Act CLXVI of 2012
on the identification, designation and protection of critical systems and facilities[1]

The National Assembly adopts the following Act for ensuring the protection of life and material assets, the continuity of essential services.

1. Interpretative provisions

Section 1[2] For the purposes of this Act:

a) *sectoral criterion*: the criteria, their thresholds, technical or functional characteristics that refer to the effect caused by the disruption or destruction of an infrastructure of a device, facility (hereinafter collectively referred to as failure) and which, if fulfilled, the device, facility, system or parts thereof may be designated as critical infrastructures, in close connection with the sector to which it belongs,

b) *essential service*: critical service necessary for the maintenance of societal or economic activities, that depend on an electronic information system, and which is included in the list of essential services,

c) *list of essential services*: the list of the essential services, to be compiled in cooperation with the relevant central government entities, and defined in a government decree,

d) operator of essential services: the organisation or economic entity that

da) provides essential services,

db) the essential service it provides depends on electronic information systems,

dc) an incident affecting the essential service provided thereby would constitute significant disruption – as defined in a government decree – in the provision of said service, and

dd) it has been identified as an operator of essential services in a procedure to this effect,

e) *EEA state*: a member state of the European Union and other states that are party to the Agreement on the European Economic Area,

f) *European critical infrastructures*: critical infrastructures designated by this Act, the failure of which would have significant effect on at least two EEA states including the effects deriving from cross-sectoral interdependencies,

g) *on-site inspection body*: the sectoral designating authority, the competent administrative authority, the advisory body participating in the designating procedure and the body entitled to carry out the on-site inspection on the basis of legislation,

h) *horizontal criterion*: the criteria, their thresholds, technical or functional characteristics that refer to the effect caused by the disruption or destruction of an infrastructure of a device, facility (hereinafter collectively referred to as failure) and which, if fulfilled, – with respect to the loss of human life incurred, the effect on health, the economic and societal effects, the effect on nature and the built environment – the device, facility, system or parts thereof may be designated as critical infrastructures, independently of the sector to which it belongs,

---

[1] Promulgated: 22.11.2012 Different provisions shall apply during an emergency. See: Government Decree 86/2020. (IV. 5.) section 4 (1).

[2] Declared by Act XXXI of 2020. section 123. Effective from 01.07.2020

i) *protection of critical infrastructures*: all activities aimed at ensuring the function, uninterrupted operation and intactness of the critical infrastructures to mitigate or eliminate threat, risk, vulnerability,

j) *critical infrastructures*: the infrastructures of a service, device, facility or system belonging to either sector defined in Annex 1, moreover the services provided by them which are indispensable for fulfilling critical societal tasks – especially healthcare, personal and asset safety of the people, providing for economic and social public services, national defence of the country – and the failure of which would have significant consequences due to the lack of continuous provision of such tasks,

k) *national critical infrastructures*: critical infrastructures designated by this Act, the failure of which would have significant effect primarily in Hungary due to the lack of continuous provision of the critical societal tasks,

l) *operator*: the natural or legal person, or entity without legal personality who is the owner, the licensee, the person authorised to dispose of or responsible for the daily operation of the infrastructures of the device, facility or system,

m) *exceptional occurrence*: such external or internal impact, that significantly endangers, prevents the proper operation, operating continuity of the designated national or European infrastructures, and which satisfies the criteria set out in the laws.

2. Designation of the national critical infrastructures

Section 2[1] (1) The operator conducts an identification test

a) within 60 days from the commencement of the operation of the critical infrastructures or the provision of the service,

b) during the operating period within 60 days from an activity change of such magnitude, that results in the fulfilment of the sectoral or horizontal criteria,

c) in the case of a potential critical infrastructures, included but not previously proposed for designation in the previous identification report, after the lapse of five years from the closing date of the identification test, during the operation period, after the lapse of five years from the designating decision becoming final,

d) on the initiative of the advisory authority.

(2) The operator shall submit the identification report the operator prepared on the basis of the identification test (hereinafter referred to as identification report) to the body designated in the government decree (hereinafter referred to as the sectoral designating authority) within 8 days following its preparation.

(3) The designating procedure for the purpose of designation as national critical infrastructures, shall be conducted ex officio by the sectoral designating authority

a) following the submission of the identification report,

b) on the basis of the case initiation proposal of the general advisory authority as set out in section 10(1) or

c) for the purpose of designation as national defence critical infrastructures, on the basis of the initiation proposal of the sectoral advisory authority for national defence.

(4) In the case set out in the above paragraph (3)c) those set out in section 10(3) shall be applied mutatis mutandis.

(5) The sectoral designating authority may decide on revoking the designation

[1] Declared by Act XXXI of 2020 section 124(1). Effective from 01.07.2020

a) ex officio as defined in paragraph (3) above, or

b) at the request of the operator.

(6) The sectoral designating authority decides on the designation of national critical infrastructures or the revocation of the designation by involving the administrative authority and on the basis examining the fulfilment of the sectoral and horizontal criteria.

