PRUDENCIÁLIS MODELLEZÉSI ÉS IT FELÜGYELETI IGAZGATÓSÁG

Frequently asked questions concerning the use of cloud services (FAQ)

TRANSLATION

Consultation

1. Is there an option for the Institutions to consult with the Supervision concerning the use of cloud services?

Yes, the Supervision is open for consultation, which should be initiated via the appointed supervisor of the institution. In complex cases of innovative financial solutions which require the involvement of several supervisory areas, and in case of innovative solutions, for which the Fintech innovator does not hold a licence, MNB Innovation Hub (https://www.mnb.hu/innovation-hub) provides a platform to seek regulatory assistance. MNB Innovation Hub can be contacted through the questionnaire[1] available on the platform.

2. When is it reasonable to consult with the Supervision?

Consultation with the Supervision is not mandatory, but we advise the Institutions to consult with MNB before entering into cloud outsourcing with high impact, involving critical functions, or to ask for guidance before provisioning cloud services if necessary.

Regulation

3. What is the regulatory background for the use of cloud services?

Generally, for the financial sector, information security requirements are set out by Government Decree No. 42/2015. (III. 12.) on protecting the information system of financial institutions, insurance undertakings, reinsurance undertakings, investment firms and commodity dealers, as well as by sectoral laws. Use of cloud services, specifically, is regulated (at the time this FAQ is published) by Recommendation 4/2019 (IV. 1.) of the Magyar Nemzeti Bank[2] on the usage of community and public cloud computing services (MNB cloud recommendation), Recommendation 7/2017 (VII. 5.) of the Magyar Nemzeti Bank[3] on the security of information systems, EBA's[4] Guidelines on outsourcing arrangements (EBA/GL/2019/02), EIOPA's[5] Guidelines on outsourcing to cloud service providers (EIOPA-BoS-20-002), and ESMA's[6] guidelines on cloud outsourcing which are currently under preparation. Outsourcing is (currently) regulated by Recommendation 7/2020 (VI. 3.) of the Magyar Nemzeti Bank on the usage of external service providers. Other relevant legislation, recommendations and guidelines are referenced in the MNB cloud recommendation.

---

[1] https://mnbpoll.mnb.hu/Survey.aspx?surveyid=70754442&lng=hu-HU

[2] English translation: https://www.mnb.hu/letoltes/4-2019-cloud-bg.pdf

[3] MNB expects the application of Recommendation 8/2020. (VI.22.) of the Magyar Nemzeti Bank beginning on 1 January 2021

[4] European Banking Authority

[5] European Insurance and Occupational Pensions Authority

[6] European Securities and Markets Authority

Definitions

4. What factors determine whether a cloud service model qualifies as private or community cloud?

If the service provided fulfils the criteria of a cloud service, but the infrastructure is under the control of the Institution in its entirety, and the service is used exclusively by the Institution, it qualifies as a private cloud. If a cloud is used exclusively by a group of companies (e.g. members of a corporate group), it constitutes a community cloud.

5. What is a private cloud?

The principal quality of a private cloud is that every constituting IT equipment and software is under the control of the organisation using it, therefore the Institution bears all responsibility concerning its hardware, software, infrastructure, and availability. These resources are not shared with outside participants, they are only accessible from inside the organisation.

6. Is managed private cloud considered as private cloud?

As a general rule, no. The MNB cloud recommendation contains no reference to managed private cloud, the definition and usage of the term is inconsistent and contradictory across the industry. According to a popular definition, a managed private cloud uses the client's data centres and devices, but the operation and maintenance of the cloud infrastructure is the task of a service provider. According to another interpretation the managed private cloud service provider operates their own cloud infrastructure and provides the service on devices which are made exclusively available to the customer. According to the MNB's interpretation, a cloud service can only be considered as private cloud if the infrastructure supporting the service provided to the Institution is segregated on a hardware level. Even in the case of such an arrangement, outsourcing regulations should be observed.

7. Is a cloud service used exclusively by the members of a group considered as private cloud?

No, such an arrangement is a community cloud. For further explanation, see Question 4.

