INFORMATION ON THE ESSENTIAL SERVICE

Summary of the way operators of an essential service and information systems of an essential service are identified

Version 1.2, March 2018

Content

Introduction

Decree No 437/2017 Coll. on the Criteria for the Determination of an Operator of Essential Service (hereinafter "the Decree") of December 8, 2017 comes into effect on February 1, 2018. The aim of the Decree is to set out criteria for the identification of operators of an essential service and the information system of essential service. This document summarizes the information as regards the new arrangements which are specified in the Decree.

For further information, please refer to the Secretariat of the National Cyber and Information Security Agency:

National Cyber and Information Security Agency
Mučednická 1125/31

616 00 Brno – Žabovřesky

Tel.: +420 541 110 777

E-mail: nckb@nukib.cz

Note:

This document provides a guideline and does not replace any legal act or implementing regulation. We reserve the right to make changes to this document.

1 Executive summary

Decree No 437/2017 Coll. on the Criteria for the Determination of an Operator of Essential Service (hereinafter "the Decree") of December 8, 2017 comes into effect on 1 February 2018.

The aim of the Decree is to set out criteria for the determination of operators of an essential service and the information system of essential service. Essential service means a service the provision of which "*is dependent on electronic communication networks or information systems"* and the disruption of which may have *"a significant impact on the security of societal or economic activities in any of the following sectors: Energy, Transport, Banking, Financial market infrastructures, Health sector, Water resource management, Digital infrastructure or Chemical industry*" according to Section 2, letter i) of Act No 181/2014 Coll., on Cyber Security (hereinafter "the ACS"). The identification of operators of an essential service and the identification of an information system of essential service are based on sectoral and impact criteria (Section 28, paragraph 2, letter e) of the ACS). Sectoral criteria further divide into Type of service, Type of entity and Special criterion for the type of entity. Impact criteria set the threshold of possible damage that must be reached by a cyber security incident in the information systems and electronic communication networks in order for the latter to fall under identification.

"The importance of the services provided in individual sectors" is to be taken into account in the process of identification (Section 22a, paragraph 1, letter a) of the ACS). This requirement is represented by the criterion called **"A special criterion for the type of entity"**. This criterion is only met by an operator that is important in the given sector, by which means the operator fulfils the above-mentioned requirement for taking into account the importance of the services provided in the individual sectors.

Sectoral criteria are described in the Decree as follows (a simplified example which corresponds to the first sector as stated in the Annex to the Decree is in the parentheses):

- Sector (Energy)
- 1.1. Subsector (Electricity) – subsectors are specified only for the sectors of energy and transport, and are labelled as "parts of the sector" in the text of the Decree
- 1.1.1. Type of service (Electricity production)
- Type of entity (Electricity producer according to the Energy Act)
- a) A special criterion for the type of entity – this is a criterion related to the importance of the provided service within the given sector (A production facility with total installed generating capacity of at least 500 MW)

Sectoral criteria build on each other and proceed from general criteria to more specific.

Thus, the pattern to be followed is: 1. – 1.1. – 1.1.1. – Type of entity – A special criterion for the type of entity

When the sectoral criteria are met by an entity, it is possible to proceed to impact criteria and to assess the impact of a cyber security incident in the system that ensures the provision of the service. Thus, the target of assessment is the impact of an incident in a system that is used by the service operator to provide the service in the particular sector.

As part of the assessment **the impact of a cyber security incident** on 1) the extent and quality of the provision of the essential service to its users, 2) economic and societal activities and public safety and 3) the mutual dependency of sectors (Section 22a, paragraph 1, letter b), points 1 – 3 of the ACS) shall be examined. This requirement is addressed by the **impact criteria**. Impact criteria set the threshold of damage that could be caused by a cyber security incident. The entity which meets the sectoral criteria shall be identified as an operator of an essential service if a potential cyber security incident in its information systems or electronic communication networks that underlie the service provision could reach any of the below specified impact thresholds.

Impact criteria are described in the Decree as follows:

The impact of a cyber security incident in the information system or in the electronic communications network on the functioning of which the service provision is dependent can cause:

I. A serious limitation, disruption (or unavailability)[1)] of the type of service which would affect more than 25,000[1)], 50,000[1)] or 500,000[1)] people

II. A serious limitation or disruption of another essential service or a limitation or disruption of a critical infrastructure element

III. Economic loss greater than 0.25 % of GDP

IV. Unavailability of the type of service for more than 1,600 people which is irreplaceable in another way unless excessive costs were to be incurred

V. More than 100[1)] or 200[1)] casualties or 1,000 injured people in need of medical treatment

VI. Disruption of public safety in a significant part of the administrative territory of a municipality with extended powers, which may require rescue and liquidation operations by the integrated rescue system units or

VII. Disclosure of sensitive data of more than 200,000 people

The impact of an incident is assessed only in cases when the assessed entity (the one providing the service and which uses the assessed system for that provision) meets the sectoral criteria.

