

DECREE

of 24 August 2021

on some requirements for incorporation into the cloud computing catalogue

Pursuant to the provisions of Section 12 paragraph 2 of Act No. 365/2000 Coll., on Public Authority Information Systems and on the Amendment to Related Acts, as amended by Act No. 261/2021 Coll., (hereinafter referred to as the “Act”), the National Cyber and Information Security Agency establishes as follows:

Section 1

Subject of the Decree

This Decree establishes

- a) Requirements for the eligibility of a cloud computing provider (hereinafter referred to as the “Provider”) to ensure a basic level of confidentiality protection, integrity, and availability of information for a public authority under Section 6m paragraph 1(a) of the Act;
- b) Requirements for achieving the basic level of confidentiality protection, integrity, and availability of information by the cloud computing offered to a public administration body under Section 6n(b) of the Act;
- c) A list of certifications and audits for the area of confidentiality protection, integrity, and availability of information under Section 6q paragraph 5(c), Section 6t paragraph 6(b), and Section 6t paragraph 7(c) of the Act, proofs of compliance therewith, and intervals for the submission of those proofs under Section 6y paragraph 2 of the Act;
- d) Requirements for the structure and requisites of the report on the execution of penetration test under Section 6t paragraph 6(d) and Section 6t paragraph 7(e) of the Act and the intervals for the submission thereof;
- e) Requirements for the audit report requisites proving the existence of a plan to ensure the continuity of operation of the offered cloud computing and a plan for a re-establishment of the provision of the offered cloud computing after an accident under Section 6t paragraph 6(e) and Section 6t paragraph 7(f) of the Act;
- f) Requirements for the structure and requisites of proof of assessment of risk sources under Section 6t paragraph 6(f) and Section 6t paragraph 7(g) of the Act; and
- g) Requirements for the structure and requisites of materials for verification of the compliance with the requirement for ensuring of confidentiality, integrity, and availability of information under Section 6t paragraph 6(g) and Section 6t paragraph 7(h) 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) Customer is a public administration that uses a cloud computing service;
- b) User is the one who uses or sets a cloud computing service through public administration system;
- c) Customer data are all data that the user provides to the provider throughout the use of the cloud computing service;

- d) Customer content is text, voice, audiovisual, picture or other data which the user entered into the cloud computing service but without their metadata and the indexes to the data;
- e) Operational data are the data generated or operational by the provider in connection with the provision of the cloud computing service;
- f) Specific operational data are such operational data that contain information about an identified or identifiable user;
- g) Processing means any operation or set of operations which are performed on customer data or operational data, whether or not by automated means, such as acquisition, recording, organising, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, spreading or otherwise making available, alignment or combination, restriction, erasing or destruction;
- h) Security levels of the offered cloud computing is such a level within which the provider classifies the offered cloud computing.

Section 3

Requirements for eligibility to ensure the basic level of confidentiality protection, integrity, and availability of information for a public authority

Provider eligible to ensure the basic level of confidentiality protection, integrity, and availability of information for a public authority under Section 6m paragraph 1(a) of the Act is such a provider who meets the requirements for eligibility to ensure the basic level of confidentiality protection, integrity, and availability of information for a public authority mentioned in Annex No. 1 to this Decree corresponding with the security level of the offered cloud computing within which the provider requests the cloud computing service to be incorporated in the cloud computing catalogue, and the cloud computing class¹⁾ within which the cloud computing service is classified.

Section 4

Requirements for the basic level of confidentiality protection, integrity, and availability of information for a public authority to be achieved by the offered cloud computing

Cloud computing which enables the achievement of at least a basic level of confidentiality protection, integrity, and availability of information for a public authority under Section 6n of the Act is a cloud computing that meets requirements for achieving the basic level of confidentiality protection, integrity, and availability of information for a public authority by the offered cloud computing mentioned in Annex No. 2 to this Decree corresponding with the security level of the offered cloud computing within which the provider requests the cloud computing service to be incorporated in the cloud computing catalogue, and the cloud computing class, and the cloud computing class within which the cloud computing service is classified.

Section 5

List of certifications and audits for the area of confidentiality protection, integrity, and availability of information, proofs of compliance therewith, and intervals for the submission of those proofs

A list of certifications and audits for the area of confidentiality protection, integrity, and availability of information under Section 6q paragraph 5(c), Section 6t paragraph 6(b), and Section 6t paragraph 7(c) of the Act, proofs of compliance therewith, and intervals for the

¹⁾ Section 2(a) of Decree No. 433/2020 Coll., On data kept in the cloud computing catalogue.

submission of those proofs under Section 6y paragraph 2 of the Act are stipulated in Annex No. 3 to this Decree.

Section 6

Requirements for the structure and requisites of the report on the execution of penetration test and the intervals for the submission thereof

Requirements for the structure and requisites of the report on the execution of penetration test under Section 6t paragraph 6(d) and Section 6t paragraph 7(e) of the Act and the intervals for the submission thereof are stipulated in Annex No. 4 to this Decree.

Section 7

Requirements for the audit report requisites proving the existence of a plan to ensure the continuity of operation of the offered cloud computing and a plan for a re-establishment of the provision of the offered cloud computing after an accident

(1) An audit report proving the existence of a plan to ensure the continuity of operation of the offered cloud computing and a plan for a re-establishment of the provision of the offered cloud computing after an accident means an audit report prepared by a subject independent of the provider proving the existence of a plan to ensure the continuity of operation of the offered cloud computing and a plan for a re-establishment of the provision of the offered cloud computing after an accident, and attests that its application has been verified.

(2) The audit report issued for the purpose of certification ČSN ISO/IEC 20000, ISO/IEC 20000, ČSN EN ISO 22301, ISO 22301, SOC 2® Type 2 or the attestation according to CSA STAR Level 2 shall be deemed to fulfil the characteristics of the audit report pursuant to the provisions of paragraph 1. The scope of the given audit report must include the offered cloud computing service.

Section 8

Requirements for the structure and requisites of proof of assessment of risk sources

Requirements for the structure and requisites of proof of assessment of risk sources under Section 6t paragraph 6(f) and Section 6t paragraph 7(g) of the Act are laid down in Annex No. 5 to this Decree.

Section 9

Requirements for the structure and requisites of materials for verification of the compliance with the requirement for ensuring confidentiality, integrity, and availability of information

(1) The structure of the materials for verification of compliance with the requirements pursuant to the provisions of Sections 3 and 4 must be clear and easily comprehensible. To ensure that the material is clear and easily comprehensible, the provider shall describe and prove the compliance with the requirements according to Section 4 for every single cloud computing service whose incorporation in the cloud computing catalogue it is requesting. If more services belonging to the same security level of the offered cloud computing and the same cloud computing class meet the requirement pursuant to the provisions of Section 4 in the same way, a single proof may be provided to prove the compliance with such a requirement, clearly stating all the cloud computing services to which the proof applies.

(2) The materials for verification of the compliance with the requirements pursuant to the provisions of Sections 3 and 4 comprise

- a) An identification of the provider under Section 37 paragraph 2 of the Code of Administrative Procedure;
- b) A description of fulfilment of each requirement for each cloud computing service which the provider requests to be incorporated in the cloud computing catalogue, or a description of the fact by which the provider proves compliance with the requirement in Annexes Nos. 1 and 2 to this Decree in column “Material by which the provider proves compliance with the requirement”; and
- c) Materials by which the provider proves compliance with the requirement under Annexes Nos. 1 and 2 to this Decree.

(3) The provider shall prove the requisites pursuant to the provisions of paragraph 2(a) and (b) using an electronic form published on the website of the National Cyber and Information Security Agency.

(4) If proving the compliance with the requirements under Sections 3 and 4 requires a reference to another document attached to the form, the reference shall be done in the form by stating the chapter, page, paragraph and possibly also the specific sentence.

(5) Both the form and the enclosures shall be filed in the electronic form, in machine-readable format ensuring the permanence of the content of the individual documents.

(6) If the compliance with any of the requirements under Sections 3 and 4 is evidenced by a solemn declaration, it must be clear from it who makes it and when and what is evidenced by it. In the event that the solemn declaration is made by a person different from the provider, the application for registration of the cloud computing offer in the cloud computing catalogue shall also be accompanied by a document authorizing this person to this solemn declaration.

Section 10 **Transitional provisions**

Compliance with the requirements mentioned in lines 7.8, 7.9, and 8.7 of Annex No. 2 to this Decree are applicable as of 1 January 2024.

Section 11 **Effect**

This Decree shall become effective on the day following the day of its publishing.

Director:
Ing. **Řehka** m.p.

Line	Requirements for the eligibility to ensure the basic level of confidentiality protection, integrity, and availability of information for the public authority	Document by which the provider proves the compliance with the requirement	Security level of the offered cloud computing				Cloud computing class		
			Low	Medium	High	Critical	cloud computing as an infrastructure	cloud computing as a platform	cloud computing as an application software
1	The provider has its registered office or place of residence in a Member State of the European Union or has a designated representative in a Member State of the European Union by analogy in accordance with Article 27 of the General Data Protection Regulation ²⁾ .	A certificate of incorporation or similar foreign records, or a written solemn declaration to the extent of the data contained in the Commercial Register if it is not entered in the Commercial Register; if the provider is registered in a public register in accordance with the law governing public registers of legal and natural persons, no document is required.	X ³⁾	X	X	X	X	X	X
2	Neither the provider nor its controlling persons ⁴⁾ have been convicted in the last 5 years of committing an offence for which they were fined at least CZK 1,000,000.00	Information from internal systems of the National Cyber and Information Security Agency. No material is required.	X	X	X	X	X	X	X

²⁾ Regulation (EC) No. 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of individuals 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).