Scope of the cloud recommendation

8. Is the MNB cloud recommendation applicable to insurance agents?

If the agent's activity encompasses the processing of client data – including the data belonging to the agent's clients – it is in the recommendation's scope.

Compliance

9. If a cloud service is compliant with EBA/EIOPA/ESMA requirements, is compliance with MNB's cloud recommendation also required?

The MNB cloud recommendation contains the requirements set out in the EBA/EIOPA/ESMA guidelines but determines further information security requirements for the entire life cycle of the service, by also taking the Hungarian legal environment into account. Therefore, compliance with MNB's cloud recommendation is also necessary.

10. Which cloud service models, solutions or service providers are accepted by the Supervision?

The Supervision sets out its requirements in a supplier and technology neutral manner, since the Supervision focuses on robust data protection, transparency, the proper management of arising risks, the adequacy of controls and legal compliance regarding the use of cloud services.

11. Is MNB Recommendation No. 4/2019 (IV. 1.) on the usage of community and public cloud computing services applicable to temporarily acquired cloud services?

The MNB cloud recommendation should also be applied to cloud services which the Institution procures for a limited amount of time (e.g. cloud bursting). For such services, the entire life cycle of cloud services apply, therefore the requirements set out in the MNB cloud recommendations should be complied with (including recommendations on entering the details of the arrangement into a register and the reporting the contract to MNB).

12. Are Institutions which are registered as service providers required to provide information to the National Cyber Defence Institute also expected to comply with the MNB cloud recommendation if they use cloud services?

Yes, provided that the Institution, organisation, person, or activity falls under any of the Acts set out in Section 39 of Act CXXXIX of 2013 on the National Bank of Hungary.

13. Which services are allowed to be outsourced into the cloud?

The services that may be outsourced are governed by sectoral laws, and by the MNB recommendation No. 27/2018. (XII.10.) on setting up and using internal safeguards and on the management and control functions of financial organisations, and MNB recommendation No. 7/2020. (VI. 3.) on the usage of external service providers. In general, services that may be outsourced may also be outsourced into the cloud, provided that risks are appropriately managed throughout the process. The MNB cloud recommendation also applies if an outsourced service provider uses cloud services while fulfilling their contract.

14. Which risk analysis methods are accepted by MNB for using cloud services?

The MNB does not favour any particular risk analysis methodology, but the risk analysis should demonstrably be able to fulfil the requirements of applicable sectoral laws, and the requirements determined by Recommendation No. 7/2017 (VII. 5.) of the Magyar Nemzeti Bank on the security of information systems.

15. What considerations should be taken into account when developing contractual requirements?

The contract should cover the entire life cycle of the service and all risks that may arise during that period. The pro forma contracts offered by the cloud service provider (CSP) may not be flexible enough to accommodate the Institution’s requirements and achieve compliance with the regulatory environment. Therefore, it is recommended that the Institutions opt for the service package offered to financial institutions. Concerning important terms of contract, at least the following should be covered:

- conditions of termination, determining the termination period,
- unconditional audit rights,
- data processing and handling locations,
- data security and data protection requirements throughout the entire service chain,
- incident management and fraud detection (forensic) processes, and
- exit strategy.

Contractual requirements are governed in detail by the MNB cloud recommendation, but sectoral laws governing outsourcing also apply, along with the cloud guidelines published by the European Supervisory Authorities.

16. What is considered best practice for the level of detail and documentation of the exit strategy?

Both an exit strategy and an exit plan should be developed.

The exit strategy should contain the conditions of initiating an exit procedure, the timeframe of the execution, and the main steps and people responsible should be set out. It should contain the source, the channel, the tools, and the structure of the Institution’s data to recoup, and it should cover the way the

service will be provided after the termination of the contract (on-premise, different service provider). Exit plans should cover the scenario of an unplanned exit.
Terms and cost of exit should also be governed by the contract.