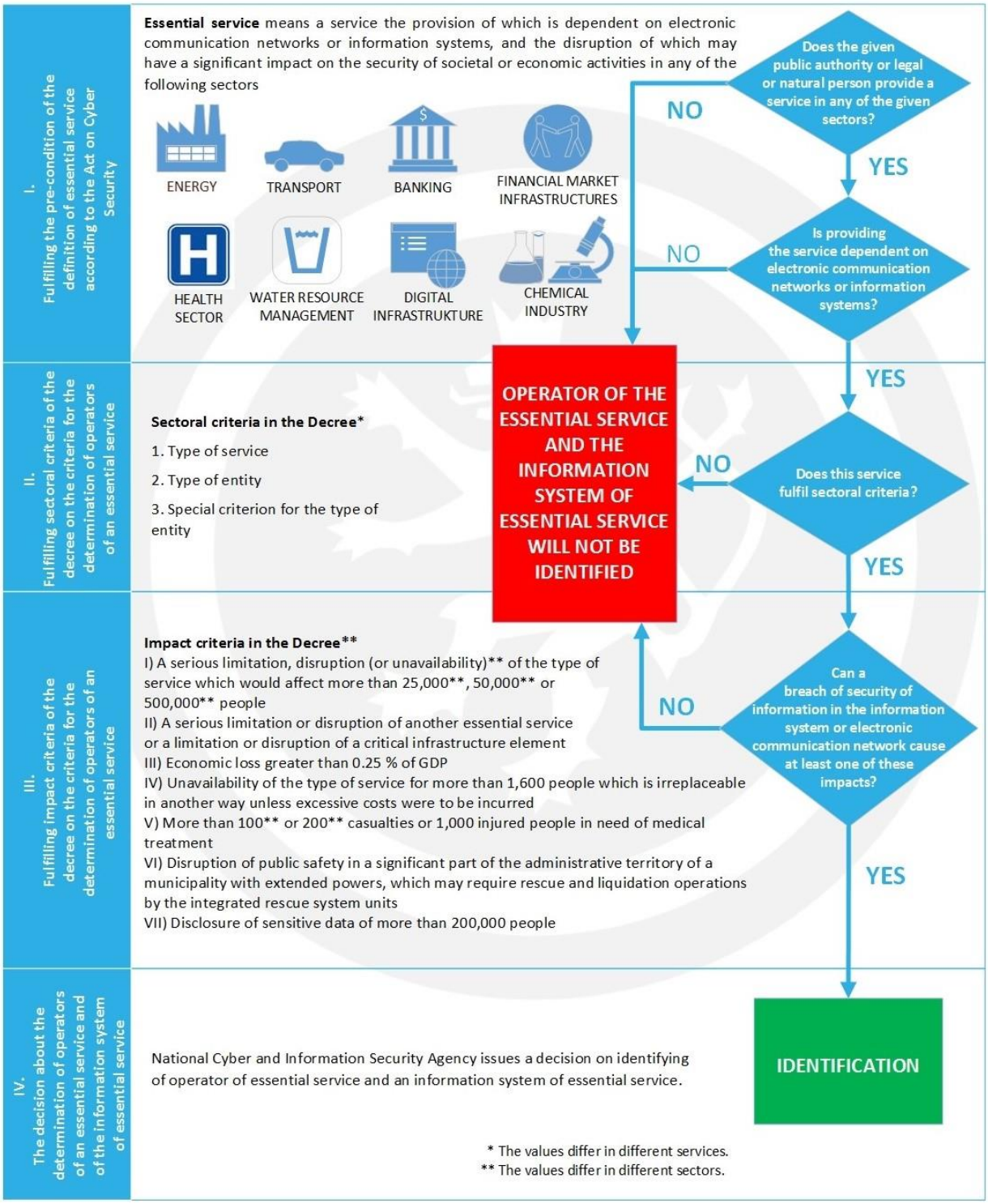
[1] The values differ in different sectors.