³⁾ The symbol “X” indicates the existence of an obligation to meet the requirements in the specified security level of the offered cloud computing and cloud computing class.

⁴⁾ Section 74 of Act No. 90/2012 Coll., on Business Corporations and Cooperatives (the Act on Business Corporations) as amended.

	<p>consisting in failure to implement or perform a security measure pursuant to the Act on Cyber Security.</p> <p>Neither the provider nor its controlling persons⁴⁾ have been convicted in the last 5 years of committing an offence for which they were fined at least CZK 500,000.00 consisting in failure to</p> <ul style="list-style-type: none">a) Submit data, operational data, and information pursuant to Section 6a paragraph 2 of the Act on Cyber Security;b) Submit data, operational data, and information pursuant to Section 6a paragraph 3 of the Act on Cyber Security;c) Destroy copies of data, operational data, and information pursuant to Section 6a paragraph 3 of the Act on Cyber Security;d) Detect a cybersecurity event pursuant to Section 7 paragraph 3 of the Act on Cyber Security;								
--	---	--	--	--	--	--	--	--	--

<p>e) Report a cybersecurity incident pursuant to Section 8 paragraphs 1 through 4 of the Act on Cyber Security</p> <p>f) fulfil obligations imposed by the National Cyber and Information Security Agency pursuant to Section 13 or Section 14 of the Act on Cyber Security;</p> <p>g) fulfil obligations imposed by the National Cyber and Information Security Agency pursuant to Section 15a paragraph 1 of the Act on Cyber Security;</p> <p>h) fulfil obligations imposed by corrective measure pursuant to Section 24 of the Act on Cyber Security;</p> <p>i) introduce or perform a security measure pursuant to Section 4 paragraph 3 of the Act on Cyber Security;</p> <p>Neither the provider nor its controlling persons have been convicted in the last 5 years of committing an offence under the Act on Inspection (Inspection</p>								
---	--	--	--	--	--	--	--	--

	Code) in connection with the control of compliance with obligations under the Cyber Security Act, for which they were fined at least CZK 150,000.00 consisting in failure to fulfil any of the obligations under Section 10 paragraph 2 or Section 10 paragraph 3 of the Act on Inspection.								
--	---	--	--	--	--	--	--	--	--

non-binding English translation

Line	Requirements for the basic level of confidentiality protection, integrity, and availability of information for a public authority to be achieved by the offered cloud computing	Document by which the provider proves compliance with the requirement	Security level of the offered cloud computing				Cloud computing class		
			Low	Medium	High	Critical	cloud computing as an infrastructure	cloud computing as a platform	cloud computing as an application software
1. Place of data processing and storing									
1.1	The provider shall provide information on all territories of countries in which customer data at rest state and specific operational data at rest are or may be stored, and shall also provide information on all territories outside the Member States of the European Union and the European Free Trade Association Member States in which it presupposes the processing of customer data and specific operational data.	<p>A written description indicating in which territories of states customer data at rest and specific operational data at rest are or may be stored and in which states outside the territory of the Member States of the European Union and the Member States of the European Free Trade Association the processing of customer data is assumed to take place and in which territories of states the processing of specific operational data is assumed to take place.</p> <p>The presumed territories of the states in which the processing of customer data or specific operational data takes place or may take</p>	X	X			X	X	X

		<p>place shall not be deemed to be:</p> <ul style="list-style-type: none">- territories of states from which technical support personnel of the cloud computing provider may connect remotely on an irregular basis to provide technical support for a cloud computing service that changes over time and cannot be specified in advance;- territories of the states to which the provider may disclose customer data or specific operational data for the provision of an optional service involving a third party							
--	--	--	--	--	--	--	--	--	--

		<p>which is not cloud computing per se, activated at the customer's choice, with the provider clearly identifying the third party to which it may disclose customer data or specific operational data and, if possible, specifying which customer data or specific operational data it normally discloses and for what estimated time it discloses customer data or specific operational data.</p>							
1.2	The provider provides information about all territories of the states from which the administration and supervision of the cloud computing service are performed.	A written description indicating from which territory of the states the administration and supervision of the cloud computing service are performed.	X	X	X	X	X	X	X

1.3	<p>Customer data at rest are stored continuously and exclusively in the territory of the Member States of the European Union and the Member States of the European Free Trade Association.</p> <p>If the cloud computing service does not meet the respective requirement, the provider clearly identifies such service and indicates whether such cloud computing service stores customer data at rest in pseudonymised form or non-pseudonymised form.</p> <p>The provider states the storage location of customer data at rest.</p> <p>Based on the designation of the cloud computing service as a cloud computing service that does not meet the requirement for storing customer at rest continuously and exclusively in the territory of the Member States of the European Union and the European Free Trade Association, this cloud computing service will be listed on the website of the National Cyber and Information Security Agency and the requirement in question does not apply to it. Such a cloud computing service will also be referred to in the cloud computing catalogue as a cloud computing service listed under that exception by citing that exception.</p>	<p>Reference to the part of the contract terms and conditions which defines the obligation to store customer data at rest continuously and exclusively in the territory of the Member States of the European Union and the European Free Trade Association,</p> <p>or where the requirement to store customer data at rest continuously and exclusively in the territory of the Member States of the European Union and the European Free Trade Association does not apply to the service, a clear indication of such service and a reference to the part of the contract terms and conditions which defines the obligation to store customer at rest in a pseudonymised form,</p> <p>or where the requirement to store customer data at rest continuously and exclusively in the territory of the Member</p>			X	X	X	X	X
-----	---	---	--	--	---	---	---	---	---

		<p>States of the European Union and the European Free Trade Association does not apply to the service and such a service stores customer data at rest in non-pseudonymised form, a clear designation of such a service.</p> <p>Furthermore, the provider documents a reference to that part of the valid certification ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 or ISO/IEC 27001 by a certification body accredited for the certification of information security management systems by one of the members of the International Accreditation Forum (IAF) or audit report SOC 2 ® Type 2, with reference to the part from which a complete list of data centres and their location to the level of the cadastral area/municipality in which the customer data will be stored as data at rest will be clear, indicating whether or not they are stored in the</p>							
--	--	--	--	--	--	--	--	--	--

		data centre in pseudonymised form.							
1.4	<p>Specific operational data are stored as a data at rest continuously and exclusively in the territory of the Member States of the European Union and the Member States of the European Free Trade Association.</p> <p>If the cloud computing service does not meet the respective requirement, the provider clearly identifies such service and indicates whether such cloud computing service stores specific operational data at rest in pseudonymised form or non-pseudonymised form.</p> <p>The provider states the storage location of specific operational data at rest.</p> <p>Based on the designation of the cloud computing service as a cloud computing service that does not meet the requirement for storing specific operational data data rest state continuously and exclusively in the territory of the Member States of the European Union and the European Free Trade Association, this cloud computing service will be listed on the website of the National Cyber and Information Security Agency and the requirement in question does not apply to it. Such a cloud computing</p>	<p>A reference to the part of the contract terms and conditions which defines the obligation to store specific operational data at rest continuously and exclusively in the territory of the Member States of the European Union and the European Free Trade Association,</p> <p>or where the requirement to store specific operational data at rest continuously and exclusively in the territory of the Member States of the European Union and the European Free Trade Association does not apply to the service, a clear indication of such service and a reference to the part of the contract terms and conditions which</p>			X	X	X	X	

	<p>service will also be referred to in the cloud computing catalogue as a cloud computing service listed under that exception by citing that exception.</p>	<p>defines the obligation to store specific operational data at rest in a pseudonymised form,</p> <p>or where the requirement to store specific operational data at rest continuously and exclusively in the territory of the Member States of the European Union and the European Free Trade Association does not apply to the service and such a service stores specific operational data at rest in non-pseudonymised form, a clear designation of such a service.</p> <p>Furthermore, the provider documents a reference to that part of the valid certification ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 or ISO/IEC 27001 by a certification body accredited for the certification of information security management systems by one of the members of the International</p>							
--	---	---	--	--	--	--	--	--	--

		Accreditation Forum (IAF) or audit report SOC 2 ® Type 2, with reference to the part from which a complete list of data centres and their location to the level of the cadastral area / municipality in which the specific operational data will be stored as data at rest will be clear, indicating whether or not they are stored in the data centre in pseudonymised form.							
1.5	Customer data are processed in the territory of the Member States of the European Union and the Member States of the European Free Trade Association. Without prejudice to the requirements set out in line 1.3 of Annex 2 to this Decree, in justified cases, for the necessary time and to the necessary extent, customer data may also be processed in the territory other states supposing that the provider describes how the customer data will be protected from information security breaches.	<p>1. The provider shall state for the cloud computing service</p> <p>a) which only processes customer data in the territory of the Member States of the European Union and the Member States of the European Free Trade Association:</p> <p>- clear identification of such cloud</p>			X		X	X	X

		<p>computing service and</p> <ul style="list-style-type: none">- a declaration of the obligation to process customer data in the territory of the Member States of the European Union and the Member States of the European Free Trade Association,b) which only processes customer content in the territory of the Member States of the European Union and the Member States of the European Free Trade Association and which processes or may process customer data without customer content outside the territory of							
--	--	--	--	--	--	--	--	--	--

