KNF | KOMISJA NADZORU FINANSOWEGO

Position of the Office of the Polish Financial Supervision Authority

on the use of cloud computing services by supervised entities

Introduction

Considering the fast technological progress and the increasingly common access to cloud computing services[1] as well as the needs reported by supervised entities in this respect, the Office of the Polish Financial Supervision Authority (UKNF, hereinafter referred to as the KNF Office) finds it necessary to present its position on the specific nature of the use of such services by supervised entities. The position presented below applies to the public and shared model of processing data containing legally protected information by means of cloud computing, as well as components of a hybrid cloud of similar nature. The KNF Office believes that cloud computing services (hereinafter referred to as the Services) constitute entrustment of service provision and thus they are subject to applicable law governing the respective financial services sector in this respect. The position presented below elaborates on selected good practices and recommendations specified in Recommendation D on the Management of Information Technology and ICT Environment Security at Banks (hereinafter referred to as Recommendation D), Recommendation D-SKOK on the Management of Information Technology and ICT Environment Security at Credit Unions, and Guidelines on the Management of Information Technology and ICT Environment Security for Insurance and Reinsurance Undertakings, General Pension Companies, Investment Fund Companies, Capital Market Infrastructure Companies, Investment Firms with regard to outsourcing, in respect of the specific nature of cloud computing.

Activities subject to outsourcing agreements should be carried out in accordance with the requirements provided for by the law and other external regulations applicable to respective sectors of the financial market.

Due to protection of secrets and legally protected information, supervised entities should in particular take into account the state in which the provider has its official seat and the states in which the provider would actually carry out the outsourced activities in the context of the legal system of those states. Protection of secrets and legally protected information, which is guaranteed in Poland also by criminal law, may be at the detriment if the legal system in the state where the provider carries out the outsourced activities does not provide for similar protection, i.e. does not penalise the disclosure of respective secrets.

I. Identification of business needs, decision-making basis, planning

The KNF Office expects the supervised entity to carry out works already at the stage of planning the use of the Services that would ensure compliance with the applicable laws and external regulations. From the moment when the supervised entity begins to use the Services, such entity

[1] Model of service provision that ensures convenient, "on demand" independent of location network access to a shared pool of configurable computing assets (mass storage servers, applications or services) which may be dynamically delivered or released with a minimum management and involvement of the service provider (based on NIST Special Publication 800-145 "The NIST Definition of Cloud Computing", National Institute of Standards and Technology).

is responsible for the compliance of the Services; therefore, before making the decision, the supervised entity should identify and determine how it can meet the applicable legal and supervisory requirements. The supervised entity should plan systematic identification, monitoring and reporting within the management information system of the compliance of the Services provided by the provider with the requirements relating to information technology and ICT environment security resulting from applicable laws, external and internal regulations, concluded agreements and standards adopted by the supervised entity.

At the stage of planning of the implementation of the Services and preparation for the decision-making process, the supervised entity should take the following matters into account:

I.1

Under the cost-benefit analysis of the planned use of the Services, the supervised entity should prepare a SWOT analysis of such solution, including, but not limited to:

a) analysis of other solutions (not based on cloud computing) that could be applied for the planned or current business operations;

b) possibility of the provider's bankruptcy or its sudden decision to abandon the provision of the Services;

c) costs and limits of possible actions in case of the provider's sudden decision to abandon the provision of the Services or in case of the supervised entity's cancellation of the ordered Services in the context of:

- return of data and taking over the processing of the entrusted data by the supervised entity, or entrusting the Services to a new provider;
- knowledge of the advantages and disadvantages, as well as of the implementation and functional limitations of the specific Services, obtained from the provider, including knowledge of technological and other limitations having impact on the possible migration of the Services to another provider or on the possible continuation of the outsourced activities by the supervised entity;

d) requirements relating to data security and protection with regard to each data security level provided for in the current classification of the used information, as well as to the estimated possibility to change such classification in the future, considering the limited capacity of the supervised entity to introduce new control mechanisms to the Services;

e) the Services support model.

