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.

164

DECREE
of the National Security Authority
of June 1, 2018,
determining the identification criteria of operated service (essential service criteria)

National Security Authority in accordance with Article 32 Paragraph 1 item b) of the Act No. 69/2018 Coll. On Cybersecurity and on Amendments and Supplements to certain Acts (hereinafter referred to as "the Act") stipulates:

Article 1

This Decree determines essential service identification criteria in accordance with Article 3 item k) first point of the Act.

Article 2

An operated service fulfils identification criteria of essential service, if it meets at least one impact criterion and at least one specific sector criterion, if stated in Annex 1.

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 No. 1

to the Decree No. 164/2018 Coll.

BANKING

Service provider (Annex No. 1 to the Act)	**Specific sector criteria** (individually)	**Impact criteria** (individually) Impact of the cybersecurity incident in the information system or network, on the functioning of which depends service operation, may cause:
Credit institutions whose business is to receive deposits or other repayable funds from the public and to provide loans on their own account	a) Number of clients exceeding 25 000. b) Market share exceeding 1% of the balance sheet total.	1. Threatening availability, authenticity, integrity or confidentiality of the stored, transferred, or processed data or related services provided or available through these networks and information systems, affecting more than 25 000 persons. 2. Limitation or disruption of operation of other essential service or critical infrastructure element. 3. Economic loss exceeding 0,1 % of GDP. 4. Economic loss or material damage to at least one user exceeding 250 000 EUR. 5. Disruption of public order, public security, emergency or distress requiring carrying out of rescue work or execution of activities and measures related with providing help in distress.

TRANSPORT

Road Transport

Service provider (Annex No. 1 to the Act)	**Specific sector criteria** (individually)	**Impact criteria** (individually) Impact of the cybersecurity incident in the information system or network, on the functioning of which depends service operation, may cause:

Transport authority responsible for management of road traffic control – public authority responsible for planning, management or road operation within its territorial jurisdiction.	Control of operations management in the road network.	1. Threatening availability, authenticity, integrity or confidentiality of the stored, transferred, or processed data or related services provided or available through these networks and information systems, affecting more than 25 000 persons. 2. Limitation or disruption of operation of other essential service or critical infrastructure element. 3. Economic loss exceeding 0,1 % of GDP. 4. Economic loss or material damage to at least one user exceeding 250 000 EUR. 5. More than 100 injured persons requiring medical attention or one casualty. 6. Disruption of public order, public security, emergency or distress requiring carrying out of rescue work or execution of activities and measures related with providing help in distress.
Intelligent transport systems operator in which information and communication technology is applied in the field of road traffic, including infrastructure, vehicles and users, and in the field of traffic control and mobility control, as well as operation, interface with other transport types.	Operation of intelligent transport system in the field of road traffic or traffic control and mobility control, as well as operation, interface with other transport types.	1. Threatening availability, authenticity, integrity or confidentiality of the stored, transferred, or processed data or related services provided or available through these networks and information systems, affecting more than 25 000 persons. 2. Limitation or disruption of operation of other essential service or critical infrastructure element. 3. Economic loss exceeding 0,1 % of GDP. 4. Economic loss or material damage to at least one user exceeding 250 000 EUR. 5. More than 100 injured persons requiring medical attention or one casualty. 6. Disruption of public order, public security, emergency or distress requiring carrying out of rescue work or execution of activities and measures related with providing help in distress.

Air Transport

Service provider (Annex No. 1 to the Act)	**Specific sector criteria** (individually)	**Impact criteria** (individually) Impact of the cybersecurity incident in the information system or network, on the functioning of which depends service operation, may cause:

Air transport operator – air transport company with valid operation license or its equivalent.	a) Air transport. b) Offer of air transport.	1. Threatening availability, authenticity, integrity or confidentiality of the stored, transferred, or processed data or related services provided or available through these networks and information systems, affecting more than 25 000 persons. 2. Limitation or disruption of operation of other essential service or critical infrastructure element. 3. Economic loss exceeding 0,1 % of GDP. 4. Economic loss or material damage to at least one user exceeding 250 000 EUR. 5. More than 100 injured persons requiring medical attention or one casualty. 6. Disruption of public order, public security, emergency or distress requiring carrying out of rescue work or execution of activities and measures related with providing help in distress.
Control authority of the airport – entity whose aim is besides other activities or without them to administer and control of airport infrastructure or airport network and coordination and control activity of respective airports or respective airport networks, airport, including the main airport and the entity operating auxiliary devices located at the airport.	Within the framework of international public airports (preferentially meant for commercial air transport).	1. Threatening availability, authenticity, integrity or confidentiality of the stored, transferred, or processed data or related services provided or available through these networks and information systems, affecting more than 25 000 persons. 2. Limitation or disruption of operation of other essential service or critical infrastructure element. 3. Economic loss exceeding 0,1 % of GDP. 4. Economic loss or material damage to at least one user exceeding 250 000 EUR. 5. More than 100 injured persons requiring medical attention or one casualty. 6. Disruption of public order, public security, emergency or distress requiring carrying out of rescue work or execution of activities and measures related with providing help in distress.
Operator providing services of air-traffic control (ATC) as services provided to: a) prevent collision: - among airplanes and - in the operation premises among airplanes and obstacles, and b) speed up and maintain proper flow of airport traffic.	a) Regional control service. b) Approach control airport service, where ATC services are provided or airport is determined as a critical infrastructure element. c) Aerodrome control service at airport, where ATC services are provided or at an airport determined as critical	1. Threatening availability, authenticity, integrity or confidentiality of the stored, transferred, or processed data or related services provided or available through these networks and information systems, affecting more than 25 000 persons. 2. Limitation or disruption of operation of other essential service or critical infrastructure element. 3. Economic loss exceeding 0,1 % of GDP. 4. Economic loss or material damage to at least one user exceeding 250 000 EUR. 5. More than 100 injured persons requiring medical attention or one casualty. 6. Disruption of public order, public security, emergency or distress requiring carrying out of rescue work or execution of activities and measures related with providing help in distress.

	infrastructure element.	

Water Transport

Service provider (Annex No. 1 to the Act)	**Specific sector criteria** (individually)	**Impact criteria** (individually) Impact of the cybersecurity incident in the information system or network, on the functioning of which depends service operation, may cause:
Company operating inland, naval and coastal personal and cargo water transport services.	Operation of water transport services or offer of water transport service operation, which is irreplaceable or would be replaceable only at a huge cost.	1. Threatening availability, authenticity, integrity or confidentiality of the stored, transferred, or processed data or related services provided or available through these networks and information systems, affecting more than 25 000 persons. 2. Limitation or disruption of operation of other essential service or critical infrastructure element. 3. Economic loss exceeding 0,1 % of GDP. 4. Economic loss or material damage to at least one user exceeding 250 000 EUR. 5. More than 100 injured persons requiring medical attention or one casualty. 6. Disruption of public order, public security, emergency or distress requiring carrying out of rescue work or execution of activities and measures related with providing help in distress.
Water transport services operator, the services meant to raise safety and effectiveness of water transport and to protect the environment, capable of interaction with traffic and is able to react to traffic situations occurring in the field of water transport services.	-	1. Threatening availability, authenticity, integrity or confidentiality of the stored, transferred, or processed data or related services provided or available through these networks and information systems, affecting more than 25 000 persons. 2. Limitation or disruption of operation of other essential service or critical infrastructure element. 3. Economic loss exceeding 0,1 % of GDP. 4. Economic loss or material damage to at least one user exceeding 250 000 EUR. 5. More than 100 injured persons requiring medical attention or one casualty. 6. Disruption of public order, public security, emergency or distress requiring carrying out of rescue work or execution of activities and measures related with providing help in distress.

Railway Transport

Service provider (Annex No. 1 to the Act)	**Specific sector criteria** (individually)	**Impact criteria** (individually) Impact of the cybersecurity incident in the information system or network, on the functioning of which depends service operation, may cause:

Infrastructure operator – authority or a company responsible mainly for establishing, administration and maintenance of railway infrastructure, including traffic control, control command and signalling. Various authorities or companies can be authorized with the function of infrastructure manager in the network or its part.	a) Authorization to establish, administer and maintain railway infrastructure, including traffic control, control command and signalling. b) Central controller console. c) Analytical checkpoint. d) Automatic building of train connections. e) Automatic train control. f) European Railway Traffic Management System.	1. Threatening availability, authenticity, integrity or confidentiality of the stored, transferred, or processed data or related services provided or available through these networks and information systems, affecting more than 25 000 persons. 2. Limitation or disruption of operation of other essential service or critical infrastructure element. 3. Economic loss exceeding 0,1 % of GDP. 4. Economic loss or material damage to at least one user exceeding 250 000 EUR. 5. More than 100 injured persons requiring medical attention or one casualty. 6. Disruption of public order, public security, emergency or distress requiring carrying out of rescue work or execution of activities and measures related with providing help in distress. 7. Paralysing personal and cargo mobility resulting in threatening the functionality of crucial entities of the national economy ensuring the primary functions of running the country (employment, provisions etc.).
Railway company – public or private company whose core activity is providing services with the aim to ensure railway transport services of persons and/or cargo if the company ensures traction, including the providers of service devices – public or private entity responsible for administration of one or several service devices or for providing one or several key services to the railway companies.	a) Provision of traction devices placed on the route of Trans-European Transport Network (TEN-T), system of international railway axes (AGC), systems of the most vital routes of international combined transport and the related premises (AGTC) or railway corridor for international cargo transport (RFC). b) Railway transport service provider, whose core activity is transport of goods and passengers on the routes of Trans-European Transport Network (TEN-T) system of international railway axes (AGC), systems of the most vital	1. Threatening availability, authenticity, integrity or confidentiality of the stored, transferred, or processed data or related services provided or available through these networks and information systems, affecting more than 25 000 persons. 2. Limitation or disruption of operation of other essential service or critical infrastructure element. 3. Economic loss exceeding 0,1 % of GDP. 4. Economic loss or material damage to at least one user exceeding 250 000 EUR. 5. More than 100 injured persons requiring medical attention or one casualty. 6. Disruption of public order, public security, emergency or distress requiring carrying out of rescue work or execution of activities and measures related with providing help in distress. 7. Paralysing personal and cargo mobility resulting in threatening the functionality of crucial entities of the national economy ensuring the primary functions of running the country (employment, provisions etc.).

	routes of international combined transport and the related premises (AGTC) or railway corridor for international cargo transport (RFC). c) Company responsible for functioning of at least one service device or for providing at least one supplementary or auxiliary service in accordance with specific legal regulation.[1]).	

Digital Infrastructure

Service provider (Annex No. 1 to the Act)	**Specific sector criteria** (individually)	**Impact criteria** (individually) Impact of the cybersecurity incident in the information system or network, on the functioning of which depends service operation, may cause:
Internet exchange point service provider for switching networks that are technically and organizationally separate.	Organization administers an autonomous system (AS) or operates data lines in the Internet network, where these interconnect the AS with two and more other AS in the overall transmission capacity of network interfaces of at least 2 Gbps. For these purposes an AS is considered only an AS with a public AS number (public ASN), not an AS with a private AS number (private ASN).	1. Threatening availability, authenticity, integrity or confidentiality of the stored, transferred, or processed data or related services provided or available through these networks and information systems, affecting more than 25 000 persons. 2. Limitation or disruption of operation of other essential service or critical infrastructure element. 3. Economic loss or material damage to at least one user exceeding 250 000 EUR. 4. Disruption of public order, public security, emergency or distress requiring carrying out of rescue work or execution of activities and measures related with providing help in distress.
Provider of service of domain names system on the internet.	a) Providing authoritative responses on its DNS servers for at least 1 000 various	1. Threatening availability, authenticity, integrity or confidentiality of the stored, transferred, or processed data or related services provided or available through these networks and information systems, affecting more than 25 000 persons.

[1]) Act No. 513/2009 Coll. on Railways and Amendment and Supplements to certain Acts.

	second level domains. b) Total number of DNS queries that are answered by the DNS servers of the organization is at least 3 000 000 in 24 hours. This indicator is calculated in 7 consequent days and includes also recursive queries, but does not include queries on local domains of the organization (DNS).	2. Limitation or disruption of operation of other essential service or critical infrastructure element. 3. Economic loss or material damage to at least one user exceeding 250 000 EUR. 4. Disruption of public order, public security, emergency or distress requiring carrying out of rescue work or execution of activities and measures related with providing help in distress.
Entity administering or operating registry of top level internet domains.	Administration or operating of registry of top level internet domains.	1. Threatening availability, authenticity, integrity or confidentiality of the stored, transferred, or processed data or related services provided or available through these networks and information systems, affecting more than 25 000 persons. 2. Limitation or disruption of operation of other essential service or critical infrastructure element. 3. Economic loss or material damage to at least one user exceeding 250 000 EUR. 4. Disruption of public order, public security, emergency or distress requiring carrying out of rescue work or execution of activities and measures related with providing help in distress.

