of notification of the incident response center under Section 19 (2) of the Hungarian Cyber Security Act, the Authority under Section 24 (1) shall call on the body concerned, setting a deadline, to terminate the activities violating laws or the infringement, in that context particularly to perform notification, data provision, cooperation obligations.

(5) Pursuant to Section 16 (2) *b)* of the Hungarian Cyber Security Act and Section 16 (3) *d)* of the Hungarian Cyber Security Act, the Authority may impose a fine to the extent set out in Annex 1 in case of breaches of law specified in Annex 1. The fine imposed range from fifty thousand forints to five million forints, which shall be paid within eight days after the Authority's decision becomes final to the account of the Authority, held by the Hungarian State Treasury.

(6) In addition to paragraphs (1) to (4), the Authority may - in the event of a repeated infringement, shall - impose a fine ranging up to three million forints also on the senior manager of the infringer in case of impeding the procedure or the non-performance of or non-compliance with data provision.

(7) While applying legal consequences, the Authority shall take into account the following aspects beyond those laid down in law:

a) the weight of the deficiencies, omissions that endanger the electronic information security or the breached security requirements according to the security classification and security level,

b) whether a serious security incident has occurred or whether there is a risk of such an incident to occur,

c) the effect of security incidents or possible effects thereof on the body concerned or other bodies,

d) the conduct of the body concerned, its cooperation with the Authority and

e) the unique or repeated nature of the incident.

8. Closed electronic information systems, as well as the authorities supervising their security and their duties

Section 14[2]

Section 15 (1)[3] The closed electronic information systems of the national defence forces, the multi-purpose vocational training institutions belonging to the control responsibility of the minister responsible for national defence that are not national defence forces, 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 are the followings:

a) the administrative decision-making system and governance control systems for national defence purposes,

b) the defence stationary and field operation management systems, operation management systems supporting international operations and exercises,

c) the systems supporting secret intercepting and secret data acquisition in the field of military national security,

d) the IT systems for government purposes to support professional tasks in the specific operating field of the Defence Council and the Government and

---

[1] Amended by Section73 b) of the Government Decree 375/2020 (VII.30.)

[2] Repealed by Section73 c) of the Government Decree 375/2020 (VII.30.) Ineffective from 31.07.2020

[3] Amended by Section72 b) of the Government Decree 375/2020 (VII.30.)

e)[1] the electronic information systems - not falling under points *a)* to *d)* - operating at 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 forces, 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 at the companies engaged in activity related to national defence interest according to laws.

(2)[2] The Government designates the director-general of the Special Service for National Security for the performance of authority, security supervision tasks related to closed electronic information systems under paragraph (1).

Section 16[3]

Section 17[4]

Section 18 (1)[5] Instead of Sections 14 to 17 of the Hungarian Cyber Security Act, Sections 19 to 22 thereof shall be applied to the authority responsible for closed electronic information security supervision, designated in this Decree (hereinafter referred to as 'designated authority').

(2)[6] In addition to paragraph (1), also Sections 3 to 10, 12 and 13 shall be applied to the authority which supervises the security of the closed electronic information systems 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 forces, 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.

Section 19 The tasks of the designated authority are

a) to examine the security classification and the determination of security levels regarding closed electronic information systems and to make a decision on the basis of the result of the examination,

b) to examine the compliance with the requirements specified in law regarding the security classification of closed electronic information systems and - related thereto - the security levels of the bodies operating a closed electronic information system,

c) to order the remedy of security deficiencies detected or brought to its attention during its examination and to check the effectiveness thereof,

d) to carry out risk analysis based on information available,

e) to commence an administrative authority procedure for investigating the notifications related to security incidents received thereby,

f) to facilitate and support the security awareness of information society,

g) to take part in exercises related to the protection of domestic and international information security, cyber security, critical information infrastructure and

h) to maintain contact and cooperate with the Authority and incident response centers.