The impact of a cyber security incident is assessed against the set impact criteria. When the impact of an incident meets at least one impact criterion, the system shall be identified as an information system of essential service. **Thus, if an entity meets sectoral criteria and a cyber security incident in its system or systems meets impact criteria, the entity shall be identified as an operator of an essential service and the system in question as an information system of an essential service.**

The process of identification and the procedure involving sectoral and impact criteria are described in Picture 1: Summary of the identification of operators of an essential service and of information systems of an essential service.

If we were to summarise the whole process of identification, it could be said that in order for an entity to be identified as an operator of an essential service, it has to be an entity providing a service in one of the sectors defined in the ACS and further specified in the Decree, and the provision of such service has to be dependent on an information system or an electronic communication network (see section I. in Picture 1). A detailed assessment of the fulfilment of the criteria can then be performed. The identification of operators of an essential service and of an information system of essential service is based on sectoral criteria (which have to be met by the entity – see section II. in Picture 1) and impact criteria (which have to be met by an incident in the system of the assessed entity – see section III. in Picture 1). When the criteria are met, the identification is made (see section IV. in Picture 1).

Picture 1 Summary of the identification of operators of an essential service and of information systems of an essential service



2 Description of sectoral determination criteria

2.1 Transposition of sectors and subsectors as defined by the Directive

The sectors and subsectors as defined by Annex II to 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 (hereinafter "the NIS Directive") have been incorporated into the national regulatory framework in their entirety in order to meet the transposition obligations. Because the NIS Directive allows the expansion of the sectors of essential service, the Czech Republic has added chemical industry to the sectors of essential service and thermal industry to the subsectors of the energy sector. It is important to note that expanding the sectors of essential services is common across Member States, e.g. Germany and France have added food industry to the sectors.

2.2 Definition of sectoral criteria

The NIS Directive defines sectoral and subsectoral criteria in general terms. In order to define the types of service and the types of entity included in the regulation more specifically, the Union law to which the NIS Directive refers to has been used.

In order to define the special criteria for the type of entity that reflect the importance of an entity for the given field, a working group composed of industry and government experts was convened. The criteria have been set based on the outputs provided by this working group.

The working group consisted of smaller groups focusing on individual sectors. A total of 14 smaller groups that met separately were established. About 120 experts from across the sectors were involved in the creation of the Decree. A proposal with the criteria for operators of essential service was introduced at the meetings of the working groups and the relevant working group commented and discussed possible options until a suitable solution was found. This procedure was crucial for the creation of the Decree due to the diversity of individual sectors and subsectors.

3 Description of impact determination criteria

3.1 Definition of impact criteria

The NIS Directive requires Member States to consider the following factors when setting the impact criteria for determining operators of an essential service and information systems of essential service (Article 6, paragraph 1 of the NIS Directive):

a) the number of users relying on the service provided by the entity;

b) dependency of other sectors referred to in Annex II on the service provided by the entity;

c) the impact that incidents could have, in terms of degree and duration, on economic and societal activities or public safety;

d) the market share of the entity;

e) the geographic spread with regard to the area that could be affected by an incident and

f) the importance of the entity for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service.

The described factors are also the basis for Section 22a, paragraph 1, letter b) of the ACS which sets that particularly the impact of a cyber security incident on the following parameters shall be taken into account:

1) extent and quality of provision of the essential service to the users which are dependent on it;

2) economic and societal activities and public safety and

3) dependency of other sectors referred to in Section 2, letter i).

The impact criteria are set in the Decree so as to cover all the above described areas set by both the NIS Directive (Article 6, paragraph 1 of the NIS Directive) and the Act (Section 22a, paragraph 1, letter b) of the ACS), and to cover them for various scenarios. When identifying the impact criteria, the nature and specific properties of individual sectors (or subsectors) were taken into account, and so the criteria vary slightly for different sectors (e.g. the subsector of air transport or the sector of banking have different threshold values for some impact criteria than e.g. the energy sector). To decide on the relevance of a specific criterion for a specific sector or subsector, materials produced by the members of working groups, consultations with experts, experience previously gained in the process of identifying critical information infrastructure, and open sources have been used.

Table 1 maps the impact criteria set out in the Decree against the requirements of the NIS Directive (Article 6, paragraph 1 of the NIS Directive) and their transposition to the ACS (Section 22a, paragraph 2 of the ACS).

