



ZWIĄZEK BANKÓW POLSKICH

Bird & Bird



Cloud Computing in the Polish Financial Sector Regulation and Standards

edited by Maciej Gawroński

November 2011

Forum of Bank Technology (FBT) introduction

This presentation forms part of the Forum of Bank Technology Report on cloud computing. Cloud computing and other solutions are increasingly popular in the banking sector. Cloud computing enables quick access to the newest resources containing software, applications, hardware platform, without investing into hardware, or without long lasting and expensive implementations.

The Forum of Bank Technology created a cloud computing group. The main purpose of this group is to prepare a report on the application cloud computing in the Global and Polish banking sector. This report described the phenomenon of cloud computing, a model of cloud processing, legal aspects, possibilities of cloud applications, barriers and restrictions as well as benefits.

The Report is scheduled for publication at the end of 2012.

The legal part of the Forum of Bank Technology Report on cloud computing, edited by Maciej Gawroński, is presented below.

From Maciej Gawroński

I hope that our presentation would be helpful for the readers. We tried to present the regulations which have to be included when considering the use of IT services in the cloud model in a clear and comprehensive manner. We are open for comments and discussions on this subject and you can contact me directly at maciej.gawronski@twobirds.com.

Maciej Gawroński

The Report is also available on the website:
<http://www.zbp.pl/site.php?s=MjIzODYxMA==>

and

<http://www.twobirds.com/English/Expertise/Pages/Poland.aspx>

Cloud Computing in the Financial Sector

Legal Part

Table of contents

1.	Cloud Computing and Regulations Concerning Personal Data Protection	7
1.1	Duties of the data controller and cloud computing	9
1.2	Personal data protection duty in the PDPA	9
1.3	Cloud computing as personal data processing outsourcing	9
1.4	Personal data processing outsourcing agreement	10
1.5	Sub processing of personal data	11
1.6	Exporting of personal data	11
1.7	Sanctions	13
1.8	Summary	13
2.	Outsourcing in the Financial Sector	16
3.	Bank Outsourcing	20
3.1	Contents of banking outsourcing restrictions	20
3.2	Formal requirements	21
3.3	Sanctions	23
3.4	Summary	23
4.	Recommendations of the Polish Financial Supervision Authority	26
5.	Industry Standards	28
5.1	ISO standards	28
5.2	British Standards Institution standards	28
5.3	SAS70 Standard and SSAE16 Standard	29
5.4	ITIL 2011	29
6.	Other Financial Sector Regulations	32
6.1	Cloud Computing in regulations concerning the investment fund sector	32
6.2	Cloud Computing in regulations concerning the pension fund sector	33
6.3	Cloud Computing in regulations concerning operations of investment firms	34
6.4	Cloud Computing in insurance activity	35
7.	Cloud Computing in Regulations Concerning Classified Information (State Secrets)	42
8.	Cloud Computing in Accounting	44
9.	Regulations with Regard to Cloud Computing in Individual European Union Member States	46
9.1	Personal data protection	46
9.2	Financial sector	47

Introduction to the legal section

The presented study tries to summarize the national regulations applicable to cloud computing in banking, as well as other areas of the financial sector. The study forms the first part of the Report on cloud computing of the Forum of Bank Technology of The Polish Bank Association working team.

So far there have been no regulations, official interpretations or recommendations in Poland directly referring to cloud computing. However there are norms regulating the outsourcing of information processing and the outsourcing of operations that an organization can carry out, using its own resources. In this document we try to interpret the existing regulations taking into account the conditions they create for the cloud computing model.

The regulations which apply to cloud computing are, first and foremost, those concerning personal data protection and outsourcing.

Data Protection. As a rule, cloud computing constitutes the outsourcing of personal data processing to another entity. The personal data protection regulation is of a general nature, thus it will be described first. We will also analyse individual regulations concerning the outsourcing in the financial sector by presenting their general logic.

There is a discrepancy between the traditional/territorial view on the personal data protection and the cloud model. Data protection authorities indicate that in the context of a cloud, the powers of the information owner towards the cloud provider are illusory, in particular, the powers to supervise the data processing (including giving some binding guidelines to the cloud provider or the possibility of an audit). The solution may give a new approach to the understanding of these powers. First of all, the right of supervision over data should be interpreted in such a way that the information owner, by selecting a cloud provider, chooses a method of data processing in a cloud. This choice would be based on the fact that the information owner can benefit from services of specified standard parameters and give it up at any time; however, the owner cannot modify or adjust the services to his or her individual needs. Secondly, the supervision and audit could be carried out through the appropriate certified third parties. Another issue is the requirement that the data owner is always aware of - where the data is and who is processing it on behalf of its owner. From a practical perspective, a good solution might be to define specific entities which can process the data, as well as areas where the data can be processed. If required in a specific case, it would be possible to locate a specific area of data processing and processing entity. From a data security perspective, there is no need for the owner to constantly follow the data or to be aware of its location at the given moment. In various European countries, the data protection authorities have different attitudes to cloud computing. Some of them approach this issue extremely restrictively while others in a friendly way. At the same time, personal data protection law at the EU level does not prohibit cloud computing. The existing discrepancies, even between various EU regulators, show that a fresh approach to the personal data protection and the phenomenon of cloud computing is needed. The work on this new approach is already underway in the European Commission.

