EUROPEAN FINANCIAL CONGRESS

Instytut Badań
nad Gospodarką Rynkową
ul. Do Studzienki 63
80-227 Gdańsk

tel. 58 524 49 01
fax. 58 524 49 09

efc@ibngr.pl
www.efcongress.com

The synthesis of experts' answers in the research conducted by the European Financial Congress[1] concerning the interpretation and application of regulations regarding outsourcing in the banking sector in Poland.

The research was conducted with regard to the regulatory uncertainty and interpretative concerns regarding simultaneous application of the banking law and the Guidelines of the EBA in the scope of using outsourcing in the banking sector.

Methodology of developing the position

The position was being developed in the following stages.

Stage 1 (September 2020)
A set of consultative questions was prepared. The group of experts cooperating with the EFC were invited to participate in the research and they were sent the consultative questions. In the invitation the experts were asked to take into consideration three legal regimes: binding acts regulating the financial sector including banking law provisions, guidelines of KNF – Polish Financial Supervision Authority (among others Recommendation D, Communication regarding using cloud computing by the supervised entities of 23 January 2020) and the Guidelines of the EBA on outsourcing issued on 25 February 2019 together with the practice of interpretation and application thereof in the European Union. Experts were guaranteed anonymity.

Stage 2 (October 2020)
Upon the invitation of the EFC, 17 opinions were submitted (from individual experts and groups of experts and institutions). All answers were collected and presented in an anonymous form to experts, who actively participated in consultations. They were asked to highlight in the opinions of other research participants the phrases that should be included in the final position as well as those they disagree with. Experts could also correct their answers under the influence of arguments presented by other experts.

Answers were obtained from experts representing:

- banks,
- IT companies, fintechs and financial market infrastructure institutions,
- consulting companies,
- law firms.

Stage 3 (October 2020)
On the grounds of obtained answers and notes given by experts, the synthetic position of the European Financial Congress, presented below, was drawn up. The final part of the synthesis includes postulates presented by experts who participated in the research as well as raised doubts and questions which require answers from the regulator.

[1] The objective of the European Financial Congress (www.efcongress.com) is to discuss issues regarding security and stability of the financial system of the European Union and Poland.

Q1: Should it be verified, if the service supplier or his subcontractors use cloud computing and if yes, how?

The bank's obligation to verify whether the service supplier or his subcontractors use cloud computing results from numerous requirements imposed on the bank with regard to outsourcing data to a cloud (Guidelines of the EBA, Communication of UKNF). In the case of neglecting this verification, the outsourcing-related risk analysis would be incomplete. First of all, it would concern assessment of compliance with the GDPR requirements, guidelines of regulators, the scale of the risk of losing access to data and the geographical risk analysis. The bank which is not certain which technologies will be applied in providing services, especially when the subject of the agreement comprises outsourcing data storing, should verify in detail whether the supplier uses or intends to use cloud computing as soon as at the stage of negotiations before concluding the agreement. In case of a lack of certainty regarding application of cloud computing in the process, it should be assumed that the supplier will use the cloud while providing services and therefore, fulfil all relevant obligations including the risk analysis and modelling of the so-called exit strategy. If, in the course of the verification, it turns out that the service is provided with an exclusion of the application of cloud computing, the bank will cease performance of further obligations related to the implementation of relevant regulations.

Declarations of the service provider, and possibly his subcontractors, should constitute an appendix to the master agreement or constitute a part thereof. The supplier, who provides services on the grounds of the previously concluded agreement, should make a relevant declaration in which he states whether he uses cloud computing and if yes, in what scope. In the event of a positive answer, if using cloud solutions justifies application of the provisions of the Communication of KNF, in order to continue further cooperation with the supplier, an annex to the agreement should be concluded to adjust the contents thereof to the requirements of the Communication of KNF.

The verification process can be divided into several threads. The first one being a survey addressed at the supplier in which he states how he intends to perform entrusted activities and, at the same time, indicates all subcontractors with particular consideration of the performed scope and used cloud technologies. The contracting authority's task is to verify the partner in terms of risk and dependency on the level of trust or market position confirmed with references, or to proceed to audit the scope entrusted under an agreement, or to resign from such audit and consciously accept presented certificates and, in consequence, any risks that may be related to such a resignation.

Obtaining the supplier's declaration on using or intention to use cloud solutions, as well as the supplier's controls or audits may be performed by periodical calls on the supplier to answer questions included in the detailed survey regarding the manner and conditions of supplier's processing of data entrusted by the bank. In justified cases, audits should be performed in person, in locations of processing data entrusted by the supplier.

In the case of material agreements the manner of possible use of the cloud should be clearly described in the agreement with the supplier or related documents. In the case

or other agreement (i.e. non-material) the issue of possible use of cloud by the supplier should be expressly clarified, if it may have an impact on the level or risk related to the agreement e.g. issues concerning data protection, or security of data and systems.

It is equally important to verify the plans of exiting services in the case of terminating cooperation and what happens with data, as well as possibilities of further commissioning subcontracting by the supplier. It is also important to verify whether entrusted data is properly secured against unauthorised access (e.g. via encryption). This type of activities should be the subject of verification at the moment of negotiating the agreement with the supplier.

Permanent activities in the customer's organisation should include periodical verification, whether the process of selecting suppliers implemented in the customer's organisation and the process of establishing requirements regarding orders of services and products take into account all expectations of the organisation. Especially, whether it takes into account preferences in the scope of subcontracting in terms of the character of providing services on the grounds of own or foreign resources (including cloud).