ENERGY SECTOR

Electricity Sector

Service provider (Annex No. 1 to the Act)	**Specific sector criteria** (individually)	**Impact criteria** (individually) Impact of the cybersecurity incident in the information system or network, on the functioning of which depends service operation, may cause:

Electricity company – an individual or a legal entity executing at least one of these activities: production, transmission, distribution, delivery or purchase of electricity and that is in connection with these activities responsible for commercial and technical tasks and/or maintenance; however not including end users who carry out purchase of electricity to the consumers, including its further purchase.	-	1. Threatening availability, authenticity, integrity or confidentiality of the stored, transferred, or processed data or related services provided or available through these networks and information systems, affecting more than 25 000 persons. 2. Limitation or disruption of operation of other essential service or critical infrastructure element. 3. Economic loss exceeding 0,1 % of GDP. 4. Economic loss or material damage to at least one user exceeding 250 000 EUR. 5. More than 100 injured persons requiring medical attention or one casualty. 6. Disruption of public order, public security, emergency or distress requiring carrying out of rescue work or execution of activities and measures related with providing help in distress.
Transmission system operator - an individual or a legal entity responsible for operation, ensuring maintenance and if necessary, development of the transmission system in the given region as well as the development of its interconnections with other systems and for ensuring long-term capacity of the system to satisfy adequate demand for electricity transmission.	-	1. Threatening availability, authenticity, integrity or confidentiality of the stored, transferred, or processed data or related services provided or available through these networks and information systems, affecting more than 25 000 persons. 2. Limitation or disruption of operation of other essential service or critical infrastructure element. 3. Economic loss exceeding 0,1 % of GDP. 4. Economic loss or material damage to at least one user exceeding 250 000 EUR. 5. More than 100 injured persons requiring medical attention or one casualty. 6. Disruption of public order, public security, emergency or distress requiring carrying out of rescue work or execution of activities and measures related with providing help in distress.

Distribution system operator - an individual or a legal entity responsible for operation, ensuring maintenance and if necessary, development of the distribution system in a given region as well as the development of its interconnections with other systems and for ensuring long-term capacity of the system to satisfy adequate demand for electricity distribution.	-	1. Threatening availability, authenticity, integrity or confidentiality of the stored, transferred, or processed data or related services provided or available through these networks and information systems, affecting more than 25 000 persons. 2. Limitation or disruption of operation of other essential service or critical infrastructure element. 3. Economic loss exceeding 0,1 % of GDP. 4. Economic loss or material damage to at least one user exceeding 250 000 EUR. 5. More than 100 injured persons requiring medical attention or one casualty. 6. Disruption of public order, public security, emergency or distress requiring carrying out of rescue work or execution of activities and measures related with providing help in distress.

Gas Industry

Service provider (Annex No. 1 to the Act)	**Specific sector criteria** (individually)	**Impact criteria** (individually) Impact of the cybersecurity incident in the information system or network, on the functioning of which depends service operation, may cause:
Gas company – an individual or a legal entity executing at least one of these activities: extraction, transmission, distribution, delivery, purchase of storing of gas including LNG, and that is responsible for commercial tasks, technical and/or maintenance in connection with these activities; however not including end users.	-	1. Threatening availability, authenticity, integrity or confidentiality of the stored, transferred, or processed data or related services provided or available through these networks and information systems, affecting more than 25 000 persons. 2. Limitation or disruption of operation of other essential service or critical infrastructure element. 3. Economic loss exceeding 0,1 % of GDP. 4. Economic loss or material damage to at least one user exceeding 250 000 EUR. 5. More than 100 injured persons requiring medical attention or one casualty. 6. Disruption of public order, public security, emergency or distress requiring carrying out of rescue work or execution of activities and measures related with providing help in distress.

