CERTIFICATION OF CLOUD COMPUTING SERVICES IN THE CZECH REPUBLIC AND IN EU

Jakub Klodwig

JUDr. Jakub Klodwig is a Ph.D. student at the Institute of Law and Technology of Masaryk University and an associate in Eldison, law firm. Available on the website: www.pravnikIT.cz, or by email: Jakub.Klodwig@law.muni.cz

Keywords: ***cybersecurity, certification, cloud computing, EUCS, SaaS, catalogue, NIS, NÚKIB***

Abstract: *The author provides an analysis of the legal regulation of cloud computing effective in the Czech Republic and its relationship to the certification of cloud computing services in the European Union. The article answers the question of how both legal regulations will co-applicate when EUCS will be finished. Although the Czech cloud computing regulation could be considered as the cloud computing certification scheme, it is argued why both legal regulations will be effective at the same time and how it will be possible to achieve one certification through the other.*

1. The rise of cloud computing

The regulation of cloud computing services is recently a hot topic. Spending on cloud computing services grew 4.5 times faster than spending on traditional usage of on-premises information technologies between 2009 and 2017, (Lesser 2017) and it is still expected to grow at an average of 17 % per year in the coming years. (Ernst & Young, s.r.o. 2021, p. 26) The shift to the cloud is on trend, which takes place not only in the private sector, but also in the academic and public sectors as well. (Gill, Tuli, Xu, Singh, Singh, Lindsay, Tuli, Smirnova, Singh, Jain, Pervaiz, Sehgal, Kaila, Misra, Aslanpour, Mehta, Stankovski, Garraghan 2019, p. 1) However the technology of cloud computing originates from private sector, it is widespread nowadays, because it is economically viable. An analysis of Ernst & Young from 2020 predicts that use of cloud computing services would save from 10% to 50% of operating costs of IT in public sector and to bring further major benefits including, for example, reduction of carbon emissions by 30 to 90%. (Ernst & Young, s.r.o. 2021)

Although cloud regulation is economically advantageous, it carries many risks associated with the outsourcing of services to third parties, especially in terms of security, which is also an aspect that legislators are trying to regulate both at national and European levels. In some countries, including United Kingdom, Denmark and Germany, there is already a specific regulation of cloud computing, which are different from each other. The Czech Republic is one of those leading countries that already have effective legal regulation of the cloud since 1. September 2020. Therefore, we will now take a closer look at the conditions under which member states can create their own legal security requirements for cloud computing services and how Czech cloud computing legislation works and if it is compatible with the upcoming European Union regulation.

2. Certification of cloud computing services

The use of cloud computing services entails the involvement of other entities in internal processes that may be essential for the company. For this reason, the choice of a specific cloud commuting provider, i.e. a specific service, is essential and can be both a benefit and a threat from a cybersecurity perspective. (Catteddu 2010, p. 1) The European Union is preparing rules for cybersecurity certification of ICT products, services, and processes, which will apply to all EU member states and the entire single market for the first time, to create a

clearly defined and reliable security standard, so all companies do not have to expose themselves to the risk of choosing an unreliable cloud computing provider.

For this purpose, Regulation (EU) No. 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA ("the European Union Agency for Cybersecurity") and on information and communication technology cybersecurity certification and repealing Regulation (EU) No. 526/2013 ("Cybersecurity Act"), was adopted as a uniform certification framework for all EU member states from 27 June 2019. The certification system under Cybersecurity Act is quite complex, with accreditation bodies, certification bodies, conformity assessment bodies (CAB) and, of course, entities interested in certification appearing in it. In addition, according to the Cybersecurity Act, there are three security levels in which goods and services can be certified. Those security levels are: Basic, which should correspond to the security minimum; Substantial, intended as a business level of security; and High security level, including the most modern security methods. (Klodwig, Jakub. Regulace cloud computing ve veřejné správě ČR, 101) The decision to undergo the certification process, as well as the choice of security level, is left purely to the will of the entity. Certification is fully voluntary unless EU or national legislation stipulates otherwise in specific cases due to 56(2) Cybersecurity Act.