(7) In the designating decision adopted pursuant to paragraph (6) above, the sectoral designating authority

a) sets a deadline for the elaboration of the operational security plan,

b) obliges the operator to engage or employ a security liaison officer, and submits the data of the security liaison officer to the registration authority within 60 days of the designating decision becoming final, and

c) may prescribe conditions for the operator to abide by related to the protection of the critical infrastructures in alignment with the unique characteristics, environment of the infrastructures and the magnitude of the threat potentially caused by the infrastructures.

(8) If the operator fails to perform its obligations set out in paragraph (2) above, the sectoral designating authority calls upon the operator in its decision containing a warning and sets a deadline for the submission of the identification report.

(9) The sectoral designating authority for national defence systems and facilities may designate infrastructures defined in Annex 1 but not belonging to the national defence sector in the interest of national defence, to become national critical infrastructures on the basis of national defence criteria set out in a government decree, without examining horizontal criteria (hereinafter referred to as non-sectoral national defence infrastructures).

(10) In the procedure for designation as non-sectoral national defence infrastructures, seeking the administrative authority may be omitted, if the infrastructure to be designated by the sectoral designating authority for national defence is a designated infrastructure already.

(11) In the designating decision the sectoral designating authority for national defence systems and facilities

a) may prescribe a deadline shorter than 60 days to the operator for the submission of the data on the security liaison officer,

b) may adopt its decision set out in paragraph (6) above in an accelerated procedure in the interest of national defence.

(12) The case initiating proposal set out in paragraph (3)b) above, is given by the sectoral advisory authority for national defence to the sectoral designating authority for national defence systems and facilities.

2/A[1] Designation and registration of operator of essential services

Section 2/A[2] (1) The operators of essential services are designated by the sectoral designating authority in the procedure set out in section 2 above.

(2) The operator of a designated national critical infrastructures is considered an operator of essential services, if

a)[3] it provides services registered in the list of essential services,

---

[1] Added by Act CXXXIV of 2017 section 42. Effective from 10.05.2018

[2] Added by Act CXXXIV of 2017 section 42. Effective from 10.05.2018

[3] Declared by Act XXXI of 2020 section 125(1). Effective from 01.07.2020

b)[1] the provision of the service it provides is dependent on electronic information systems, and

c)[2] an incident affecting the service it provides would cause significant disruption – as defined in the government decree – in ensuring the service it provides.

(3) The sectoral designating authority rules on registering the operator in the list of the operators of essential services in its decision on the designation of a national critical infrastructure.

(3a)[3] The Government defines the list of essential services necessary for maintaining critical societal and economic activities.

(4) The list of the operators of essential services is kept by the registration authority.

(5) The registration authority deletes the operator from the list of the operators of essential services if the sectoral designating authority decides on the revocation of the designation of being a national critical infrastructure.

(6) The registration authority reviews and if necessary, updates the list of the operators of essential services every two years prior to reporting to the European Commission.

Section 2/B[4] (1) In the case of operators of systems and infrastructures that were not designated as national critical infrastructures in the procedure set out in section 2, but they satisfy the criteria set out in section 2/A(2) on the identification of an operator of essential service, the identification is conducted by the authority designated in a government decree.

(2) The authority set out in paragraph (1) above acts ex officio when identifying an operator as one providing essential service.

(3) The authority set out in paragraph (1) above rules in a decision on including the operator in the list of the operators of essential services and informs the authority keeping the registry. The authority set out in paragraph (1) above may decide on the deletion from the list of the operators of essential services

a) ex officio or

b) at the request of the operator of essential services.

(4) For the purpose of conducting the identification procedure, the authority set out in paragraph (1) above is entitled to – with the exception of personal data – request data reporting from

a) the service provider, economic entity providing a service defined in the registry for essential services,

b) the organisation exercising authoritative, supervisory or control power over the service provider set out in point a) above,

c) public registers.

(5) If the entity identified as an operator of essential service disagrees with the identification, then it proves that it does not satisfy the criteria relevant for identification as an operator of essential service.

(6) The Government defines the thresholds necessary for determining the relevant supply level on the basis of the users dependent on said service or the significance of the concrete economic operator providing essential service, in decrees separately for sectors.

---

[1] Modified by Act CXXI of 2018 section 109a)
[2] Declared by Act XXXI of 2020 section 125(2). Effective from 01.07.2020
[3] Added by Act CXVI of 2019 section 36(1). Effective from 01.04.2020
[4] Added by Act XXXI of 2020 section 126. Effective from 01.07.2020

3. Designation of European critical infrastructures

Section 3 (1)[1] The designating procedure for a European critical infrastructure is conducted by the sectoral designating authority ex officio

a)[2] following the submission of the identification report prepared on the basis of the identification test by the operator,

b) on the basis of the initiative of an EEA state, or

c) on the basis of the initiative of the advisory authority made at the sectoral designating authority.

(1a)[3] The sectoral designating authority may decide on the revocation of the designation

a) ex officio,

b) ex officio on the basis of the initiative of an EEA state, or

c)[4] on the basis of the declaration of the operator.

(2)[5] The initiative to be designated as a European critical infrastructure and the identification report submitted by the operator – with the exception of section (1)c) above

with the involvement of the advisory authority – are examined by the sectoral designating authority and informs the minister responsible for disaster management through the minister responsible for the relevant sector on its opinion related to the designation to be a European critical infrastructure.