Operator of gas refinery and natural gas processing plant.	-	1. Threatening availability, authenticity, integrity or confidentiality of the stored, transferred, or processed data or related services provided or available through these networks and information systems, affecting more than 25 000 persons. 2. Limitation or disruption of operation of other essential service or critical infrastructure element. 3. Economic loss exceeding 0,1 % of GDP. 4. Economic loss or material damage to at least one user exceeding 250 000 EUR. 5. More than 100 injured persons requiring medical attention or one casualty. 6. Disruption of public order, public security, emergency or distress requiring carrying out of rescue work or execution of activities and measures related with providing help in distress.
Supplier company – an individual or a legal entity that carries out sale including further sale of natural gas including LNG to the consumers.	-	1. Threatening availability, authenticity, integrity or confidentiality of the stored, transferred, or processed data or related services provided or available through these networks and information systems, affecting more than 25 000 persons. 2. Limitation or disruption of operation of other essential service or critical infrastructure element. 3. Economic loss exceeding 0,1 % of GDP. 4. Economic loss or material damage to at least one user exceeding 250 000 EUR. 5. More than 100 injured persons requiring medical attention or one casualty. 6. Disruption of public order, public security, emergency or distress requiring carrying out of rescue work or execution of activities and measures related with providing help in distress.
Operator of transmission system – an individual or a legal entity carrying out transmission and being responsible for operation, ensuring maintenance and if necessary, development of transmission system in a given region or its interconnection with other systems and as well as for ensuring long-time capacity of the system to satisfy the adequate demand for transmission of natural gas.	-	1. Threatening availability, authenticity, integrity or confidentiality of the stored, transferred, or processed data or related services provided or available through these networks and information systems, affecting more than 25 000 persons. 2. Limitation or disruption of operation of other essential service or critical infrastructure element. 3. Economic loss exceeding 0,1 % of GDP. 4. Economic loss or material damage to at least one user exceeding 250 000 EUR. 5. More than 100 injured persons requiring medical attention or one casualty. 6. Disruption of public order, public security, emergency or distress requiring carrying out of rescue work or execution of activities and measures related with providing help in distress.

Operator of distribution system – an individual or a legal entity carrying out distribution and being responsible for operation, ensuring maintenance and if necessary, development of distribution system in a given region or its interconnection with other systems and as well as for ensuring long-time capacity of the system to satisfy the adequate demand for distribution of natural gas.	-	1. Threatening availability, authenticity, integrity or confidentiality of the stored, transferred, or processed data or related services provided or available through these networks and information systems, affecting more than 25 000 persons. 2. Limitation or disruption of operation of other essential service or critical infrastructure element. 3. Economic loss exceeding 0,1 % of GDP. 4. Economic loss or material damage to at least one user exceeding 250 000 EUR. 5. More than 100 injured persons requiring medical attention or one casualty. Disruption of public order, public security, emergency or distress requiring carrying out of rescue work or execution of activities and measures related with providing help in distress.
Storage operator – an individual or a legal entity carrying out storing and being responsible for operation of a (natural gas) storage.	-	1. Threatening availability, authenticity, integrity or confidentiality of the stored, transferred, or processed data or related services provided or available through these networks and information systems, affecting more than 25 000 persons. 2. Limitation or disruption of operation of other essential service or critical infrastructure element. 3. Economic loss exceeding 0,1 % of GDP. 4. Economic loss or material damage to at least one user exceeding 250 000 EUR. 5. More than 100 injured persons requiring medical attention or one casualty. 6. Disruption of public order, public security, emergency or distress requiring carrying out of rescue work or execution of activities and measures related with providing help in distress.
LNG facility operator – an individual or a legal entity carrying out liquefaction of natural gas or import, unloading and regasification of LNG, and being responsible for LNG facility operation.	-	1. Threatening availability, authenticity, integrity or confidentiality of the stored, transferred, or processed data or related services provided or available through these networks and information systems, affecting more than 25 000 persons. 2. Limitation or disruption of operation of other essential service or critical infrastructure element. 3. Economic loss exceeding 0,1 % of GDP. 4. Economic loss or material damage to at least one user exceeding 250 000 EUR. 5. More than 100 injured persons requiring medical attention or one casualty. 6. Disruption of public order, public security, emergency or distress requiring carrying out of rescue work or execution of activities and measures related with providing help in distress.