		<p>the Member States of the European Union and the Member States of the European Free Trade Association:</p> <ul style="list-style-type: none">- clear identification of such cloud computing service,- information on the intended state territory where the processing of customer data without customer content takes place or may take place, and information on the expected duration, expected extent and intended purpose of the processing of customer data without customer content in the relevant intended state							
--	--	--	--	--	--	--	--	--	--

		<p>territory, and stating whether or not the customer data without customer content are pseudonymised in the case of such processing. For customer data without customer content processed outside the territory of the Member States of the European Union and the Member States of the European Free Trade Association, a description of how they will be protected within the meaning of Chapter V of the General Data Protection Regulation,</p> <p>c) which processes or</p>						
--	--	---	--	--	--	--	--	--

		<p>may process customer data outside the territory of the Member States of the European Union and the Member States of the European Free Trade Association,</p> <ul style="list-style-type: none">- clear identification of such cloud computing service,- information on the intended state territory where the processing of customer data takes place or may take place, and information on the expected duration, expected extent and intended purpose of the processing of customer data in the relevant intended state territory and						
--	--	---	--	--	--	--	--	--

		<p>stating whether or not the customer data are pseudonymised in the case of such processing. For customer data processed outside the territory of the Member States of the European Union and the Member States of the European Free Trade Association, a description of how they will be protected at least within the meaning of Chapter V of the General Data Protection Regulation.</p> <p>2. The presumed territories of the states in which the processing of customer data takes place or may take</p>							
--	--	--	--	--	--	--	--	--	--

		<p>place shall not be deemed to be:</p> <ul style="list-style-type: none">- territories of states from which technical support personnel of the cloud computing provider may connect remotely on an irregular basis to provide technical support for a cloud computing service that changes over time and cannot be specified in advance;- territories of the states to which the provider may disclose customer data for the provision of an optional service involving a third party which is not cloud							
--	--	--	--	--	--	--	--	--	--

		<p>computing per se, activated at the customer's choice, with the provider clearly identifying the third party to which it may disclose customer data and, if possible, specifying which customer data it normally discloses and for what estimated time it discloses the customer data.</p>							
1.6	<p>Specific operational data are processed in the territory of the Member States of the European Union and the Member States of the European Free Trade Association. Without prejudice to the requirements set out in line 1.4 of Annex 2 to this Decree, in justified cases, for the necessary time and to the necessary extent, specific operational data may also be processed in the territory of other states supposing that the provider describes how the specific operational data will be protected from information security breaches.</p>	<p>1. The provider shall state for the cloud computing service</p> <p>a) which only processes specific operational data in the territory of the Member States of the European Union and the Member States of the</p>			X		X	X	X

		<p>European Free Trade Association:</p> <ul style="list-style-type: none">- clear identification of such cloud computing service and- a declaration of the obligation to process specific operational data in the territory of the Member States of the European Union and the Member States of the European Free Trade Association, <p>b) which processes or may process specific operational data outside the territory of the Member States of the European Union and the Member States</p>							
--	--	---	--	--	--	--	--	--	--

		<p>of the European Free Trade Association:</p> <ul style="list-style-type: none">- clear identification of such cloud computing service,- information on the intended state territory where the processing of specific operational data takes place or may take place, and information on the expected duration, expected extent and intended purpose of the processing of specific operational data in the relevant intended state territory, and stating whether or not the specific operational data are pseudonymised							
--	--	--	--	--	--	--	--	--	--

		<p>in the case of such processing. For specific operational data processed outside the territory of the Member States of the European Union and the Member States of the European Free Trade Association, a description of how they will be protected at least within the meaning of Chapter V of the General Data Protection Regulation.</p> <p>2. The presumed territories of the states in which the processing of specific operational data takes place or may take place shall not be deemed to be:</p>							
--	--	--	--	--	--	--	--	--	--

		<ul style="list-style-type: none">- territories of states from which technical support personnel of the cloud computing provider may connect remotely on an irregular basis to provide technical support for a cloud computing service that changes over time and cannot be specified in advance;- territories of the states to which the provider may disclose specific operational data for the provision of an optional service involving a third party which is not cloud computing per se, activated at							
--	--	---	--	--	--	--	--	--	--

		<p>the customer's choice, with the provider clearly identifying the third party to which it may disclose specific operational data and, if possible, specifying which specific operational data it normally discloses and for what estimated time it discloses the specific operational data.</p>							
1.7	<p>The provider requires the customer's consent for cases of processing customer data outside the territory of the Member States of the European Union and the Member States of the European Free Trade Association, which is expressed in a separate document containing information on the intended territory of the state where the customer data processing takes place or may take place.</p> <p>The provider informs the customer about the expected duration, expected extent and intended purpose of processing customer</p>	<p>A document separate from the terms of service or contract, or a reference to the clearly stated text of the contractual documentation requiring the customer's consent for cases of customer data processing outside the territory of the Member States of the European Union and the European Free Trade Association containing</p>			X		X	X	X

	<p>data in the relevant intended state territory and whether or not the customer data are pseudonymised in the case of such processing.</p> <p>Alternatively to requiring consent and informing the customer, the provider requires customer consent for customer data processing cases in each individual case of customer data processing outside the territory of the Member States of the European Union and the European Free Trade Association in the basic settings of the cloud computing service.</p>	<p>information about the intended state territory in which the customer data processing takes place or may take place,</p> <p>or a reference to a specific part of the terms of service or a part of the draft contract documentation or product specification showing that the provider requires customer consent in each individual case of processing customer data outside the territory of the Member States of the European Union and the European Free Trade Association in the basic settings of the service.</p>							
1.8	<p>Customer data and specific operational data are processed in the territory of the Czech Republic. Without prejudice to the requirements set out in line 6.6 of Annex 2 to this Decree, in justified cases, for the necessary time and to the necessary extent, customer data and specific operational data may also be processed outside the territory of the Czech Republic supposing that the provider describes how the customer data will be protected from information security breaches</p> <p>and only with the explicit written consent of the customer expressed in a separate</p>	<p>A reference to the specific part of the terms of cloud computing service or a part of the draft contract showing the obligation to only process customer data and specific operational data in the territory of the Czech Republic, and also a reference to that part of the valid certification ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 or</p>				X	X	X	X

	<p>document that contains information about the intended territory of the state in which the customer data are or may be processed and information about the expected duration, expected extent and intended purpose of processing customer data in the relevant intended state territory and indicating whether or not the customer data are pseudonymised in the case of such processing,</p> <p>Or only if the provider requires customer consent in each individual case of processing customer data and specific operational data outside the territory of the Czech Republic.</p>	<p>ISO/IEC 27001 by a certification body accredited for the certification of information security management systems by one of the members of the International Accreditation Forum (IAF) or audit report SOC 2 ® Type 2 showing a complete list of data centres and their location to the level of the cadastral area / municipality in which the customer data and specific operational data will be stored.</p> <p>For a cloud computing service that processes or may process customer data and specific operational data outside the territory of the Czech Republic, the provider shall clearly designate such service and provide information about the assumed territory of the state where customer data and specific operational data are or may be processed, and information about the expected duration, expected extent and</p>							
--	---	---	--	--	--	--	--	--	--

		<p>intended purpose of the processing of customer data and specific operational data in the relevant intended state territory, and indicating whether or not the customer data and specific operational data are pseudonymised in the case of such processing.</p> <p>For a cloud computing service that processes or may process customer data and specific operational data outside the territory of the Czech Republic, the provider shall provide A document separate from the terms of service or contract, or a reference to a clearly stated text of the contractual documentation requiring the customer's consent for cases of customer data processing outside the territory of the Czech Republic, which contain information about the assumed state territory in which customer data are or may be processed, and information about the expected duration,</p>							
--	--	--	--	--	--	--	--	--	--

		<p>expected extent and intended purpose of processing customer data in the relevant intended state territory, and indicating whether or not the customer data are pseudonymised in the case of such processing,</p> <p>or a reference to a specific part of the terms of service or a part of the draft contract documentation or product specification showing that the provider requires customer consent in each individual case of processing customer data outside the territory of the Czech Republic.</p>							
2. Applications for access to and disclosure of data									
2.1	<p>If the provider receives a legally binding request for access to or disclosure of customer data and specific operational data from a foreign authority, it does not comply with this request and refers the requester to the customer or informs the customer about such a request without delay, unless the law to which the provider is subject prohibits the to do so.</p>	<p>A solemn declaration or a reference to the part of the draft contract, a specific part of the terms and conditions for the provision of a cloud computing service or another description of the cloud computing service showing that if the provider receives a legally binding request</p>	X	X			X	X	X

		<p>for access to or disclosure of customer data and specific operational data from a foreign authority, it refers this requester to the customer or informs the customer of such a request without delay,</p> <p>or an audit report issued for the purposes of the certification ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 or ISO/IEC 27001 by a certification body accredited for the certification of information security management systems by one of the members of the International Accreditation Forum (IAF) or audit report SOC 2 ® Type 2 with reference to the part showing that if the provider receives a legally binding request from a foreign authority for access to or disclosure of customer data and specific operational data, it refers the requester to the customer or informs the customer about such a request without delay.</p>							
--	--	--	--	--	--	--	--	--	--

