Government Decree 270/2018. (XII.20.)

on the supervision of the electronic information security of information society services and the rules of procedure for security incidents

The Government,

acting on the basis of authorization pursuant to Section 17 (1a) *a)*, *c)* to *f)* of Act CVIII of 2001 on certain aspects of electronic commerce services and information society services,

acting within its function laid down in Article 15 (1) of the Fundamental Law,

orders as follows:

1. Scope

Section 1 (1) This Decree shall apply to

a) the service providers providing notifiable services (hereinafter referred to as 'digital service provider') determined in the Act CVIII of 2001 on certain aspects of electronic commerce services and information society services (hereinafter referred to as 'Hungarian Electronic Commerce Act') which are not micro and small enterprises according to the Act on small and medium-sized enterprises and aid for their development, as well as

b) the intermediary service providers under the Hungarian Electronic Commerce Act.

(2) This Decree may not be applied to the digital service providers designated as European or national critical infrastructures.

2. Powers and duties of the Authority

Section 2 (1) The Government designates the Special Service for National Security as the authority pursuant to Section 6/B (3) of the Hungarian Electronic Commerce Act (hereinafter referred to as 'Authority').

(2) To prevent, investigate, eradicate and limit the spread of security incidents (hereinafter referred to as 'security incident') under the Act L of 2013 on the electronic information security of state and municipal bodies (hereinafter referred to as 'Hungarian Cyber Security Act'), the Authority shall

a) keep records based on registration;

b) maintain contacts

ba) with digital service providers and intermediary service providers,

bb) with law enforcement agencies,

bc) with the competent sectoral authorities of other Member States of the European Union,

bd) with the Hungarian National Authority for Data Protection and Freedom of Information,

be) with the appointed representatives of the digital service providers not established in the European Union, but offering their services within Hungary;

c) monitor the domestic application of 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;

d) if necessary, oblige service providers to

da) provide the data necessary to determine the security of their electronic information systems, including the data regarding their security policies, as well,

db) ensure an adequate level of security, to prevent, report and respond to security incidents and rectify the deficiencies observed;

e) inform the public of each security incident, if necessary;

f) oblige digital service providers to inform the public, if necessary;

g) carry out official authority controls regarding the performance of duties of digital service providers;

h) take measures against intermediary service providers upon the request of the incident response centre (hereinafter referred to as 'incident response centre') under Section 19 (1) of the Hungarian Cyber Security Act, designated in the Government Decree on the functions and powers of incident response centres, and the rules for security incident response and technical investigation, and for conducting vulnerability testing.

(3) If the place of the central administration or the representative of a digital service provider is in one of the Member States, while its electronic information systems are located in one or more other Member States, the Authority shall cooperate with the competent authority of the Member State in which the central administration or the place of representation is situated.

Section 3 (1) The Authority shall process

a) the company name of the digital service provider,

b) the its registered seat,

c) its company registration number,

d) its electronic contact details and

e) the type of the notifiable services provided thereby

in the record under Section 2 (2) *a)*.

(2) The data of a digital service provider shall be deleted from the authority record on the basis of the company notification submitted to the Authority about the termination of its activities or on the basis of the notification submitted to the Authority about the designation of the company as European or national critical infrastructure, within eight days after the notification. The company shall submit the notification to the Authority within eight days after finalization of the decision designating it to be a European or national critical infrastructure.

(3) In the proceedings of the Authority, submission of the application to the government window is excluded, and there is opportunity for call for remedy of deficiencies two times in the proceeding.

(4) The Authority shall commence an official authority procedure, if data are provided that any digital service provider does not perform the information security requirements set out in law. Such data may be provided by the competent authority of the other Member State in which Member State the given service is provided.

(5) In the context of an official procedure and as a further measure, the Authority

a) shall inform the incident response centre and other bodies concerned, if necessary,

b) shall inform the designating authority if an operator of essential service is affected,

c) shall take other preventive measures,

d) shall initiate proceedings falling within the competence of another authority.

(6) In order to carry out its tasks, the Authority is entitled to - with the least possible disturbance to the operation and management of the digital service provider concerned with the measure -

a) enter the premises related to the information technology activities of the digital service provider concerned,

b) carry out inspections at the sites concerned that provide data processing to the digital service provider concerned, perform technical manipulation of data or are affected by information technology, and during that is entitled to access and check any instrument, document, contract, active or passive device, information system, security measure related to electronic information security as well as to make copies of electronic or paper-based instruments, documents, contracts, databases related to electronic information security, and

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

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

(7) The Authority shall have the right to carry out on-site investigation or check by requesting the necessary documents regarding the performance of security elements pursuant to the Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact [hereinafter referred to as 'Commission Implementing Regulation (EU) 2018/151'] by digital service providers.

(8) The head of the digital service provider concerned shall be notified in writing about the ordering of an on-site investigation in advance, ten days before the start of the on-site investigation.

(9) The prior notice of the investigation may be omitted, if

a) a serious security incident has occurred under the Hungarian Cyber Security Act,

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

c) on the basis of the available data the digital service provider concerned would presumably frustrate the effective conduct of the on-site investigation.

(10) The digital service provider concerned with the on-site investigation and other contributor concerned shall cooperate with the Authority.

(11) The Authority is entitled to take the result of an inspection carried out by an independent qualified inspector into consideration during its procedure, and shall accept the use of certificates and accreditations in accordance with European or internationally accepted standards and regulations relevant to the security of electronic information systems, during its procedure.