Crude Oil and Petroleum Products

Service provider (Annex No. 1 to the Act)	**Specific sector criteria** (individually)	**Impact criteria** (individually) Impact of the cybersecurity incident in the information system or network, on the functioning of which depends service operation, may cause:

Operator of a facility for extraction, refining and processing of crude oil, its storing and transportation.	a) Facility for extraction, processing, refining or treatment of crude oil with installed yearly generation capacity at least 2 000 000 t. b) Storage or a storage complex with capacity of at least 20 000 m^3. c) LPG storing facility with capacity of at least 20 000 m^3. d) Products with transfer capacity of products exceeding 2 000 000 t yearly. e) Crude oil transfer facilities. f) Technical dispatch used for operation of refinery, storage, crude oil transfer facility or treatment, processing or treatment of crude oil.	1. Threatening availability, authenticity, integrity or confidentiality of the stored, transferred, or processed data or related services provided or available through these networks and information systems, affecting more than 25 000 persons. 2. Limitation or disruption of operation of other essential service or critical infrastructure element. 3. Economic loss exceeding 0,1 % of GDP. 4. Economic loss or material damage to at least one user exceeding 250 000 EUR. 5. More than 100 injured persons requiring medical attention or one casualty. 6. Disruption of public order, public security, emergency or distress requiring carrying out of rescue work or execution of activities and measures related with providing help in distress.
Oil pipeline operator.	a) Intrastate oil pipeline with transfer capacity exceeding 500 000t yearly. b) Terminal facility for transmitting the crude oil. c) Technical dispatch used for oil pipeline operation.	1. Threatening availability, authenticity, integrity or confidentiality of the stored, transferred, or processed data or related services provided or available through these networks and information systems, affecting more than 25 000 persons. 2. Limitation or disruption of operation of other essential service or critical infrastructure element. 3. Economic loss exceeding 0,1 % of GDP. 4. Economic loss or material damage to at least one user exceeding 250 000 EUR. 5. More than 100 injured persons requiring medical attention or one casualty. 6. Disruption of public order, public security, emergency or distress requiring carrying out of rescue work or execution of activities and measures related with providing help in distress .

Heating Industry

Service provider (Annex No. 1 to the Act)	**Specific sector criteria** (individually)	**Impact criteria** (individually)

		Impact of the cybersecurity incident in the information system or network, on the functioning of which depends service operation, may cause:
Heat producer according to specific legal regulation.[2])	a) Source of heat energy. b) Technical dispatch used for heat production.	1. Threatening availability, authenticity, integrity or confidentiality of the stored, transferred, or processed data or related services provided or available through these networks and information systems, affecting more than 25 000 persons. 2. Limitation or disruption of operation of other essential service or critical infrastructure element. 3. Economic loss exceeding 0,1 % of GDP. 4. Economic loss or material damage to at least one user exceeding 250 000 EUR. 5. More than 100 injured persons requiring medical attention or one casualty. 6. Disruption of public order, public security, emergency or distress requiring carrying out of rescue work or execution of activities and measures related with providing help in distress.
Heat supplier according to specific legal regulation.[2])	a) Heat distribution facilities. b) Technical dispatch used for heat energy supplying system operation.	1. Threatening availability, authenticity, integrity or confidentiality of the stored, transferred, or processed data or related services provided or available through these networks and information systems, affecting more than 25 000 persons. 2. Limitation or disruption of operation of other essential service or critical infrastructure element. 3. Economic loss exceeding 0,1 % of GDP. 4. Economic loss or material damage to at least one user exceeding 250 000 EUR. 5. More than 100 injured persons requiring medical attention or one casualty. 6. Disruption of public order, public security, emergency or distress requiring carrying out of rescue work or execution of activities and measures related with providing help in distress.

Financial Markets Infrastructure

Service provider (Annex No. 1 to the Act)	**Specific sector criteria** (individually)	**Impact criteria** (individually)

[2]) Act No. 657/2004 Coll. on Heat Energy Industry as amended.