Table 1: The comparison of suggested impact criteria in the Decree with the requirements of the Act on Cyber Security and the NIS directive

The impact criterion according to the Decree The impact of a cyber security incident in the information system or in the electronic communications network on the functioning of which the service provision is dependent can cause	**The impact areas that shall be taken into account according to Section 22a, paragraph 2 of the ACS**	**The impact areas according to Article 6, paragraph 1 of the NIS Directive**
I) A serious limitation, disruption (or unavailability) of the type of service which would affect more than 25,000, 50,000 or 500,000 people	1) extent and quality of the provision of an essential service to its users;	a)
II) A serious limitation or disruption of another essential service or a limitation or disruption of a critical infrastructure element	3) interdependency of sectors	b)
III) Economic loss greater than 0.25 % of GDP	2) economic and societal activities and public safety	c), d)
IV) Unavailability of the type of service for more than 1,600 people which is irreplaceable in another way unless excessive costs were to be incurred	1) extent and quality of the provision of an essential service to its users	f)
V) More than 100 or 200 casualties or 1,000 injured people in need of medical treatment	2) economic and societal activities and public safety	c)

VI) Disruption of public safety in a significant part of the administrative territory of a municipality with extended powers, which may require rescue and liquidation operations by the integrated rescue system units or	2) economic and societal activities and public safety	a), c), e)
VI) Disclosure of sensitive data of more than 200,000 people	2) economic and societal activities and public safety	c)

3.2 Impact criteria for identifying an information system of essential service

The impact of a cyber security incident in the information system or in the electronic communications network on the functioning of which the service provision is dependent can cause (I.– VII.):

The impact has to be caused by a cyber security incident, i.e. by compromising availability, confidentiality or integrity of the system on which the provision of the service is dependent (the first column in the Annex to the Decree). The incident in the information or communication system may therefore have the following impacts.

I. A serious limitation, disruption (or unavailability) of the type of service which would affect more than 25,000, 50,000 or 500,000 people

The aim of the criterion is to set a threshold for the impact of a cyber security incident on the provision of a service for a particular number of people.

Within this impact criterion, unavailability applies only to the subsectors of electricity, gas and thermal industry, due to their specific properties, particularly the irreplaceability of these services.

This criterion corresponds to the requirements in Section 22a, paragraph 1, letter b), point 1 of the ACS and in Article 6, paragraph 1, letter a) of the NIS Directive.

50,000 inhabitants is the average population in a municipality with extended powers[2] (an element of the administrative division of the Czech Republic according to Section 6 of Act No

[2] THE NUMBER OF INHABITANTS IN MUNICIPALITIES as of 1 January 2017 © Czech Statistical Office, Prague, 2017. p. 9-12. Available in Czech at: https://www.czso.cz/csu/czso/pocet-obyvatel-v-obcich-k-112017.

128/2000 Coll. on Municipalities and according to the Act No 314/2002 Coll. on the Identification of a Municipality with a Commissioned Municipal Office and on the Identification of a Municipality with Extended Powers), rounded to the nearest 10,000.

The thresholds for some sectors are different – this concerns the banking sector and the thermal industry and the threshold values are:

- **25,000 people** in the subsector of thermal industry = a half of the average population in the administrative territory of a municipality with extended powers; a lower threshold in this subsector is due to sectoral specific properties of thermal industry, heating plants usually ensure supplies to fewer people.

- **500,000 people** in the banking sector = ten times the average population of the administrative territory of a municipality with extended powers; a higher threshold in this sector is again due to its specific property – immediate services in the banking sector are provided to a large number of users and the threshold for a significant entity is therefore higher.

A serious limitation or disruption of a service means that there is a significant disruption or limitation to the extent or quality (as opposed to unavailability which means that the service is not available in any extent or quality). In practice it can mean there is a significant waiting time extension, not all customers are accommodated, there may be risks to availability or limitations of availability, some supporting services may not be available, more complex tasks cannot be performed, the service has to be managed/provided in other than the usual way, etc.

The type of service is the service provided by the assessed entity which meets the sectoral criteria. This service is defined under the heading “type of service”. The service operator meets the special criterion for the type of entity.

A person is every service user/customer. Only the number of service users/customers to which a facility is able to provide the service can be taken into account for identification, further consideration can also be given to the geographic location and the catchment area.

II. A serious limitation or disruption of another essential service or a limitation or disruption of a critical infrastructure element

This criterion reflects the dependency of other already identified services on the assessed type of service.