Information security

17. Is the redundancy provided by a single data centre adequate for the use of cloud services?

The redundancy provided by a single data centre is not enough, since it does not address major risks which potentially result in the loss of that data centre (i.e. natural disasters), the loss of internet connectivity to a certain region, or a blackout. Backups should also be stored in a different location which is not likely to be affected by the risks of the primary site, therefore the use of a single data centre is not adequate.

18. Is CSP independent backup necessary in every case?

Backups stored independently from the CSP[7] should be ensured based on the criticality of the functions and data, while taking relevant risks into consideration. The Institution should determine whether an independent backup is necessary, and define the data that should be included, the frequency and method of creating backups, and where and how backup data should be stored. CSP independent backup can be implemented on-premise by the Institution or through a different CSP – but in the latter case, the storage of backups also falls under the purview of the MNB cloud recommendation. Independent backups should also be ensured while using Software as a Service (SaaS) or similar, CSP specific services – in a risk-proportionate manner – which should enable the Institution to restore the service as required by the business continuity plans and the exit strategy. The feasibility of CSP independent backup should be assessed during the preliminary analysis, considering the materiality of the service.

Accountability

19. What duties does the Institution have concerning the tasks performed by the CSP?

CSPs contractually agree to offer certain service elements based on the service model (e.g. Infrastructure as a Service, Platform as a Service, Software as a Service). Institutions should, prior to signing the contract, analyse the risks attached to each cloud service element, assess the controls implemented by the CSP, and should make a documented decision about the Institutions' requirements which need to be met before the Institution deems the risks of a service acceptable. Naturally, if the risks cannot be mitigated adequately, signing the contract is not advised. The Institution should periodically assess whether the CSP is performing its tasks in an adequate manner, and whether the operational risks presented by running the services in the cloud require corrective actions or the amendment or termination of the contract. If a major incident occurs, an unscheduled assessment should be performed.
For other service elements (e.g. user administration), CSPs only offer the possibility to ensure the security of the service, but the actual settings, administration should be performed by the Institution.
The separation of tasks should be defined in the contract.
Responsibility and accountability for both the service offered to clients, and the protection of clients' data and assets, remain with the Institution – even if they choose to opt for using a cloud service.

[7] such backups that are prepared and stored independently from the primary cloud service provider

Data protection

20. Is the inclusion of a CSP residing outside the EEA acceptable?

Institutions should comply with the sectoral legislation and recommendations – but besides those, legal requirements for data protection (e.g. EU General Data Protection Regulation) and information security should also be met. If the usage of a cloud service involves a country which is either not an EEA[8] member state or a country which does not have data protection equivalent to the EU's, the Institution should be able to provide sufficient information to the relevant authorities about both the risks arising from such an outsourcing and the methods of risk mitigation. Therefore, moving data to a location outside the EEA creates additional assessment and control requirements, which should be enforced through contractual and/or technological means.

Auditing cloud services

21. What are the requirements for accepting third party audit reports and certifications concerning cloud services?

Reports and certifications issued by third parties (which are independent from the Institution) should provide assurance on the existence and the effective operating of controls; their scope should cover the service in its entirety (timescale, processing locations, controls, services, systems, etc.). The personnel conducting the audit/certification should possess relevant skills which satisfy the needs of the Institution. The Institution should have the right to inspect relevant audit findings and evidence and should be able to interpret the findings and recommendation within its own risk management framework. Findings and recommendations should be rectified in a documented manner.
Multiple clients may conduct joint audits at the CSP.
CSPs are not supervised or evaluated by the Supervision, but the Supervision reserves the right to conduct an audit of outsourcing at the CSP if necessary.
If the procurement of the cloud service qualifies as outsourcing, the audit requirements for outsourcing arrangements set out by sectoral laws should also be adhered to.

22. To what extent does the Supervision accept independent audit reports or certifications in the context of cloud services?

The Central Bank of Hungary (MNB) may take third party audit reports into account at its own discretion, depending on their scope, level of detail, reliability, and level of independence. The audit processes of the Institution should set out the conditions based on which the Institution accepts third party reports and certifications, and it should be able to demonstrate that the reports accepted by the Institution satisfy these conditions, and comply with legal and regulatory requirements.

[8] European Economic Area