		Impact of the cybersecurity incident in the information system or network, on the functioning of which depends service operation, may cause:
Trading venue operator according to specific legal regulation.[3])	-	1. Threatening availability, authenticity, integrity or confidentiality of the stored, transferred, or processed data or related services provided or available through these networks and information systems, affecting more than 25 000 persons. 2. Limitation or disruption of operation of other essential service or critical infrastructure element. 3. Economic loss exceeding 0,1 % of GDP. 4. Economic loss or material damage to at least one user exceeding 250 000 EUR. 5. Disruption of public order, public security, emergency or distress requiring carrying out of rescue work or execution of activities and measures related with providing help in distress.
Central counterparty – legal entity that interposes itself between the counterparties to the contracts traded on one or more financial markets, becoming the buyer to every seller and the seller to every buyer	-	1. Threatening availability, authenticity, integrity or confidentiality of the stored, transferred, or processed data or related services provided or available through these networks and information systems, affecting more than 25 000 persons. 2. Limitation or disruption of operation of other essential service or critical infrastructure element. 3. Economic loss exceeding 0,1 % of GDP. 4. Economic loss or material damage to at least one user exceeding 250 000 EUR. 5. More than 100 injured persons requiring medical attention or one casualty. 6. Disruption of public order, public security, emergency or distress requiring carrying out of rescue work or execution of activities and measures related with providing help in distress.

Post

[3]) Act No. 429/2002 Coll. on Stock Exchange as amended.

Service provider (Annex No. 1 to the Act)	**Specific sector criteria** (individually)	**Impact criteria** (individually) Impact of the cybersecurity incident in the information system or network, on the functioning of which depends service operation, may cause:
Postal company providing one or more postal services or postal cashless payment according to specific legal regulation.[4])	-	1. Threatening availability, authenticity, integrity or confidentiality of the stored, transferred, or processed data or related services provided or available through these networks and information systems, affecting more than 25 000 persons. 2. Limitation or disruption of operation of other essential service or critical infrastructure element. 3. Economic loss exceeding 0,1 % of GDP. 4. Economic loss or material damage to at least one user exceeding 250 000 EUR. 5. More than 100 injured persons requiring medical attention or one casualty. 6. Disruption of public order, public security, emergency or distress requiring carrying out of rescue work or execution of activities and measures related with providing help in distress.

INDUSTRY

Pharmaceutical Industry

Service provider (Annex No. 1 to the Act)	**Specific sector criteria** (individually)	**Impact criteria** (individually) Impact of the cybersecurity incident in the information system or network, on the functioning of which depends service operation, may cause:
Manager of the medicinal products according to specific legal regulation.[5])	-	1. Threatening availability, authenticity, integrity or confidentiality of the stored, transferred, or processed data or related services provided or available through these networks and information systems, affecting more than 25 000 persons. 2. Limitation or disruption of operation of other essential service or critical infrastructure element. 3. Economic loss exceeding 0,1 % of GDP. 4. Economic loss or material damage to at least one user exceeding 250 000 EUR. 5. More than 100 injured persons requiring medical attention or one casualty. 6. Disruption of public order, public security, emergency or distress requiring carrying out of rescue work or execution of activities and measures related with providing help in distress.

Chemical Industry

[4]) Act No. 362/2011 Coll. on Postal Services and Amendment and Supplements to certain Acts as amended.

[5]) Act No. 657/2004 Coll. on Medicinal Products and Medical Devices and Amendment and Supplements to certain Acts as amended.

Service provider (Annex No. 1 to the Act)	**Specific sector criteria** (individually)	**Impact criteria** (individually) Impact of the cybersecurity incident in the information system or network, on the functioning of which depends service operation, may cause:
Supplier, producer, importer and subsequent user of substances and mixtures according to specific legal regulation.[6])	-	1. Threatening availability, authenticity, integrity or confidentiality of the stored, transferred, or processed data or related services provided or available through these networks and information systems, affecting more than 25 000 persons. 2. Limitation or disruption of operation of other essential service or critical infrastructure element. 3. Economic loss exceeding 0,1 % of GDP. 4. Economic loss or material damage to at least one user exceeding 250 000 EUR. 5. More than 100 injured persons requiring medical attention or one casualty. 6. Disruption of public order, public security, emergency or distress requiring carrying out of rescue work or execution of activities and measures related with providing help in distress.

WATER AND ATMOSPHERE

Hydraulic Structures

Service provider (Annex No. 1 to the Act)	**Specific sector criteria** (individually)	**Impact criteria** (individually) Impact of the cybersecurity incident in the information system or network, on the functioning of which depends service operation, may cause:
Owner, administrator or lessee of the hydraulic structure according to specific legal regulation.[7])	-	1. Threatening availability, authenticity, integrity or confidentiality of the stored, transferred, or processed data or related services provided or available through these networks and information systems, affecting more than 25 000 persons. 2. Limitation or disruption of operation of other essential service or critical infrastructure element. 3. Economic loss exceeding 0,1 % of GDP. 4. Economic loss or material damage to at least one user exceeding 250 000 EUR. 5. More than 100 injured persons requiring medical attention or one casualty. 6. Disruption of public order, public security, emergency or distress requiring carrying out of rescue work or execution of activities and measures related with providing help in distress.

