OFFICIAL INFORMATION
OF THE CZECH NATIONAL BANK
of 19 August 2016

regarding the pursuit of business in the financial market – cloud computing

I. Purpose and definition of terms

1. The purpose of this Official Information is to inform entities referred to in Article II about the Czech National Bank's approach to the use of cloud computing by supervised entities while exercising financial market supervision.

2. For the purposes of this Official Information, "cloud computing" refers to a model applied in the area of information and communication systems and technologies that enables network access to configurable computing resources (e.g. networks, servers, data storage, applications and services) that are shared by a large number of users and whose capacity is provisioned and released with minimum management effort or intervention of the cloud computing provider.[1] The term "cloud computing" does not occur in the financial market legal regulations.[2]

3. This Official Information follows up on the Official Information of the Czech National Bank of 10 December 2010 regarding the conduct of business in the financial market: Qualitative requirements for the conduct of business – fundamental information, and on the Official Information of the Czech National Bank of 27 May 2011 regarding the pursuit of business in the financial market – operational risk in the area of information systems.

II. Applicability

4. The Official Information applies to a bank, credit union, insurance company and reinsurance company (hereinafter "financial services provider").

5. The Official Information can also be used as a methodological tool by other entities subject to Czech National Bank supervision under Act No. 6/1993 Coll., on the Czech National Bank, as amended, if they use or are planning to use cloud computing.

6. The Official Information also contains information concerning other entities, in particular cloud computing providers.

III. Foundations, principles

7. The legal regulations governing the pursuit of business in the financial market do not prohibit the use of cloud computing. However, financial services providers are obliged to ensure that the activities they carry on are compliant with all the relevant legislative requirements, in particular to ensure sound and prudent pursuit of business in the financial

[1] The definition of "cloud computing" reflects that of the National Institute of Standards and Technology in the USA (2009), which reads: *"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."* (http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf).
[2] This Official Information describes the legal situation as of 10 August 2016. In view of potential legislative changes, the current legal situation must be taken into account when applying this Official Information.

market on a continuous basis also if cloud computing is used by financial services provider.

8. The use of cloud computing within financial services providers' governance systems[3] has all the attributes of outsourcing, i.e. the performance of certain functions or activities of financial services provider by another entity. In the legal regulations, "outsourcing" is referred to using various terms, such as "externally ensured activities" and "activities performed through another person".

9. The relevant European authorities and regulations confirm the consistency of outsourcing legal rules set forth for the insurance sector, banking sector and capital market sector.[4]

10. The proportionality principle is applied to the use of cloud computing by financial services providers and to the supervision thereof.[5] Under the proportionality principle, financial services providers cannot entirely exclude the application of any of the rules contained in the legal regulations, but the manner of application thereof should be proportionate to the nature, scale and complexity of the activities concerned, the related risks and other relevant circumstances of the case.

IV. Final provisions

11. More detailed information of the Czech National Bank on cloud computing is contained in the annex hereto.

12. Given the dynamic development of information and communications systems and technologies, continuous account should be taken of changes in the environment in which financial services providers and cloud computing providers operate, in particular changes in the technological and legal environment, in the regulatory framework and in the area of recognised standards and practices regarding cloud computing.[6]

13. This Official Information shall take effect on the date of its promulgation in the Bulletin of the Czech National Bank.

Vice-Governor:

Mojmír Hampl

[3] For example, Article 7 of Act No. 277/2009 Coll., on Insurance, as amended, Article 8(b) of Act No. 21/1992 Coll., on Banks, as amended, and Article 7(a) of Act No. 87/1995 Coll., on Credit Unions, as amended.

[4] For example, recital 37 of Directive 2009/138/EC on the taking-up and pursuit of the business of insurance and reinsurance (Solvency II) and point 18 of the Guidelines on Internal Governance (GL 44) (EBA BS 2011 116) of the European Banking Authority in conjunction with the CEBS Guidelines on outsourcing (2010), pp. 1 and 2.