---

[1] Declared by Section 68 of the Government Decree 375/2020 (VII.30.) Effective from 31.07.2020
[2] Amended by Section 1 of the Government Decree 22/2016 (II.17.)
[3] Repealed by Section 73 d) of the Government Decree 375/2020 (VII.30.) Ineffective from 31.07.2020
[4] Repealed by Section 73 d) of the Government Decree 375/2020 (VII.30.) Ineffective from 31.07.2020
[5] Amended by Section 72 c) of the Government Decree 375/2020 (VII.30.)
[6] Declared by Section 69 of the Government Decree 375/2020 (VII.30.) Effective from 31.07.2020

Section 20 For the purpose of ensuring the security of closed electronic information systems and the data stored therein, the designated authority is entitled to take, order or check all measures regarding the security of closed electronic information systems with which the threats endangering the closed electronic information systems concerned may be handled. For this purpose, it is entitled to

a) examine the compliance with the security requirements specified in law and the procedural rules related thereto,

b) request the documents necessary to confirm the compliance with the requirements,

c) check the compliance with the information security requirements in the planning phase of development projects from central budget and European Union source and to make proposals to that effect,

d) ensure professional participation in the planning phase of development projects and to carry out activities to examine the incorporation of security requirements, as well as

e) prepare an action plan for the elimination of vulnerability.

Section 21 (1) The designated authority shall keep a record regarding the closed electronic information systems according to the rules for official records set out in the Hungarian Cyber Security Act.

(2) The body operating a closed electronic information system shall send the data under the Hungarian Cyber Security Act and the changes therein to the designated authority within eight days.

Section 22 (1) The designated authority shall carry out the investigation based on the annual audit plan approved by the minister responsible for the management, governance or supervision of the body operating a closed electronic information system or based on individual instructions.

(2) If the designated authority concludes that the body operating a closed electronic information does not perform or does not comply with the security requirements and the procedural rules related thereto, it shall call on the body concerned to perform the security requirements specified in law and the procedural rules related thereto.

9. The authority responsible for the security supervision of electronic information systems for national defence purposes and its duties[1]

Section 23[2]

Section 24 (1)[3] The Government designates the director-general of the Special Service for National Security as the authority responsible for the security supervision of electronic information systems for national defence purposes.

(2) Sections 3 to 10, 12 and 13 and instead of Sections 14 to 17 of the Hungarian Cyber Security Act Sections 19 to 22 thereof shall be applied to the authority under paragraph (1).

Section 25[4]

10. The information security supervisor

[1] Declared by Section 70 of the Government Decree 375/2020 (VII.30.) Effective from 31.07.2020
[2] Repealed by Section 73 e) of the Government Decree 375/2020 (VII.30.) Ineffective from 31.07.2020
[3] Amended by Section 1 of the Government Decree 22/2016 (II.17.)
[4] Repealed by Section 73 f) of the Government Decree 375/2020 (VII.30.) Ineffective from 31.07.2020

Section 26 (1) As an information security supervisor (hereinafter referred to as 'supervisor') such person may be seconded who undertakes the secondment and meets the requirements laid down in the Hungarian Cyber Security Act and in this Decree. The leadership experience outside administration, gained in a relationship for employment under Section 8 (5) of the Act CXCIX of 2011 on public servants may be accounted for the duration provided as for the supervisor's leadership experience. The minister responsible for e-government (hereinafter referred to as 'Minister') shall exercise the employer's rights over the supervisor.

(2) The supervisor may be seconded to more bodies concerned at the same time, if the reasons of secondment allow it.

(3) The minister shall second the supervisor by issuing a credential for a definite period to supervise the electronic information security activity of the body concerned. The secondment may be extended before the end of the period of secondment not more than once, pending the completion of ongoing measures. While determining the duration of secondment, the seriousness of the infringements of the body concerned and the security measures necessary to prevent threats shall be taken into account. The credential about the secondment shall contain the purpose and the subject of the secondment, the circumstances giving rise to the secondment, the legal reference, the duration of the secondment, the data necessary for the identification of the information security supervisor in a proper way.

(4) A person cannot be seconded as a supervisor

a) who is in a relationship for employment with the body concerned,

b) who was in a relationship for employment with the body concerned in the three years preceding the secondment,

c) who is or was in a regular and enduring agency or business relationship at the date of the secondment or in the three years preceding the secondment,

d) who is a relative of the head of the body concerned, of the economic leader or an employee thereof during the secondment,

e) who is the representative of the body concerned during the secondment and until three years after the termination thereof, as well as

f) from whom the objective assessment of the given situation cannot be required because of a business interest or other reason (partiality).