I.2

In order to prepare for the implementation, the supervised entity should in particular:

a) have full knowledge of the possible configuration of the planned Services;

b) define the requirements resulting from applicable laws, external and internal regulations, concluded agreements and standards adopted by the supervised entity,

business, functional and technical requirements, as well as conditions of assuring compliance with those requirements, in particular:

- conduct an inventory and classification of the information to be entrusted to the provider of the Services;
- determine the data security and protection rules and mechanisms with regard to each data security level provided for in the classification, in accordance with applicable regulations (laws, external regulations, internal regulations).

The procedure for carrying out works in order to implement the Services should guarantee accountability for the performed activities in terms of roles, powers, responsibility, schedule, budget and quality of those activities. Moreover, the procedure should define the rules of risk and change management, as well as determine the boundary conditions of abandonment of the implementation of the Services. The supervised entity should specify the points and methods of measurement of the effectiveness of those operations adequate to each context of implementation of those operations.

II. Services risk management

Before implementing the Services, the supervised entity should prepare a comprehensive risk assessment (identification, analysis, evaluation) and a risk treatment plan (in accordance with ISO/IEC 27005:2011 and PN-ISO/IEC 27005:2011 standards), taking into account all life cycle stages of the Services, the relationship between the supervised entity and the provider, as well as the impact of inclusion of the Services in the current information security management system (based on the good practices described in ISO/IEC 27001, PN-ISO/IEC 27001:2014-12 standards (certification is not required)-, hereinafter referred to as ISMS), including, but not limited to, the risks specific for cloud computing both for the provider and for the supervised entity, in particular caused by the following factors:

a) geographical distribution of the processed or stored data in the context of assuring compliance of the provided Services with applicable Polish laws, external and internal regulations, and standards adopted by the supervised entity;

b) procedure for, and scope of, access of the employees and subcontractors of the provider, and of the potential third parties, to the entrusted data, resulting both from internal regulations of the provider and subcontractors and from applicable laws and external regulations;

c) limited impact of the supervised entity on the form and scope of the new functionalities of the Services;

d) limited possibility of exercising control of the provider’s operations with regard to the provided Services, such control consisting in direct verification of the control mechanisms applied by the provider, including methods of protection and control of access to the provider’s premises where the Services are provided;

e) weakness of the mechanisms of isolation of the resources used by the provider to process or store the data, as well as vulnerabilities of the Service management interfaces made available to the provider's customers;

f) form of the process of deleting the entrusted data and lack of direct control of that process;

g) provider's possibility to unilaterally fix and change the price and other conditions of the provision of the Services, combined with the duration of the notice period;

h) deterioration of the quality of provision of the Services under the circumstances or within the scopes not included in the SLA;

i) users' access to the Services from an internal network of the supervised entity and from outside that network;

j) specific nature of the mechanisms ensuring integration of the Services with the systems of the supervised entity, including all available models of authentication for cloud resources offered by the provider as part of the Services;

k) using the Services on mobile devices.

II.1

The supervised entity should manage the risks leading to non-compliance with applicable laws, external and internal regulations, and standards adopted by the supervised entity, through application of adequate control mechanisms; such risks cannot be accepted or transferred.

II.2

The estimated levels of risk of the Services (before and after application of additional control mechanisms) should be compared to adequate levels of risk relating to ICT solutions that do not use such technologies. The result of such comparison should be considered a valid reason for abandonment of implementation or cancellation of the Services.

The process of Services risk management should be continuous, monitoring operations should effectively identify the moment of necessary review of the Services risk, in particular in the case of identification of a new risk or in the case of material changes in the procedure or scope of use of the Services, or in the relationship with the provider. Regardless of the monitoring results, the Services risk should be subject to a regular review (at least once a year).

The supervised entity should have the up-to-date knowledge of the ISMS of the provider and of its subcontractors; in particular, the supervised entity should be able to view the current and regular assessment of the relevant ISMS prepared by independent experts, internal control and audit units of the provider and of its subcontractors; this would be the condition for effective implementation of the Services risk management process.