According to Article 48 of the Cybersecurity Act, the Commission may ask ENISA to prepare a European cybersecurity certification scheme. One of the first schemes that shall be soon completed is the European Cybersecurity Certification Scheme for Cloud Services ("EUCS"). The problem is that due to Article 57 of the Cybersecurity Act the adoption of the pan-European certification scheme cancels and replaces all national certification schemes for cybersecurity products and services, which brings with it the question of whether the Czech regulation of cloud computing is a certification scheme or not.[1] Because if the new Czech cloud computing regulation would be possible to subordinate under the definition of the National cybersecurity certification scheme, the Czech legal regulation of cloud computing would be at least partially derogated since the entry of the EUCS into force.

According to Article 2(10) of the Cybersecurity Act, the national cybersecurity certification scheme is defined as a *"comprehensive set of rules, technical requirements, standards and procedures developed and adopted by a national public authority and that apply to the certification or conformity assessment of ICT products, ICT services and ICT processes falling under the scope of the specific scheme".* Cloud computing services surely are ICT services, and their Czech regulation sets comprehensive rules, technical requirements, standards, and procedures within which the Czech authorities assess their compliance. This means that the Czech regulation of cloud computing might be subordinated to the definition of Article 2(10) of the Cybersecurity Act. (Klodwig, Jakub. Regulace cloud computing ve veřejné správě ČR, 107) However, there is more to be told about Czech regulation.

3. Czech regulation of cloud computing services

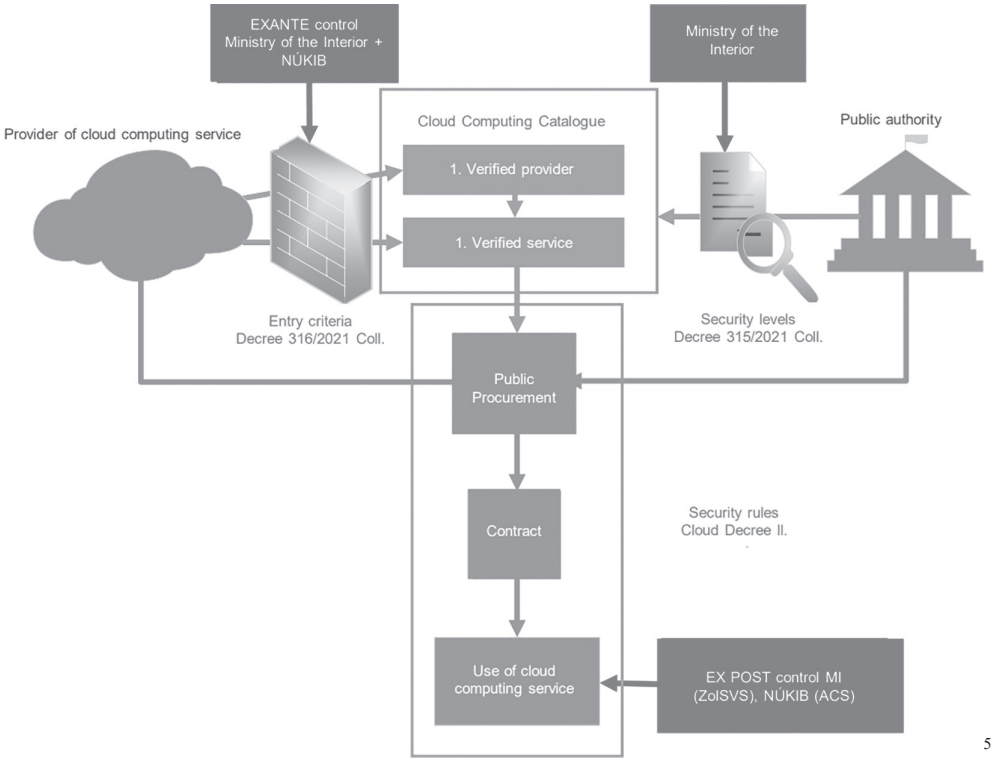
The regulation of cloud computing is in the Czech legal system divided into The Act No 181/2014 Coll. On Cybersecurity and change of related acts ("ACS") and the Act No. 365/2000 Coll. on Public Administration Information Systems and on Amendments to Certain Other Acts ("APAIS"). Although both laws affect partially different range of subjects,[2] they materially follow each other and together form a comprehensive regulatory system. The focal point of regulation is the cloud computing catalogue, which is a publicly available list on the websites of Czech Ministry of Interior.[3] All cloud computing inquiries from public administration bodies, offers of cloud computing providers, cloud computing providers themselves, and all cloud computing services already used by public bodies must be signed on the relevant list there.[4]