(3) The minister responsible for disaster management together with the minister responsible for and having powers over the relevant sector initiates the conclusion of the international agreement related to the designation of European critical infrastructures.

(4) The sectoral designating authority adopts a decision on being designated as a European critical infrastructure, within 30 days from the international agreement entering into force, pursuant to the rules of administrative authority procedures. The decision defines the obligations of the operator of the European critical infrastructures, the deadlines for implementation and their monitoring pursuant to those defined in the international agreement.

4. Common rules for the national critical infrastructures and the European critical infrastructures

Section 4[6] (1)[7] Only such person may participate on behalf of the designating authority and the administrative authority (hereinafter jointly referred to as authority)

a) in the administrative procedure for designation (hereinafter jointly referred to as designating procedure) and

b) in the administrative procedure for the revocation of the designation (hereinafter jointly referred to as procedure for the revocation of designation)

in the national critical infrastructures and the European critical infrastructures,

---

[1] Declared by Act CXVI of 2016 section 94(1). Effective from 01.01.2017
[2] Modified by Act XXXI of 2020 section 140a)
[3] Added by Act CXVI of 2016 section 94(2). Effective from 01.01.2017
[4] Modified by Act XXXI of 2020 section 140b)
[5] Declared by Act CXVI of 2016 section 94(3). Effective from 01.01.2017
[6] Declared by Act CXXI of 2018 section 106. Effective from 01.01.2019
[7] Modified by Act XXXI of 2020 section 140c)

c)[1] in the case of critical infrastructures for national defence in the monitoring as well besides the procedures set out in points a) and b) above,

as regards whom national security clearance was performed as set out in the relevant laws on national security services, and with respect to whom no risk was identified.

(2)[2] In the identification test relevant for the European critical infrastructures only such person may participate on behalf of the intermediate body engaged by the operator as regards whom national security clearance was performed as set out in the relevant laws on national security services, and with respect to whom no risk was identified.

(3)[3] During the performance of the tasks set out in this Act, thus especially in the designating procedure and the authority monitoring procedure, classified data, personal data or sensitive data, business secret, banking secret, payment secret, insurance secret, securities secret, treasury secret may be made known to the authority, the administrative authority and the advisory bodies participating in the procedure provided such data is related to the procedure and for the time period necessary for the procedure – in accordance with the limitations set out for classified data and information security in the interest of national security and national defence.

Section 5 (1) The entity designated in a government decree for such purposes registers and manages (hereinafter referred to as registration authority)

a)[4] name, registered seat or residential address, mailing address, company registration number or registration number for sole entrepreneurs, statistical code, and tax number, name of the representative, phone number, email address of the operator,

b)[5] natural identification data, phone number, e-mail address, relevant qualification, serial number of the document verifying the qualification of the security liaison officer,

c)[6] name, address of the national critical infrastructures, services and name and address of those European critical infrastructures, services where Hungary is a party affected,

d) the operational security plan,

e)[7] the decision of the sectoral designating authority on the designation and the revocation of the designation of the European critical infrastructures or of the national critical infrastructures,

f)[8] the documents related to authority monitoring,

g)[9] the information security rules and policies.

(2) The purpose of processing the data set out in paragraph (1) above is

a)[10] to ensure conducting the procedure for designation, revocation of designation,

b) to satisfy the obligations related to the protection of the critical infrastructures, to ensure authority monitoring,

---

[1] Added by Act XXXI of 2020 section 127(1). Effective from 01.07.2020
[2] Modified by Act XXXI of 2020 section 140d)
[3] Added by Act XXXI of 2020 section 127(2). Effective from 01.07.2020
[4] Modified by Act XXXI of 2020 section 140e)
[5] Modified by Act XXXI of 2020 section 140e)
[6] Declared by Act XXXI of 2020 section 128(1). Effective from 01.07.2020
[7] Modified by Act CXVI of 2016 section 97(1)
[8] Added by Act XXXI of 2020 section 128(2). Effective from 01.07.2020
[9] Added by Act XXXI of 2020 section 128(2). Effective from 01.07.2020
[10] Modified by Act XXXI of 2020 section 141a)

c)[1] to ensure the regular authority monitoring of the satisfaction of the conditions prescribed in the decision adopted pursuant to the designating procedure set out in section 2(7) above.

(3)[2] The registration authority registers the data set out in paragraph (1) above on the basis of the authority decision adopted in the designating procedure by the sectoral designating authority and pursuant to the data reporting of the operator. The sectoral designating authority is obliged to send the relevant decision of the registration authority immediately following it becomes final. Simultaneously with sending the decision, the sectoral designating authority informs the registration authority on the data set out in paragraph (1)c) above.

