DECREE

of 24 August 2021

on security levels for the use of cloud computing by public authorities

Pursuant to the provisions of Section 28 paragraph 2(a) of Act No. 181/2014 Coll., on Cybersecurity and on the Amendment to Related Acts (the Act on Cybersecurity),), as amended by Act No. 205/2017 Coll., (hereinafter referred to as the "Act"), the National Cyber and Information Security Agency establishes as follows:

Section 1
Subject matter

The Decree establishes the security levels for the use of cloud computing by public authorities under Section 6(e) of the Act.

Section 2
Definition of terms

For the purposes of this Decree, the terms below are understood to have the following meanings

a) Enquired cloud computing is an information or communication system as a whole or its part, which can be operated using cloud computing and which a public authority is obliged to classify within a security level;
b) A part of information or communication system is such a part of the system which is clearly separable, ensures purposeful and systematic information activity[1)], can be performed using cloud computing, and is defined with respect to functional categories, architecture, operating model, and security;
c) Impact area is a defined area in which an impact of a cybersecurity incident on the enquired cloud computing can have an impact on the safety and health of people, protection of personal data, criminal proceedings, public order, international relationship, management and operation, credibility, financial model, or provision of services;
d) Low, medium, high, or critical level of impact is a value reflecting the impact of a cybersecurity incident on the enquired cloud computing in every impact area.

Section 3
Security levels

Security levels for the use of cloud computing by public authority express the potential impacts of a cybersecurity incident on the enquired cloud computing. The security level can be low, medium, high or critical.

[1)] Section 2 (a) of Act No. 365/2000 Coll., on Public Administration Information Systems and amending certain other acts as amended.

Section 4

Classification of the enquired cloud computing within a security level

(1) The public authority shall classify the enquired cloud computing within a security level pursuant to Annex to this Decree. The public authority shall assess the materialisation of the level of impact which the enquired cloud computing can have in every impact area. The level of impact in every impact area is given by the worst impact possible of the cybersecurity incident.

(2) When establishing the worst possible impact of a cybersecurity incident, the public authority shall consider the potential infringement of integrity and availability of the enquired cloud computing and the nature of the information or communication system as a whole, which represents the enquired cloud computing. If only a certain part of the information or communication system represents the enquired cloud computing, the relation of this part to the security level of the information or communication system as a whole shall also be considered.

(3) The security level for the use of the enquired cloud computing by a public authority is the same as the highest level of impact that the enquired cloud computing reaches in the assessment of the individual impact areas.

(4) An information or communication system which is an important information system according to the law classifies within the high security level provided that this information or communication system as a whole is the enquired cloud computing unless it is classified within the critical security level by the public authority in accordance with the procedures laid down in the preceding paragraphs.

(5) An information or communication system that is a critical information infrastructure according to the law classifies within the critical security level provided that this information or communication system as a whole is the enquired cloud computing.

(6) The highest established security level of the information or communication system as a whole must be set for at least one part of the information or communication system, which is the enquired cloud computing.

(7) The public authority shall make a written record of the procedure of establishing the security level of the enquired cloud computing in accordance with the preceding paragraphs. National Cyber and Information Security Agency shall publish a sample written record on its website.

Section 5

Entry into force

This decree enters into force on the day following the day of its publishing.

Director:

Ing. **Řehka** m.p.

Levels and areas of impact for classification of the enquired cloud computing within a security level

Impact level	Impact area								
	A. Human safety and health	**B. Protection of personal data**	**C. Criminal proceedings**	**D. Public order**	**E. International relationships**	**F. Management and operation**	**G. Credibility**	**H. Financial model**	**I. Provisions of services**
1. Low	It cannot cause injury of an individual or a group of people.	It cannot affect the enquired cloud computing, or it can have a negative impact on the enquired cloud computing which meets up to two criteria from the first group of criteria for the impact area B. Protection of personal data.	It cannot create conditions for committing the offences of misappropriation of authority powers, misuse of powers of an official or counterfeiting or alteration of an authentic instrument, nor can it make the investigation thereof more difficult.	It cannot cause mass disturbance nor otherwise prejudice public order.	It cannot have a negative impact on the image of the Czech Republic abroad.	It cannot prejudice the proper functioning or management of even a part of the public authority, or it can prejudice the proper functioning of a part or the whole public authority but cannot significantly limit or stop the performance of important activities of the public authority.	It cannot have a negative impact on the relationship with other parts of the public authority nor other organisations nor public relations, or it can have a negative impact on the relationship with them, but the negative impact may only be local.	It cannot, even indirectly, cause financial losses or it can cause financial losses smaller than 1% of the normal annual expenditures of the public authority's budget.	It cannot cause a limitation, breach, or unavailability of any of the provided services, or it can cause a limitation, breach or unavailability of the services provided for 5,000 people or less.
2. Medium	It can cause injury of an individual or a group of up to 100 people.	It can have a negative impact on the enquired cloud computing which meets three or more criteria from the first group of criteria or one criterion from the second group of criteria for the impact area B. Protection of personal data.	It can create conditions for committing the offences of misappropriation of authority powers, misuse of powers of an official or counterfeiting or alteration of an authentic instrument, or it can make the investigation thereof more difficult.	It can cause mass disturbance or otherwise prejudice public order with local impacts.	It can have a negative impact on the image of the Czech Republic in the neighbouring countries.	It can prejudice the proper functioning of a part or the whole public authority, whereby it can significantly limit or stop the performance of important activities of the public authority.	It can have a negative impact on the relationship with other parts of the public authority, other organisations or public relations but the negative impact may only be regional.	It can cause financial losses amounting to 1% to 5% of the normal annual expenditures of the public authority's budget, where these losses amount to CZK 100,000.00 or more. If the financial loss equals an amount lower than CZK 100,000.00, the low impact level applies.	It can cause a limitation, breach or unavailability of services provided for more than 5,000 but up to 50,000 people.