[1] In this context, also Art. 57(2) provides: "Member States shall not introduce new national cybersecurity certification schemes for ICT products, ICT services and ICT processes already covered by a European cybersecurity certification scheme that is in force."

[2] Act on Cybersecurity determines duties for a public authority, while the Act on Public Administration Information Systems set duties for public administration bodies.

[3] Available at: https://www.mvcr.cz/clanek/egovernment-cloud.aspx?q=Y2hudW09NQ%3D%3D.

[4] In accordance with § 6k APAIS.



5

The process starts with a public administration body that wants to use a cloud computing service. In that case the public administration body must register its inquiry of cloud computing services in the appropriate security level of the cloud computing catalogue, which is controlled by the Ministry of Interior.[6] Unlike the EUCS, the Czech regulation distinguishes four security levels, which are specified in the Decree No. 315/2021 Coll. on security levels for the use of cloud computing by public authorities ("Decree on Security Levels").[7] The first three security levels (Low, Medium, and High) are available exclusively for private providers. In the fourth, the Critical security level, cloud computing services could only be offered by the state cloud computing provider, the creation of which is foreseen by the law.

Private providers must first apply for incorporation of themselves as cloud computing providers[8] and then register their cloud computing services as well.[9] It is necessary that they document all the requirements for cloud computing providers including following:

– The residency of cloud computing provider is in EU member state or designation of his representative is in EU member state.
– The provider nor his controlling person have been convicted of an offence consisting in the failure to introduce or implement security measures pursuant to the Czech Cybersecurity Act.
– And has been verified by Czech public authorities, including intelligence services.

5 Available at: https://nukib.cz/en/cyber-security/regulation-and-audit/support-materials/.
6 In accordance with § 6o APAIS.
7 Decree No. 315/2021 Coll. on security levels for the use of cloud computing by public authorities is available at: https://www.nukib.cz/download/publications_en/legislation/DECREE%20No.%20315_2021.pdf.
8 In accordance with § 6q APAIS.
9 In accordance with § 6t APAIS.

After cloud computing provider is incorporated in cloud computing register, it is still required for their cloud computing services to be registered too, to document for example:

- The information on all countries where customer data is or may be stored in an inactive state.
- The information on all countries from which the cloud computing service is administered and supervised.
- If the Provider receives a legally binding request from a foreign authority to disclose or transfer Customer Data, the Provider shall not comply with the request and shall refer the requestor to the Customer or at least inform the Customer of the request without delay.
- Once a year, or based on recurring cybersecurity incidents, or in the event of a discrepancy with the declared parameters, the provider shall allow the Czech authorities to perform a compliance check free of charge in relation to the cloud computing service.
- The availability of the cloud computing service with uninterrupted operating time.
- The connection to the Internet Exchange Point (IXP) in the Czech Republic.
- The business continuity plan and the disaster recovery plan for the service provided.
- The synchronous replication (backup) of data to at least one backup data centre with sufficient capacity to take over the cloud computing service provided from the primary data centre.
- The provision of tools or services to increase resilience to DoS/DDoS attacks.
- The enablement of the cloud computing service to be operated through a management portal or other form of administration console remotely accessible to the customer in a continuous mode.
- The enablement of the import or export of data larger than 2 TB by sending encrypted storage media.
- The protection of customer content by encrypting it in transit and in cloud storage.
- The allowance the customer to use its own encryption key (BYOK).
- The records of access by its internal and external personnel to unencrypted customer data that occurred without the customer's prior permission in each case.
- The cloud computing service follows the requirements of EN ISO/IEC 27001, EN ISO/IEC 27001, or ISO/IEC 27001.
- Having a SOC 2® Type 2 audit report or audit report assessing compliance with the current Cloud Computing Compliance Criteria Catalogue C5 requirements issued by BSI, in Type 2 form that is no more than 24 months old.
- Implementation of the tool for monitoring and evaluating cyber security events.
- Informing processes in the event of a security breach of Customer data information without undue delay, but at the latest within 72 hours of becoming aware of the security breach of Customer data.
- Performation of regular vulnerability scans and penetration tests.