2.2	<p>If the provider receives a legally binding request for access to or disclosure of customer data and specific operational data from a foreign authority, it refers the requester to the customer or informs the customer about such a request without delay. If the law to which the provider is subject prohibits the provider to inform the customer, it shall make every possible legal effort to obtain the lifting of this prohibition and use all available remedies to challenge such prohibition or to suspend the effects of the prohibition until the court decides on the substance. If the provider does not obtain the lifting of the prohibition to inform the customer, then the provider informs the customer after the expiry of the legal prohibition, e.g. after the expiration of the non-disclosure period ordered by law or court.</p>	<p>A solemn declaration or a reference to a part of the draft contract, a specific part of the terms and conditions for providing a cloud computing service or another description of the cloud computing service showing that if the provider receives a legally binding request for access to or disclosure of customer data and specific operational data from a foreign authority, it does not comply with this request and refers the requester to the customer or informs the customer of such a request without delay, or if the law to which the provider is subject prohibits the provider from informing the customer, the provider makes all possible legal efforts to obtain the lifting of this prohibition and uses all available remedies to challenge such a prohibition, or to suspend the effects of the prohibition until the court decides on the substance, and if the provider does not obtain</p>			X	X	X	X	X
-----	--	--	--	--	---	---	---	---	---

		<p>the lifting of the prohibition to inform the customer, then the provider informs the customer after the expiry of the legal prohibition, e.g. after the expiration of the non-disclosure period ordered by law or court.</p> <p>Or an audit report issued for the certification ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 or ISO/IEC 27001 by a certification body that has been accredited to carry out audits and certification of information security management systems by a member of the International Accreditation Forum (IAF), or audit report SOC 2® Type 2, with reference to the part showing that if the provider receives a legally binding request for access to or disclosure of customer data and specific operational data from a foreign authority, it does not comply with this request and refers the requester to the</p>						
--	--	--	--	--	--	--	--	--

		customer or informs the customer of such a request without delay, or if the law to which the provider is subject prohibits the provider from informing the customer, the provider makes all possible legal efforts to obtain the lifting of this prohibition and uses all available remedies to challenge such a prohibition, or to suspend the effects of the prohibition until the court decides on the substance, and if the provider does not obtain the lifting of the prohibition to inform the customer, then the provider informs the customer after the expiry of the legal prohibition, e.g. after the expiration of the non-disclosure period ordered by law or court.							
2.3	If the provider receives a request for access to or disclosure of customer data and specific operational data from a foreign authority, it shall review the legality of such request, particularly making a legal assessment to determine whether the request from the foreign authority has a feasible, applicable and valid legal basis, is legally binding and the scope of the customer data and specific operational data provided or	A solemn declaration or a reference to part of the draft contract, a specific part of the terms and conditions of the cloud computing service or another description of the cloud computing service showing that the provider will review the	X	X			X	X	X

	<p>made available is proportionate to the purpose of the request. The provider undertakes to disclose customer data and specific operational data to a foreign authority only if the legal assessment indicates that the foreign authority's request has a feasible, applicable and valid legal basis, is legally binding, and the scope of customer data and specific operational data provided or made available is proportionate to the purpose of the request.</p> <p>The provider shall make a record of the documents used for the assessment, which it shall keep for the purposes of inspection for at least 5 years or provably hand over to the customer.</p>	<p>legality of foreign authorities' requests for disclosure, particularly making a legal assessment to determine whether the foreign authority's request has a feasible, applicable and valid legal basis, is legally binding, and the scope of customer data and specific operational data provided or made available is proportionate to the purpose of the request, and the provider shall only disclose customer data and specific operational data to a foreign authority if the legal assessment proves that the foreign authority's request has a feasible, applicable and valid legal basis, is legally binding, and the scope of customer data and specific operational data provided or made available is proportionate to the purpose of the request,</p> <p>or an audit report issued for the certification ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 or ISO/IEC 27001 by a</p>							
--	---	--	--	--	--	--	--	--	--

		<p>certification body that has been accredited to carry out audits and certification of information security management systems by a member of the International Accreditation Forum (IAF), or audit report SOC 2® Type 2, with a reference made to the part showing that the provider will review the legality of foreign authorities' requests for disclosure, particularly making a legal assessment to determine whether the foreign authority's request has a feasible and valid legal basis, is legally binding, and the scope of customer data and specific operational data provided or made available is proportionate to the purpose of the request, and the provider shall only disclose customer data and specific operational data to a foreign authority if the legal assessment proves that the foreign authority's request has a feasible, applicable and</p>							
--	--	---	--	--	--	--	--	--	--

		valid legal basis, is legally binding, and the scope of customer data and specific operational data provided or made available is proportionate to the purpose of the request.							
2.4	<p>If the provider receives a request for access to or disclosure of customer data and specific operational data from a foreign authority, it shall review the legality of such request, particularly making a legal assessment to determine whether the request from the foreign authority has a feasible and valid legal basis, is legally binding and the extent of customer data and specific operational data provided or made available is proportionate to the purpose of the request, and shall make all possible legal efforts to prevent the disclosure or transfer of customer data and specific operational data requested by a foreign authority without the customer's consent, particularly taking into account legal requirements and obligations under the legislation of the European Union and the Czech Republic, and will seek to abolish the obligation to make available or disclose customer data and specific operational data.</p> <p>The provider shall make a record of the documents used for the assessment, which it shall keep for the purposes of inspection for at least 10 years or provably hand over to the customer.</p>	<p>A solemn declaration or a reference to part of the draft contract, a specific part of the terms and conditions of the cloud computing service or another description of the cloud computing service showing that the provider will review the legality of foreign authorities' requests for disclosure, particularly making a legal assessment to determine whether the foreign authority's request has a feasible and valid legal basis, is legally binding, and the extent of the customer data and specific operational data provided or made available is proportionate to the purpose of the request, and shall make all possible legal efforts to prevent the disclosure or transfer of customer data and specific</p>			X	X	X	X	

		<p>operational data requested by a foreign authority without the customer's consent, particularly taking into account legal requirements and obligations under the legislation of the European Union and the Czech Republic, and will seek to abolish the obligation to make available or disclose customer data and specific operational data,</p> <p>or an audit report issued for the certification ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 or ISO/IEC 27001 by a certification body that has been accredited to carry out audits and certification of information security management systems by a member of the International Accreditation Forum (IAF), or audit report SOC 2® Type 2, with a reference made to the part showing that the provider will review the legality of foreign authorities' requests for</p>							
--	--	---	--	--	--	--	--	--	--

		disclosure, particularly making a legal assessment to determine whether the foreign authority's request has a feasible and valid legal basis, is legally binding, and the scope of the customer data and specific operational data provided or made available is proportionate to the purpose of the request, and shall make all possible legal efforts to prevent the disclosure or transfer of customer data and specific operational data requested by a foreign authority without the customer's consent, particularly taking into account legal requirements and obligations under the legislation of the European Union and the Czech Republic, and will seek to abolish the obligation to make available or disclose customer data and specific operational data.							
2.5	The provider clearly and comprehensibly states his obligations arising from the legislation of countries other than the	A written description of the obligations arising from the legislation of	X	X	X	X	X	X	X

	Member States of the European Union, in which the provider assumes the processing of customer data according to lines 1.1, 1.5, and 1.6 of Annex 2 to this Decree concerning access to and disclosure of customer data and specific operational data.	countries other than the Member States of the European Union, in which the provider assumes the processing of customer data according to lines 1.1, 1.5, and 1.6 of Annex 2 to this Decree concerning access to and disclosure of customer data and specific operational data. The written description must be of such quality that it is possible for the customer to assess the suitability of the legal system with regard to the processing of customer data and specific operational data.							
2.6	If the provider receives a request for access to or disclosure of customer data and specific operational data from a foreign authority, it shall reject this request and shall not disclose the data nor make them available.	A solemn declaration or a reference to a part of the draft contract, a specific part of the terms and conditions for the provision of a cloud computing service or another description of the cloud computing service indicating that if the provider receives a request for access to or disclosure of customer data and specific operational data from a				X	X	X	X

		<p>foreign authority, the provider will reject the request and will not disclose the data nor will make them available,</p> <p>or an audit report issued for the certification ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 or ISO/IEC 27001 by a certification body that has been accredited to carry out audits and certification of information security management systems by a member of the International Accreditation Forum (IAF), or audit report SOC 2® Type 2, with a reference made to the part showing that the provider, if it receives a request for access to or disclosure of customer data and specific operational data from a foreign authority, will reject the request and will not disclose the data nor will make them available.</p>							
--	--	---	--	--	--	--	--	--	--