The importance of impact which this criterion represents is not determined by its extent or the dependency of a certain number of people on the given service but by the mere fact that

the limitation of such service can limit or disrupt the provision of another already identified essential service or the operation of an identified critical infrastructure element.

This criterion's effect is not limited only to the Czech Republic but given the harmonisation of essential services from the European Union perspective, it can also have a cross-border effect. This will be the case when the impact of an incident threatens an essential service already identified in another Member State.

This criterion corresponds to the requirements in Section 22a, paragraph 1, letter b), point 3 of the ACS and in Article 6, paragraph 1, letter b) of the NIS Directive.

A serious limitation or disruption of a service means that there is a significant disruption or limitation to the extent or quality (as opposed to unavailability which means that the service is not available in any extent or quality). In practice it can mean there is a significant waiting time extension, not all customers are accommodated, there may be risks to availability or limitations of availability, some supporting services may not be available, more complex tasks cannot be performed, the service has to be managed/provided in other than the usual way, etc.

The **limitation or disruption of the operation** means that the service is not provided in its standard quality (e.g. the time in which the service user/customer is satisfied is extended, there are queues, the quality standard is reduced, failures can occur).

The phrase "**other essential services**" refers to the already identified essential services in the Czech Republic or another Member State.

The **operation of an identified critical infrastructure element** means the operation of any critical infrastructure element which has already been identified.

The conjunction **or** means that for the purposes of identification, the first condition and second condition can be fulfilled alternatively or both at the same time.

III. Economic loss greater than 0.25 % of GDP

The third impact criterion is the possibility of economic loss amounting to at least 0.25 % of GDP.

A wide range of losses is considered to be economic loss, especially economic losses incurred due to disruptions of service provision, penalties or costs for damage remediation.

In contrast to the previous criteria, this criterion primarily aims at the economic situation which would occur in relation to the disruption of the service.

This criterion corresponds to the requirements in Section 22a, paragraph 1, letter b), point 2 of the ACS and in Article 6, paragraph 1, letters c) or d) of the NIS Directive.

For the purpose of calculating **economic loss**, the following shall be included in the economic loss:

1) Economic loss resulting from business disruption.
2) Expected penalty (fine) in case standards, regulations, or contracts are breached, including penalty for environmental damage.
3) Costs of environmental damage remediation, property damage or injuries.
4) Other potential specific costs.

IV. Unavailability of the type of service for more than 1,600 people which is irreplaceable in another way unless excessive costs were to be incurred

The aim of the criterion is to set a threshold for the impact of a cyber security incident on the provision of a service for a particular number of people for whom the service is irreplaceable in another way.

This criterion is not applied in the subsector of electricity, gas and thermal industry and in the banking sector. This is due to their specific sectoral properties, mainly the immediate provision of services to a large number of users.

This criterion corresponds to the requirements in Section 22a, paragraph 1, letter b), point 1 of the ACS and in Article 6, paragraph 1, letter f) of the NIS Directive.

This criterion reflects the average number of inhabitants in a municipality in the Czech Republic.[3]

Unavailability means that the service is not available in any extent or quality.

The type of service is the service provided by the assessed entity which meets the sectoral criteria. The service is defined in the Decree under the column with the heading “type of service”.

A person stands for each service user/customer; only the number of service users/customers to which a facility is able to provide the service can be taken into account for the identification, further consideration can also be given to the geographic location and the catchment area.

Replaceability in another way means there are ways by which the same result can be achieved besides the solution in question. The provided service therefore has to be unique and cannot be easily replaced to fulfil the criterion. Typically, this will apply to sectors with networks that only have one infrastructure, which is irreplaceable.

[3] THE NUMBER OF INHABITANTS IN THE MUNICIPALITIES as of 1 January 2017 © Czech Statistical Office, Prague, 2017. p. 9-12. Available in Czech at: https://www.czso.cz/csu/czso/pocet-obyvatel-v-obcich-k-112017.

When assessing whether the "**costs incurred would be excessive**", the costs have to be assessed in light of the specific circumstances of the given case. It can help to mainly focus on the financial costs, the time expended and other costs incurred to ensure the alternative service provision. To give an example, in order for the service to be ensured there either has to be an information system in place or the service provider will have to employ twice as many employees or maintain technological redundancy, etc. In such a case, the costs would be excessive. These are costs that, when incurred to ensure an alternative solution for the service, would be inappropriate compared to the standard ways in which the service is usually ensured.