(4) The registration authority may forward data from the registry as follows:

a)[3] to the authorities participating in the designating procedure, in the procedure for the revocation of the designation, for the purpose of ensuring the conducting of the designating procedure, the procedure for the revocation of the designation,

b) to the body coordinating the monitoring of the European critical infrastructures or the national critical infrastructures (hereinafter referred to as monitoring coordinating body) for the purpose of ensuring coordinating tasks,

c)[4] to the body conducting the on-site monitoring of the European critical infrastructures or the national critical infrastructures, for the purpose of conducting the on-site monitoring,

d) to the competent authorities for official monitoring as regards the European critical infrastructures or the national critical infrastructures on the basis of legal regulations, for the purpose of conducting the official monitoring,

e)[5] in the case of an exceptional occurrence, for the purpose of assisting the activities of the bodies participating in the case management and the recovery,

f)[6] to the regional and local bodies of the national disaster management, for the purpose of performing its administrative, preventive, liaison and informative tasks and for the management of exceptional occurrence,

g)[7] to the authority set out in sections 2(5) and 14(1) of the act on the electronic information security of state and municipal bodies (hereinafter referred to as Hungarian Cyber Security Act), to the single point of contact designated in a government decree pursuant to Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016, and the incident response centre set out in section 19(1) and (2) of the Hungarian Cyber Security Act, for the purpose of performing their tasks,

h)[8] to the advisory authority of the national defence sector, for the purpose of assessing the scope of possible critical infrastructures for national defence,

i)[9] to the advisory authority of the national defence sector during the period of special legal order or national defence emergency, for the purpose of arranging for the enhanced protection of the national critical infrastructures,

---

[1] Modified by Act XXXI of 2020 section 140f)
[2] Declared by Act XXXI of 2020 section 128(3). Effective from 01.07.2020
[3] Declared by Act XXXI of 2020 section 128(4). Effective from 01.07.2020
[4] Modified by Act XXXI of 2020 section 141b)
[5] Added by Act CXVI of 2016 section 95(1). Effective from 01.01.2017
[6] Added by Act CXVI of 2016 section 95(1). Effective from 01.01.2017
[7] Added by Act CXXI of 2018 section 107. Effective from 01.01.2019
[8] Added by Act CV of 2019 section 71. Effective from 01.01.2020
[9] Declared by Act XXXI of 2020 section 128(5). Effective from 01.07.2020

j)[1] to the provider of the uniform digital radiocommunication system (hereinafter referred to as UDS) service, for the purpose of ensuring UDS service for communication for government purposes,

k)[2] in the interest of national defence and counter-terrorism, on the basis of a separate, justified request submitted by the body responsible for the task.

(5)[3] The data of the European critical infrastructures or the national critical infrastructures are deleted by the registration authority and all authorities affected by the designating procedure, within 30 days after the decision of the sectoral designating authority on the revocation of the designation of the infrastructures becomes final, and the registration authority informs the operator thereof in writing.

(6)[4] The sectoral designating authority is obliged to immediately send

a) the final decision on the revocation of the designation or the refusal of the designation to all authorities affected in the designating procedure,

b) the final decision on the revocation of the designation to the registration authority.

Section 6[5] (1) The operator of the European critical infrastructures or the national critical infrastructures – with the exception of those contained in paragraph (9) below – elaborates the operational security plan in compliance with the material and formal requirements set out in the designating decision of the sectoral designating authority, within the deadline set out in the decision of the authority, and sends such to the designating authority by electronic means.

(2) Before its registration, within 60 days the sectoral designating authority examines the operational security plan in respect of the material and formal aspects, in the interest of the fulfilment of the material and formal requirements set out in its decision, and in the case of incompleteness, it calls upon the operator to remedy the deficiency. If the infrastructures were designated by the national defence sector as well, the sectoral designating authority obtains the opinion of the sectoral designating authority for national defence, in the case of a national defence infrastructures by sending the operational security plan for the purpose of examining the material and formal compliance. The sectoral designating authority sends the adopted operational security plan to the registration authority and the operator.

(3) The critical infrastructures for national defence designated by the sectoral designating authority for national defence may be registered irrespective of the examination of the operational security plan and any eventual deficiency remedy as regards such plan. If the examination of the operational security plan or the deficiency remedy thereof is in progress, the designating authority for national defence informs the registration authority about such fact.

(4) The operational security plan includes the critical infrastructures, services and the organisational structure and the system of resources in place to protect them. The operational security plan – by means of risk analysis and risk management – defines those security measures, the elaboration and operation of which ensure the protection, business continuity and restoration of operation of the European critical infrastructures or the national critical infrastructures, moreover defines those provisional measures that need to be implemented according to the different levels of risks and threat.

---

[1] Added by Act XXXI of 2020 section 128(6). Effective from 01.07.2020
[2] Added by Act XXXI of 2020 section 128(6). Effective from 01.07.2020
[3] Declared by Act XXXI of 2020 section 128(7). Effective from 01.07.2020
[4] Declared by Act L of 2017 section 426(2). Effective from 01.01.2018
[5] Declared by Act XXXI of 2020 section 129. Effective from 01.07.2020

(5) The operational security plan of critical infrastructures for national defence includes the order of contact and cooperation with the competent national defence bodies, as set out in the decision issued by the sectoral authority.

(6) The operator of the European critical infrastructures or the national critical infrastructures modifies the operational security plan forthwith, in the case of any change that effects the provision of services, activities, conditions for operation or protection of the critical infrastructures. The rules set out in paragraph (2) above shall apply to the examination, approval and sending of the modified operational security plan.

(7) The operator ensures and regularly monitors the feasibility of those contained in the operational security plan and the information security rules and policies. In the interest of the above, the operators defined by the central body of the national disaster management conduct such exercises with the direction of the central or regional body of the national disaster management, involving the sectoral designating authority, where the organisational structure and the resources system described in the operational security plan, and the resilience of information technology- and network security is exercised (hereinafter referred to as complex exercise).

