COLLECTION OF LAWS OF
THE SLOVAK REPUBLIC

2018

Declared: June 14, 2018 Time version of the regulation effective from: June 15, 2018

Content is legally binding.

165

DECREE

of the National Security Authority

of June 1, 2018,

determining the identification criteria for each category of serious cybersecurity incidents and the details of cybersecurity incidents reporting

The National Security Authority (hereinafter referred to as "the Authority") pursuant to Section 32 Par. 1 item e) of the Act No. 69/2018 on Cybersecurity and on the Amendment to Certain Acts (hereinafter referred to as "the Act") provides:

Article 1

(1) Identification criteria for the category of serious cybersecurity incident of the first Level (I), the second Level (II) and the third Level (III), depending on the parameters mentioned in Section 24 Par. 2 item a) to e) of the Act are listed in Annex 1.

(2) A cybersecurity incident is identified as a serious cybersecurity incident if it meets at least one identification criterion for a serious cybersecurity incident category.

Article 2

(1) The reporting of cybersecurity incidents according to Section 24 Par. 4 of the Act contains, to the extent necessary for proper identification, in particular information

a) about who reports a serious cybersecurity incident, and that
   1. identifying details and
   2. contact details,
b) about a serious cybersecurity incident, and that
   1. cybersecurity incident time data,
   2. a detailed description of the duration of cybersecurity incident; and
   3. the extent of the damage caused by a cybersecurity incident,
c) about a service hit by a serious cybersecurity incident, and that
   1. a specific description of all the assets affected; and
   2. the impact of a cybersecurity incident on a service provided,
d) about a serious cybersecurity incident handling, and that
   1. state of the cybersecurity incident handling,

2. remedial measures taken, and
3. a description of the consequences of a cybersecurity incident.

(2) An example of cybersecurity incident reporting is published by the Authority through the Cybersecurity Single Information System and at its website.

Article 3

This Decree adopts the legally binding acts of the European Union stated in Annex 2.

Article 4

This Decree enters into force on June 15, 2018.

Jozef Magala

Annex 1 to the Decree No. 165/2018

The impact of a cybersecurity incident, depending on:		Serious cybersecurity incident		
		Category I.	**Category II.**	**Category III.**
Section 24 Par. 2 item a) of the Act	Number of essential service users hit by a cyber security incident.	The incident has led to conduct that threatens the availability, authenticity, integrity or confidentiality of the data stored, transferred or processed or related services of the operator of essential service provided or accessible through these networks and information systems affecting more than 25,000 people.	The incident has led to conduct that threatens the availability, authenticity, integrity or confidentiality of the data stored, transferred or processed or related services of the operator of essential service provided or accessible through these networks and information systems affecting more than 50,000 people.	The incident has led to conduct that threatens the availability, authenticity, integrity or confidentiality of the data stored, transferred or processed or related services of the operator of essential service provided or accessible through these networks and information systems affecting more than 100,000 people.
Section 24 Par. 2 item b) of the Act **and** **Section 24 Par. 2 item c) of the Act**	Duration of cyber security incident (time data of cyber security incident) and geographic spread of cyber security incident.	Limitation or disruption of the operation of essential service or critical infrastructure element in more than 15,000 user hours, with the term user hour referring to the number of affected users in the territory of at least one district within 60 minutes.	Limitation or disruption of the operation of essential service or critical infrastructure element in more than 100,000 user hours, with the term user hour referring to the number of affected users in the territory of at least one district within 60 minutes.	Limitation or disruption of the operation of essential service or critical infrastructure element in more than 500,000 user hours, with the term user hour referring to the number of affected users throughout the territory of the Slovak Republic within 60 minutes.
Section 24 Par. 2 item d) of the Act	Degree of disruption of essential service performance.		The incident caused total unavailability of the type of service for which a substitute solution can be provided.	The incident caused total unavailability of the type of service for which it is not possible to provide a substitute solution.

Section 24 Par. 2 item e) of the Act	The extent of a cybersecurity incident impact on the state´s economic or social activities.	Incident caused a) economic loss or material damage to at least one user exceeding EUR 250 000, b) more than 1 000 injured persons requiring medical treatment or loss of one casualty, or c) disruption of public order or public security in a significant part of the district.	Incident caused a) economic loss or material damage to at least one user exceeding EUR 500 000, b) life causalities of more than 100 dead or 3 500 injured persons requiring medical treatment, or c) disruption of public order or public security in a significant part of the district.	Incident caused a) economic loss or material damage to at least one user exceeding EUR 1 000 000, b) life causalities of more than 500 dead or 5 000 injured persons requiring medical treatment, or c) disruption of public order or public security in a significant part of the Slovak Republic.

Note:

1. Given the number of users affected by a cybersecurity incident, in particular users using the service to provide their own services, the operator of essential service evaluates the number of:
a) natural persons and legal entities affected by a cybersecurity incident with whom he has entered into a service contract, or
b) affected users who used the service (based on the operational data).

2. The duration of a cybersecurity incident is the period from disruption of the proper provision of the service in terms of availability, authenticity, integrity or confidentiality up to the provision of that service has been renewed.

3. In the case of a geographic spread of cybersecurity incident (a cybersecurity incident area), the operator of essential service evaluates the impact of a cybersecurity incident on providing its services in certain geographic areas.

4. The degree of limitation or disruption of the operation of essential service or critical infrastructure element is measured by one or more of those characteristics that are disrupted by a cybersecurity incident: accessibility, authenticity, integrity or confidentiality of data or related services.

5. The extent of the impact of a cybersecurity incident on the state´s economic or social activities is value-based assessment (for example, the nature of contractual customer relationships, the potential number of users affected by a cybersecurity incident, causing serious material or non-material damage).

Annex 2 to the Decree No. 165/2018

LIST OF ADOPTED LEGALLY BINDING ACTS OF THE EUROPEAN UNION

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to ensure a high common level of network and information systems in the Union (OJ L 194, 19 July 2016).

Publisher of the Laws of the Slovak Republic, the content administrator and the operator of the legal and information portal Slov-Lex available at website of www.slov-lex.skje
the Slovak Republic´s Ministry of Justice, Župné námestie 13, 813 11 Bratislava, tel.: 02 888 91 137, fax: 02/52442853, e-mail: helpdesk@slov-lex.sk.