Government Decree 249/2017 (IX.5.)

on the identification, designation and protection of critical systems and facilities of the information and communication technologies sector

The Government, acting on the basis of authorisation by section 14 a), d) and g) of Act CLXVI of 2012 on the identification, designation and protection of critical systems and facilities, acting within its functions provided for in Article 15(1) of the Fundamental Law, decrees the follows:

1. Interpretative provisions

Section 1 (1) For the purpose of this decree

a)[1] *information and communication technologies (ICT) sector*: the sector defined in rows 23-27 of the table in Annex 1 in Act CLXVI of 2012 on the identification, designation and protection of critical systems and facilities (hereinafter CIP Act) which table is subdivided into the sub-sectors set out therein,

b) *internet infrastructure*: the set of physical and technical facilities that provide internet services, including public data exchange centres, as well as infrastructures providing internet access,

c) *postal service*: the service pursuant to section 3(1)-(3) of Act CLIX of 2012 on postal services,

d)[2] *authoritative DNS service*: a service providing for the direct queries of the domain name data managed by top-level domain name registrars as part of the top-level domain name registry service,

e)[3] *recursive DNS service*: a DNS service that forwards users' domain name queries to the appropriate authoritative DNS providers in the hierarchically structured domain name system and forwards the responses to the query provided by the authoritative DNS provider to the user; an additional part may be DNS caching, which is the temporary storage of responses to domain name queries provided by authoritative DNS providers and the service provided to user queries based on stored domain name data.

[1] Modified by Government Decree 375/2020 (VII.30.) section 100a).

[2] Added by Government Decree 375/2020 (VII.30.) section 93. Effective from 31.07.2020

[3] Added by Government Decree 375/2020 (VII.30.) section 93. Effective from 31.07.2020

2. Scope of the decree

Section 2 (1)[1] The scope of this decree does not cover the closed information system belonging to the ICT sector, as defined in Act L of 2013 on the information security of state and municipal bodies (hereinafter Hungarian Cyber Security Act) and the electronic information system for defence purposes as defined in the 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.

(2) The scope of this decree does not cover the critical infrastructures in the ICT sector, operated for experimental, research and educational purposes within an experimental, research, educational institution.

3. Acting authorities

Section 3 (1)[2] As regards the designation and the revocation of the designation of the national critical infrastructures that belong to the sub-sector set out in rows 23-25 of Annex 1 of the Hungarian CIP Act, the Office of the National Media and Communications Authority (hereinafter Office of the NMHH) shall act as the sectoral designating authority.

(2) In the procedure under paragraph (1) above, the designating authority shall decide on the designation on the basis of

a)[3] the sectoral criteria set out in sections 9-10/A and

b) the horizontal criteria set out in Government Decree 65/2013 (III.8.) on the implementation of Act CLXVI of 2012 on the identification, designation and protection of critical systems and facilities (hereinafter Implementation decree of the Hungarian CIP Act).

Section 4 (1) The Office of the NMHH shall be assisted pursuant to section 3(1) by a decision-preparatory committee, with the performance of its tasks.

(2) The organisational and operational rules of the NMHH shall define

a) the number of members,

b) the organisation,

c) the operating rules,

d) the qualifications and professional requirements of its members

of the decision-preparatory committee.

Section 5 (1)[4] As regards the designation and the revocation of the designation of the national critical infrastructures and the European critical infrastructure that belong to the sub-sector set out in row 26 of Annex 1 of the Hungarian CIP Act, the minister responsible for postal matters shall act as the advisory authority.

(2)[5] As regards the designation and the revocation of the designation of the national critical infrastructures that belong to the sub-sector set out in row 26 of Annex 1 of the Hungarian CIP Act, and the European critical infrastructures that belong to the sub-sector set

---

[1] Declared by Government Decree 394/2017 (XII.13.) section 11(1). Effective from 10.05.2018

[2] Modified by Government Decree 375/2020 (VII.30.) section 100b)

[3] Modified by Government Decree 375/2020 (VII.30.) section 100c)

[4] Modified by Government Decree 375/2020 (VII.30.) section 100d)

[5] Modified by Government Decree 375/2020 (VII.30.) section 100e)

out in row 26 of Annex 1 of the Hungarian CIP Act, the Office of the NMHH shall act as the sectoral designating authority.

Section 6 (1)[1] As regards the designation and the revocation of the designation of the national critical infrastructures and the European critical infrastructures that belong to the sub-sector set out in row 27 of Annex 1 of the Hungarian CIP Act, the Office of the NMHH shall act as the sectoral designating authority.

