Stepping onto the clouds

– briefly about what to do for clouds to finally appear over the Polish financial market

Step I – basics and what to pay attention to

Introduction

In January 2020, the Financial Supervision Authority (KNF) issued a Communication which was soon after referred to as the „KNF Cloud Communication" („the Communication"). Some time later, KNF published a list of frequently asked questions and answers (Q&A), which was then updated after feedback from various participants of the financial market in Poland. The last update of the Q&A document took place at the end of March 2021. The following practical analysis and summary of the information included in the Communication will enable the entities supervised by KNF, as well as the potential IT services providers offering services to these entities, to understand key aspects of the Communication and the conclusions resulting from it. Due to the broad scope of the topic, the whole analysis has been divided into two parts:

- **Step I** – basics and what to pay attention to
- **Step II** – how to make your first step in the clouds and not fall down

Source:

Communication from the KNF on information processing by supervised entities using public or hybrid cloud computing services of 23 January 2020

Questions and answers (Q&A) on the application of the KNF Communication of 23 January 2020

MARCIN STADNIK
HEAD OF SII FINANCIAL SERVICES,
BANKING & INSURANCE INDUSTRY

Who does this concern?

The subjective scope of the Communication is identical to the scope of financial market supervision exercised by the Financial Supervision Authority. All supervised entities are obliged to follow the Communication guidelines. Therefore, it should be borne in mind that, in addition to the fairly obvious market participants, their ranks also include:

- **insurance agents**, when processing legally protected information in the cloud
- capital market infrastructure entities, investment firms
- **investment funds** – if their transfer agents, who maintain the register of participants at the request of investment funds, use the cloud service for this activity – the Communication guidelines also apply to such funds; the obligation in this area rests with Investment Fund Company (TFI), as the body of the fund
- **foreign branches** of insurance and reinsurance companies within the meaning of the Act on Insurance and Reinsurance Activity (UDUR)
- **MIP, AISP and PISP***

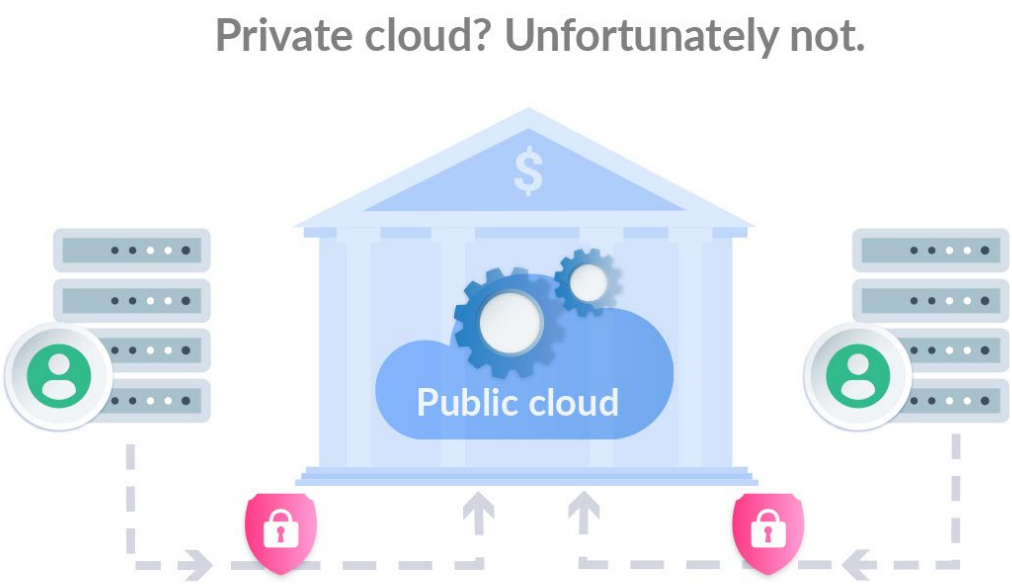
* Under PSD2, respectively: Small Payment Institution, Account Information Service Provider, Payment Initiation Service Provider are supervised entities within the meaning of the Act on KNF's supervision, therefore the Communication shall apply to them in its entirety.