(8) The adequacy of the complex exercise is assessed by the central or regional body of the national disaster management, involving the sectoral designating authority. If the assessor establishes the operational security plan and the information security rules and policies to be inadequate during the complex exercise, the assessor obliges the operator to modify the operational security plan and the information security rules and policies and to redo the complex exercise.

(9) If upon designation of the critical infrastructures as a European critical infrastructures or national critical infrastructures, the operator has such a security document that includes the material elements of the operational security plan, then upon the request of the operator, the sectoral designating authority may decide that such security document replaces the operational security plan.

(10) In the case set out in paragraph (9) above, the security document shall be sent to the registration authority for the purpose of registration pursuant to section 5.

(11) The operator informs the on-call services of the regional body of the national disaster management immediately upon the befalling of an exceptional occurrence, in the form described on the website of the central body of the national disaster management, as well as the sectoral designating authority. With respect to critical infrastructures for national defence, the operator immediately informs the on-call services designated by the minister responsible for national defence, as well.

(12) The operational security plan and its annexes or the security document replacing them is not public.

(13) If the risk associated with the befalling of the exceptional occurrence was not examined, then the operator modifies the operational security plan forthwith in order to manage the newly occurred risk. The rules set out in paragraph (2) above apply in the case of the modified operational security plan.

(14) The operator of the European critical infrastructures or the national critical infrastructures provides for the engagement or employment of a security liaison officer, and continuously provides for the conditions necessary for the activities of the security liaison officer. The tasks of the security liaison officer are the following:

a) liaising among the operator and the authorities participating in the designating procedure, moreover in the case of critical infrastructures for national defence, with the national defence bodies set out in paragraph (5) above,

b) elaborating the operational security plan.

(15) The security liaison officer may be a person with a clean criminal record, having the qualifications set out in a government decree. The security liaison officer verifies the fulfilment of the clean criminal record requirement.

(16) The operator of the European critical infrastructures and the national critical infrastructures reports the data set out in section 5(1) a)-c) within 60 days from the designating decision becoming final to the registration authority on the electronic form published by the authority.

(17) With the exception of the critical infrastructures for national defence within the sector, the operator of the European critical infrastructures and the national critical infrastructures and the sectoral designating authority provide to national disaster management bodies – within 60 days of the designating decision becoming final – the electronic data included in their registries and supervisory systems that support the prompt response capabilities of the national disaster management bodies participating in the remedial actions, and promote successful intervention and restoration.

Section 7[1] The operator of the European critical infrastructures or the national critical infrastructures is responsible for the costs of the elaboration, modification and exercising of the operational security plan, the employment costs of the security liaison officer, and the costs related to the organisational structure and resources system serving the purpose of protecting the critical infrastructures as included in the operational security plan.

Section 8 (1) The central body of the national disaster management – with the exception set out in paragraph (2) above – is the body coordinating monitoring. The central body of the national disaster management regularly monitors the European critical infrastructures or the national critical infrastructures.

(2)[2] As regards critical infrastructures for national defence as well as the critical infrastructures of the national disaster management, the body coordinating the monitoring and the body conducting the on-site inspection is designated by the Government in a decree.

(3)[3] The European critical infrastructures and the national critical infrastructures shall be monitored at least every five years within the framework of complex administrative monitoring (hereinafter referred to as complex monitoring). The complex monitoring shall be carried out by taking into account national security and – in the case of a non-sectoral critical infrastructure for national defence – national defence considerations.

(4)[4] The monitoring coordinating body coordinates the complex monitoring, where it may involve the body conducting the on-site inspection in the complex monitoring and may hold a joint complex monitoring together with the body conducting the on-site inspection. The body conducting the on-site inspection cooperates with the monitoring coordinating body in connection with the complex monitoring.

(5)[5] The body conducting the on-site inspection informs the monitoring coordinating body on the results of its on-site inspection other than the complex monitoring as regards the

---

[1] Declared by Act XXXI of 2020 section 129. Effective from 01.07.2020
[2] Modified by Act CCLI of 2013 section 26
[3] Declared by Act XXXI of 2020 section 130. Effective from 01.07.2020
[4] Declared by Act XXXI of 2020 section 130. Effective from 01.07.2020
[5] Declared by Act XXXI of 2020 section 130. Effective from 01.07.2020

European critical infrastructures or the national infrastructures, within 15 days following the closing of the inspection.

(6)[1] The monitoring coordinating body also coordinates within the framework of the complex monitoring the information technology and network security administrative monitoring related to the protection of the critical infrastructures. At the request of the monitoring coordinating body, the authority responsible for electronic information security conducts an information technology and network security administrative inspection and informs the monitoring coordinating body on the results of such inspection within 15 days following the closing of the inspection.

(7)[2] Within the framework of the complex monitoring or the on-site inspection the sectoral designating authority and the monitoring coordinating body may inspect at the European critical infrastructures or the national critical infrastructures, whether the security liaison officer has a clean criminal record, for which purpose either may request data from the criminal records system. The data request may only be aimed at the security liaison officer having a clean criminal record.