II.3

The supervised entity should have documents confirming the level of fulfilment of the requirements relating to the efficiency of control mechanisms implemented by the provider and its subcontractors that would mitigate the risks related to the provided Services, including:

a) a list of provider's obligations resulting from the provisions of the agreement, declaration of professional competencies and/or performance security;

b) provider's certificates of conformity with relevant international norms and standards, such as ISO 27001, ISO 27017, ISO 27018, ISAE 3000, ISAE 3400, ISAE 3402, SSAE 16;

c) provider's audit reports, where the audit was conducted by third party companies upon request of the provider or of the supervised entity;

d) results of provider's internal audits relating to the Services, conducted to date;

e) provider's action plans ensuring continuous and uninterrupted operations within the scope specified by the agreement, Disaster Recovery solutions, methods of ensuring high availability of the Services, procedures for the preparation, storage and archiving of backup copies;

f) assessment of proper protection of the used data centres, computer and ICT equipment, offered by the provider;

g) assessment (in the form of a legal opinion) when and on what conditions the provider is obliged to deliver adequate data to state authorities or third parties (based on the regulations effective in the provider's state) and what kind of notification the provider commits to deliver to the supervised entity in order to fulfil its obligation, in particular in a situation where the provider who, despite declaration of processing the data on the territory of the EU, is obliged, in specific circumstances, to deliver the data beyond the borders of the EU due to local law applicable to the provider's seat and to its operations.

II.4

The risk management system applied by the supervised entity should take into account the risks related to subcontracting specific activities covered by the Services by the provider.

If the risk is considered too high, the supervised entity should not accept subcontracting activities covered by the Services to a specific subcontractor or third party.

II.5

The supervised entity should assess and manage the risk of termination of cooperation with the provider with regard to the Services, in particular considering the possibility of provider's sudden and unexpected abandonment of such cooperation e.g. as a result of liquidation of the provider's company or the provider's abandonment of the provision of the Services, or as a result of a decision of the supervised entity. The supervised entity should have a strategy applicable to termination of use of the Services and an action plan mitigating such risk.

The termination strategy should include, but not be limited to, the following matters:

a) conditions of the agreement with the provider should enable the supervised entity to safely terminate the use of the Services, including the return of the data in proper format, scope and in accordance with an adequate procedure;

b) identification of activities relating to data migration, including a schedule, IT and specification of security requirements as well as specification of the necessary tools.

III. Requirements relating agreements with providers

The agreement between the supervised entity and the provider should guarantee that the provider's operations with regard to the used Services can be controlled; in particular, the agreement should include the provisions specifying:

a) scope of the parties' liability;

b) scope of information and documentation delivered by the provider with regard to the provision of the Services;

c) declaration that the Services would be provided in accordance with the requirements laid down in applicable laws, external and internal regulations, and standards adopted by the supervised entity;

d) possibility to modify the conditions of the Services provision, the mechanisms allowing for changes in the scope and areas of implementation of the agreement, extension of its scope, addition of new functionalities;

e) conditions of termination;

f) notice period and procedures for the safe termination of cooperation, including the return and deletion of data;

g) the right to conduct audit or certification by the supervised entity and third parties companies authorized by it, including the right to carry out on-site inspections at locations where data are stored and processed;

h) possibility for the KNF Office to perform its control obligations;

i) guarantees, sureties and liquidated damages, definition of the force majeure, force majeure events, and procedures in case of occurrence of such events;

j) determination of the scope of liability for the damages incurred by the customers, in accordance with applicable law;

k) inclusion of the licensing rules and intellectual property rights;

l) determination of the language, form, conditions and subject matter of the Services, as well as the support for the Services;

m) rules of, and procedure for, the management of reported problems with the provided Services;

n) obligation to ensure adequate level of security and protection of the entrusted data, determination of location of the centres where the data is to be stored and processed, in particular where the subcontractors would be handling the data;

o) quality parameters (under SLA) and continuity parameters of the Services (RTO[2] and RPO[3]);

p) rules of exchange and protection of information, including the conditions of granting access to information to the employees of third parties;

q) information protection and security requirements, including additional conditions of granting access to information with high level of confidentiality;