(5) The secondment of the supervisor may be terminated before the expiry of the period specified in the credential, if

a) the reason for secondment is averted and the summary report of the supervisor is accepted by the Authority or

b) the supervisor is recalled by the minister.

(6) The minister shall recall the supervisor, if

a) the Authority establishes that the security requirements do not prevail at the body concerned attributable to the supervisor or

b) a circumstance giving rise to exclusion under paragraph (4) has arisen or the Minister becomes aware of the circumstance giving rise to exclusion that existed at the date of the secondment.

(7) The Minister is entitled to second a new supervisor in case of paragraph (5) *b)*.

(8) The Minister shall immediately inform the head of the body concerned about the termination of the secondment of the supervisor in writing.

Section 27 (1) In the context of the compliance and performance of the security requirements specified in law and the procedural rules related thereto, the supervisor is entitled to

a) request written or oral information, data provision from the heads or any colleagues of the body concerned,

b) access all documents, instruments related to information technology at the body concerned, and to request copies, extracts to be made,

c) enter all the premises related to information technology at the body concerned,

d) propose immediate measures to the head of the body concerned for prevention of direct threat (limitation and shutdown of operation),

e) propose measures to establish or restore lawful operation, in that context particularly to initiate the review of regulations concerned,

f) give an opinion about the measures concerning also the electronic information security related to operation in advance and

g) object the measures, decisions made or omitted based on the Hungarian Cyber Security Act by the body concerned.

(2) The supervisor shall

a) present the credential at the body concerned,

b) monitor the compliance with security requirements and procedures set out in law and the performance of the duties specified in law at the body concerned from the beginning of the secondment,

c) detect the reasons which led to the non-performance of the obligations or possibly to the development of threat,

d) prepare an action plan for the implementation of necessary measures based on point *c)* and the known conditions for the operation of the body concerned,

e) initiate immediate measures that their introduction shall not make the performance of the main activity impossible, and inform the Authority immediately about them,

f) follow the rules regarding confidentiality obligations,

g) report continuously the measures taken to the Authority, the report shall demonstrate the measures taken, the compliance with security measures, the measures necessary to further the development of electronic information security, as well as

h) prepare a summary report about his/her operation at the termination of the secondment, including the measures taken and their results, as well as the additional proposed measures on the acceptance of which the Authority shall decide.

11.[1]

Section 28[2]

12. Miscellaneous provisions regarding the Authority

[1] Repealed by Section 54 of the Government Decree 323/2018 (XII.28.) Ineffective from 01.01.2019
[2] Repealed by Section 54 of the Government Decree 323/2018 (XII.28.) Ineffective from 01.01.2019

Section 29 (1)[1] To ensure the application of electronic information security rules, the body designated for the registration of the European and national critical infrastructures and for processing the data of the records and the Authority, as well as the incident response center under Section 19 (1) of the Hungarian Cyber Security Act shall exchange information about their findings detected in relation to the European and domestic critical systems and infrastructures regarding electronic information security.

(2) The information under paragraph (1) shall be provided immediately, if its subject detects threats endangering electronic information security or refers to a security incident. Based on the notification, the bodies concerned shall immediately commence the measure falling within their competence, coordinated with each other.

12/A.[2] The single point of contact responsible for the security of electronic information systems

Section 29/A[3] (1) The Authority shall perform the tasks of the single point of contact under the Directive, under which it shall

a) ensure the cooperation between authorities and the authorities of the EEA Member States concerned,

b)[4] cooperate with the incident response center under Section 19 (1) of the Hungarian Cyber Security Act and the authority under Section 6/B (3) of the Act CVIII of 2001 on certain aspects of electronic commerce services and information society services for the purpose of investigating the compliance with the Directive,

c) send the data related to the investigation of compliance and the result of the investigation to the European Commission in case of electronic information systems of the operators of essential services identified according to the Directive,

d) inform the Member States concerned about the security incidents occurred in the electronic information systems of the operators of essential services identified and the digital service providers, if the security incidents caused a significant disruptive effect on service provision, and it shall send a summary report about these security incidents to the Cooperation group of the European Union established for this task (hereinafter referred to as 'Cooperation group'),

e) cooperate with the Hungarian and international network security bodies, especially with the Cooperation group and the CSIRTs network established by the Directive,

f) if necessary, consult and cooperate with law enforcement agencies and the Hungarian National Authority for Data Protection and Freedom of Information.