In the case of a decision on permitting performance of the subject of the tender by the contractor/subcontractor with the use of foreign resources (including cloud), the analysis of risk factors related to the performance of the subject of the tender should be provided for, including correlations of responsibility for performance and recourse of possible loses in the case of any problems with performance of the agreement.

Q2: What solutions should be used at a contract level in case the supplier providing services within outsourcing banking services uses subcontractors and further subcontractors?

It should be assumed that "outsourcing" is a concept broader than entrusting performance of activities under the banking law. Therefore, it is possible that a given agreement will be qualified as outsourcing both, from the point of view of national law and the Guidelines of the EBA, as well as that it will constitute outsourcing only on the grounds of the Guidelines of the EBA.

In compliance with KNF's position, in principle, the Guidelines of the EBA should be applied as elaborating on the discussed area more extensively. However, in the event that national provisions, recommendations or interpretative positions forwarded by the supervisory authority to all banks include stricter provisions understood as requiring increased effort or limiting the freedom of the bank's activity with regard to the provisions of the Guidelines of the EBA, national provisions, recommendations or interpretative positions forwarded by the supervisory authority to all banks should be applied in a given case. Whereas, when national provisions, hitherto issued recommendations or interpretative positions forwarded by the supervisory authority to all banks include provisions less strict than the Guidelines of the EBA, the Guidelines of the EBA should be used in a given case.

It should also be added that in compliance with the Position of KNF, the Guidelines of the EBA do not apply to cloud services. In this scope, the contents of the Cloud Communication should be taken into account.

In principle, solutions resulting from the banking law in the scope of sub-outsourcing are more far-reaching than the Guidelines of the EBA, since they limit the possibility of using subcontractors exclusively to perform auxiliary activities or to emergency situations, making this possibility conditional on the indication thereof in the agreement.

Therefore, in the situation when a given agreement constitutes entrusting performance of activities under the banking law and the supplier is to provide services with the use of subcontractors, the agreement has to directly provide for such a possibility and the auxiliary activities that the subcontractor would have to perform should be indicated in the agreement. Furthermore, at the stage of contracting, the bank should ensure the possibility of controlling outsourced activities and information constituting the legally protected secret. The agreement should also ensure that other requirements resulting from the banking law, as well as recommendations and guidelines of KNF are fulfilled while entrusting performance of activities.

Supervision requires that in the case that the outsourcing agreement provides for sub-outsourcing of critical or material functions, it also ensures fulfilment of requirements resulting from the Guidelines of the EBA (section 13.1) stricter than those resulting from the Polish law, as well as recommendations and guidelines of KNF.

Moreover, irrespective of the fact whether a given outsourcing agreement constitutes entrusting in accordance with the provisions of the banking law or not, before conclusion of the outsourcing agreement, the bank should assess in compliance with section 12.2 of the Guidelines of the EBA all significant threats resulting from using the supplier, subcontractors and further subcontractors and, if necessary, properly reflect them in the agreement with the supplier (e.g. with provisions imposing on him certain obligations, limitations or bans).

The supplier's obligation to include specific contractual provisions in the agreement concluded by him with the sub-supplier through the agency of whom he will provide the banking cloud service, constitutes a particularly important element of the agreement. The bank should oblige the entity providing the service to conclude a proper contractual provision in the agreement with the sub-supplier which would make this agreement an agreement on providing services to the benefit of a third party (pursuant to Article 393 of the Civil Code) and in the case of the Polish law, would entitle the bank to demand direct provision of services by the sub-supplier. An important matter in the context of the obligation to include relevant contractual provision also comprises the matter of liability and relevant qualifications of the team that will provide the service, including identification of persons who will have access to sensitive information covered with banking secrecy. While securing its own interests (as has been indicated above, in this respect the bank is obliged to supervise the correctness of processing data in the cloud), the bank should oblige the supplier to obtain from the sub-supplier a list of persons who, within further outsourcing, will receive access to confidential information covered with banking secrecy (or encryption

key), as well as the obligation to submit to the bank a documented procedure of protecting processed data against unauthorised access in compliance with the requirements included, among others, in the cloud communication. The bank should require that supplier and sub-suppliers, if necessary, update this data on an ongoing basis.

In the case of new agreements with suppliers of services, the contractual obligation (or in a form of an annex in the event of already existing agreements) to ensure proper quality of offered services in the "cloud" both, provided by themselves or by entities cooperating with them that is subcontractors (for which the supplier of the service takes full responsibility), as well as their full compliance with the guidelines of UKNF, is crucial.

The agreement should specify responsibilities of the supplier, as well as his obligation to ensure compliance of the subcontractor and the right to audit the supplier and sub-suppliers (in the agreement with the supplier, the supplier's task is to include relevant provisions in the agreement with the sub-supplier) together with the right to object further sub-outsourcing or terminate the agreement.

The agreement concluded with the supplier should include all information (including the principles of security of the supplier and possible subcontractors), as well as the parameters allowing determination of the level or risk related to providing services and the place of performance thereof. The same requirements should concern agreements concluded with subcontractors. The supplier is obliged to verify the bank's requirements in the scope of the security of information and guarantee meeting them by his subcontractors or to signal the necessity to specify separate security requirements. Agreements with subcontractors should include clauses concerning the Supplier's full responsibility for activities of subcontractors and obligations of subcontractors in the same scope in which the supplier is obliged.