Cloud types according to the Communication:

Key definitions:

- **public cloud** – cloud available for public use, owned or directly managed by a cloud service provider; cloud resources are shared with other entities
- **private cloud** – cloud available for the exclusive use of one entity, owned or directly managed by that entity
- **hybrid cloud** – cloud, consisting of a combination of two or more separate clouds (public, private, community clouds), which allows the transfer of information processing activities between the clouds which create it
- **community cloud** – cloud which is used exclusively by a specific group of entities related by shares or under a cooperation agreement, with pre-defined common rules and requirements, among others, in the area of compliance and security of information processing, owned or managed directly or indirectly by an entity or entities in the group or at its or their request; it may be public or private – depending on who owns or directly manages the cloud infrastructure:
  - if the provider, this cloud is public
  - if the supervised entity (alone or in cooperation with other entities supervised under a cooperation agreement or a capital group), this cloud is private

Private community cloud **cannot be managed by a third party** on behalf of the supervised entities.



Key aspects differentiating clouds:

- exclusivity of access to the cloud or no exclusivity on the part of the supervised entity
- ownership or direct management of the cloud by the supervised entity
- **Ownership or direct management** is understood in particular (though not exclusively) as:
  - possibility to make changes to the infrastructure (including hardware replacement, software update),
  - deciding on the rules for physical access to the infrastructure,
  - deciding on the rules for the physical and logical protection of the infrastructure.

Ownership of the cloud **does not mean** that the supervised entity should be at the same time its owner. However, the supervised entity should ensure that the owned cloud is secure in legal and actual terms for the duration of its use, taking into account the time needed to securely migrate to another cloud or moving back from the cloud to the on-premise infrastructure.

Direct cloud management means that the supervised entity, **without the involvement of a third party,** controls the cloud **within the limits of the staff resources at their disposal and under its control**. Cloud managers (administrators) should perform activities for the benefit of the supervised entity in a direct relationship i.e. without the involvement of third parties, e.g.:

- IT team cannot provide services for the benefit of the supervised entity through a job agency,
- actions cannot be performed through the secondment of a specific person by an IT company with which the supervised entity signed an agreement on the provision of IT services,
- actions cannot be performed through the secondment of a specific person by an IT company within the capital group to which the supervised entity belongs.

Not obvious examples of a public cloud which may seem to be private

If:

- the place of the physical installation of the IT infrastructure is the server room of the supervised entity or the data processing center chosen by the supervised entity

and

- cloud management is remote, performed by a cloud service provider or a third party using a secure internet connection,

the service configured in such a way is a **public cloud**.

If:

- cloud infrastructure is not intended for the exclusive use of one entity,
- the supervised entity may create a virtual private cloud on a scalable infrastructure of a cloud service provider (e.g. Virtual Private Cloud),

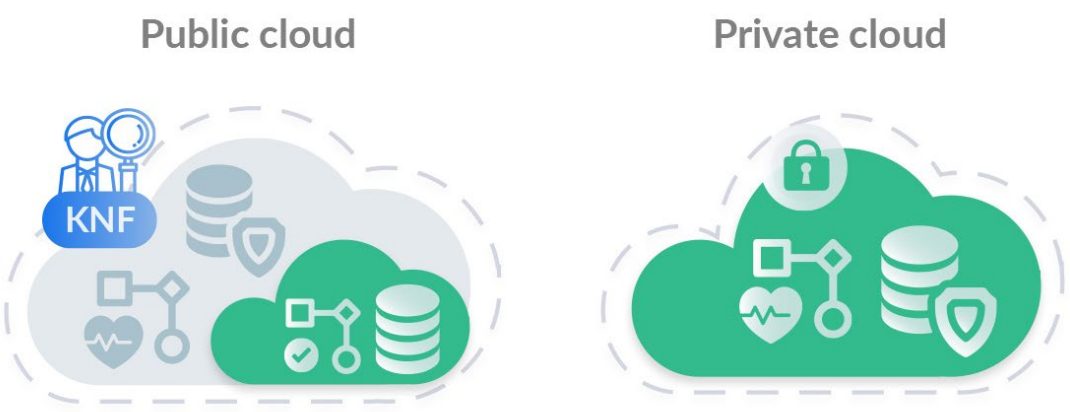
the service configured in such a way is a **public cloud**.

The use of virtual servers with the guarantee of resources (VPS – Virtual Private Server), which are based on virtual partitioning of a physical machine into several smaller virtual servers, **cannot be treated as using a private cloud** by the supervised entity, as defined in the Communication. Using virtual servers, the supervised entity does not directly manage the cloud infrastructure on which the virtual server is running, which means the cloud is **public**.