r) guaranteeing that the tasks, the scope of liability and the accountability of activities taken by any subcontractor, agent, intermediary or person having access to the data and being involved with their handling or processing would be transparent and could be clearly identified by the supervised entity at any time;

s) rules of suboutsourcing;

t) a list of subcontractors with locations, qualification and scope of activities carried out by subcontractors;

u) specification of the requirements relating to the provider's IT processes, including security, maintenance, operation and development management, as well as security requirements relating to human resources management;

v) procedures for incident management and cooperation in this respect, including both employees of the supervised entity and providers of the Services, as well as – in the case of material risk of a specific incident - also other third parties (customers, contractors etc.), ensuring that the stakeholders are promptly notified and that the performed activities are adequate to the materiality level of the incident;

w) the Services support offered by the provider: the supervised entity should consider that, due to the fact that the services provided by the provider are often global, agreements might not determine time zones or they might determine such zones in the manner that is disadvantageous for the supervised entity and thus the supervised entity should ensure that the period of solving problems under the offered support would be covered by the guaranteed level of the provided Services;

x) court jurisdiction and governing law of the agreement allowing for the effective recovery of claims resulting from the agreement by the supervised entity.

When possible, the supervised entity should use the extended compliance and security programs offered by the provider which allow in particular for: direct contact and communication with security officers and compliance unit officers of the provider, use of extended scope of

[2] RTO (Recovery Time Objective) – time in which the services need to be restored after failure.
[3] RPO (Recovery Point Objective) – acceptable level of data loss in time units.

information about incidents, including incidents relating to the infrastructure of the provider or other customers of the provider, that may affect the security of the supervised entity's data.

IV. Functioning of the Services

IV.1

In order to effectively fulfil its obligations resulting from the responsibility for the quality and security of the services provided to customers and contractors and for the security of their data, the supervised entity should in particular ensure that it has the adequate level of expertise and skills to prepare, implement, manage and control all aspects of use of the Services.

The supervised entity should remain in continuous contact with the employees designated and duly authorised by the provider, who are fully competent for the delivery of clarifications and information relating to the provider's operations, processes and procedures applicable to the ordered data processing Services and their security, without material limitations that may affect the effectiveness of operation of the ISMS.

The rules of cooperation between the supervised entity and the provider should take into account e.g. the rules of communication and coordination of activities carried out by the provider (e.g. with regard to data migration, maintenance, ICT infrastructure scanning etc.), which would mitigate their negative impact on the quality and security of the services provided by the supervised entity.

The supervised entity should duly take into account the specific nature of the Services in the conducted monitoring, control and audit activities under the ISMS.

IV.2

The supervised entity should implement the security and protection mechanisms with regard to the Services, as well as the mechanisms of protection of its resources and IT infrastructure related to the use of the Services, in the form of operations included in the formalised ICT environment management system of the supervised entity.

The supervised entity should receive confirmation from the provider that the Services are provided in accordance with data security and protection requirements on a regular basis, at least once a year or after every material change in the related business processes, services, configurations or legal environment.

IV.3

In order to meet the requirements relating to information security during transmission, the supervised entity should ensure that data transmission between the supervised entity and the provider's infrastructure, between the resources in the provider's infrastructure and between the provider's infrastructure and other outsourcers are protected against unauthorised access and modification, and that network traffic availability and expected capacity are guaranteed.

In order to meet the abovementioned requirements, the supervised entity and the provider, under their respective areas of competence, should guarantee e.g.:

a) encryption and protection of integrity of the transmitted and stored data by means of uncompromised methods;

b) strong authentication of privileged users and authentication of devices for data transmission purposes;

c) high availability of network connections and adequate required capacity.

IV.4

The supervise entity and the provider should provide in particular the following components of the Information Security Management System:

a) coherent introduction of data security requirements relating to respective competence, e.g. by setting an adequate level of access control;

b) definition of data availability parameters in accordance with RTO and RPO of business processes using the Services;

c) agreement on the methods of safe deletion of the processed data (including backup copies and data stored in archives, copies and snapshots of virtual machines etc.) and provider's commitment to carry out and document, upon request of the supervised entity, the above activities;

d) assurance of compliance of the Services with regard to the provider's competence with the security requirements of the supervised entity should include aspects of information confidentiality, integrity and availability, as well as accountability of user operations;

e) regardless of the location offered under the Services, the supervised entity should provide a location for storage of backup copies of data considered critical on the basis of relevant classification of information by the supervised entity, and determine the procedure for and the scope of delivered copies, as well as the format of the stored data.