The contract should, in principle, include the provision on the possibility or even necessity to conduct by the contracting authority periodical (at least once a year) targeted audits in the scope of entrusted activities. It is important that the supplier ensures the possibility of carrying out audits and controls at sub-suppliers' at the level not lower than the one concerning the supplier, although the contracting authority having assessed the risk may resign from verifying subcontractors on the basis of the documents delivered by the contractor and confirming the appropriate level of securities and verifications; in this case certificates may be accepted as compliant with relevant ISO norms. Audits conducted at the contractor's may be replaced with the recognised and delivered by the contractor certificate in the scope covered with the agreement. The contracting authority should also have the right, in justified cases, to request regular information on the financial condition of subcontractors.

In the scope of banking outsourcing, it is important to make sure that suppliers and their products or services meet the requirements and regulations imposed by sector supervision authorities. It is worth at the level of the contact to secure the necessity of the supplier to submit to these obligations by referring to clauses related to the obligations of contracting institutions that are subject to regulations.

Moving on to more technical issues, it is crucial to pay attention to the manner of securing and retrieving data in the case of changing the supplier or terminating the agreement. Relevant obligations associated with cooperation in termination of the agreement (e.g. a plan of exit, data migration, documentation) should be contractually secured.

The supplier should be obliged to inform the contracting authority of changing the sub-supplier and allow verification, if the service generates additional risk factors in new conditions. The supplier should confirm compliance of the service with regulations and observe if there are any regulatory changes that force introducing changes to the framework of service functioning (and adapt the service respectively). It is also worth ensuring the possibility to inspect the supplier's Data Centre.

The bank should guarantee its access to the information on security principles of the subcontractor, as well as the possibility to verify these documents.

Below, contractual solutions concerning the subcontractor have been compiled, which should be included in the agreement on qualified outsourcing:

- using services provided by the subcontractor (other than the one indicated in the agreement at the moment of conclusion), is admissible only upon obtaining prior consent of the Bank in the form of an annex to the agreement;
- in the case of using services provided by subcontractors irrespective of the Bank's consent, the supplier takes the risk and assumes full liability for performance of obligations and damages caused by subcontractors in the course of and on the occasion of execution of the agreement, the same as for own activity or negligence;
- the supplier will impose on subcontractors the obligation to adhere to all principles, rules and obligations specified in the agreement, in the scope, in which they refer to the scope of works of the subcontractor entrusted for performance by the supplier;
- the supplier ensures that he and his subcontractor have regularly tested plans of business continuity and emergency procedures ensuring continuous and uninterrupted business in the scope covered with the agreement; plans constitute an appendix to the agreement;
- the supplier ensures that both his employees and subcontractors participating in the performance of the subject of the agreement are subject to the same obligation to keep confidentiality as the supplier;
- the agreement must expressly specify both the subcontractor engaged to provide services and the description of activities entrusted to him (the scope of the subcontractor's obligations may constitute only activities which are auxiliary with regard to the main service provided by the supplier);
- activities are performed by the subcontractor on the grounds of Article 6a par. 7 point 1 of the banking law upon joint fulfilment of the conditions below:
    - only in the scope of the activities aimed at the performance of the main service (so-called auxiliary activities) specified in the agreement;
    - the supplier will oblige the subcontractor in a concluded agreement to adhere to the obligations of the supplier resulting from the agreement in the scope of which such obligations concern activities performed by the subcontractor;

- the supplier will oblige the subcontractor in a concluded agreement to ensure the same quality level of services and confidentiality as results from the agreement;
- the supplier will oblige the subcontractor in a concluded agreement to introduce the ban on using further subcontractors;
- the supplier undertakes to ensure in a concluded agreement that the subcontractor is liable for damages caused as a result of non-performance or undue performance of obligations resulting from the agreement concluded by the supplier and the subcontractor in compliance with binding legal provisions;
- the supplier undertakes to ensure that employees of the subcontractor have relevant experience and qualifications allowing due performance of activities resulting from the agreement;
- the supplier undertakes to ensure that the subcontractor is fully informed of legal and regulatory requirements related to performed activities resulting from the Agreement, in particular, concerning keeping bank secrecy.

Q3: How should the architecture of the considered solution be tested in order to determine levels of sub-suppliers/subcontractors in the context of the ban on further sub-outsourcing (Article 6a par. 7 of the Banking Law)?

Within the risk analysis and exit option, one should ancillarily verify these issues, even if within the framework of the need to monitor on an ongoing basis the compliance of the processing by the entity providing the data cloud service with obligations imposed on the bank in this scope, especially resulting from the Communication of the Polish Financial Supervision Authority of 23 January 2020 on information processing by supervised entities using public or hybrid cloud computing services. Furthermore, in compliance with Recommendation 2 of Recommendation D, a formalised system of information should function in a bank, adjusted to the level of the identified risk. It seems that this element should be taken into account within determination of relations between the bank and the entity providing cloud services. It seems valid that the bank in the agreement on cloud computing services univocally obliges the provider to each time inform about engaging sub-suppliers in the provided services. Since the bank is obliged to monitor the risk on an ongoing basis, it seems that in this respect the bank can, with the use of all available manners, within the conducted analysis, verify in which scope the supplier provides services through the agency of sub-suppliers.

In order to ensure a proper level of control, each entrusting of activities to a subcontractor should be preceded with a proper statement at least 30 days in advance so that the enterprise can undertake proper verification activities or raise objections.

Description of the architecture of a considered solution should cover all services used in a given solution. Each service should be verified in terms of the place and parameters of providing services, as well as the supplier of the service. There might be a solution developed with the use of services provided by various suppliers or one supplier commissioning services to sub-suppliers. Determining services described in the architecture of a solution, as well as the service provider will allow determining the risk of the solution.

The architecture must be examined by a qualified employee of the contracting authority or appointed entity that has proper competences and verifies on behalf of the contracting authority the architecture's compliance with the declared outline. The contractor must agree to such a verification and inform the contracting authority in the case of material changes that influence the security and architecture of the solution.