[5] For example, Article 29(3) and Article 41(2) in conjunction with recitals 19 and 31 of Directive 2009/138/ES and Article 74(2) of Directive 2013/36/EU on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC.

[6] For example, European Union Agency For Network And Information Security (ENISA): Secure Use of Cloud Computing in the Finance Sector – Good practices and recommendations; December 2015 (https://www.enisa.europa.eu/publications/cloud-in-finance); Australian Prudential Regulation Authority (APRA): Information paper on outsourcing involving shared computing services, including cloud; July 2015 (http://www.apra.gov.au/mediareleases/pages/15_17.aspx).

Annex

Financial Market Regulation and International Cooperation Department
Responsible employee:
Věra Mazánková, telephone number: 224 412 821

Annex

More detailed information about the approach of the Czech National Bank to cloud computing

General information

1. An information and communication system[1] that is adequate, efficient and effective as a whole and in its parts is an obligatory part of a financial services provider's governance system.

2. Where a financial services provider arranges to have some of its functions or activities which it could otherwise perform itself, performed on the basis of a mutual agreement through a third party by using cloud computing, such an arrangement constitutes outsourcing.[2]

3. If outsourcing is used, the financial services provider's governance system must ensure sound and prudent pursuit of business on a continuous basis, including compliance with the financial services provider's legal obligations as regards, for example, risk management, internal control mechanisms, information flows, personal data protection and cyber security.

Proportionality

4. Compliance with the regulatory requirements applying to outsourcing can be lightened or modified proportionately to the nature of the processed data and operations, the degree of complexity of the use of cloud computing, the concrete person of the cloud computing provider and other relevant facts and circumstances.[3] The same goes for compliance with the legal rules applying to chain outsourcing.[4] Lightening or modification is acceptable, for example, in the case of information and communication systems for the support of cooperation and information exchange only within the financial services provider or within the group of which it is a member, or in the case of the storage or processing of publicly available data. However, if the resulting situation, even after taking the proportionality principle into account, is inconsistent with the legal obligations applying to financial services providers, the financial services provider should not use cloud computing in the area in question.

Assessment by the supervisory authority

5. When exercising supervision of financial services providers that use or are planning to use cloud computing, including the potential use of cloud computing by a financial services provider on the basis of a contractual agreement within the group of which it is a member, the Czech National Bank assesses whether the financial services provider

   a) defines in its strategies its overall approach to, and main principles of, the use of cloud computing in a sufficiently clear and specific manner,[5]

   b) takes due account in its strategies, principles and related internal rules and procedures of the specificities ensuing from the nature of cloud computing, including their effect on

---

[1] For example, Article 41(2) of Directive 2009/138/EC and Article 23 in conjunction with Article 7(1)(d) of Decree No. 163/2014 Coll., on the performance of the activity of banks, credit unions and investment firms.

[2] For example, Article 49 of Directive 2009/138/EC in conjunction with recital 28 and Article 12(1) of Decree No. 163/2014 Coll.

[3] For example, Article 49(2) of Directive 2009/138/EC and Article 258 of Regulation (EU) No. 35/2015 of the European Parliament and of the Council, supplementing Directive 2009/138/EC of the European Parliament and of the Council on the taking-up and pursuit of the business of insurance and reinsurance (Solvency II), and Article 12 and Annexes 6 and 7 of Decree No. 163/2014 Coll.

[4] For example, Article 274(4)(l) of Regulation No. 35/2015 and point 8 of Annex 7 of Decree No. 163/2014 Coll.

[5] For example, Article 258(2) and (3) of Regulation No. 35/2015 and Article 18(1)(d) and (f) and (2)(d) of Decree No. 163/2014 Coll.

1. compliance with the financial services provider's legal obligations, including obligations towards clients and the obligation to ensure business continuity, and
2. the financial services provider's ability to prove compliance with its legal obligations to the Czech National Bank, including documentation of the procedures applied.