3. Authorisation to perform the inspection									
3.1	Once a year, or on the basis of recurring cybersecurity incidents, or in case of conflict with declared parameters, the provider shall allow the Ministry of the Interior or the National Cyber and Information Security Agency to perform compliance checks pursuant to Section 6i paragraphs 2 and 3 of the Act on Information Systems of Public Administration and according to the Act on Inspection in relation to the given cloud computing service free of charge at all places and facilities related to the provision of cloud computing services, and at the same time provide all cooperation required by these authorities, except for access to or disclosure of customer data without the consent of the respective customer.	No material is required. Compliance with this requirement will be verified by the Ministry of the Interior or the National Cyber and Information Security Agency within their own agendas.	X	X	X	X	X	X	X
4. Service availability levels									
4.1	The provider is able to ensure the availability of a cloud computing service with uninterrupted operating time at least in the mentioned levels evaluated on a monthly basis, including the time required for service interventions, measured at the Internet Exchange Point (IXP) declared by the provider.	A reference to a specific part of the terms and conditions for the provision of a cloud computing service or a part of a draft contract in which the provider shall guarantee to ensure availability at least at the specified levels, or an audit report issued for the certification ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 or ISO/IEC 27001 by a certification body that	-	99.45 (%)	99.90 (%)	99.99 (%)	X	X	X

		has been accredited to carry out audits and certification of information security management systems by a member of the International Accreditation Forum (IAF), or audit report SOC 2® Type 2, with a reference made to the part showing that the provider is able to ensure the availability of a cloud computing service with uninterrupted operating time at least in the mentioned levels evaluated on a monthly basis, including the time required for service interventions, measured at the Internet Exchange Point (IXP) declared by the provider.							
4.2	The provider is able to ensure the availability of a cloud computing service with an operating time of at least 10 hours on working days at the specified level evaluated on a monthly basis, including the time required for service interventions, measured at the Internet Exchange Point (IXP) declared by the provider.	A reference to a specific part of the terms and conditions for the provision of a cloud computing service or a part of a draft contract in which the provider shall guarantee to ensure availability at least at the specified levels,	96.16 (%)	-	-	-	X	X	X

		<p>or an audit report issued for the certification ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 or ISO/IEC 27001 by a certification body that has been accredited to carry out audits and certification of information security management systems by a member of the International Accreditation Forum (IAF), or audit report SOC 2® Type 2, with a reference made to the part showing that the provider is able to ensure the availability of a cloud computing service with an operating time of at least 10 hours on working days at the specified level evaluated on a monthly basis, including the time required for service interventions, measured at the Internet Exchange Point (IXP) declared by the provider.</p>							
5. Connection to Internet exchange node (IXP)									
5.1	The provider has ensured a connection to an Internet Exchange Point (IXP) in the Czech Republic.	An extract from a publicly available database of entities			X	X	X	X	X

		<p>connected to the Internet Exchange Point,</p> <p>or a valid contract with an Internet Exchange Point Service provider,</p> <p>or a solemn declaration by the provider that it has ensured a connection to an Internet Exchange Point (IXP) in the Czech Republic.</p>							
6. Ensuring provision of cloud computing services									
6.1	<p>The provider has prepared a plan to ensure the continuity of operation and a plan for a re-establishment after an accident related to the provided cloud computing service to ensure the availability specified in lines 4.1 and 4.2 of Annex No. 2 to this Decree.</p>	<p>Strategy to ensure operation continuity</p> <p>and strategy to re-establish operation after an accident,</p> <p>or an audit report prepared by a subject independent of the provider, which proves the existence of a plan to ensure the continuity of operation of the offered cloud computing service and a plan for a re-establishment of the provision of the offered cloud computing service after an accident, and attests that its application has been</p>	X	X			X	X	X

		<p>verified, particularly an audit report issued for the certification ČSN ISO/IEC 20000, ISO/IEC 20000, ČSN EN ISO 22301 or ISO 22301, SOC 2® Type2 or an attestation pursuant to CSA STAR Level 2 or a valid certificate ČSN ISO/IEC 20000, ISO/IEC 20000, ČSN EN ISO 22301, or ISO 22301 by a subject independent of the provider.</p> <p>The scope of the given certification or audit report must include the offered cloud computing service. If the scope of the audit report or certification does not specifically include the cloud computing service requested by the provider to be entered in the cloud computing catalogue, the provider shall provide a solemn declaration as to which cloud computing services fall within the scope of the audit report or certification.</p>							
6.2	The provider has prepared a plan to ensure the continuity of operation and a plan for a re-establishment after an accident related to	Strategy to ensure operation continuity			X	X	X	X	X

	<p>the provided cloud computing service to ensure the availability specified in lines 4.1 and 4.2 of Annex No. 2 to this Decree.</p>	<p>and strategy to re-establish operation after an accident,</p> <p>or an audit report prepared by a subject independent of the provider, which proves the existence of a plan to ensure the continuity of operation of the offered cloud computing service and a plan for a re-establishment of the provision of the offered cloud computing service after an accident, and attests that its application has been verified, particularly an audit report issued for the certification ČSN ISO/IEC 20000, ISO/IEC 20000, ČSN EN ISO 22301 or ISO 22301, SOC 2® Type 2 or an attestation pursuant to CSA STAR Level 2.</p> <p>The scope of the given audit report must include the offered cloud computing service. If the scope of the audit report or certification does not specifically include the cloud computing service requested by the</p>							
--	--	---	--	--	--	--	--	--	--

		provider to be entered in the cloud computing catalogue, the provider shall provide a solemn declaration as to which cloud computing services fall within the scope of the audit report or certification.							
6.3	The provider enables synchronous replication (backup) of data to at least one backup data centre, which has sufficient capacity to take over the cloud computing service provided from the primary data centre.	A reference to a specific part of the terms and conditions for the provision of a cloud computing service or a part of a draft contract or product specification or audit report issued for the certification of ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 or ISO/IEC 27001 by a certification body accredited to perform audits and certification of information security management systems by one of the members of the International Accreditation Forum (IAF), or audit report SOC 2® Type 2, with a reference made to the part from which the possibility of synchronous replication (backup) of data to the backup data centre is evident.			X	X		X	X

6.4	<p>The provider shall ensure that the primary data centre and at least one backup data centre, which has sufficient capacity to take over the service provided from the primary data centre, are at a sufficient distance from natural sources of risk and sources of risk caused by human activities leading to disruption or restriction of cloud computing service or information security, or adequate security measures have been taken, or the primary data centre and at least one backup data centre with sufficient capacity to take over the service provided from the primary data centre are at a distance from each other of at least 50 km, and both data centres have physical protection against natural disasters, deliberate attack or accidents designed and applied.</p>	<p>A reference to a specific part of the terms and conditions for the provision of a cloud computing service or a part of a draft contract or product specification or audit report issued for the certification of ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 or ISO/IEC 27001 by a certification body accredited to perform audits and certification of information security management systems by one of the members of the International Accreditation Forum (IAF), or audit report SOC 2® Type 2, with a reference made to the part from which the establishment of at least one backup data centre with a sufficient capacity to take over the service provided from the primary data centre is evident,</p> <p>and</p> <p>to document a sufficient distance or the adoption of an adequate safety measure, a report or</p>	X	X	X	X	X	X	X
-----	--	---	---	---	---	---	---	---	---

		<p>other document on the assessment of natural sources of risks and sources of risks caused by human activities, which contains the requisites listed in Annex No. 5 to this Decree,</p> <p>or to demonstrate a distance of at least 50 km between the data centres and the design and application of physical protection against natural disasters, intentional attacks or accidents, a reference to that part of the valid ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 or ISO/IEC 27001 certification by a certification body which has been accredited for the certification of information security management systems by one of the members of the International Accreditation Forum (IAF) or the SOC 2® Type 2 audit report, showing a complete list of data centres and their locations to the level of the cadastral area/municipality from</p>							
--	--	--	--	--	--	--	--	--	--

		which the cloud service is provided, and from which it will be apparent that physical protection against natural disasters, deliberate attack or accidents is designed and applied.							
6.5	The provider ensures that the primary and backup data centres, in which customer data are stored at rest, are located either all in the Czech Republic or at least in the territory of two different Member States of the European Union and the European Free Trade Association. This requirement does not apply to the cloud computing services making use of the exemption from the requirements of line 1.4 of Annex 2 to this Decree.	A reference to the part of valid certification under ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 or ISO/IEC 27001 by a certification body which has been accredited for the certification of information security management systems by one of the members of the International Accreditation Forum (IAF) or the SOC 2® Type 2 audit report, showing a complete list of data centres and their locations to the level of the cadastral area/municipality in which customer data at rest are stored.			X		X	X	X
6.6	The provider ensures that the primary data centre and all backup data centres from which the cloud computing service is provided are located in the Czech Republic, except in cases of explicit written permission of the customer to store customer-encrypted customer data at rest in another Member	A reference to the part of valid certification under ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 or ISO/IEC 27001 by a certification body which				X	X	X	X

	State of the European Union and European Free Trade Association.	has been accredited for the certification of information security management systems by one of the members of the International Accreditation Forum (IAF) or the SOC 2® Type 2 audit report, showing a complete list of data centres and their locations to the level of the cadastral area/municipality in which customer content will be stored as a data at rest in the long term.							
6.7	The provider is able to provide tools or services to increase resistance to DoS/DDoS attacks.	A reference to a specific part of the terms and conditions for the provision of a cloud computing service or to a description of an optional cloud computing service indicating the tool or service used to increase resistance to DoS/DDoS attacks, or an audit report issued for the certification of ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 or ISO/IEC 27001 by a certification body that has been accredited to carry out audits and certification	X	X	X	X	X	X	X

		of information security management systems by a member of the International Accreditation Forum (IAF), or SOC 2® Type 2 audit report, with a reference made to the part showing that the provider is able to provide tools or services to increase resistance to DoS/DDoS attacks, and indicating the tool or service used to increase resistance to DoS/DDoS attacks.							
6.8	The provider enables the operation of the cloud computing service using a management portal or another form of administration console remotely accessible to the customer in a continuous mode.	A reference to a specific part of the terms and conditions for providing a cloud computing service, part of a draft contract or technical documentation showing that the provider allows the cloud computing service to be operated using a management portal or another form of administration console remotely accessible to the customer in continuous mode.			X	X	X	X	X
7. Data handling									
7.1	The provider allows the import or export of data in a volume greater than 2 TB by sending encrypted storage media.	A reference to a specific part of the terms and conditions for providing			X	X	X	X	X

		a cloud computing service, part of a draft contract or product specification showing that the provider allows the import or export of data in a volume greater than 2 TB by sending encrypted storage media.							
7.2	The provider protects customer content by encrypting it during transmission and in storage in the cloud computing service.	<p>A reference to a specific part of the terms and conditions for providing a cloud computing service, part of a draft contract or product specification of the cloud computing service showing that the provider protects customer content by encrypting it during transmission and in storages in the cloud computing service.</p> <p>Or an audit report issued for the certification of ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 or ISO/IEC 27001 by a certification body that has been accredited to carry out audits and certification of information security management systems by a member of the International</p>	X	X	X	X	X	X	X