The physical and logical location of particular elements of the architecture/infrastructure of the design solution should be especially examined with a particular recognition of legal conditions and in terms of recourse correlations in the scope of SLM/SLA due to the potentially contradictory conditions in the infrastructure locations outside the country of the contracting authority/contractor with whom the contracting authority concludes the agreement.

The basic method of such examination can be connected with the analysis of **data flow and access**. In the case of using such a method, we verify how our (that is bank's) data is administered by the supplier. Is it copied and whereto? Who can access it and in which scope? This method is relatively simple in use, since it is difficult for the supplier not to give answers to thus formulated questions. In many cases the issue of access to data will be additionally regulated by other provisions (e.g. the GDPR) and in examinations it is worth using what is/should be the effect of applying such provisions. Even though expressing the term "access to data" in legal language constitutes a certain challenge, at the technical level it is relatively simple.

Apart from the flow of data, the approach to the **flow of information** may be material and significantly more difficult. As far as the service provider shares data with other entity in an already processed form (e.g. sets of data necessary for a portfolio analysis), limitation at the architecture level may not be sufficient. Therefore, it is worth moving on to the question about **external sources of knowledge/information** used by the sub-supplier to perform the service. From the point of view of the architecture of the solution, the question concerns **feeding** subcontractors' systems with the **data** externally.

It is also worth learning the results of the global study conducted at the turn of 2019 and 2020 in the scope of TPRM – third party risk management. It showed that as many as 57% of studied financial institutions base on contractual agreements with a third party or the assessment/monitoring of subcontractors (fourth parties) by third parties. It is worth noticing that 246 organisations participated in the study, including 123 global financial institutions varying in the scope of the scale of activity and complexity, as well as maturity of the outsourcing risk management process. Results of the survey show how most often organisations approach the examination of the risk related to the activity of subcontractors of their suppliers (fourth parties).

1/3 of surveyed organisations providing financial services rely on contractual terms and conditions with their third parties in the scope of monitoring fourth parties. Relying by institutions on the risk assessment of subcontractors conducted by a third party is a common practice (25% of respondents). In 17% of cases, while assessing the risk of third parties institutions base on the agreement concluded between a third party and a

fourth party, which requires great transparency of the model of providing services to the benefit of the bank in the scope of engaging fourth parties.

Not many respondents (9%) conduct their own independent reviews of fourth parties, despite the fact that this number increased in comparison with the study conducted at the turn of 2018/2019. Only 6% of respondents indicated that fourth parties are not monitored.

Engaging by third parties further subcontractors is today, on the global scale, a common phenomenon considering the complexity of technological solutions, chains of connections and possibility of cost optimisation. Allowing the possibility of providing services by fourth parties within the basic outsourcing agreement is tempting for banks and their subcontractors and this trend will surely intensify in the future. However, it requires an efficient risk management system regarding such relations, explicit consents given in the outsourcing agreement by the bank, and ensuring control of fourth parties by third parties, and in justified cases (depending on the risk/materiality/criticality of the outsourcing relation) also the control of fourth parties by the bank.

To sum up, the range of available solutions in the scope of monitoring fourth parties is wide and includes the following solutions:

- relying on the agreement with a third party,
- relying on the risk assessment conducted by the third party,
- relying on the agreement between the third party and the fourth party,
- conducting an independent review of fourth parties.

Q4: How should the scope of responsibilities of the subcontractor – insourcer be defined in agreements on outsourcing banking services?

In compliance with the banking law, the supplier's liability towards the bank for damages caused to customers as a result of non-performance or undue performance of the outsourcing agreement cannot be excluded or limited. This provision is absolutely binding, therefore, no contractual provisions between parties can change or replace it. However, both banks and, above all, suppliers are aware not only of the existence, but also character of this provision.

Despite the above, there is no one good answer to this question. It depends on the type of the subject of outsourcing and its characteristics. However, irrespective of the subject of outsourcing in the agreement on outsourcing banking services, the supplier is fully responsible for the performance of obligations and damages caused by subcontractors in the course of and on the occasion of the performance of the agreement, as well as for own activity and negligence and this fact should be reflected in the bank's agreement with the supplier. It is important, since the bank as the contracting authority should not enter into relations with a subcontractor. At the contract level, the contractor should be fully liable for his subcontractor.

As it seems, it would be the most beneficial from the perspective of the bank if the supplier assumed liability in compliance with the liability similar in construction to the several liability, however, due to the lack of a direct contractual relation between the

bank and the sub-supplier, the contractual liability will only refer to the supplier. The bank would be entitled to a tort-based claim against the sub-supplier. It seems important to extend the supplier's liability with the non-performance of the obligation by the sub-supplier. Theoretically, in the case of the Polish law application, such an issue is regulated under Article 474 of the Civil Code or Article 429 of the Civil Code. It seems important, especially in the case of establishing which law applies to the agreement other than Polish law, to incorporate in the agreement relevant provisions reflecting the contents of the above articles. In the case of undue performance of the agreement on providing services due to reasons attributable to the subcontractor, it would allow the bank to bring a claim directly against the supplier who would immediately have the right to recourse against the sub-supplier.

Q5: Which organisational and legal difficulties may arise with regard to conclusion of agreements on outsourcing banking services?