The use of the cloud by supervised entities as described above is **allowed**, however, **it involves the obligation to follow the Communication guidelines**.

Only **direct management of the cloud by the supervised entity** (with the exclusive use of the infrastructure in the IaaS model but **not in PaaS or SaaS models**) results in the recognition of the service as **a private cloud.**

On the other hand, if the service provided to a supervised entity by a third party is **based on a private cloud** (owned and managed by a third party), the supervised entity uses a **public cloud**.



When is cloud outsourcing specific?

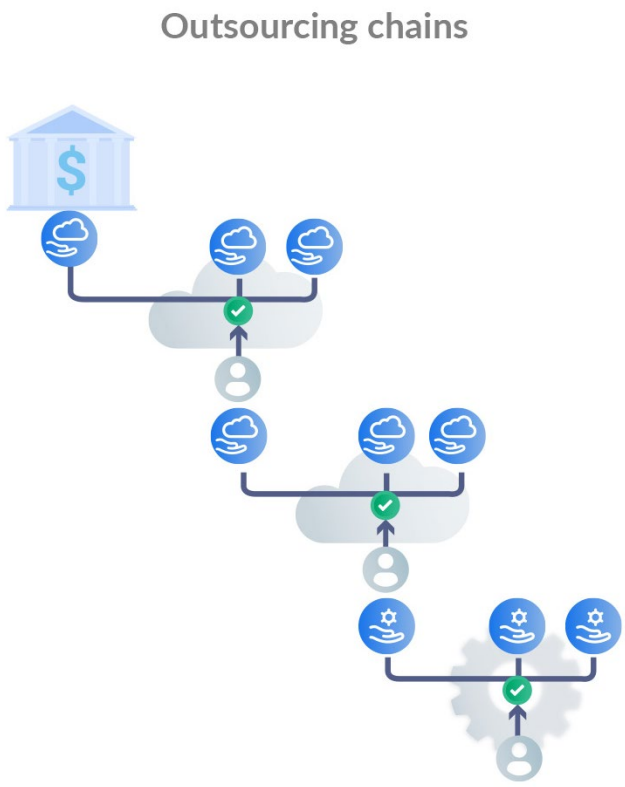
The cloud information processing service is understood as entrusting the processing activities and – depending on the category of information processed and actual processing activities – can be treated as cloud outsourcing or special cloud outsourcing.

- **cloud outsourcing** is understood as an agreement under which a cloud service provider provides the supervised entity with a service which supports the execution of a process, service or task which the supervised entity would perform on its own if the cloud service was unavailable.
- **specific cloud outsourcing** is understood as outsourcing in which the supervised entity entrusts the cloud service provider with the performance, by means of a cloud service, of those activities or functions of the supervised entity, which – if lacking or interrupted due to a failure or violation of the rules of safe cloud computing – **would have a significant impact on the continuous fulfillment** by the supervised entity of the requirements underlying its license to run or conduct supervised activities or **pose a material threat to the supervised entity's financial performance, or the reliability or continuity** of its supervised activity.

Therefore, the basis of the **specific outsourcing definition** is the concept of critical and essential functions, activities and processes of the supervised entity from the perspective of the supervised activity carried out.

The supervised entity should **continuously monitor** which processes and to what extent are processed using the cloud **in case the scale of the process to be assessed changes**. A process which was not initially assessed as critical and important may increase in scale over time and in consequence be reclassified as key and critical.

KNF reserves the right to verify the assessment made by the supervised entity as to the criticality and importance of a particular process. That is why **the supervised entity should have documented justification for the qualification of all processes and functions in the context of their criticality and importance.**



In which cases should the Communication guidelines be applied?

The subjective scope – the supervised entity should determine – for each cloud service which is planned or already in use – whether legally protected information is processed, and whether the processing activity can be defined as specific cloud outsourcing. If the cloud is used for activities related to regulated operations, the Communication applies.

KNF expects the supervised entities to use the reference model, specified in the Communication, if:

- the information to be processed is **legally protected information**

  or

- the processing of information is **specific cloud outsourcing**

  and

- information processing takes place in a public or a hybrid cloud (to the extent it is based on a public cloud).

The Communication does not apply to information (unless legally protected) processing in a private cloud.

The supervised entity should determine whether **legally protected information is processed** and whether the processing activity can be defined as **specific cloud outsourcing**.