V. More than 100 or 200 casualties or 1,000 injured people in need of medical treatment

The number of 100 or 200 casualties or 1,000 injured in need of medical treatment that would be caused in relation to the disruption of the given service due to a cyber security incident in an information system.

This criterion corresponds to the requirements in Section 22a, paragraph 1 (b), point 2 of the ACS and in Article 6, paragraph 1(c) of the NIS Directive.

This criterion is different for the sector of air transport where the threshold value is set to 200 people dead. This criterion is not applied in the banking, financial markets infrastructure and digital infrastructure sectors because a causal link between the impact of a cyber security incident in these sectors and deaths is not expected.

VI. Disruption of public safety in a significant part of the administrative territory of a municipality with extended powers, which may require rescue and liquidation operations by the integrated rescue system units

A disruption of public safety is primarily a situation in which the state security or the security of individual state authorities or institutions is threatened or the safety of an individual or public or private property is threatened.

A significant part can be understood from the point of view of the size of the territory, population concentration or the concentration of important companies.

This criterion corresponds to the requirements in Section 22a, paragraph 1, b), point 2 of the ACS and in Article 6, paragraph 1, letters a), c) or e) of the NIS Directive.

Public safety means the protection of an individual and the society against attacks that threaten e.g. the state security or security of state authorities, institutions and government functions, security of an individual, particularly honour, dignity and physical integrity, or the state property, or the property of an individual.

A significant part of the administrative territory of a municipality with extended powers means a territory assessed from the point of view of a quantitative criterion (e.g. the size of the territory) as well as qualitative criterion (depending on the population concentration, concentration of important companies, administrative centres, etc.). A municipality with extended powers is defined by the division of the Czech Republic according to Section 6 of Act No 128/2000 Coll. on Municipalities and according to the Act No 314/2002 Coll. on the Identification of a Municipality with a Commissioned Municipal Office and on the Identification of a Municipality with Extended Powers.

Rescue operations are operations aimed at preventing or reducing the immediate effect of the risks caused by an incident, especially in relation to threats to life, health, property or the environment, and operations that lead to the termination of the causes of such risks.

Liquidation operations are operations aimed at eliminating consequences caused by an incident.

Integrated rescue system units are the Fire Rescue Service of the Czech Republic, the units of fire protection included in the regional coverage by the units of fire protection system, the providers of ambulance and rescue services and the Police of the Czech Republic.

Other integrated rescue system units are the designated forces and resources of the armed forces, public health protection authorities, rescue services, emergency services, professional and other services, civil protection sites, and non-profit organizations and citizens' groups which can be used for rescue and liquidation operations.

VII. Disclosure of sensitive data of more than 200,000 people

This criterion is applied only to the health sector.

This criterion reflects the need to protect systems with large amounts of sensitive personal data.

Personal data means any information related to a recognized or a recognizable person. An entity is considered to be recognized or recognizable when it can be directly or indirectly identified especially on the basis of a number, code or one or two features that are specific to a physical, physiological, psychological, economic, cultural or social identity.[4]

Sensitive data means personal data referring to nationality, racial or ethnic origin, political opinions, memberships in trade unions, religion and philosophical beliefs, criminal convictions, health status and sexual life of the concerned entity and genetic data about the

[4] Section 4, letter a) of the Act No 101/2000 Coll. on the Protection of Personal Data and on Amendment to Some Acts.

concerned entity; sensitive data is also biometric data which allow the direct identification or authentication of the concerned entity.[5]

This criterion corresponds to the requirements in Section 22a, paragraph 1, letter b), point 2 of the ACS and in Article 6, paragraph 1, letter c) of the NIS Directive.

Direct identification means that a person can be directly identified, including in other ways than only on the grounds of the information the data controller has.

Indirect identification is a process that leads to the identification of a specific person but only after greater effort is exerted, because the data controller e.g. only has his/her description or photographs but not the identification details.

An identification number is the date of birth, a personal identification number, an employee number assigned by an employer, a phone number, an IP address or e.g. a bank account number.

An identification code is e.g. an identifier of a data mailbox of a natural person or a computer's host name.

Physical or physiological identity is the appearance of the person, the shape of the face, head and body as a whole, height, weight, the colour of hair or eyes.

Psychological identity is understood as information about behaviour, responses of the person in certain situations or the motivation behind such behaviour.

An economic identity is information about property, claims and liabilities, about income or its sources.

Cultural identity includes interests, hobbies and the abilities of the person.

Social identity includes marital status, education, job or other activities.