3. Essential requirements for the security of the electronic and information systems of digital service providers

Section 4 Digital service providers shall ensure the availability of the proper documents which enable the competent authority to investigate the adequacy of the security elements used for the security of service providers' systems and facilities.

Section 5 (1) Digital service providers shall register electronically in the form published on the website of the Authority by providing data specified in Section 3 (1).

(2) The digital service provider which falls within the scope of this Decree only after this Decree's entry into force shall submit the data specified in Section 3 (1) in the form determined in paragraph (1) within 90 days after the change.

(3) The digital service provider shall notify the Authority about the changes in the data specified in Section 3 (1) and about its termination within 8 days.

4. Rules related to significant security incidents and their notification

Section 6 (1) The digital service provider shall immediately report to the incident response centre the security incident occurred in its electronic information systems, which security incident has a significant impact on the provision of the notifiable service it offers within the European Union.

(2) When determining the significance of the impact of security incidents, the parameters set out in the Commission Implementing Regulation (EU) 2018/151 shall be taken into consideration.

(3) For the purpose of determining the significance of the impact of security incidents, the digital service providers' notification shall contain the following data as well:

a) the number of users affected by the security incident, in particular users relying on the service concerned for the provision of their own services,

b) the duration of the security incident,

c) the geographic spread with regard to the area affected by the security incident,

d) the extent of the disruption on the functioning of the service,

e) the extent of the impact on economic and societal activities.

(4) The obligation to notify a security incident shall only apply, where the digital service provider has access to the information needed to assess the impact of a security incident on the basis of the parameters referred to in the paragraph (2).

(5) Following the technical assessment of a security incident, the incident response centre shall provide the available information with a summary report to the competent authority for the purpose of initiating and conducting authority proceedings.

(6) Based on the summary report of the incident response centre in the course of a procedure ex officio, the Authority

a) shall investigate the preventive and incident response activities of the digital service provider;

b) shall examine the compliance with requirements set out in Sections 4 and 5;

c) shall asses the adequacy of the security measures of the digital service provider;

d) is entitled to carry out the acts set out in Section 3 during the investigation;

e) as a result of the investigation, shall adopt an official decision, the content of which shall be at least the following:

ea) establishing the occurrence of a security incident,
eb) proposed remedial action,
ec) measures proposed to prevent further damage;
f) may inform the public or require the digital service provider to do so after prior consultation with the incident response centre, if it is necessary to prevent a security incident or to respond to an ongoing security incident, or where disclosure of a security incident is otherwise in the interest of the public.

5. Application of legal consequences

Section 7 (1) The Authority shall call the head of the digital service provider concerned - setting a deadline - to
a) eliminate deficiencies, omissions or breaches of security requirements that endanger electronic information security,
b) fulfil obligations specified in law,
c) take the measure expected.
(2) The Authority shall oblige the digital service provider concerned to take immediate measures, if deficiencies, omissions or breaches of security requirements that endanger electronic information security threaten with the occurrence of a serious security incident. In this context, it may propose disciplinary liability to the employer.
(3) Based on Section 6/C of the Hungarian Electronic Commerce Act, the Authority may impose fines to the extent set out in Annex 1 in case of any breach of law set out in Annex 1.
Section 8 If the intermediary service provider does not fulfil its obligation to cooperate under the Government Decree on the functions and powers of incident response centres, and the rules for security incident response and technical investigation, and for conducting vulnerability testing, upon notification to the incident response centre, the Authority shall call on, setting a deadline, the body concerned to engage in law-abiding conduct and may impose a fine after the failure to meet the time limit.
Section 9 (1) The fine that can be imposed may range from fifty thousand forints to five million forints, which shall be paid within 8 days after the authority decision becomes final (hereinafter referred to as 'payment') to the account of the Authority which is specified in the decision and is held by the Hungarian State Treasury.
(2) When making the payment the text 'digital fine', the decision number and the name of the person liable for payment of the fine shall be indicated in the transfer notification box.
(3) In the case of the coexistence of more irregularities, the amount of the fine is the sum of the fines that may be imposed for each infringement, not exceeding the upper limit of five million forints.
Section 10 (1) The payment of the fine does not release from criminal and civil liability as well as from the obligation to cease the irregularities giving rise to the imposition of the fine.
(2) The fine may be imposed repeatedly under the same facts - with the exception of irregularities which can be rectified immediately - after two months following the disclosure of the final decision imposing the fine.

6. Final provisions

Section 11 (1) This Decree shall enter into force on 1 January 2019 with exception set out in paragraph (2).

(2) Sections 2 (2) *h)*, 7 (3), 8 to 10 and Annex 1 shall enter into force on the 16th day after promulgation of this Decree.

Section 12 (1) The provisions of this Decree shall be applied also to the cases being in progress at the date of the entry into force of this Decree.

(2) The Interior Ministry's National Directorate General for Disaster Control shall transfer the data and ongoing proceedings related to Government Decree 410/2017. (XII. 15.) on digital service providers to the Special Service for National Security until 15 January 2019.

Section 13 (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.

(2) This Decree lays down the provisions necessary for the implementation of the Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact.

Section 14[1]

Annex 1 to the Government Decree 270/2018. (XII.20.)

The amount of the fine that may be imposed for each breach of law

	A	B	C
1.	Name of the breach of law	Minimum amount of the fine (HUF)	Maximum amount of the 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 competent authority	400 000	5 000 000

[1] Repealed by Section 12 of the Act 2010 of CXXX. Ineffective from 02.01.2019