(2) Within the framework of the information provision under paragraph (1) *c),* the national single point of contact shall send the following data to the European Commission:

a) the national measures enabling the identification of the operators of essential services,

---

[1] Amended by Section 53 of the Government Decree 323/2018 (XII.28.)
[2] Added by Section 49 of the Government Decree 323/2018 (XII.28.) Effective from 01.01.2019
[3] Added by Section 49 of the Government Decree 323/2018 (XII.28.) Effective from 01.01.2019
[4] Amended by Section 73 g) of the Government Decree 375/2020 (VII.30.)

b) the list of essential services provided for the maintenance of critical societal, economic activities,

c) the number of the operators of essential services and their significance under the aspect of the sector concerned,

d) the number of the users relying on the given services or the level of supply of the operators of essential services and

e) the information about the competence of the incident response centers and the procedure serving the security incident response.

13. Final provisions

Section 30 (1) This Decree shall enter into force on the third day after its promulgation with the exception set out in paragraph (2).

(2) Section 32 *a)* shall enter into force on 1 January 2016.

Section 31[1] This Decree serves the purpose of compliance with

a) 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 and

b) the Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market.

Section 32[2] (1) The single point of contact shall send the information under Section 29/A (2) *a)* to *d)* to the European Commission until 9 November 2018 for the first time and thereafter at least every two years.

(2) The single point of contact shall submit a summary report about the notifications from the operators of essential services and the digital service providers to the Cooperation group under the Directive until 9 November 2018 and thereafter once a year, and the report shall contain the number of notifications, the nature of the notified security incidents and the measures taken.

(3)[3] The National Directorate General for Disaster Management shall provide information to the single point of contact for the report under Section 29/A (2) until 31 October 2018 for the first time, thereafter at least every two years.

Section 33[4] (1) The provisions amended by the Government Decree 375/2020 (VII.30.) on the amendment of certain cyber security and other government decrees shall be applied also to the proceedings already pending when the Government Decree 375/2020 (VII.30.) on the amendment of certain cyber security and other government decrees entered into force.

(2) The National Directorate General for Disaster Management shall transmit the data related to the electronic information systems of the infrastructures designated as European or national critical infrastructures under the act on the identification, designation and protection of critical systems and facilities, as well as the ongoing procedures to the Special Service for National Security on the day following the entry into force of the Government Decree 375/2020 (VII.30.) on the amendment of certain cyber security and other government decrees.

---

[1] Declared by Section 50 of the Government Decree 323/2018 (XII.28.) Effective from 01.01.2019

[2] Declared by Section 51 of the Government Decree 323/2018 (XII.28.) Effective from 01.01.2019

[3] Amended by Section 72 d) of the Government Decree 375/2020 (VII.30.)

[4] Added by Section 71 of the Government Decree 375/2020 (VII.30.) Effective from 31.07.2020

Annex 1 to the Government Decree 187/2015 (VII.13.) [1]

The amount of the fine that may be imposed for each infringement

	A	B	C
1.	Name of infringement	Minimum amount of fine (HUF)	Maximum amount of fine (HUF)
2.	failure to register	50 000	100 000
3.	failure to notify data change	50 000	500 000
4.	failure to prepare a risk analysis	200 000	500 000
5.	failure to introduce and apply security measures proportionate to the risks	300 000	5 000 000
6.	failure to review the risk analysis and the necessary security measures immediately after a security incident, otherwise annually in documented form; failure to make the necessary changes based on the deficiencies identified during the review	200 000	2 000 000
7.	failure to notify a security incident	300 000	5 000 000
8.	failure to fulfil an obligation set out in the final, to be enforced decision of the Authority	400 000	5 000 000

[1] Added by Section 52, Annex 1 of the Government Decree 323/2018 (XII.28.) Effective from 13.01.2019