In many cases it may be a challenge to determine whether a given service is included in the "outsourcing banking services". A good example is the discussion, whether the email service in a bank constitutes outsourcing banking services. Consequences of such a resolution may be far-reaching, since the interpretation, in compliance with which using mail with servers located on cloud computing is classified as outsourcing banking services, for a long time suspended the introduction of cloud technologies in banks. It is worth noticing that there are still many support functions, which are not classified as outsourcing banking services (e.g. HR services), as a result of which, determining the boundary requires assessment in each specific case. Furthermore, unclear requirements of KNF related to the criteria that sub-supplier has to meet in order to be included in the outsourcing chain are also problematic.

Formal-legal requirements are perceived as significant obstacles. The necessity to obtain a consent of the regulator to transfer data outside the EU is especially difficult for the smaller entities. In the case of using services of joint centres located in countries with low costs of conducting activity e.g. in Asia, obtaining documents for a given entity according to the list of KNF and translating them is very time consuming and expensive, especially since the Polish outsourcing regime in this scope is unique and is not based on the risk principle, i.e. each outsourcing is treated the same.

Furthermore, it is more and more often necessary to collect documents for two entities simultaneously, i.e. for the main supplier of services and for the entity which would be a supplier in the case of an event activating an emergency plan. For entities acting within capital groups, it may mean the necessity to organise a given area for a Polish bank individually, whereas other members of the group use common solutions. An alternative would be to delay implementation in the whole group.

Moreover, the issue of the law relevant for the agreement on providing bank cloud services in the event the parties decide to apply the law of the country other than the native country, also seems to be a significant problem.

In the case of using by the bank cloud computing the source of difficulty may also be emergency outsourcing. The bank securing the continuity of business may conclude an

agreement on providing services in the cloud which protects it against breaking the continuity of business. In such a case the bank should, despite the provision of the service being of ad hoc nature, fulfil legal obligations imposed on it.

Fulfilment of necessary regulatory requirements concerning organisational issues (assessment of the agreement, supplier, risk etc.) may constitute a significant burden especially for smaller organisations. The same applies to legal requirements, since suppliers do not willingly adhere thereto. It primarily concerns requirements regarding audit, liability, location of processed data, especially in the case of suppliers of cloud computing services. Anyway, there is a certain risk that the full audit and control may be almost unfeasible. The issue with the audit will be especially visible in big structures using complex cloud infrastructure comprising many sub-suppliers.

Cloud computing service providers are in majority large entities providing services globally (Microsoft, Google, Amazon Web Services). They are not willing to accept obligations in a scope that is broader than the one specified in their standard agreements, rules and regulations, especially, if they result only from Polish provisions or guidelines of supervisory authorities and are not universally binding provisions in the European Union or in the jurisdiction of countries on the grounds of which agreements of such suppliers of cloud computing services are drawn up. A certain solution to this situation would consist in conducting an external audit by a renowned auditor.

A significant challenge related to outsourcing consists in transferring the business process outside, which is related to losing full control over execution thereof; in this case, full, accountable mechanisms of monitoring the status of the service and security thereof should be taken care of and ensured. It is a challenge to monitor and manage suppliers and their subcontractors, in particular, the auditability of agreed terms and principles of outsourcing banking services both, in the scope of the correctness of services and, in particular, in the scope of data and information that will be entrusted and the flow thereof. It especially applies to personal data (the GDPR requirements) and information protected with bank secrecy. To this end, it is important to precisely specify the boundaries of liability and obligations of both parties in the agreement.

While referring to the issue of security in the case of outsourcing agreements, the lack of the actual spread of databases, where data transferred by banks under a concluded agreement on cloud computing will be stored, should be indicated as one of the main problems.

One of the basic areas of discussion concerning outsourcing banking services regards the level of suppliers' liability. Thus, it should be expected that this topic will remain one of the main areas of negotiations in outsourcing agreements. It is related to determining not the level, but boundaries of liability. A good and possibly the most important illustration of this issue is the matter of security. In the case of the unlimited liability of the supplier, discussions on the scope in which he is responsible for the security will be very difficult, especially if the supplier does not provide a due warranty in the scope of services provided by himself or his subcontractor.

A challenge may be related to including in the agreement areas which are difficult to describe in a parametric form. It is easy to set e.g. which bandwidth or a maximum disk

area is to be made available. It is much more difficult to define effective work of the system (e.g. “response time”), especially in more complex scenarios. In standard outsourcing available resources were by definition limited to those specified in the agreement. One of the features of “cloud computing” is its flexible reaction to periodical large demand for power. Describing these situations in agreements may not be easy.

In the case of outsourcing material or critical functions it is required to reinforce the regime in the scope of the construction of outsourcing agreements, contents of the register of these agreements, plans of business continuity or risk assessment and internal control. Whereas, a significant difficulty consists in classifying a given agreement as the outsourcing agreement and the critical function important pursuant to the Guidelines of the EBA. Although the Guidelines specify detailed criteria (factors) while determining, whether the outsourcing agreement concerns a critical or material function, institutions have a certain freedom in the scope of calibration of these criteria and should be based on the assessment of the risk of the relation with a third party. It may lead to the agreement with the same supplier on an analogous scope of services to be perceived (and classified) differently by various banks and, in consequence, lead to the necessity of including in agreements various requirements and meeting them.

One should strive for monitoring third parties (the scope, frequency), reviews and assessments of suppliers in the context of resources held by banks that are proper for the risk level. Bigger support of technology in order to implement an effective system of third party risk management covering both 1st and 2nd line of defence is unavoidable in order to, wherever possible, automate and standardise the process.

Taking into account the current context of cooperation with third parties considering the non-standard activities of the organisation during COVID-19 pandemic, banks faced new challenges and difficulties regarding operating and financial resilience of their suppliers, as well as security of data processes within performance of outsourcing agreements.