Those are specified differently for each security level in the Decree No. 316/2021 Coll. on some requirements for incorporation into the cloud computing catalogue ("Decree on requirements for incorporation")[10] and are checked by the Ministry of Interior with cooperation to the National Cyber and Information Security Agency ("NÚKIB") as part of Ex Ante control (see the diagram above).

After both the provider and the service are registered in the catalogue, a public procurement can take place with such an offer through a dynamic purchasing system (see above in blue). This will ensure that the most suitable offer is selected for the inquiry in at least the same security level. If the inquiry and offer are paired, the contract could be signed by both parties and the cloud computing service is ready to use. From the moment

[10] Decree No. 316/2021 Coll. on some requirements for incorporation into the cloud computing catalogue, available at: https://www.nukib.cz/download/publications_en/legislation/DECREE%20No.%20316_2021.pdf

of signing the contract Ex Post control could take place to verify that all contractual clauses required by The Decree on Security Rules[11] are properly set.

4. The relationship between Czech and European cloud computing legislation

Czech legislators were aware of the upcoming European certification when preparing the Czech regulation. Moreover, the risk of duplicity regulation was pointed out in the interdepartmental comment procedure by some concerned authorities, including for example, the Czech Chamber of Commerce. (Hospodářská komora České republiky 2021) So the requirements of the cloud computing decrees were already coordinated when they were created with the upcoming requirements of the EUCS in the relevant security levels. The security levels themselves should thus correspond to each other, and the author of cloud computing decrees (NÚKIB) expects to modify Decree on Requirements for Incorporation and The Decree on Security Rules according to its statements after the finalization of the EUCS. (*CyberCon 2021 – Martin Klumpar – Regulace využití služeb cloud computingu orgány veřejné moci* 2021)

The final relationship between equivalent security levels of the Czech cloud computing regulation and EUCS cannot be predicted with absolute certainty, as the cybersecurity requirements of the EUCS have not been finalized yet. However, according to the latest published EUCS proposal, it is possible to assume that the Low security level according to Decree on Security Levels will correspond to the Substantial security level of EUCS, and the Medium security level will be equivalent to the High security level of EUCS. After all, this also corresponds to the justification of the Decree on Requirements for Incorporation, which states: „*...requirements for High and Critical security levels are completely excluded from the potential scope of Cybersecurity Act, as they are related, among other things, to public and national security, which is excluded from the scope of Cybersecurity Act."*(Národní úřad pro kybernetickou a informační bezpečnost 2021, p. 4)

The cited justification refers to Article 16(10) of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union ("NIS Directive"), which states: "*Without prejudice to Article 1(6), Member States shall not impose any further security or notification requirements on digital service providers*." Article 1(6) of NIS Directive contains an exception to this general prohibition for regulation in the interest of national security and the preservation of public order in the member states.[12] Recital 54 of NIS Directive[13] furthermore explicitly develops the exception when it allows for the possibility of public administration bodies to contractually accept other security requirements beyond the scope of existing regulation, if public administration bodies conclude a contract with digital service providers offering cloud computing services. Similarly, recital 56 of NIS Directive[14] expressly allows member states to set additional security requirements for public administration bodies that conclude contracts with digital service providers offering cloud computing.

The exception for national security and public security in Article 1(6) of NIS Directive is used by the Czech legislator to set its own further security requirements in the interest of public security in the High security lev-

[11] The Decree on Security Rules is still not in force, although it is expected to be finalized by the end of this year (2022).