6. The Czech National Bank assesses, in particular, whether the financial services provider
   a) takes due account of the effect of cloud computing specificities on the scope, content, traceability and recoverability of information about the governance processes of the cloud computing provider,
   b) takes due account of the effect of cloud computing specificities on the control activities (controllability) and auditing of outsourced processes performed by the cloud computing provider, the financial services provider or any other competent persons designated or accepted by them,
   c) recognises, assesses and takes due account of all other important effects of cloud computing specificities that are relevant to the assessment of risks relating to the outsourcing,
   d) takes due account of the fact that transparency and the financial services provider's ability to perform effective controls of outsourced functions and activities tends to decrease as the complexity of the cloud computing it uses increases, and adopts appropriate measures to mitigate the related risks or their impacts, including consideration of the possibilities of insurance, or decides to limit the outsourcing, and
   e) recognises, assesses and takes due account of the effect of cloud computing specificities in all stages of the outsourcing life cycle.[6]

7. The Czech National Bank also assesses compliance with other prerequisites for the sound and prudent use of cloud computing by the financial services provider, in particular whether the financial services provider
   a) has assessed the impacts of incorporating cloud computing services into its existing organisational arrangements, stipulated procedures and its activities in order to identify new risks to which it may be exposed,[7]
   b) takes due account of the fact that the use of outsourcing does not affect the financial services provider's ultimate responsibility for sound and prudent pursuit of business, and whether, in order to comply with its legal obligations, it continuously has sufficient expert capacity to prepare, implement, manage and control the overall use of cloud computing and individual cases of its use,
   c) regularly assesses whether its internal rules on cloud computing and the real activities it performs are consistent with the legislation setting forth its obligations, including those lying outside the scope of the supervisory authority of the Czech National Bank, for example in the area of personal data protection and cyber security,
   d) has sufficient information in all stages of the outsourcing relationship life cycle about governance processes relevant to the assessment of all risks arising from the use of cloud computing, as well as documents and information about the cloud computing provider's

[6] The life cycle comprises the following stages and elements: the preparation of the contractual relationship, the contract itself, the operation and use of the service, and the end of the contractual relationship; see, for example, point 1.116 of the EIOPA Guidelines on system of governance (EIOPA-BoS-14/253).

[7] For example, Article 44(1) and (2)(e) and (f) of Directive 2009/138/EC, Articles 258 and 260(1)(f) and (g) of Regulation No. 35/2015, points 1.3, 1.26, 1.34(d), 2.121, 2.3 and 2.6 of Guidelines EIOPA-BoS-14/253 and Article 34(1) of Decree No. 163/2014 Coll.

internal risk mitigation procedures and measures, and whether those documents and other available information enable the financial services provider to continuously identify and assess the risks it undertakes in relation to the use of cloud computing, to assess the cloud computing provider and the services it provides, and to assess the effectiveness of the outsourcing,

e) has the right to conduct directly or assign a control or audit of processes that are important for the security and availability of data, services and outsourced activities on site at the cloud computing provider,

f) can, in all stages of the outsourcing relationship life cycle, continuously and without unnecessary restraints contact the cloud computing provider's designated employees who are fully competent and have been authorised in advance by the cloud computing provider to provide explanations and information concerning the cloud computing provider's internal processes and procedures relating to the outsourced functions, data and services, including explanations of information, findings and remedial measures concerning audit reports written by the internal auditor of the cloud computing provider or an external cloud computing assessor where relevant to the outsourcing,

g) has put in place procedures for identifying and managing risks associated with cloud computing and applies them on a continuous basis and the procedures enable it to ensure traceability and reconstruction of the procedures actually applied,

h) has conducted an analysis of the risks of the use of cloud computing, which analysis is updated regularly and upon any important change relating to the use of cloud computing, and whether the specific risks of cloud computing at least in the organisational, technical and compliance areas are identified in the risk analysis,