(8) The body conducting the on-site inspection and, in the case set out in paragraph (1) above, the central body of the national disaster management transfer the personal data learnt pursuant to paragraph (7) above – if it is established during the administrative inspection that the security liaison officer fails to meet the criterion of a clean criminal record – to the sectoral designating authority for the purpose of conducting the procedure pursuant to section 9.

(9) The personal data learnt pursuant to paragraphs (7) and (8) above are processed

a) by the body conducting the on-site inspection for the duration of the on-site inspection and for the period of the data transfer to the sectoral designating authority,

b) in the case of paragraph (1) above by the central body of the national disaster management for the duration of the administrative inspection and for the period of the data transfer to the sectoral designating authority,

c)[3] by the sectoral designating authority in the procedure pursuant to section 9 for the duration of the administrative inspection and until the decision pursuant to section 9 becoming final.

Section 9 If the operator of the European critical infrastructures or national critical infrastructures fails to abide by those set out in this Act, in other legal regulations issued pursuant to the authorisation set out in this Act, or the prescriptions contained in the decision of the sectoral designating authority, the sectoral designating authority, in its decision

a) calls upon the operator of the European critical infrastructures or national critical infrastructures to comply with its obligations,

b) obliges the operator to modify the operational security plan or to prepare a new operational security plan,

c) may levy a fine in the amount set out in a government decree.

Section 9/A[4] The bodies participating in the maintenance, repairs and management, elimination of extraordinary occurrences affecting the designated critical infrastructures as well as further participants are obliged to ensure, that the operation of the infrastructures is limited for the shortest period of time possible.

---

[1] Declared by Act XXXI of 2020 section 130. Effective from 01.07.2020
[2] Declared by Act XXXI of 2020 section 130. Effective from 01.07.2020
[3] Declared by Act L of 2017 section 426(3). Effective from 01.01.2018
[4] Added by Act XXXI of 2020 section 132. Effective from 01.07.2020

Section 9/B[1] In the case of the national defence sector and the critical infrastructures for national defence, the provisions on information security set out in sections 4-9 above, are not applicable.

5.[2] Competence of the general advisory authority

Section 10[3] (1) With consideration to disaster management, public order, public safety, civil defence, national security, counter-terrorism the central body of the national disaster management is the general advisory authority as regards designation as national critical infrastructures.

(2) The general advisory body assesses the status of the sectors and sub-sectors semi-annually – by taking into account the fulfilment of the sectoral and horizontal criteria, and the findings of the assessment pursuant to section 13(2) – and on the basis of such assessment it sends its case initiating proposal to the sectoral designating authority. The sectoral designating authority commences an administrative procedure ex officio for the designation of the critical infrastructures, services, operators included in the case initiating proposal.

(3) Following the commencement of the ex officio procedure for designation, the operator may prove that it does not meet the sectoral and horizontal criteria.

(4) On the basis of the case initiating proposal the sectoral designating authority is obliged to commence the procedure for the revocation of the designation as national critical infrastructures, if such proposal was included therein.

Section 11[4] In excess of those defined in section 10(2) above, the general advisory authority continuously analyses, assesses the dependencies among the individual sectors and subsectors, in this regard, for the purpose of preparing its case initiating proposal it is entitled to request data reporting – with the exception of personal data –

a) from advisory bodies,

b) from the sectoral designating and advisory authorities,

c) from public records,

d) from public administration bodies, legal persons, other entities without legal personality and natural persons. The body or person sought may not deny data reporting.

Section 12[5] In the administrative procedure commenced on the basis of the case initiating proposal, the sectoral designating authority may only examine the sectoral criteria. Procurement of the opinion of the administrative authority in such procedure is not needed. The opinion of the administrative authority is replaced by the case initiating proposal of the general advisory authority.

(2) If the sectoral designating authority establishes the existence of at least one sectoral criterion, it adopts the decision set out in section 2(6) above, by taking into consideration those set out in section 2(3)b) above.

Section 12/A[6] Sections 10-12 above are applicable with the following deviations with respect to the national defence sector and the critical infrastructures for national defence:

---

[1] Added by Act XXXI of 2020 section 132. Effective from 01.07.2020
[2] Declared by Act XXXI of 2020 section 133. Effective from 01.07.2020
[3] Declared by Act XXXI of 2020 section 133. Effective from 01.07.2020
[4] Declared by Act XXXI of 2020 section 133. Effective from 01.07.2020
[5] Declared by Act XXXI of 2020 section 133. Effective from 01.07.2020
[6] Added by Act XXXI of 2020 section 133. Effective from 01.07.2020

a) as regards national defence infrastructure, the body pursuant to section 10(1) above does not qualify as a general advisory body, even if the considerations prescribed therein occur;

b) as regards the national defence sector and the critical infrastructures for national defence, the fulfilment of the horizontal criteria and the findings of the assessment pursuant to section 13(2) below are not considered;

c) as regards non-sectoral critical infrastructures for national defence, the advisory body of the national defence sector shall be considered the general advisory body.