[12] Article 6(1) of NIS Directive: „*This Directive is without prejudice to the actions taken by Member States to safeguard their essential State functions, in particular to safeguard national security, including actions protecting information the disclosure of which Member States consider contrary to the essential interests of their security, and to maintain law and order, in particular to allow for the investigation, detection and prosecution of criminal offences."*

[13] Recital 54 of NIS Directive: *"Where public administrations in Member States use services offered by digital service providers, in particular cloud computing services, they might wish to require from the providers of such services additional security measures beyond what digital service providers would normally offer in compliance with the requirements of this Directive. They should be able to do so by means of contractual obligations."*

[14] Recital 56 of NIS Directive: *"This Directive should not preclude Member States from adopting national measures requiring public-sector bodies to ensure specific security requirements when they contract cloud computing services. Any such national measures should apply to the public-sector body concerned and not to the cloud computing service provider."*

el and for national security in the Critical security level. A similar exception can also be found in Article 1(2) of Cybersecurity Act.[15] This provision is key for the Czech legal regulation of cloud computing in the context of the Article 57(1) of Cybersecurity Act, which stipulates that national certification systems cease to be effective from the date specified in the implementing act and possibly also Article 57(2) Cybersecurity Act, which prohibits Member States from introducing new national cyber security certification systems for services that are already included in the European certification system. Although it was concluded above that the Czech cloud computing regulation can be subordinated to the national cybersecurity certification scheme, the adoption of EUCS will not cause its derogation due to those mentioned exceptions.

Both regulatory systems are supposed to co-applicate as it is expected by NÚKIB in justification of the Decree on Requirements for Incorporation, where NÚKIB states that it will coordinate the expected development in EU regulation by adapting further requirements in the Decree on Requirements for Incorporation with EUCS. (Národní úřad pro kybernetickou a informační bezpečnost 2021, p. 4) Therefore, it can be concluded that it will create a single functioning system in which the Czech regulation will follow the pan-European certification of cloud computing services, only with some possible further requirements in High and in Critical security levels.

Cloud computing service providers would thus have a choice whether to have their services assessed and possibly registered into the catalogue within the framework of Czech legislation, or to undergo pan-European certification of their services according to the EUCS.

If they choose the way of EUCS, then they might be subsequently able to register into the catalogue without the control of their services by the Czech public authority. Because if the providers have their services certified by EUCS, it can be assumed that this will also automatically mean meeting the relevant security level according to the Decree on Requirements for Incorporation. In such a case, it is sufficient to register only the cloud computing provider himself in the catalogue so that he can provide his services to the Czech public administration bodies. An example can be a situation where the provider obtains the European certification of its cloud computing service according to EUCS in the High level. The certificate obtained in such a case will simultaneously demonstrate the fulfilment of the security requirements of the Medium security level according to the Decree on Security Levels. After the provider‘s own incorporation into the catalogue, the provider can also register his service in the catalogue thanks to the EUCS certificate without further assessment of the certified service by the Ministry of the Interior and subsequently offer it to Czech public administration bodies at a Medium security level.(Klodwig 2022, p. 94)

Nevertheless, the other way around (that is to register into the Czech catalogue and then request certification due to EUCS) might not be possible. The reason is obvious and lies in the difference between these two methods. Except for obvious differences such as the different composition of the authorities involved, the assessment of only services and not providers (by EUCS), and different security levels, the crucial difference is in the way control is carried out. While the assessment of the fulfilment of security requirements in the Czech legal system is carried out by the control of documentation, focusing on e.g. certificates, reports on penetration tests and sworn statements, the assessment of requirements according to the EUCS is actually carried out by conformity assessment bodies (CAB) and specialized laboratories. Therefore, while the Czech cloud computing regulatory system mainly checks the documentation of what has already been checked or declared by another entity, EUCS certification is a real fact check that will physically assess the fulfilment of all required criteria.

[15] Article 1(2) of Cybersecurity Act states: ”This Regulation is without prejudice to the competences of the Member States regarding activities concerning public security, defence, national security and the activities of the State in areas of criminal law.”