i) uses the risk analysis for the purposes of
   1. preparing the contractual relationship,
   2. managing operational,[8] reputational and concentration risks and other risks relating to cloud computing and its use, and
   3. controls of the outsourcing provider, for example in the areas of security principles, security monitoring and security incident management,

j) has established cloud computing security principles in which it specifies the main principles and procedures for ensuring confidentiality, integrity and availability of information,

k) is informed about the countries in which its data are or may be stored, and identifies and takes account of data location risks,

l) is familiar with the procedures applied by the cloud computing provider for responding to any events (security incidents) that would jeopardise or disrupt the information systems security or security of the financial services provider´s data,

m) has made an assurance that the cloud computing provider's working methods in the area of secure access to information are at least at the same levels of those the financial services provider would use to comply with its governance system principles if it performed the activity itself,

n) knows the conditions of access of the cloud computing provider's employees to the financial services provider's data, including measures applied and checks of compliance with requirements, and whether it has ensured that cases where the cloud computing

[8] Operational risk includes, for example, legal risk, compliance risk, outsourcing risk, system risk, model risk and the risk of inadequate or failed persons or processes.

provider's employees have access to the financial services provider's data is limited to what is absolutely necessary (servicing),

o) has ensured that the cloud computing provider records events that jeopardise or disrupt the security of information systems and allows the financial services provider to obtain all information concerning incidents that jeopardise or disrupt the security of the financial services provider's data,

p) has ensured that if an employee of the cloud computing provider or another person working for it (chain outsourcing) gains access to its data during data processing in cases other than servicing, this is immediately reported to it as a security incident,

q) has concentrated in its contingency plans notably on the situation of limited access to its own data and the transfer of its own data back or to another outsourcing provider,

r) has included in its contingency plans the event of unexpected termination of the cloud computing provider's operations,

s) ensures up-to-date, regular expert assessment and assurance and also independent expert assessment and assurance of governance processes,[9] including identification, description and assessment of all risks undertaken by the financial services provider in relation to the use of cloud computing, and whether it uses all available means and forms in this assessment and assurance, including findings from its own controls of the cloud computing provider and an external independent assessment conducted at the cloud computing provider in accordance with internationally recognised standards for the risk management in the area of nformation and communication systems and technologies,

t) has relevant documentation meeting the traceability and reconstruction requirements for each independent expert assurance of governance processes conducted, and whether the documentation regarding such assurance, in particular the report on findings, is permanently available to it, and can provide this documentation to the Czech National Bank when requested[10] so it can be used for the purposes of supervision exercised by the Czech National Bank under the relevant legislation, and

u) the contract documentation enables the financial services provider to unilaterally terminate the outsourcing relationship.

8. The Czech National Bank also assesses whether the financial services provider has ensured further prerequisites for the effective supervision of outsourcing by the Czech National Bank taking into account the specificities of cloud computing. As part of this, it also assesses whether the financial services provider

   a) has notified the Czech National Bank under its outsourcing reporting duty[11] of the person or persons providing independent external expert assessment and assurance about cloud computing to the cloud computing provider; the purpose is to ensure timely notification of the Czech National Bank of the person who the cloud computer provider has designated as the external cloud computing assessor, and

   b) has ensured potential direct exchange of information between the outsourcing provider and the Czech National Bank and further requested cooperation between the cloud computing provider and the Czech National Bank, including the designation of contact persons of the cloud computing provider for such purposes, and further rules necessary for effective supervision.

[9] For example, the third subparagraph of Article 41(1) of Directive 2009/138/EC in conjunction with Articles 258(6) and 266 of Regulation No. 35/2015.
[10] For example, Article 35(1) of Directive 2009/138/EC.
[11] For example, Article 49(3) of Directive 2009/138/EC and Article 107 of Decree No. 163/2014 Coll.