6. Report to the European Commission

Section 13[1] (1) The Government submits yearly reports to the European Commission

a) on the number of critical infrastructures designated as European critical infrastructures for each sector, and on the number of the member states of the European Union, that depend on the European critical infrastructures,

b) on the types of the vulnerability points, and the types of the threats and risks they may encounter for those sectors in which European critical infrastructures are designated.

(2) For the purpose of compiling the report pursuant to paragraph (1) above, the sectoral designating authorities and the registration authority assess the status of the sectors and subsectors yearly – taking into consideration the fulfilment of the sectoral criteria – and the assessment for the relevant year is sent to the Government through the minister responsible for disaster management until 30 April each year.

6/A.[2] *Extraordinary measures that may apply during the special legal order*

Section 13/A[3] During the period of special legal order, disparate provisions may be introduced by way of a decree with respect to the procedures on critical systems as regards

a) determining competence and jurisdiction,

b) designating the authority proceeding,

c) deadline for processing and other time periods,

d) exclusion of the administrative authority,

e) order of legal remedies,

f) non-contestability before courts,

g) rules of implementation.

(2) In the case of introducing special legal order, the following may be defined in a decree:

a) appointment of a member of the Government to coordinate the activities of the relevant critical system,

b) delegation of Government liaison professionals to the relevant critical infrastructures,

c) competence of the professionals set out in point b) above,

d) content of the cooperation obligation of the relevant critical system,

e) conditions and order of the takeover of the supervision of the relevant critical system.

(3) During the period of special legal order, designation as national critical infrastructures pursuant to paragraphs (1) and (2) above shall be reviewed until the sixtieth days following

[1] Declared by Act XXXI of 2020 section 134. Effective from 01.07.2020
[2] Added by Act XXXI of 2020 section 135. Effective from 01.07.2020
[3] Added by Act XXXI of 2020 section 135. Effective from 01.07.2020

the termination of the special legal order. The review is done by the authority proceeding pursuant to paragraph (1)b) above, with the involvement of the sectoral designating authority appointed in the government decree.

7. Final provisions

Section 14 The Government shall be authorised to determine the following in a decree[1]

a) appoint the sectoral designating authority, the advisory authority, the body conducting the on-site inspection, the monitoring coordinating body pursuant to section 8(2)[2]

b)[3] determine the rules of procedure for the identification procedure and the administrative inspection in general, and specifically for each sector, determine the rules of procedure for the revocation of the designation[4],

c)[5] determine the rules of cooperation among the authorities participating in the identification test, the designating procedure, the administrative inspection, the procedure for the revocation of the designation[6],

d) determine the sectoral and horizontal criteria[7],

e) define the amount of the administrative fine to be levied pursuant to sections 9 and 12, and the rules of procedure for levying such fine[8],

f) appoint the registration authority and define the detailed rules of procedure for keeping the registry, reporting the data to be included in the registry and the order for requesting data from the registry[9],

g) determine the qualification requirements for the security liaison officer[10],

h) determine the possible sectoral material and formal requirements of the operational security plan[11],

i) determine the rules related to taking network security measures[12]

---

[1] See Government Decree 359/2015 (XII.2.)

[2] See Government Decree 65/2013 (III.8.), Government Decree 512/2013 (XII.29.), Government Decree 540/2013 (XII.30.), Government Decree 541/2013 (XII.30.), Government Decree 246/2015 (IX.8.), Government Decree 330/2015 (XI.10.), Government Decree 359/2015 (XII.2.) section 3, Government Decree 249/2017 (IX.5.), Government Decree 161/2019 (VII.4.), Government Decree 374/2020 (VII.30.)

[3] Modified by Act XXXI of 2020 section 140g)

[4] See Government Decree 65/2013 (III.8.); Government Decree 246/2015 (IX.8.), Government Decree 359/2015 (XII.2.) sections 4-5, Government Decree 249/2017 (IX.5.) , Government Decree 161/2019 (VII.4.) , Government Decree 374/2020 (VII.30.)

[5] Modified by Act XXXI of 2020 section 140h)

[6] See Government Decree 65/2013 (III.8.), Government Decree 246/2015 (IX.8.), Government Decree 161/2019 (VII.4.), Government Decree 374/2020 (VII.30.)

[7] See Government Decree 65/2013 (III.8.), Government Decree 512/2013 (XII.29.), Government Decree 540/2013 (XII.30.) , Government Decree 541/2013 (XII.30.) , Government Decree 246/2015 (IX.8.), Government Decree 330/2015 (XI.10.), Government Decree 359/2015 (XII.2.) section 2, Government Decree 249/2017 (IX.5.) , Government Decree 161/2019 (VII.4.), Government Decree 374/2020 (VII.30.)

[8] See Government Decree 65/2013 (III.8.)

[9] See Government Decree 65/2013 (III.8.), Government Decree 161/2019 (VII.4.)

[10] See Government Decree 65/2013 (III.8.), Government Decree 512/2013 (XII.29.), Government Decree 540/2013 (XII.30.), Government Decree 541/2013 (XII.30.), Government Decree 246/2015 (IX.8.), Government Decree 330/2015 (XI.10.), Government Decree 359/2015 (XII.2.) section 6, Government Decree 249/2017 (IX.5.), Government Decree 161/2019 (VII.4.), Government Decree 374/2020 (VII.30.)