(2) In the procedure under paragraph (1) above, the designating authority shall decide on the designation on the basis of

a)[2] the sectoral criteria set out in sections 10/A, 12 and 14(2) and

b) the horizontal criteria set out in the implementation decree of the Hungarian CIP Act.

Section 7[3]

Section 8[4] The on-site monitoring related to the ICT sector shall be performed by the Office of the NMHH as regards national critical infrastructures and European critical infrastructures designated pursuant to sections 3(1), 5(2) and 6(1).

3/A.[5] Specific rules on the identification testing of critical infrastructures

Section 8/A[6] In the course of the identification test of the critical infrastructures that belong to the sub-sector pursuant to rows 23-25 of the table of Annex 1 of the Hungarian CIP Act, Section 2(1) of the implementation decree of the Hungarian CIP Act shall be applied with the addition that those electronic communications service providers are obliged to prepare an identification report net sales of which reached HUF 1 billion in the previous business year.

Section 8/B[7] In the course of the identification test of the critical infrastructures that belong to the sub-sector pursuant to rows 23-25 of the table of Annex 1 of the Hungarian CIP Act, Section 2(1) of the implementation decree of the Hungarian CIP Act shall be applied with the addition that the identification report shall include

a) a description of the operator 's complete network infrastructure; and

b) in relation to certain sub-sectors of the ICT sector as set out in the table of Annex 1 of the Hungarian CIP Act, which other electronic communications service providers use the operator's potential critical infrastructures examined.

4. Sectoral criteria for national critical infrastructures that belong to the ICT sector

Section 9[8] Irrespective of the technology used, an infrastructure that belongs to the sub-sector set out in rows 23 and 24 of the table of Annex 1 of the Hungarian CIP Act may be designated as a national critical infrastructure, if by its use

a) the electronic communications service provider, in the territory of Hungary, on the basis of a contract or legal provision to that effect

---

[1] Declared by Government Decree 375/2020 (VII.30.) section 94. Effective from 31.07.2020

[2] Modified by Government Decree 375/2020 (VII.30.) section 100f)

[3] Repealed by Government Decree 375/2020 (VII.30.) section 101a). Ineffective from 31.07.2020

[4] Declared by Government Decree 375/2020 (VII.30.) section 95. Effective from 31.07.2020

[5] Added by Government Decree 375/2020 (VII.30.) section 96. Effective from 31.07.2020

[6] Added by Government Decree 375/2020 (VII.30.) section 96. Effective from 31.07.2020

[7] Added by Government Decree 375/2020 (VII.30.) section 96. Effective from 31.07.2020

[8] Declared by Government Decree 375/2020 (VII.30.) section 97. Effective from 31.07.2020

aa) provides internet access services or provides the internet infrastructure necessary for the provision of the service, or

ab) provides electronic communications services or provides the electronic communications networks necessary for the provision of the service, the operation of which may directly or indirectly affect a total of more than twenty thousand subscribers, or

b) the universal electronic communications service provider provides universal electronic communications services pursuant to Act C of 2003 on Electronic Communications (hereinafter EC Act).

Section 10[1] An infrastructure that belongs to the sub-sector set out in row 25 of the table of Annex 1 of the Hungarian CIP Act may be designated as a national critical infrastructure, if the broadcasting service provided through its use is available to at least 70% of the population of Hungary.

Section 10/A[2] An infrastructure that belongs to the sub-sector set out in rows 23-25 and 27 of the table of Annex 1 of the Hungarian CIP Act may be designated as a national critical infrastructure, if it is used by an operator belonging to one of the sectors defined in Annex 1 of the Hungarian CIP Act for the purpose of operating its critical infrastructure.

Section 11[3] As regards the sub-sector set out in row 26 of the table of Annex 1 of the Hungarian CIP Act, the following may be designated as a national critical infrastructure in relation to the universal postal service provider

a) its infrastructure designated in its plan of defence measures and emergency response which is required during the special legal order only for the operation of postal services provided to demanding-responsive bodies, as defined in the laws or

b) its infrastructure defined in its business continuity plan, in the event of the outage of which the average daily central delivery processing capacity required to operate the postal services falls below 40% and cannot be replaced by an infrastructure capable of performing the same activity for more than 48 hours.

Section 12[4] The infrastructure that belongs to the sub-sector set out in row 27 of the table of Annex 1 of the Hungarian CIP Act may be designated as a national critical infrastructure, which serves the purpose of ensuring the operation of a network for governmental purposes or the ICT system or systems, and which

a) supports the administrative procedures of at least 10,000 natural persons, or

b) supports the forecasting, signalling of an emergency threatening also human life, or the averting of a disaster threatening human life.