Problems occurring or growing with regard to the epidemic include, among others:

- difficulties in assessing the scope in which service providers can continue their activity in stressful conditions for a long period of time;
- difficulties in identifying and understanding correlations and sensitivity to the surrounding changes;
- fears concerning data security and risk of data leakage caused by the popularisation of remote work among suppliers;
- a lack of the possibility to conduct a relevant risk assessment process of third parties based on up-to-date data during pandemic;
- technical possibilities of monitoring financial situation of third parties.

Finally, an especially difficult issue consists in the termination of cooperation with the supplier. The agreement should describe this process in detail. It will be most often related to changing the service provider. As in the case of a classic change of the supplier, data migration is necessary. This activity is always complex and often contributes to extending the duration of projects. In a classic situation it only means extending the time of using the current solution on the grounds of a held licence (it

might be necessary to extend the term of the technical support agreement concluded with the current supplier). In the case of cloud solutions it is necessary to extend the agreement and provide services. Such a possibility should be remembered as soon as at the moment of signing the agreement so as to ensure the possibility of extending it on unchanged terms and conditions.

Q6: Which regulatory limitations regarding outsourcing banking services may be the most difficult to fulfil?

Regulatory limitations that are the most difficult to fulfil result from the lack of coherence between provisions regarding outsourcing banking services in the Banking Law and provisions in the Guidelines of the EBA concerning outsourcing. It results, among others, from adopting by KNF national approach to the Guidelines of the EBA in the scope of cloud computing. The Polish supervisor is the only one who announced that it will not follow the Guidelines of the EBA regarding cloud computing. Whereas, it should be remembered that the vast majority of cloud computing suppliers are foreign institutions that apply the international law. Negotiations of agreements governed by national legal provisions with a foreign supplier require experts in the area of national and international law. Additionally, a big challenge for ensuring quality, continuity and responsibility for services commissioned by the entities subject to outsourcing banking services consists in the legal conditions and diversity resulting from the regulations binding locally for various sectors.

For instance, limitation of the outsourcing chain in compliance with Article 6a of the Banking Law. This difficulty will be especially visible when the supplier performs activities entrusted by the bank on the grounds of cloud computing provided to him by the subcontractor. A chain is thus established:

bank → insourcer → cloud computing supplier (subcontractor of the supplier)

However, in practice, cloud computing suppliers are often suppliers of a cloud platform within which they also share other specific services, which are, however, provided by other sub-suppliers cooperating with the cloud computing supplier. On the grounds of binding provisions, using such additional services by the bank would be impossible in the model of cooperation within which a direct supplier of these services to the bank would be a supplier providing aggregated own services, services of the cloud computing supplier and his sub-supplier, since it would extend the outsourcing chain too much.

Thus, on the one hand, cloud solutions are, in principle, acceptable, but on the other hand, regulations are not concurrent with the practice. Therefore, the regulator should be expected to provide an in-depth analysis of the issue and possible solutions. Perhaps, considering the priorities of the supervision, there is no acceptable solution, but then, it should be clearly stated, since solutions to issues resulting from regulations with which banks have to deal with, remain within competence of the regulator.

A separate issue comprises adjusting internal regulations in the enterprise and agreements with suppliers to the guidelines of UKNF concerning cloud computing.

Often the contractor does not want to agree to the imposed provisions in agreements which he is not able to execute especially in the times of pandemic and even if he agrees thereto, they often remain “empty”, especially in the case of global suppliers of cloud computing.

A serious problem consists in conducting audits, control and supervision over performance of entrusted activities and, in particular, security of entrusted data and information. There are areas where it does not generate problems e.g. running a bank facility, but there are areas where it is difficult and in special cases of cloud solutions almost unfeasible. It should be decided whether it is worth keeping strict restrictions, adherence to which significantly hinders obtaining a technologically secure outsourcer.

The contracting authority should properly supervise the contractor. Fulfilment of thus defined requirement might be difficult. Proper supervision is a concept which is quite difficult to define and requires analysing the risk and engagement of quite broadly developed organisational and technical methods guaranteeing the possibility of documenting any activities of the contractor, ensuring evidence in disputable matters. For instance, in the case of large spread data bases, it may comprise the bank’s verification of correctness of data processing in cloud computing from the perspective of obligations imposed on this entity, especially in the scope of periodical risk analysis and adjusting relevant mechanisms thereto. On the other hand, one should avoid situations when data of several banks will be stored in databases located in the same place.

The bank requires the possibility of inspecting supplier’s internal procedures (e.g. the obligation to indicate by the bank change management methods, testing procedures etc.). Non-bank entities in the area of providing services to banks are in this scope treated as banks, which may be a serious challenge to all interested parties including regulators and supervisory entities. Therefore, a regulator has to propose to banks a realistic solution that would ensure proper level of security or ban using outsourcing, especially cloud solutions.

Another challenge comprises the obligation to draw up and implement plans of business continuity with regard to material and critical functions, especially at a level of service provider and ensuring the “exit” strategy for material and critical functions. Barriers concern possibilities of identifying alternative solutions and preparing plans for a transitional period i.e. until the moment of entrusting service provision to other supplier or back to the financial institution, as well as testing plans of continuity and exit strategies.

A separate case comprises the regulatory approach which is not proportional to the risk scale. One of the regulatory restrictions concerning outsourcing banking services comprises an absolute obligation to use all tools and outsourcing obligations specified in binding provisions (e.g. Articles 6a-6d of the Banking Law) in the same scope and dimension towards all suppliers irrespective of the size of a supplier or the scope of entrusted works. It should be possible to apply these tools and obligations on the grounds of the conducted risk analysis with a consideration of the principle of proportionality.