Nationality means belonging to a particular nation (the General Data Protection Regulation[6] does not state this criterion explicitly).

Racial origin means belonging to a particular race.

Ethnic origin means belonging to a particular ethnic group.

[5] Section 4, letter b) of the Act No 101/2000 Coll. on the Protection of Personal Data and on Amendment to Some Acts.
6 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Political opinions do not include ipso facto the information about membership in a political party or movement.

Membership in trade unions includes information about the membership of a person in trade unions.

Religion means primarily information about the membership of a person in registered churches.

A philosophical belief means primarily a relationship of a person to unregistered religious or other communities.

A criminal conviction means information about actual convictions, not information about other stages of criminal proceedings (the General Data Protection Regulation does not state this criterion explicitly).

Health status means information about a specific disease in the past or about a current disease, the injury of the person or received treatment, information about medical examinations in the past, information about hospitalisation or information about pregnancy.

Sexual life includes information about sexual partners of the person or sexual practices or activities the person practices, seeks or prefers.

Genetic data is information acquired using analysis of the human deoxyribonucleic acid (DNA).

Biometric data is data that allows direct identification or authentication of the entity, which is understood to mean fingerprints, palm prints or footprints, retinal image or iris image, a recording of the dynamic demonstration of walking, but also facial or speech analysis.

A person is in this case everyone about whom the information system possesses a separate record.

4 Process of assessing the fulfilment of the criteria

The text of this chapter gives an example and directly refers to the Annex to the Decree, namely the table for the sector energy, the subsector of electricity. This process is detailed in Picture 2: The picture summarizing the identification of essential service operators using impact and sectoral criteria.

(Example**: 1. Energy – 1.1. Electricity – 1.1.1. Electricity production**).

In order for an entity to be identified as an operator of an essential service, it has to operate a service in at least one of the sectors defined in the ACS and further specified in the Decree. The provision of such service has to be dependent on an information system or an electronic communication network (Section 2, letter i) and j) of the ACS). A detailed assessment of meeting the criteria can then be performed.

The first column of the table in the Annex to the Decree defines the activity (service) subject to regulation. In this case, it is thus the activity of electricity production.

The second column of the table defines the entity that provides the service. It defines the set of entities – **service operators** – the regulation **could be** applied to. Relevant national legislation or Union law has been used for the definitions in the first and the second column of the table. In the example, the type of entity is the entity that complies with the definition of an electricity producer in accordance with the Act No 458/2000 Coll., the Energy Act.

The third column of the table introduces the limitation to the most important service operators in the sector. In this case, it is a production facility with total installed generating capacity of at least 500 MW.

The last column of the table sets impact criteria which have to be met by a potential impact of an incident in the information system or in the electronic communication network which is used for the provision of the service defined in the previous columns. In assessment whether the entity meets the criteria or not, general factors in the table shall be considered first and then the assessment shall proceed to specific factors.

Put simply:

Sectors – based on the NIS Directive and defined in Section 2, letter j) of the ACS.

Subsectors – based on the NIS Directive, further specify the sectors and are only established for some sectors.

The column with the headline "**Type of service**" defines the service within the sector of national economy to which the regulation is applied.

The column with the headline "**Type of entity**" says which entities providing the service in a given sector or subsector shall be assessed. This is the set of entities from which the essential service operators shall be determined.

The column with the headline "**Special criterion for the type of entity**" is used to filter important operators of a given service at whom the regulation is aimed and other operators the regulation is not concerned with. It focuses on the quality or quantity of the provided service.