Section 13 If as regards the infrastructures set out in sections 9-12 above, the necessity arises to designate them as non-sectoral critical infrastructures for national defence, pursuant to section 4(1)a)-b) of Government Decree 359/2015 (XII.2.) on the identification, designation and protection of critical instruments for national defence, the advisory authority of the national defence sector or the operator of the infrastructure shall initiate - prior to the identification procedure - consultations with the sectoral designating authority specified in sections 3(1), 5(2) and 6(1).

---

[1] Declared by Government Decree 375/2020 (VII.30.) section 97. Effective from 31.07.2020

[2] Added by Government Decree 375/2020 (VII.30.) section 98. Effective from 31.07.2020

[3] Modified by Government Decree 375/2020 (VII.30.) section 100d)

[4] Modified by Government Decree 375/2020 (VII.30.) sections 100g), 101b)

4/A.[1] Extent of significant disruptive effect in the digital infrastructure sector

Section 13/A[2] (1) In the case of fixed internet access service, a nomadic internet access service and a mobile internet access service set out in rows 28-30 of the table of Annex 3 of the implementation decree of the Hungarian CIP Act, a security incident affecting the service provided by the operator causes significant disruptive effect in the provision of the service, if the infrastructure operated by the operator for the purpose of providing the service

a) may directly or indirectly affect a total of more than twenty thousand subscribers by its operation,

b) is used by the universal electronic communications service provider to provide universal electronic communications service in accordance with the EC Act, or

c) is used to operate a national critical infrastructure of an operator belonging to one of the sectors specified in Annex 1 of the Hungarian CIP Act.

(2) In the case of a data exchange (IXP) service set out in row 31 of the table in Annex 3 of the implementation decree of the Hungarian CIP Act, a security incident affecting the service provided by the organisation or economic entity causes a significant disruptive effect in the provision of the service if

a) the capacity of the data exchange centre falls below 50% of the total available capacity for a period exceeding 1 hour, or

b) an incident involving a data exchange centre means a breach of data integrity, authenticity or confidentiality of more than 100,000 of the customers of the related organisations.

(3) In the case of a DNS service according to row 32 of the table in Annex 3 of the implementation decree of the Hungarian CIP Act, a security incident affecting the service provided by the organisation or economic entity causes a significant disruptive effect in the provision of the service if the recursive DNS service fails for more than 2 hours or the databases on DNS servers are compromised, affecting at least 100,000 users.

(4) In the case of the top-level domain name registration service according to row 33 of the table of Annex 3 of the implementation decree of the Hungarian CIP Act, a security incident affecting the service provided by the organisation or economic entity causes a significant disruptive effect in the provision of the service if

a) the TLD registrar's authorized DNS service becomes unavailable in the case of more than 50,000 domain names for more than 2 hours, or

b) changes to DNS records managed by the TLD registrar cannot be made by domain name holders for a period of more than 24 hours.

4/B.[3] Thresholds in the digital infrastructure sector

Section 13/B[4] (1) In the case of fixed internet access service, nomadic internet access service and mobile internet access service set out in rows 28-30 of the table of Annex 3 of the

[1] Added by Government Decree 375/2020 (VII.30.) section 99. Effective from 31.07.2020
[2] Added by Government Decree 375/2020 (VII.30.) section 99. Effective from 31.07.2020
[3] Added by Government Decree 375/2020 (VII.30.) section 99. Effective from 31.07.2020
[4] Added by Government Decree 375/2020 (VII.30.) section 99. Effective from 31.07.2020

implementation decree of the Hungarian CIP Act, the relevant thresholds for determining the level of service are set pursuant to section 13/A(1)a)-c).

(2) In the case of the data exchange (IXP) service according to row 31 of the table of Annex 3 of the implementation decree of the Hungarian CIP Act, the following may be designated as an operator of essential services:

a) the Budapest Data Exchange Center,

b) any data exchange centre providing connection to at least 25 technically independent networks (autonomous system).

(3) In the case of the DNS service according to row 32 of the table of Annex 3 of the implementation decree of the Hungarian CIP Act, the following may be designated as an operator of essential services:

a) any electronic communications service provider designated as an operator of essential services that also provides DNS services to its customers;

b) any DNS provider that provides recursive DNS queries to at least 100,000 different users.

(4) In the case of the top-level domain name registration service according to row 33 of the table of Annex 3 of the implementation decree of the Hungarian CIP Act, the following may be designated as an operator of essential services:

a) any electronic communications service provider designated as an operator of essential services that also provides TLD registration services to its customers,

b) any TLD registrar service provider that manages at least 100,000 registered TLD domain names.