For example, a large entrepreneur using various Data Processing Centres (DPCs) has different capacity to draw up and implement an emergency plan with the use of various DPCs. Whereas, a micro-entrepreneur or a small entrepreneur, as well as many fintechs providing innovative solutions are entities who, at a stage of establishing their market potential, are not at a disposal of significant resources and do not have the same capacity to guarantee execution of an emergency plan as a large entrepreneur.

It is, indeed, a significant hindrance, however, this problem exceeds the discussion on outsourcing and is, first of all, associated with fintechs. On the one hand, a situation when security of a large bank depends on a small entity cannot be allowed. Therefore, it is necessary to assess the risk in detail, however, it is impossible to execute without testing a given solution in real conditions, on a small scale. Perhaps, a regulatory sandbox would be helpful.

Q7: How should the consent to disclose bank secrecy be obtained when a given agreement is not concluded in the regime of outsourcing banking services, yet, the bank secrecy is disclosed?

In such a case (if it is not possible to transfer the bank secrecy on the grounds of a specific provision) Article 104 par. 3 of the Banking Law applies and thus, such a consent should be given in writing or on IT data carrier and include consent to transfer specific information or indicate an organisational unit to which data can be transferred.

In compliance with regulations of the Civil Code an electronic form requires signing with a qualified electronic signature. It seems that for the purposes of processing data in the scope exceeding statutory disclosing of information covered with bank secrecy, a consent in one of the aforementioned forms should be obtained. It may be valid to make an attempt to obtain consent to processing this data by the Bank in an electronic form, in the form of information addressed to the customer including the instructions on proceeding, for example by using communication via electronic access to the bank account upon logging in. The customer granting the consent, complying with the regime provided for in the Civil Code, should sign such a consent with an electronic signature. Granting consent by the Customer should be documented and archived by the bank.

Postulates of experts

Answers to questions given by experts show that regulations concerning outsourcing and interpretation thereof raise a number of doubts due to the incoherence of definitions, incoherence of requirements or due to the deviations from the practice commonly used in the European Union's financial market. It has several consequences:

- Polish banks often have a weaker competitive position in comparison to banks from other Member States.

- Polish banks have more difficulties in negotiating and concluding outsourcing agreements with suppliers operating in the European Union market, especially the largest entities, which by operating in the European Union market are forced to agree to the European Union's legal requirements, but they do not want to accept Polish provisions which differ from the European Union's provisions.
- In the case of bank groups, the necessity to apply in Poland standards and solutions other than standards and solutions applied in remaining Member States significantly increases costs of the activity, which affects results of Polish banks.

It is impossible to state *a priori* in which cases it is possible to change principles or practice. However, wherever the market signals doubts, a dialogue between the regulator and the market is necessary in order to lead to a change or satisfactorily explain to the market rationality of premises used by the regulator.

The most important issues occurring in answers given by experts have been presented below.

1. Incoherence of regulations.

   Banks are obliged to adhere to the Guidelines of the EBA with regard to outsourcing. KNF confirmed that it intends to follow them. At the same time, as the only supervisor, it announced that it will not follow guidelines with the exception of the part concerning cloud and cloud services. This area is regulated by a relevant Communication of KNF. Unfortunately, in the Guidelines of the EBA cloud services constitute one of the outsourced services, whereas the Communication of KNF refers to processing information in cloud computing. Answers given by experts imply that so far coherence between these two documents have not been preserved due to different constructions of each. Meanwhile, the incoherence of provisions translates into the incoherence of decisions, which in the long-term deregulates the market. Therefore, it is important for the regulator together with the market to critically analyse both regulations and fill in the loopholes, as well as delete contradictory provisions.

   For example, one of the experts underlines that it is not clear what is understood as outsourcing banking services, i.e. is it the same as outsourcing regulated in the Banking Law or does it have a significantly broader meaning in compliance with the Guidelines of the EBA on outsourcing issued on 25 February 2019 ("**Guidelines of the EBA**").

   Position of KNF of 16 September 2019 on selected matters related to entry into force of the Guidelines of the EBA and consideration thereof in the bank's activity ("**Position of KNF**") directly indicates that due to the definition of "outsourcing" included in the Guidelines of the EBA, it should be adopted that "outsourcing" is a concept broader than entrusting performance of activities pursuant to the Banking Law. Therefore, it is possible that a given agreement will be qualified as outsourcing both, from the point of view of national law and the Guidelines of the

EBA, as well as that it will constitute outsourcing only on the grounds of the Guidelines of the EBA.

2. Questions without answers.

   Experts indicate ambiguities concerning classification of specific cases.

   - Whether so-called B2B agreements that are standard on the IT market (standard type of agreement with programmers) should be treated as outsourcing i.e. whether an in-house programmer employed on the grounds of a B2B agreement should be treated in compliance with the rules for typical suppliers and be covered with the scope of guidelines concerning outsourcing? Analogous problems occur with suppliers using services provided by programmers employed on B2B agreements in the context of possible sub-outsourcing. It should be interpreted whether the approach will be based on the economic sense of the agreement in compliance with the IT market (and then will not be treated as outsourcing/sub-outsourcing) or on the literal meaning of the guidelines of the EBA (outsourcing as any agreement concluded with a supplier).
   - If a supplier of a cloud solution does not have access to legally protected data transferred by the bank to its supplier, if data are encrypted, is it valid to classify cloud solutions as subcontractors irrespective of a formula of such a solution (IaaS, PaaS, SaaS) and irrespective of whether cloud is of public or shared character? The fact of using cloud solutions by their suppliers should be perceived as one of premises in the process of assessing risk related to using a given supplier, however, it should not be a decisive element and it should possibly be taken into account from the point of view of plans of business continuity and security in the scope of the continuous provision of services to a client and not from a point of view of classifying this third party as a subcontractor.