IV.5

The supervised entity should ensure that it has the necessary knowledge of the incident management process of the provider and its subcontractors in order to use it in the process of Services risk management, in particular for risk assessment and preparation of the risk management plan.

All changes in the incident management process of the provider and its subcontractors should be immediately notified to the supervised entity in accordance with the procedure and within the scope allowing for effective operation of the ISMS of the supervised entity.

The procedure and the scope of incident management of the provider and its subcontractors, as well as the rules of cooperation in case of an incident, should guarantee to the supervised entity that the provider would provide the Services in accordance with the requirements specified in applicable laws, external and internal regulations, and standards adopted by the supervised entity.

In particular, the supervised entity should obtain a guarantee that the provider and its subcontractors:

a) register and store information about events affecting the maintenance of information security attributes (confidentiality, integrity, availability) and that access to such information is adequately managed and monitored;

b) have adequate procedures for reacting to such events, including material risk scenario analyses;

c) use the data format and the incident information delivery mechanism that meet the requirements specified by the supervised entity;

d) have rules covering potential integration with event and incident management support systems of the supervised entity in accordance with the procedure and within the scope resulting from relevant risk management plans of the supervised entity in the context of effective operation of the control mechanisms referred to in those plans;

e) would immediately provide information to the supervised entity about any incidents that might directly or indirectly compromise the security of the entrusted data, in accordance with the procedure and within the scope allowing for effective operation of the ISMS of the supervised entity;

f) would immediately provide all information about the currently carried out and projected activities related to incident management, upon each request of the supervised entity;

g) would guarantee the delivery of the incident report compliant with the requirements of the ISMS of the supervised entity, including, but not limited to, description of the implemented remedial and preventive measures;

h) would guarantee that each access of an employee of the provider or its subcontractor unrelated to the activities entrusted under the Services would be immediately treated and reported to the supervised entity as an incident;

i) have an effective process and rules of collection and securing evidence related to incidents, which could be used in potential court proceedings, and they would deliver such evidence, as the case may be, upon request of the supervised entity, among others in the form of audit trails of activities related to the entrusted data in the form of e.g. adequately segregated log records, image copies or states of virtual machines.

V. Termination of cooperation with the provider

The supervised entity should have an adequate action plan in case of errors or malfunctioning of the Services, as well as it should have and test, under the business continuity management process, the solutions assuring continuity of the processes implemented by the Services.

Another important risk management aspect with regard to termination of cooperation with the provider is having an effective action plan including, but not limited to:

a) conditions of the agreement with the provider, which should enable the supervised entity to safely terminate the provision of the Services, including the return of the data in adequate format, time and in accordance with an adequate procedure;

b) estimated impact of termination of cooperation with the provider on the operation of the business processes using the Services in case the provider or the supervised entity abandon the Services;

c) data migration method, including schedule, specifications of ICT environment and security requirements, as well as necessary tools, impact on the organisational structure and ICT environment and security management processes;

V.1

In order to limit the risk related to termination of cooperation with the provider with regard to the Services, the supervised entity should provide the necessary staff, technical means and technologies, in particular:

a) infrastructure required for effective processing of the returned data so that the processes using the Services could function without delays and potential interruption of their continuity would not affect the relevant parameters of their business continuity plans;

b) project team necessary for the implementation and ensuring of continuation of the previously entrusted activities independently or for their entrusting to a new provider;

c) detailed implementation plan for operations related to abandonment of the Services, taking into account the most negative scenarios, schedule of activities with specific resources, milestones and division of responsibilities, required tools, necessary test scenarios and acceptance criteria for the tests of processing the data recovered by the supervised entity or entrusted to a new provider.