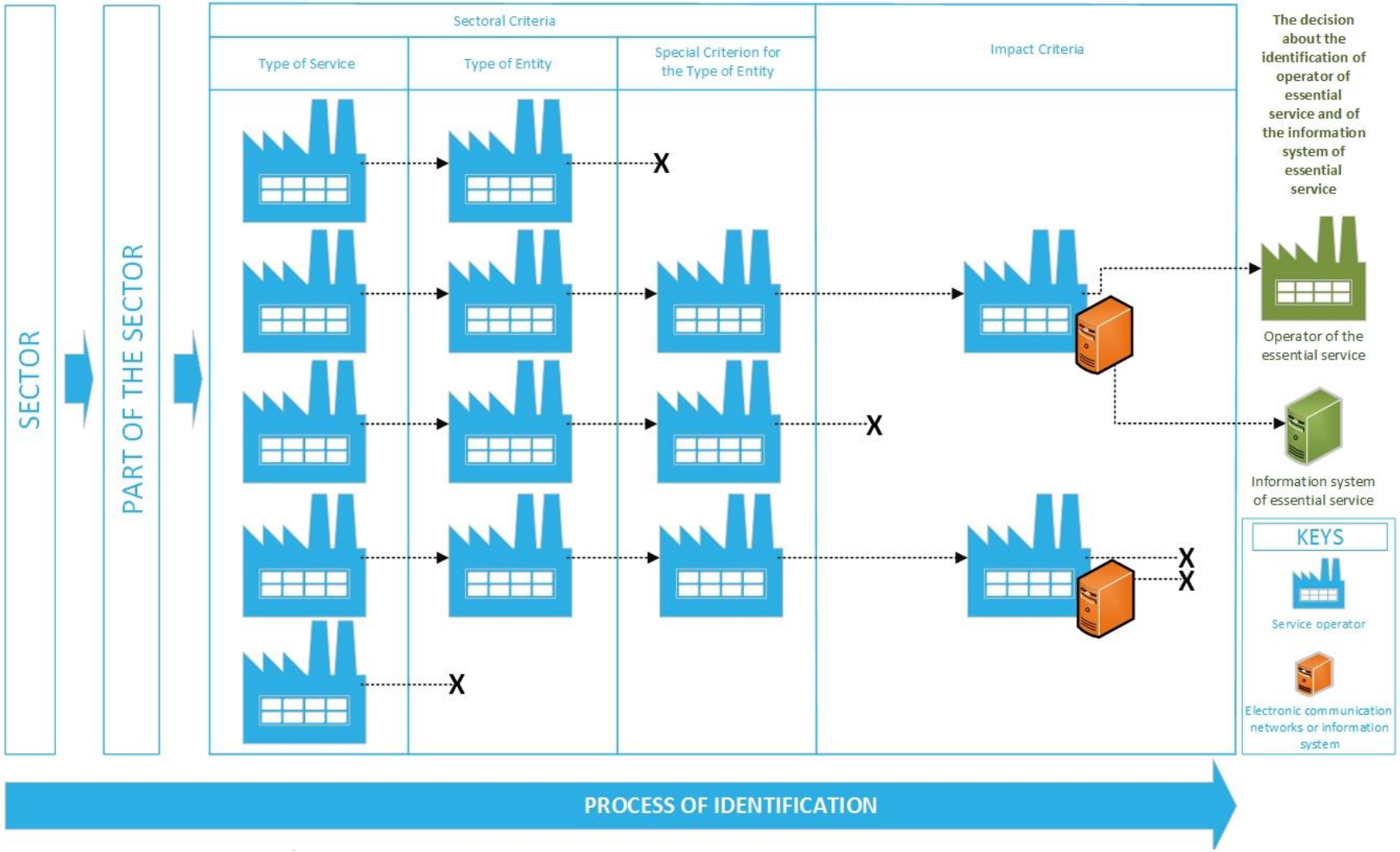
The last column "**Impact criteria**", i.e. the impact of a cyber security incident in the information system or the electronic communication network on which the provision of the service is dependent, identifies impacts on society which are of such importance that it is necessary to prevent them. The systems the disruption of which could cause such impacts have to be secured and protected.

In order for an entity to be identified as an essential service operator, **it has to meet at least one criterion in each column**, i.e. the type of service, the type of entity, and a special criterion for the type of entity stated in the same row in the given sector or subsector in the Annex to the Decree.

The identification by the National Cyber and Information Security Agency itself shall be performed in the following way (example: 1. Energy – 1.1. Electricity – 1.1.1. Electricity production):

a) A list of electricity producers in accordance with the Act No 458/2000 Coll., the Energy Act is acquired from the relevant authority;
b) only producers that meet at least one special criterion for the type of entity are selected;
c) the entities selected according to the previous point are assessed by the National Cyber and Information Security Agency against the impact criteria and
d) the systems that meet impact criteria are identified as information systems of essential service. The entity responsible for the service's provision is identified as an operator of an essential service.

Picture 2: The picture summarizing the identification of operators of an essential service using impact and sectoral criteria (Example: 1. Energy – 1.1. Electricity – 1.1.1. Electricity production):



Document version

Date	Version:	Changed (name)	Change
January 4, 2018	1.0	Dep. RAP	Document creation
March 20, 2018	1.1	Dep. RAP	Graphic changes
March 29, 2018	1.2	Dep. RAP	Correction of the Picture 1