3. The requirement of unlimited liability of the outsourcer for damages caused to the bank's customers.

   The majority of experts criticise this requirement. Simultaneously, many experts postulate full liability of the outsourcer's subcontractor for caused damages by using rational arguments. Of course, in no event can it exceed the damage actually caused to the customer or the bank.

   Some experts indicate that in the view of the absolutely binding provision, banks coerce relevant clauses in agreements, yet, as they claim themselves, these clauses are "empty" and it is known that in case of any issues such clauses are ineffective. It is probably the worst possible solution, since in practice it prevents from assessing the risk.

While approaching the matter without emotions, it should be stated that entrusting an outsourcer with performance of certain activities, especially critical ones, cannot increase the risk of the bank's activity. Of course, the bank must properly assess all risk factors and monitor performance of entrusted activities, however, the outsourcer should be fully liable for culpable loss caused by him. The largest outsourcers are the biggest opponents of this provision. However, at the same time, those are the most advanced enterprises, so the risk that they will be exposed to indemnity that could affect them is low.

Almost 20 years have passed as of the introduction of this provision, the reality and environment have changed. In this situation, it would be appropriate for KNF to conduct legal and business analysis of this issue to solve this problem. An in-depth, reliable analysis that would take into consideration both benefits for the bank from the binding provision, as well as losses that could occur as a result of maintaining the binding law, should answer the regulator's and banks' question on possible change of the discussed provision and consequences of each possible decision.

4. A difference between outsourcing and insourcing.

   One of the questions concerned the scope of responsibility of the subcontractor - insourcer. Sent answers allow suspecting that it is necessary to provide additional explanations of the regulator with regard to the difference between outsourcing and insourcing, especially in the scope of sub-contracting. It is of crucial importance, since, whereas in the case of outsourcing the principles are universal and do not depend on the structure in which the outsourcing solution functions, in the case of insourcing it will depend on the approach to the group, commissioning activities to an entity that belongs to a group and, in consequence, the necessity (or not) to obtain permits etc.

5. Other postulates concerning outsourcing.

   One of the experts postulates further liberalisation of the Banking Law in the scope of the possibility to use sub-outsourcing by eliminating restrictions and requirements more restrictive than those resulting from the Guidelines of the EBA:

   - The possibility of a chain of subcontractors should be provided for. Perhaps, limiting the length of the chain should be considered, however, it should be at least multi-step.
   - Subcontractor of the subcontractor should be reported to the contracting authority/bank, however, the subcontractor should not obtain consent to select a given subcontractor and if such a consent was considered required, withdrawal thereof would have to be justified with irregularities attributable to a further subcontractor.
   - The subcontractor could present the principles of providing services by a further subcontractor, especially in the form of Rules and Regulations or Specifications.

Principles of changing these documents by a further subcontractor should be binding for the contracting authority/bank.

- Lifting the ban on further sub-outsourcing (Article 6a par. 7 of the Banking Law) should be postulated. It would simplify many regulatory and legal issues. This ban is not congruent with the reality and complexity of the IT world.

6. Proportional approach to requirements.

   One of the regulatory restrictions concerning outsourcing banking services comprises an absolute obligation to use all tools and outsourcing obligations specified in binding provisions (e.g. Articles 6a-6d of the Banking Law) in the same scope and dimension towards all suppliers irrespective of the size of their activity or the scope of entrusted works. It should be possible to apply these tools and obligations on the grounds of the conducted risk analysis with a consideration of the principle of proportionality.

   For example, a large entrepreneur using various Data Processing Centres (DPCs) has different capacity to draw up and implement an emergency plan with the use of various DPCs. Whereas, a micro-entrepreneur or a small entrepreneur, as well as many fintechs providing innovative solutions are entities who, at a stage of establishing their market potential, are not at a disposal of significant resources and do not have the same capacity to guarantee execution of an emergency plan as a large entrepreneur.

   This is a significant problem. Undoubtedly, the risk assessment-based approach is necessary instead of limitation to rigid legal principles. From this point of view services proposed by a small entrepreneur or an innovative fintech are very risky and may even threaten the bank's security if not properly tested. Nevertheless, such an approach would lead to a vicious cycle: in order to assess the entity's risk, one would have to test its activity, which cannot be done, since it would be too risky for the bank. In such a situation, a proper solution would be to conduct tests on a small scale and in real conditions that is in a regulatory sandbox.

7. Consent to access bank secrecy.

   Requirements of the banking supervision with regard to obtaining consent and its specificity basically exclude disclosing the bank secrecy towards a service provider on the basis of a consent from customers. In effect, it leads to qualification of a series of services, the connection of which with the banking activity is loose, as outsourcing banking services.

   Therefore, one should expect changes in the law allowing transferring information covered with bank secrecy so service providers without the necessity to obtain customer's consent in fulfilling by the bank the boundary conditions of such sharing information. It could be, for example:

- conducting risk assessment of the entity,
- concluding an agreement on providing services which includes clauses concerning data security (similar to European Model Clauses concerning personal data),
- unlimited liability of such an entity towards the subject of data.

It seems that in Poland restrictions that apply to sharing information covered with bank secrecy with a third party are much stricter than in other European countries. Therefore, it is important that also in this case the regulator analyses binding provisions, their impact on banks' functioning and, if the analysis indicates validity of reservations, amends provisions accordingly.