		Accreditation Forum (IAF), or SOC 2® Type 2 audit report, with a reference made to the part showing that the provider protects customer content by encrypting it during transmission and in storages in the cloud computing service.							
7.3	The provider enables the protection of customer content by encryption during transmission and in storage in the cloud computing service using one of the algorithms listed in the recommendation in the field of cryptographic means issued by the National Cyber and Information Security Agency and published on its website.	A reference to a specific part of the terms and conditions for providing a cloud computing service, part of a draft contract or product specification of the cloud computing service showing the method of encryption during transmission and in the storage in the cloud computing service.		X	X	X	X	X	X
7.4	The provider allows the customer to use their own encryption key (BYOK).	A reference to a specific part of the terms and conditions for providing a cloud computing service, part of a draft contract or product specification of the cloud computing service showing that the provider allows the customer to use their own encryption key, either by generating it in a certified hardware security module			X		X	X	X

		(hereinafter referred to as the “HSM module”) located at the provider under remote customer management, or by importing these keys from other resources under customer management.							
7.5	The provider allows the storage of encryption keys in a certified HSM module of protection level FIPS 140-2 level 2 and higher, FIPS 140-3 level 2 and higher or certification according to Common Criteria at least EAL4 and higher, which is under remote customer management or installation of HSM customer module into the provider’s infrastructure.	A reference to a specific part of the terms and conditions for providing a cloud computing service, part of a draft contract or product specification of the cloud computing service showing that the provider allows the storage of encryption keys in a certified HSM module of protection level FIPS 140-2 level 2 and higher, FIPS 140-3 level 2 and higher or certification according to Common Criteria at least EAL4 and higher, which is under remote customer management or installation of HSM customer module into the provider’s infrastructure.				X	X	X	X

7.6	The provider enables safe disposal of cryptographic keys stored in a certified HSM module controlled by the customer.	A reference to a specific part of the terms and conditions for providing a cloud computing service, part of a draft contract or product specification of the cloud computing service showing that safe disposal of cryptographic keys stored in a certified HSM module controlled by the customer is possible and a commitment to allow/secure the disposal of the supreme access key upon the termination of the cloud computing service.				X	X	X	X
7.7	Upon termination of the cloud computing service, the provider enables safe disposal of cryptographic keys that encrypt customer content in the storage in accordance with the Cybersecurity Decree.	A reference to a specific part of the terms and conditions for providing a cloud computing service, part of a draft contract or product specification of the cloud computing service showing a description of the safe disposal of data in accordance with the Cybersecurity Decree.			X		X	X	X
7.8	The provider draws up a record of the access of their internal and external employees to unencrypted customer data, which occurred without prior consent of the customer in the case. This record must contain at least the reason, time, duration, type and extent of the	A reference to a specific part of the terms and conditions for providing a cloud computing service, part of a draft contract or product	X	X	X	X	X	X	X

	<p>access and sufficient other information necessary for the customer to assess the risk of the access.</p>	<p>specification of the cloud computing service,</p> <p>Or an audit report issued for the certification of ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 or ISO/IEC 27001 by a certification body that has been accredited to carry out audits and certification of information security management systems by a member of the International Accreditation Forum (IAF), or SOC 2® Type 2 audit report, with a reference made to the part showing that the provider draws up a record of the access of their internal and external employees to unencrypted customer data, which occurred without prior consent of the customer in the case, and that such record contains the reason, time, duration, type and extent of the access.</p>							
7.9	<p>The provider allows the customer access to the record created in accordance with line 7.8 of Annex No. 2 to this Decree, and for</p>	<p>A reference to a specific part of the terms and conditions for providing a cloud computing service, part of a draft</p>	X	X	X	X	X	X	X

	<p>this purpose, the provider shall keep the record for at least 7 days.</p> <p>The provider may not allow access to the record if internal and external employees access unencrypted customer content based on a request from a foreign authority for access to or disclosure of data, and notifying the customer of this request is not possible in accordance with points 2.1, 2.2 of Annex 2 to this Decree.</p>	<p>contract or product specification of the cloud computing service,</p> <p>Or an audit report issued for the certification of ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 or ISO/IEC 27001 by a certification body that has been accredited to carry out audits and certification of information security management systems by a member of the International Accreditation Forum (IAF), or SOC 2® Type 2 audit report, with a reference made to the part showing that the provider allows the customer access to the record created in accordance with line 7.8 of Annex No. 2 to this Decree, and for this purpose keeps the record for at least 7 days.</p>							
8. Certification of cloud computing services									
8.1	The provider operates a cloud computing service within the scope of the information security management system which is in accordance with the requirements of the	A solemn declaration that the information security management system, to the extent of	X				X	X	X

	Cybersecurity Decree or with the requirements of ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 or ISO/IEC 27001.	which the cloud computing service is operated, is in accordance with the requirements of the Cybersecurity Decree or the requirements of ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 or ISO/IEC 27001 and the declaration of applicability of the individual measures.							
8.2	The provider holds a valid certification ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 by a certification body that has been accredited to perform audits and certification of information security management systems by one of the members of the International Accreditation Forum (IAF), whose scope of certification includes the assessed cloud computing service.	A valid certificate ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 or ISO/IEC 27001 by a certification body that has been accredited to perform audits and certification of information security management systems by one of the members of the International Accreditation Forum (IAF) with the designation of the provider, where the scope of the certification specifically includes the cloud computing service which the provider requests to be incorporated in the cloud computing catalogue,		X			X	X	X

		Or, if the scope of certification indicated on the certificate does not specifically include the cloud computing service requested by the provider to be incorporated in the cloud computing catalogue, a solemn declaration as to which services fall within the scope of the information security management system for which the certificate was issued.							
8.3	The provider holds a valid certification ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 by a certification body that has been accredited to perform audits and certification of information security management systems by one of the members of the International Accreditation Forum (IAF), whose scope of certification includes the assessed cloud computing service.	A valid certificate ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 or ISO/IEC 27001 by a certification body that has been accredited to perform audits and certification of information security management systems by one of the members of the International Accreditation Forum (IAF) with the designation of the provider, where the scope of the certification specifically includes the cloud computing service which the provider requests to be incorporated in the			X	X	X	X	X

		<p>cloud computing catalogue,</p> <p>Or, if the scope of certification indicated on the certificate does not specifically include the cloud computing service requested by the provider to be incorporated in the cloud computing catalogue, a solemn declaration as to which services fall within the scope of the information security management system for which the certificate was issued, and the relevant declaration of applicability.</p>							
8.4	<p>The provider holds a valid certification ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 by a certification body that has been accredited to perform audits and certification of information security management systems by one of the members of the International Accreditation Forum (IAF), whose scope of certification includes the assessed cloud computing service operated in compliance with the procedures stipulated in the ČSN ISO/IEC 27017 or ISO/IEC 27017 standards.</p>	<p>A valid certificate ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 or ISO/IEC 27001 by a certification body that has been accredited to perform audits and certification of information security management systems by one of the members of the International Accreditation Forum (IAF) with the designation of the provider, where the</p>		X			X	X	X

		<p>scope of the certification specifically includes the cloud computing service which the provider requests to be incorporated in the cloud computing catalogue and operated in compliance with the procedures stipulated in the ČSN ISO/IEC 27017 or ISO/IEC 27017 standards,</p> <p>Or, if the scope of certification indicated on the certificate does not specifically include the cloud computing service requested by the provider to be incorporated in the cloud computing catalogue, a solemn declaration as to which services fall within the scope of the information security management system for which the certificate was issued.</p>							
8.5	The provider holds a valid certification ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 or ISO/IEC 27001 by a certification body that has been accredited to perform audits and certification of information security management systems by one of the members of the International Accreditation Forum (IAF), whose scope of certification includes the assessed cloud computing service	A valid certificate ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 or ISO/IEC 27001 by a certification body that has been accredited to perform audits and certification of information security			X	X	X	X	X