Securing Drinking Water

[6]) Act No. 67/2010 Coll. on Requirements for Placing Chemical Substances and Chemical Mixtures on the Market and Amendment and Supplements to certain Acts (Chemical Act) as amended.

[7]) Act No. 364/2004 Coll. on Waters and on Amendment of the Act of Slovak National Council No. 372/1990 Coll. on Offences as amended (Water Act) as amended.

Service provider (Annex No. 1 to the Act)	**Specific sector criteria** (individually)	**Impact criteria** (individually) Impact of the cybersecurity incident in the information system or network, on the functioning of which depends service operation, may cause:
Supplier and distributor of drinking water, cooking water, food preparation or other domestic usage, regardless of its origin and the fact, that it is provided from distribution network, water tank or in bottles or other containers; except for distributor that distributes water not as its core activity, but distributes other commodities and goods not considered essential service.	a) Production, supply or distribution of drinking water. b) Water treatment plant. c) Water treatment station. d) Water pipeline or sewage system operation.	1. Threatening availability, authenticity, integrity or confidentiality of the stored, transferred, or processed data or related services provided or available through these networks and information systems, affecting more than 25 000 persons. 2. Limitation or disruption of operation of other essential service or critical infrastructure element. 3. Economic loss exceeding 0,1 % of GDP. 4. Economic loss or material damage to at least one user exceeding 250 000 EUR. 5. More than 100 injured persons requiring medical attention or one casualty. 6. Disruption of public order, public security, emergency or distress requiring carrying out of rescue work or execution of activities and measures related with providing help in distress.

HEALTH CARE INDUSTRY

Service provider (Annex No. 1 to the Act)	**Specific sector criteria** (individually)	**Impact criteria** (individually) Impact of the cybersecurity incident in the information system or network, on the functioning of which depends service operation, may cause:
Health care provider – an individual or a legal entity or other entity providing health care in the territory of a European Union member state.	a) Total number of acute hospital beds at least 500 in the last 3 calendar years. b) Status of highly specialized traumatological care centre according to specific legal regulation.[8]) c) Laboratory services.	1. Threatening availability, authenticity, integrity or confidentiality of the stored, transferred, or processed data or related services provided or available through these networks and information systems, affecting more than 25 000 persons. 2. Limitation or disruption of operation of other essential service or critical infrastructure element. 3. Economic loss exceeding 0,1 % of GDP. 4. Economic loss or material damage to at least one user exceeding 250 000 EUR. 5. More than 100 injured persons requiring medical attention or one casualty. 6. Disruption of public order, public security, emergency or distress requiring carrying out of rescue work or execution of activities and measures related with providing help in distress.

PUBLIC ADMINISTRATION

[8]) Act No. 576/2004 Coll. on Health Care, services concerning Providing Health Care and on Amendment and Supplements to certain Acts as amended.

Service provider (Annex No. 1 to the Act)	**Specific sector criteria** (individually)	**Impact criteria** (individually) Impact of the cybersecurity incident in the information system or network, on the functioning of which depends service operation, may cause:
Public administration body.	Based on risk evaluation within the organization a service defined as substantial service in one subsector of: a) security, b) information systems of public administration, c) defence, d) intelligence services, or e) classified information in relation to functioning of the respective central body in accordance with the act.	1. Threatening availability, authenticity, integrity or confidentiality of the stored, transferred, or processed data or related services provided or available through these networks and information systems, affecting more than 25 000 persons. 2. Limitation or disruption of operation of other essential service or critical infrastructure element. 3. Economic loss exceeding 0,1 % of GDP. 4. Economic loss or material damage to at least one user exceeding 250 000 EUR. 5. More than 100 injured persons requiring medical attention or one casualty. 6. Disruption of public order, public security, emergency or distress requiring carrying out of rescue work or execution of activities and measures related with providing help in distress.

Annex No. 2

to the Decree No. 164/2018 Coll.

List of adopted legally binding acts of the European Union

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