[11] See Government Decree 65/2013 (III.8.), Government Decree 246/2015 (IX.8.), Government Decree 359/2015 (XII.2.) section 7, Government Decree 161/2019 (VII.4.)

[12] See Government Decree 65/2013 (III.8.), Government Decree 233/2013 (VI.30.) sections 7-8, 10, Government Decree 185/2015 (VII.13.) title 6

j)[1] define the list of the essential services necessary to maintain critical societal and economic activities,

k)[2] determine the detailed sectoral rules related to exceptional occurrences[3],

l)[4] appoint the authority conducting the identification procedure set out in section 2/B above, and the authority with the competence of information security administrative tasks, and determine the special rules for the identification procedure, monitoring and define the rules of procedure for the revocation of the identification,

m)[5] determine the thresholds set out in section 2/B(6) for each sector and the magnitude of significant disruption set out in section 2/A[6].

Section 15 (1) This Act shall enter into force on the first day of the fourth month following its promulgation – with the exception of paragraphs (2) and (3) below.

(2) Annex 2 shall enter into force on 1 July 2013.

(3) Annex 3 shall enter into force on 1 January 2014.

Section 15/A[7] (1) With regard to the national critical infrastructures of the operator already designated when Act CXXXIV of 2017 on the modification of acts related to home affair tasks and other relevant acts (hereinafter referred to as Tv1) entered into force, the operator submits to the designating authority a supplement to the identification report within sixty days from Tv1 entering into force, in which the operator makes a statement on its compliance with the criteria set out in section 2/A(2)b) and c).

(2)[8]

(3) The sectoral designating authority decides on the inclusion of the operator in the list of the operators of essential services within 30 days following the submission of the supplement to the identification report set out in paragraph (1), on the basis of the supplement to the identification report and the available operational security plan.

Section 15/B[9] The identification test set out in section 2(1) of Act XXXI of 2020 (hereinafter referred to as Amending Act) on the modification of certain acts enhancing the safety of citizens shall be carried out within 60 days following the Amending Act's entering into force, in the case of critical infrastructures operating for more than 60 days prior to the Amending Act's entering into force.

Section 15/C[10] Pursuant to Article 54(4) of the Fundamental Law, subheading 6/A and section 15/D of this Act qualifies as cardinal.

Section 15/D[11] The prescriptions defined in section 13/A(3) declared by the Amending Act, shall be applied in the case of the designation of national critical infrastructures designated during the state of emergency declared by Government Decree 40/2020 (III.11.) on the declaration of state of danger.

---

[1] Added by Act CXVI of 2019 section 36(2). Effective from 01.04.2020
[2] Added by Act XXXI of 2020 section 136(2). Effective from 01.07.2020
[3] See Government Decree 374/2020 (VII.30.)
[4] Added by Act XXXI of 2020 section 136(2). Effective from 01.07.2020
[5] Added by Act XXXI of 2020 section 136(2). Effective from 01.07.2020
[6] See Government Decree 374/2020 (VII.30.)
[7] Added by Act CXXXIV of 2017 section 43. Effective from 10.05.2018
[8] Repealed by Act XXXI of 2020 section 141(c). Ineffective from 01.07.2020
[9] Added by Act XXXI of 2020 section 137. Effective from 01.07.2020
[10] Added by Act XXXI of 2020 section 137. Effective from 01.07.2020
[11] Added by Act XXXI of 2020 section 138. Effective from 01.07.2020

Section 16 This Act serves the purpose of compliance with the Council Directive (EU) 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

Section 17[1] 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.

Annex 1 to Act CLXVI of 2012[2]

	A	B
1.	**SECTOR**	**SUB-SECTOR**
2.	Energy	infrastructures of the electric energy system (with the exception of the infrastructures covered by the regulations for nuclear safety and radiation protection, physical protection and safeguards supervision of nuclear plants)
3.		petroleum industry
4.		natural gas industry
5.		district heating
6.	Transport	road transport
7.		rail transport
8.		aviation
9.		waterborne transport
10.		logistics centres
11.	Agriculture	farming
12.		food industry
13.		distribution networks
14.	Healthcare	active inpatient care, and services required for their operation
15.		rescue services management
16.		health reserves and blood stocks
17.		high level safety biological laboratories
18.		pharmaceutical wholesale
19.	Social security	IT systems and records related to the use of social security benefits
20.	Finance	trading, payment, clearing and settlement infrastructures and systems for financial instruments
21.		bank and credit institution security
22.		cash supply

[1] Added by Act CXXXIV of 2017 section 44. Effective from 10.05.2018
[2] Declared by Act XXXI of 2020 section 139, Annex 3. Effective from 01.07.2020

23.	Information and communication technologies	internet access service and internet infrastructures
24.		electronic communications services, electronic communication networks
25.		broadcasting
26.		postal services
27.		government electronic information systems
28.	Water	drinking-water services
29.		quality control for surface- and groundwater
30.		wastewater disposal and treatment
31.		protection of water bases
32.		flood control facilities, dams
33.	National defence	national defence systems and facilities
34.	Public security	infrastructures of law enforcement agencies

Annexes 2-4 to Act CLXVI of 2012[1]

[1] Repealed by Act XXXI of 2020 section 141(d). Ineffective from 01.07.2020