5. Conclusion

The rise of cloud computing services can represent, from the point of view of cyber security both a benefit and a threat. It always depends on the reliability of the selected cloud computing provider and the security of its specific cloud computing services. Both member states and the European Union are striving to introduce its own cybersecurity regulation, which means that their relationship needs to be analysed.

Both Czech and European regulations of cloud computing are quite different, they have a different goal, different subjects, and also a different method of checking security requirements. Thus, while EUCS carries out factual control and creates a unified certification system for the entire unified digital market, the Czech legislation only performs documentation control and aims to ensure the safe purchase of modern cloud computing services by Czech public administration bodies. Given that the two regulations have a significantly different goal, method and nature, and the Czech public authorities have stated that they are ready to adequately adapt the Czech regulation of cloud computing depending on the final version of EUCS, I conclude that these two regulations should coexist side by side and achieve their goals in a mutual connection.

6. Sources

1. Catteddu, Daniele, 2010. *Cloud Computing: Benefits, Risks and Recommendations for Information Security*. Online. 2010. Springer Berlin Heidelberg. [Accessed 21 October 2021]. Communications in Computer and Information Science.
2. *CyberCon 2021 – Martin Klumpar – Regulace využití služeb cloud computingu orgány veřejné moci*, 2021. Online. Brno, [Accessed 27 September 2022]. CyberCon 2021. Available from: https://www.youtube.com/watch?v=7YBHLXjd0Go
3. ERNST & YOUNG, S.R.O., 2021. *Analýza využití cloud computingu veřejnou správou v České republice*. 23 April 2021.
4. Gill, Sukhpal Singh, Tuli, Shreshth, Xu, Minxian, Singh, Inderpreet, Singh, Karan Vijay, Lindsay, Dominic, Tuli, Shikhar, Smirnova, Daria, Singh, Manmeet, Jain, Udit, Pervaiz, Haris, Sehgal, Bhanu, Kaila, Sukhwinder, Misra, Sanjay, Aslanpour, Mohammad Sadegh, Mehta, Harshit, Stankovski, Vlado and Garraghan, Peter, 2019. Transformative Effects of IoT, Blockchain and Artificial Intelligence on Cloud Computing: Evolution, Vision, Trends and Open Challenges. *Internet of Things*. 1 December 2019. Vol. 8, p. 100118. DOI 10.1016/j.iot.2019.100118.
5. CZECH CHAMBER OF COMMERCE, 2021. *Comments on the material of the National Cyber and Information Security Agency.* Online. 9 February 2021. [Accessed 29 January 2022]. Available from: https://www.komora.cz/files/uploads/2021/02/4_Uplatn%C4%9Bn%C3%A9-p%C5%99ipom%C3%ADnky.pdf
6. Klodwig, Jakub, 2022. *Příručka právní regulace cloud computingu*. Online. 2022. Brno: Nugis Finem. Available from: https://publishing.nugisfinem.org/prirucka-pravni-regulace-cloudu/?utm_campaign=newsletter-ovvm&utm_source=newsletter_PrFMU&utm_medium=email
7. Klodwig, Jakub, 2022. *Regulace cloud computingu ve veřejné správě ČR.* Online. 2022. Brno: Masaryk University. Rigorous thesis. Available from: https://is.muni.cz/auth/th/ucadp/
8. Lesser, Alex, 2017. The Cloud Vs. In-House Infrastructure: Deciding Which Is Best For Your Organization. *Forbes*. Online. 25 July 2017. [Accessed 23 January 2022]. Available from: https://www.forbes.com/sites/forbestechcouncil/2017/07/25/the-cloud-vs-in-house-infrastructure-deciding-which-is-best-for-your-organization/
9. NATIONAL CYBER AND INFORMATION SECURITY AGENCY, 2021. *Justification of Decree No. 316/2021 Coll., on some requirements for incorporation into the cloud computing catalogue.* Online. 1 September 2022. [Accessed 13 September 2022]. Available from: https://www.nukib.cz/images/2021-08-31_oduvodneni_vyhlaska-vstupni-kriteria.pdf

This article was supported by MUNI/A/1293/2022 “Právo a technologie XI”.