4/C.[1] Extraordinary occurrences

Section 13/C[2] (1) The following are considered as extraordinary occurrences in the ICT sector

a) the outage of the utilities used, affecting the facility, the provision of the services, foreseeably for more than 4 hours,

b) any event which leads to the cessation of the necessary conditions or the transformation of the core activity,

c) malfunction, disturbance of a facility, device or equipment, that has at least one of the following effects:

ca) malfunction of the fixed internet access service affecting 30% of subscribers, foreseeably for a period of more than 4 hours,

cb) malfunction of the mobile radiotelephone- or mobile internet access service, affecting at least 30% of the area served, foreseeably for a period of more than 4 hours,

cc) significant deterioration in the quality of mobile radiotelephone service, in particular a decrease in the proportion of successful calls for a period of more than 2 hours, to an extent of more than 35% compared to the average of the year preceding the event,

cd) malfunction of electronic communication networks that leads to service outage in the electronic communication networks fulfilling the demands of governmental, law

[1] Added by Government Decree 375/2020 (VII.30.) section 99. Effective from: 31.07.2020

[2] Added by Government Decree 375/2020 (VII.30.) section 99. Effective from: 31.07.2020

enforcement, national defence, disaster control needs, and in the infrastructures under the act on the identification, designation and protection of critical systems and facilities, or affects an international interconnection or emergency service,

ce) an event making the provision of cable television, digital terrestrial or satellite broadcasting services impossible or significantly jeopardizing it, and the resulting situation which renders the media service of a national public service media provider or a media player with significant influence unavailable for a period of more than 2 hours,

cf) disturbance which interferes with the normal operation of the postal service for more than 5 hours,

cg) any event occurring during a special legal order, risk of disaster, national defence emergency or health crisis which leads to the cessation or transformation of the provision of electronic communication-, postal- and broadcasting services,

d) if the competent authority imposes a health quarantine on the designated critical infrastructure,

e) critical shortage of human resources to such an extent that may lead to the cessation or suspension of the activity.

(2) The data reporting obligation set out in section 6(11) of the Hungarian CIP Act, on the extraordinary occurrence pursuant to paragraph (1) above, shall be performed to the Office of the NMHH via the NMHH Data Gate, by e-mail in case of the inoperability of the NMHH Data Gate, by telephone or telefax in case of the inoperability of the electronic mail system or in the absence of the necessary network access for performing the above by courier.

5. Sectoral criteria for European critical infrastructures in the ICT sector

Section 14 (1)[1] Pursuant to row 26 of the table of Annex 1 of the Hungarian CIP Act, infrastructures operated for the purpose of international postal services provided by the universal postal service provider may be designated as a European critical infrastructure, if in the event of its failure the provision of international postal services becomes impossible for a period exceeding 48 hours, and it may not be replaced during this period by an instrument performing the same activity.

(2)[2] Pursuant to row 27 of the table in Annex 1 of the Hungarian CIP Act, such infrastructure may be designated as a European critical infrastructure which is part of an international network or system or which provides direct access to international networks or systems, the failure of the service it provides may not be replaced by another infrastructure, and which ensures or supports

a) the fulfilment of an obligation to cooperate at government level with an EEA State or States, or

b) in the framework of an international commitment, the management of disaster relief and counter-terrorism tasks

[1] Modified by Government Decree 375/2020 (VII.30.) section 100d).

[2] Modified by Government Decree 375/2020 (VII.30.) section 100g)

6. Qualification requirements and conditions of employment of the security liaison officer employed by the operator of a facility in the ICT sector

Section 15 (1) In the case of the ICT sector, the following shall be deemed as the specialised qualification defined in section 6(1) of the implementation decree of the Hungarian CIP Act with regard to the security liaison officer

a) a higher education degree recognized as such by the operator,

b) at least five years employment in the ICT sector and a qualification in defence administration or equivalent, or

c) the qualification relevant to the information security officer under the Hungarian Cyber Security Act.

(2) In the case of universal postal services, the legal qualification shall also be deemed as the specialised qualification defined in section 6(1) of the implementation decree of the Hungarian CIP Act – in addition to those defined in paragraph (1) – with regard to the security liaison officer.

7. Final provisions

Section 16 This decree shall enter into force on the 180th day following its promulgation.

Section 17[1] This decree serves the purpose of compliance with the Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[1] Added by Government Decree 394/2017 (XII.13.) section 11(2). Effective from 10.05.2018