	<p>operated in compliance with the procedures stipulated in the ČSN EN ISO/IEC 27017 or EN ISO/IEC 27017 standards.</p>	<p>management systems by one of the members of the International Accreditation Forum (IAF) with the designation of the provider, where the scope of the certification specifically includes the cloud computing service which the provider requests to be incorporated in the cloud computing catalogue and operated in compliance with the procedures stipulated in the ČSN ISO/IEC 27017 or ISO/IEC 27017 standards,</p> <p>Or, if the scope of certification indicated on the certificate does not specifically include the cloud computing service requested by the provider to be entered in the cloud computing catalogue, a solemn declaration as to which services fall within the scope of the information security management system for which the certificate was issued, and the relevant</p>							
--	---	---	--	--	--	--	--	--	--

		declaration of applicability.							
8.6	The provider holds a valid certification ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 by a certification body that has been accredited to perform audits and certification of information security management systems by one of the members of the International Accreditation Forum (IAF), whose scope of certification includes the assessed cloud computing service operated in compliance with the procedures stipulated in the ČSN ISO/IEC 27018 or ISO/IEC 27018 standards.	<p>A valid certificate ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 or ISO/IEC 27001 by a certification body that has been accredited to perform audits and certification of information security management systems by one of the members of the International Accreditation Forum (IAF) with the designation of the provider, where the scope of the certification specifically includes the cloud computing service which the provider requests to be incorporated in the cloud computing catalogue and which is operated in compliance with the procedures stipulated in the ČSN ISO/IEC 27018 or ISO/IEC 27018 standards,</p> <p>Or, if the scope of certification indicated on the certificate does not specifically include the cloud computing</p>			X	X	X	X	X

		service requested by the provider to be incorporated in the cloud computing catalogue, a solemn declaration as to which services fall within the scope of the information security management system for which the certificate was issued, and the relevant declaration of applicability.							
8.7	The provider holds an SOC 2® Type 2 audit report or an audit report on the assessment of compliance with the current requirements of the Cloud Computing Compliance Criteria Catalogue C5 issued by BSI, in the form of Type 2, not older than 24 months, whose scope includes the assessed cloud computing service, and which was issued by an independent auditor.	Audit report SOC 2® Type 2 in the domains of security, availability, process integrity, confidentiality, and privacy or an audit report on the assessment of compliance with the current requirements of Cloud Computing Compliance issued by BSI, in the form of Type 2.			X	X	X	X	X
9. Cybersecurity events and cybersecurity incidents									
9.1	The provider has implemented a tool to monitor and evaluate cybersecurity events.	A reference to a specific part of the terms and conditions for the provision of a cloud computing service, part of a draft contract or another description of the cloud computing service indicating that	X				X	X	X

		<p>the provider has implemented a tool to monitor and evaluate cybersecurity events,</p> <p>Or an audit report issued for the certification of ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 or ISO/IEC 27001 by a certification body that has been accredited to carry out audits and certification of information security management systems by a member of the International Accreditation Forum (IAF), or SOC 2® Type 2 audit report, with reference to the part showing that the provider has implemented a tool to monitor and evaluate cybersecurity events.</p>							
9.2	<p>The provider has implemented a tool to monitor and evaluate cybersecurity events. The provider will enable remote access to all events related to a specific customer to the customer. New events shall be made available to the customer without undue delay after the occurrence of the event, but no later than within 24 hours.</p>	<p>A reference to a specific part of the terms and conditions for the provision of a cloud computing service, part of a draft contract or other description of the cloud computing service indicating that the provider has implemented a tool to monitor and evaluate</p>		X	X	X	X	X	X

		<p>cybersecurity events and will enable remote access to all events related to a specific customer to the customer, making new events available to the customer without undue delay, but no later than within 24 hours after the occurrence of the event,</p> <p>Or an audit report issued for the certification of ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 or ISO/IEC 27001 by a certification body that has been accredited to carry out audits and certification of information security management systems by a member of the International Accreditation Forum (IAF), or SOC 2® Type 2 audit report, with reference to the part showing that the provider has implemented a tool to monitor and evaluate cybersecurity events, will enable remote access to all events related to a specific customer, and will make new events available to</p>							
--	--	--	--	--	--	--	--	--	--

		the customer without undue delay after the occurrence of the event, but no later than within 24 hours.							
9.3	In the event of a breach of customer data information and specific operational data, the provider shall inform the customer without undue delay, but no later than within 72 hours from the moment when the provider became aware of the breach of the customer data security. As soon as the resolution of the incident is completed, the provider informs the customer about the measures taken.	A reference to a specific part of the terms and conditions for the provision of the cloud computing service, part of the draft contract or other description of the cloud computing service indicating that, in case of breach of customer data and specific operational data, the provider informs the customer without undue delay, but no later than within 72 hours from the moment the provider became aware of the breach of the customer data security.	X	X	X	X	X	X	X
10. Testing cloud computer services									
10.1	The provider performs regular vulnerability scans. A cloud computing service to be incorporated in the cloud computing catalogue must be included in the vulnerability scan scope.	Three records of vulnerability scans executed not earlier than 3 months before the application for incorporation of the cloud computing service in the cloud computing catalogue,	X	X	X	X	X	X	X

		<p>Or an audit report issued for the certification of ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 or ISO/IEC 27001 by a certification body that has been accredited to carry out audits and certification of information security management systems by a member of the International Accreditation Forum (IAF), or audit report SOC 2® Type 2, with reference to the part showing that vulnerability scans are executed regularly at such an interval which will show that at least 3 vulnerability scans had been executed not earlier than 3 months before the application for cloud computing service incorporation to the cloud computing catalogue was filed.</p>							
10.2	<p>The provider ensures that penetration tests are executed by an entity that is independent of the provider. The cloud computing service to be incorporated in the cloud computing catalogue must be included in the scope of the penetration test.</p>	<p>A report on the execution of a penetration test executed according to the NIST 800-115 standard or in accordance with the OSSTMM methodology. The penetration test shall be</p>			X	X	X	X	

		executed by an entity that is independent of the provider. The penetration test report must not be older than 24 months before the application for incorporation of the cloud computing service in the cloud computing catalogue.							
10.3	The provider ensures that penetration tests are executed by an entity that is independent of the provider. The cloud computing service to be incorporated in the cloud computing catalogue must be included in the scope of the penetration test.	A report on the execution of a penetration test, during which the risks will be verified at least according to the OWASP Top 10 Web Application Security Risks standard. The penetration test shall be executed by an entity that is independent of the provider. The penetration test report must not be older than 24 months before the application for incorporation of the cloud computing service in the cloud computing catalogue.			X	X			X

List of certifications for the area of protection of confidentiality, integrity, and availability of information	
<ul style="list-style-type: none"> • ČSN EN ISO/IEC 27001, EN ISO/IEC 27001, or ISO/IEC 27001 • ČSN ISO/IEC 27017 or ISO/IEC 27017 • ČSN ISO/IEC 27018 or ISO/IEC 27018 	
Proofs of compliance	
For line 8.2 of Annex No. 2 to this Decree	A valid certificate ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 or ISO/IEC 27001 by a certification body that has been accredited to perform audits and certification of information security management systems by one of the members of the International Accreditation Forum (IAF), with the designation of the provider, where the scope of certification specifically includes the cloud computing service requested by the provider to be incorporated in the cloud computing catalogue, or if the scope of certification stated on the certificate does not specifically include the cloud computing service requested by the provider to be incorporated in the cloud computing catalogue, a solemn declaration as to which cloud computing services fall within the scope of the information security management system for which the certificate was issued, and a relevant declaration of applicability.
For line 8.3 of Annex No. 2 to this Decree	A valid certificate ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 or ISO/IEC 27001 by a certification body that has been accredited to perform audits and certification of information security management systems by one of the members of the International Accreditation Forum (IAF), with the designation of the provider, where the scope of certification specifically includes the cloud computing service requested by the provider to be incorporated in the cloud computing catalogue, or if the scope of certification stated on the certificate does not specifically include the cloud computing service requested by the provider to be incorporated in the cloud computing catalogue, a solemn declaration as to which cloud computing services fall within the scope of the information security management system for which the certificate was issued, and a relevant declaration of applicability.
For line 8.4 of Annex No. 2 to this Decree	A valid certificate ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 or ISO/IEC 27001 by a certification body that has been accredited to perform audits and certification of information security management systems by one of the members of the International Accreditation Forum (IAF), with the designation of the provider, where the scope of certification specifically includes the cloud computing service requested by the provider to be incorporated in the cloud computing catalogue and operated in compliance with the procedures stipulated in the ČSN ISO/IEC 27017 or ISO/IEC 27017 standard, or if the scope of certification stated on the certificate does not specifically include the cloud computing service requested by the provider to be incorporated in the cloud computing catalogue, a solemn declaration as to which cloud computing services fall within the scope of the information security management system for which the certificate was issued, and a relevant declaration of applicability.
For line 8.5 of Annex No. 2 to this Decree	A valid certificate ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 or ISO/IEC 27001 by a certification body that has been accredited to perform audits and certification of information security management systems by one of the members of the International Accreditation Forum (IAF), with the designation of the provider, where the scope of certification specifically includes the cloud computing service requested by the provider to be incorporated in the cloud computing catalogue and operated in compliance with the procedures stipulated in the ČSN ISO/IEC 27017 or ISO/IEC 27017 standard, or if the scope of certification stated on the certificate does not specifically include the cloud computing service incorporated by the