» Therefore, if the processing concerns information other than legally protected and outsourcing does not qualify as specific, the Communication may, but does not have to, be used.

In case of doubt, the more stringent requirement should be adopted.

The use of the Communication should be with respect to **the principle of proportionality**, at the same time taking into account the reference model. The principle of proportionality should be applied at the stage of assessing the risk associated with the planning of processing activities and the adequacy of the safeguards used for the information processed. The principle of proportionality should not be interpreted as permission for smaller supervised entities to use **less effective safeguards** for the information processed than those described in the Communication. In other words, it is about applying this principle **in proportion to the assessed risk**, and not to the scale of activity of the supervised entity.

The Communication does not apply where relevant specific legal provisions impose the obligation to meet certain technical or organizational requirements on the processing of certain information which would exclude the possibility to comply with this Communication. In other words:

» The Communication is an „addition" to the specific legal regulations applicable to a given category of supervised entities, but where the requirements of the Communication conflict with the specific provisions of those regulations, those legal regulations shall prevail.

The Communication guidelines do not have to be applied during the design and operation of **test or development environments** in a cloud, as long as **legally protected information is not processed**.

Legally protected information must always be encrypted at rest and in transit.

And what about EU regulations on outsourcing and cloud computing?

The Communication outlines the national approach to the outsourcing of cloud-based information processing for the financial sector (**reference model**). Guidelines, recommendations and other documents presenting the position of the European supervisory bodies, which relate to the processing of information in a public or a hybrid cloud, **do not apply to the supervised entities** to the extent that they contradict the Communication. **The national approach** presented in the Communication **applies in this case**.

Chains in the clouds or clouds in chains?

Outsourcing chain

- relationship which consists in a cloud service provider entrusting certain activities (performed to deliver a cloud service to a supervised entity) to its subvendor and further subvendors

or

- relationship which consists in a cloud service provider providing a cloud service to another provider which uses the cloud service to provide its own service to a supervised entity.

Of course, everything within the limits of outsourcing allowed by legal regulations applicable to the supervised entity. The supervised entity should assess the admissibility of the transfer of a particular type of data within the legally permitted outsourcing chain, i.e. for example, the number of entities in it.

Admissibility and scope of actions related to **legally protected information**, entrusted by the supervised entity should be interpreted as: **no prohibition on individual activities is not an admission** to perform a specific activity.

- **Subvendor** is an entity which provides services to a cloud service provider for the purpose of providing the cloud service to a supervised entity and has or may have identified access to information processed by the supervised entity.

If it does not or may not have access to the information, it is not a subvendor.

- **Tenant** – a cloud service instance assigned to a supervised entity. The key feature of a tenant is its default logical separation (in terms of configuration and information processing) from other tenants.

Each supervised entity may have multiple tenants with the same cloud service provider, provided that all the requirements concerning tenant separation are met.

SaaS – if a provider (other than a cloud provider) offers a SaaS-based software delivery service to multiple supervised entities, and **the data of these entities are separated only in a logical way**, i.e. each supervised entity has its own independent system instance, from the point of view of the supervised entity, regardless of the model of other services used by the provider (other than cloud), the service is offered in the **public cloud** model.

The fact of not having a **contractual relationship with the subvendor does not exempt the supervised entity from obligations specified in the Communication**. The supervised entity should therefore ensure what legal, corporate or logical safeguards will enable the subvendor to effectively apply the Communication guidelines and follow the law. KNF recommends that the cloud subvendor should be directly involved in the process of assessing the security of the processing **of legally protected information** and information covered by **specific outsourcing**.

- **Information disclosure** is understood as a situation in which information is processed in a cloud in a manner which is either unencrypted or encrypted at rest or in transit but the cloud service provider or its subvendor in the outsourcing chain has access to the encryption keys and the information encrypted with those keys.

Last but not least, the very important position of KNF, highlighted several times in the Communication and the Q&A document:

» encryption of information does not reduce the importance of information, nor does it change its classification and assessment (e.g. as legally protected information), in particular, **encryption cannot be considered data deletion** from the infrastructure of the cloud service provider.

If you want to learn more about the practical aspects of the KNF guidelines on how to prepare for a cloud migration, what to require from cloud providers and how to properly notify KNF of your plans to migrate to the cloud, please read the second part of this study, which will be published shortly.