3. High	It can cause injuries of a group of more than 100 but up to 2,500 people or direct threat to or loss of life of an individual or a group of up to 250 people.	It can have a negative impact on the enquired cloud computing which meets two or more criteria from the second group of criteria for the impact area B. Protection of personal data.	It can prejudice investigation of crime or court proceedings active within law enforcement authorities.	It can cause mass disturbance or otherwise severely prejudice public order with regional impacts.	It can have a negative impact on the image of the Czech Republic worldwide.	It can prejudice the proper functioning of a part or the whole public authority, whereby it can significantly limit or stop the performance of important activities of the public authority and prejudice the management, damage the development, or harm the pursuit of the objectives and interests of the public authority.	It can have a negative impact on the relationship with other parts of the public authority, other organisations, or public relations but it may only have nation-wide or temporary international negative impacts.	It can cause financial losses exceeding 5% but not higher than 10% of the normal annual expenditures of the public authority's budget, where these losses amount to CZK 1,000,000.00 or more, or can cause economic losses to the state amounting to 0.1% to 0.5% of the gross domestic product. If the financial loss equals an amount lower than CZK 1,000,000.00, the medium impact level applies.	It can cause a limitation, breach or unavailability of services provided for more than 50,000 people.
4. Critical	It can cause injuries of a group of more than 2,500 people or direct threat to or loss of lives of a group of more than 250 people.	It can cause limitation to or prejudice processing personal data which are necessary to ensure the security or defence policy interests of the Czech Republic.	It can severely undermine the long-term ability to investigate crime or challenge court proceedings within law enforcement authorities.	An element of a critical infrastructure operated by a public authority which classifies the enquired cloud computing within the security level can be affected, and it can cause mass disturbance or otherwise severely prejudice public order with nation-wide impacts.	It can have a negative impact on or damage the diplomatic relationships of the Czech Republic.	An element of a critical infrastructure operated by a public authority which classifies the enquired cloud computing within the security level can be affected, and it can prejudice the proper functioning of a part or the whole public authority, whereby it can significantly limit or stop the performance of important activities of the public authority and prejudice the management, damage the development, or harm the pursuit of the objectives and interests of the public authority.	An element of a critical infrastructure operated by a public authority which classifies the enquired cloud computing within the security level can be affected, and it can have a negative impact on the relationship with other parts of the public authority, other organisations or public relations and it can have long-term international consequences.	It can cause financial losses exceeding 10% of the normal annual expenditures of the public authority's budget, where these losses amount to CZK 10,000,000.00 or more, or can cause economic losses to the state amounting to more than 0.5% of the gross domestic product. If the financial loss equals an amount lower than CZK 10,000,000.00, the high impact level applies.	An element of a critical infrastructure operated by a public authority which classifies the enquired cloud computing within the security level can be affected, and it can cause an extensive limitation of provision of necessary service or other serious interference with their daily way of life more affecting more than 125,000 people.

Criterion groups for the impact area B. Protection of personal data

(1) The first criterion group comprises the following criteria:

a) Personal data are processed that enable without any further to represent or act on behalf of the data subject in contexts meaning damage to honour, reputation or character or enabling subscribe to services or goods or withdraw money or other assets on an account of the data subject;

b) Personal data are processed based on which the data subject is classifiable as a member of group with a time-limited or context-based vulnerability;

c) Processing of personal data which affects, or for which can be reasonably assumed that it will affect, 5,000 to 10,000 data subjects;

d) Personal data are publicly available to an unlimited number of bodies or persons, and

e) The personal data are processed by a system interconnected with other processing performed by the same administrator of personal data, or the personal data have been obtained from other administrators of personal data.

(2) The second criterion group comprises the following criteria:

a) Special categories of personal data or data of highly personal nature are processed, particularly financial data relating to the assets, amount of funds, debts or loans, or the payment behaviour, records of history of private calls of the data subjects, information from e-mail of the data subjects, etc.;

b) Processing of personal data which affects, or for which can be reasonably assumed that it will affect, more than 10,000 data subjects; and

c) The decisions affecting the data subject are automated.