	provider to be included in the cloud computing catalogue, a solemn declaration as to which cloud computing services fall within the scope of the information security management system for which the certificate was issued, and a relevant declaration of applicability.
For line 8.6 of Annex No. 2 to this Decree	A valid certificate ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 or ISO/IEC 27001 by a certification body that has been accredited to perform audits and certification of information security management systems by one of the members of the International Accreditation Forum (IAF), with the designation of the provider, where the scope of certification specifically includes the cloud computing service requested by the provider to be incorporated in the cloud computing catalogue and operated in compliance with the procedures stipulated in the ČSN ISO/IEC 27018 or ISO/IEC 27018 standard, or if the scope of certification stated on the certificate does not specifically include the cloud computing service requested by the provider to be incorporated in the cloud computing catalogue, a solemn declaration as to which cloud computing services fall within the scope of the information security management system for which the certificate has been issued, and a relevant declaration of applicability.
For line 8.7 of Annex No. 2 to this Decree	An SOC 2® Type 2 audit report in the domains of security, availability, process integrity, confidentiality, and privacy, or an audit report on the assessment of compliance with the current requirements of the Cloud Computing Compliance Criteria Catalogue (C5) issued by BSI, in the form of Type 2; the audit reports must not be older than 24 months as of the date of submission of the application for incorporation in the cloud computing catalogue.
Every 15 months of the registration of the cloud computing service in the cloud computing catalogue kept by the Ministry of the Interior, the provider shall supply	
For line 8.2 of Annex No. 2 to this Decree	Proof of validity of the certificate or a valid certificate ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 or ISO/IEC 27001 by a certification body that has been accredited to perform audits and certification of information security management systems by one of the members of the International Accreditation Forum (IAF), with a designation of the provider, not older than 3 months at the time of its submission, where the scope of certification specifically includes the cloud computing service incorporated in the cloud computing catalogue, or if the scope of certification stated on the certificate does not include the cloud computing service listed in the cloud computing catalogue, a solemn declaration as to which services fall within the scope of the information security management system for which the certificate has been issued, and a relevant declaration of applicability.
For line 8.3 of Annex No. 2 to this Decree	Proof of validity of the certificate or a valid certificate ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 or ISO/IEC 27001 by a certification body that has been accredited to perform audits and certification of information security management systems by one of the members of the International Accreditation Forum (IAF), with a designation of the provider, not older than 3 months at the time of its submission, where the scope of certification specifically includes the cloud computing service incorporated in the cloud computing catalogue, or if the scope of certification stated on the certificate does not include the cloud computing service incorporated in the cloud computing catalogue, a solemn declaration as to which services fall within the scope of the information security management system for which the certificate has been issued, and a relevant declaration of applicability.
For line 8.4 of Annex No. 2 to this Decree	Proof of validity of the certificate or a valid certificate ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 or ISO/IEC 27001 by a certification body that has been accredited to perform audits and certification of information security management systems by one of the members of the International Accreditation Forum (IAF), with a designation of the provider, not older than 3 months at the time of its submission, where the scope of certification specifically includes the cloud computing service incorporated in the cloud computing catalogue and operated in compliance with the procedures stipulated in the ČSN ISO/IEC 27017 or ISO/IEC 27017 standard, or if the scope of certification stated on the certificate does not specifically include the cloud computing service incorporated in the cloud computing catalogue, a solemn declaration as to which cloud computing services fall within the scope of the information security management system for which the certificate has been issued, and a relevant declaration of applicability.
For line 8.5 of Annex No. 2 to this Decree	Proof of validity of the certificate or a valid certificate ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 or ISO/IEC 27001 by a certification body that has been accredited to perform audits and certification of information security management systems by one of the members of the International Accreditation Forum (IAF), with a designation of the provider, not older than 3 months at the time of its submission, where the scope of certification specifically includes the cloud computing service incorporated in the cloud computing catalogue and operated in compliance with the procedures stipulated in the ČSN ISO/IEC 27017 or ISO/IEC 27017 standard, or if the scope of certification stated on the certificate does not specifically include

	the cloud computing service incorporated in the cloud computing catalogue, a solemn declaration as to which cloud computing services fall within the scope of the information security management system for which the certificate has been issued, and a relevant declaration of applicability.
For line 8.6 of Annex No. 2 to this Decree	Proof of validity of the certificate or a valid certificate ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 or ISO/IEC 27001 by a certification body that has been accredited to perform audits and certification of information security management systems by one of the members of the International Accreditation Forum (IAF), with a designation of the provider, not older than 3 months at the time of its submission, where the scope of certification specifically includes the cloud computing service incorporated in the cloud computing catalogue and operated in compliance with the procedures stipulated in the ČSN ISO/IEC 27018 or ISO/IEC 27018 standard, or if the scope of certification stated on the certificate does not specifically include the cloud computing service incorporated in the cloud computing catalogue, a solemn declaration as to which cloud computing services fall within the scope of the information security management system for which the certificate has been issued, and a relevant declaration of applicability.
If the provider proves any of the facts by submitting an SOC 2® Type 2 audit report, this audit report may not be older than 24 months as of the date of submission of the application for incorporation in the cloud computing catalogue or as of the documented fact.	
Every 24 months of the registration of the cloud computing service in the cloud computing catalogue kept by the Ministry of the Interior, the provider shall supply	
For line 8.7 of Annex No. 2 to this Decree	An SOC 2® Type 2 audit report in the domains of security, availability, process integrity, confidentiality, and privacy, or an audit report on the assessment of compliance with the current requirements of the Cloud Computing Compliance Criteria Catalogue (C5) issued by BSI, in the form of Type 2; the audit reports must not be older than 24 months.

Requirements for the structure and requisites of the report on penetration test execution	
For line 10.1 of Annex No. 2 to this Decree	Three records of vulnerability scans performed a maximum of 3 months before submitting an application for incorporation in the cloud computing catalogue or an audit report issued for certification ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 or ISO/IEC 27001 by a certification body that has been accredited for conducting audits and certification of information security management systems by any member of the International Accreditation Forum (IAF), or an SOC 2® Type 2 audit report, with reference to the part showing that vulnerability scans are performed regularly at an interval from which it will follow that at least 3 vulnerability scans had been performed no more than 3 months before the application for incorporation in the cloud computing catalogue was submitted.
For line 10.2 of Annex No. 2 to this Decree	A report on the execution of a penetration test performed in accordance with the NIST 800-115 standard or in accordance with the OSSTMM methodology, performed by an entity that is independent of the provider. The penetration test report must not be older than 24 months before applying for incorporation in the cloud computing catalogue.
For line 10.3 of Annex No. 2 to this Decree	A report on penetration test that verifies risks at least in accordance with the OWASP Top 10 Web Application Security Risks standard, performed by an entity that is independent of the provider. The penetration test report must not be older than 24 months before applying for incorporation in the cloud computing catalogue.
Every 24 months of the incorporation of the cloud computing service in the cloud computing catalogue, the provider shall submit to the Ministry of the Interior	
For line 10.1 of Annex No. 2 to this Decree	Four records of executing vulnerability scans executed every 6 months of the incorporation in the cloud computing catalogue or an audit report issued for certification ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 or ISO/IEC 27001 by a certification body that has been accredited to perform audits and certification of information security management systems by a member of the International Accreditation Forum (IAF), or an SOC 2® Type 2 audit report, with reference to the part showing that at least 4 vulnerability scans were performed every 6 months of the incorporation in the cloud computing catalogue.
For line 10.2 of Annex No. 2 to this Decree	A report on the execution of a penetration test executed according to the NIST 800-115 standard or in accordance with the OSSTMM methodology, performed by an entity that is independent of the provider. The penetration test report must not be older than 23 months from the incorporation in the cloud computing catalogue or the delivery of the previous penetration test report.
For line 10.3 of Annex No. 2 to this Decree	A report on execution of a penetration test that verifies the risks at least in accordance with the OWASP Top 10 Web Application Security Risks standard performed by an entity that is independent of the provider. The penetration test report must not be older than 23 months from the incorporation in the cloud computing catalogue or the delivery of the previous penetration test report.

<p>For line 6.4 of Annex No. 2 to this Decree</p>	<p>The report or other evidence of assessment of the natural sources of risk and the sources of risk caused by human activities must include in a clear and comprehensible manner:</p> <ul style="list-style-type: none">• identification of the subject of the cloud computing provider,• identification of the assessed locations of the primary/backup data centres,• Identification of the report processor,• the date of processing of the report. <ol style="list-style-type: none">1. Site plan, layout, and constructional concept of the primary/backup data centre building - a brief description of the building in terms of layout and location of the building in relation to the surrounding buildings and geolocation, or a description of the operational technology.2. Threat analysis of each primary/backup data centre from which the cloud computing service is provided, including:<ol style="list-style-type: none">a) identification of the risk sources,b) probability of activating the source of risk,c) impact level,d) description of potential damage,e) designation of the risk in the risk matrix,f) stating of the significance of the risk,g) the countermeasures applied.3. The report will be annexed by selected scales of the probability of activation of the source of risk and level of impact, criteria for assessing the significance of risks and a processed risk matrix that combines the probability of activation of the source of risk and the level of impact and shows the resulting risks with a relevant degree of acceptability. <p>The report shall particularly consider the following sources of risk:</p> <ul style="list-style-type: none">• fire,• heavy rainfall,
---	---

- flood,
- tsunami,
- hail,
- extremely high temperatures,
- long-term drought,
- extreme wind,
- tornado,
- extremely low temperatures,
- snow calamity,
- avalanche,
- frost and black ice,
- geomagnetic anomalies,
- earthquake,
- sinkholes,
- slope instability,
- volcanic eruption,
- serious accident - plane crash,
- epidemics - mass infections of persons,
- serious breach of the security of the communication network and loss of integrity of the communication network,
- large-scale disruption of electricity supplies,
- radiation accident.