Outsourcing in financial sector. Regulations of the financial sector concerning outsourcing of different activities to external entities focus on whether the activity or the process being subject to the outsourcing, are critical to the organization. Such activities, in particular, relate to access to information protected by law, but also others, of which disruption would undermine a financial institution's ability to provide services to its customers.

If an activity is critical, regulations are based on the following assumptions: **(i) liability** - unlimited liability of the service provider for damage, **(ii) security of information** – a financial institution is expected by the regulators to know and control its operating risk, **(iii) business continuity** – regarded as one of the aspects of information security, **(iv) risk monitoring** – knowledge of the actual outsourcing risk, where, likewise in the case of personal data protection, the EU treats the data processing outside the European Economic Area with much greater mistrust (and thus with greater formalism).

Future. Limitations and concerns, mentioned above and described in greater detail in the following part of this document, influence the cloud computing model development rate. However, it seems that adopting the cloud computing model will take place in the near future. Even today a large part of the most popular “consumer services” is being provided by using cloud computing. The consumer is convenience as the B2C process is rather unstoppable. In the B2B area the process is slower, administratively more controlled, and gives potential customers greater responsibility. Nevertheless, considering the possible economic benefits and a faint difference in terms of the technology towards the currently used IT solutions, the expansion of the cloud computing services will also be expected.

Cloud Computing and Regulations Concerning Personal Data Protection

1. Cloud Computing and Regulations Concerning Personal Data Protection

Personal data protection regulations. The basic provisions regulating cloud computing, although they do not refer to it directly, are the provisions on personal data protection. These provisions are, in particular:

- (i) Personal Data Protection Act of 29 August 1997 (Journal of Laws No 02.101.926) (hereinafter the “**PDPA**”), which constitutes the implementation of
- (ii) Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter the “**Directive**”); and
- (iii) Regulation of the Minister of Interior and Administration of 29 April 2004 concerning documentation of personal data processing, as well as technical and organisational conditions which should be met by IT hardware and systems used to process personal data (Journal of Laws No 04.100.1024) (hereinafter the “**Regulation**”); and
- (iv) Particular sector regulations indicated in items 1.2 and 1.4 below.
- (v) Special personal data protection principles in relation to the provision of services by electronic means are regulated in the Act on Providing Services by Electronic Means of 18 July 2002 (Journal of Laws No 02.144.1204) (hereinafter the “**APSEM**”).

Basic terms. According to the PDPA, **personal data** refers to any information relating to an identified or identifiable natural person, on the basis of which it is possible to identify the identity of that person whether directly or indirectly (e.g. employee data, customer or potential customer data, email addresses, telephone numbers). In other words, these are relationships between various elements of data about a person, leading to a specific person.

The personal data “owner”, so to speak – the entity that decides about the purposes and means of the processing of personal data, is called the **personal data controller**. E.g. the controller of a bank’s customer data is the bank.

The controller may carry out operations on personal data on its own or outsource them to a subcontractor, called a **personal data processor**. The processor is an entity operating on behalf of the data controller and is authorised by the data controller to process personal data.

In cloud computing, we often encounter situations in which the data controller is the user and the data processor is the provider of services in a cloud. Other configurations are also possible.

The processing of personal data regulated by the PDPA is presented very broadly because it covers any operations on personal data, such as collecting, recording, storing, processing, providing access to and deleting information, especially those performed within IT systems.

Scope of application of personal data provisions. In the light of the Directive and Opinion 8/2010 of Article 29 Working Party¹ on applicable law of 16 December 2010 (the “**Opinion**”), it should be assumed that the PDPA applies to data controllers (e.g. cloud users) **(i)** having their registered office within the territory of Poland or conducting permanent and separate operations in Poland (e.g. in the form of a branch) or **(ii)** having their registered

¹ The Article 29 Working Party is an independent European advisory body with regard to personal data and privacy protection, composed of representatives from personal data protection authorities of each EU Member State.

office outside of the European Economic Area (hereinafter the “EEA”), but using technical means located within the territory of Poland to process personal data (on condition that those means are not used exclusively to process personal data). Technical means of the data controller from outside the EEA are deemed to be, among other things, the data controller’s servers located within the EEA, but also the technical means of a data processor within the EEA to whom the data controller from outside the EEA outsourced the processing of personal data. According to a novel opinion, expressed in the Opinion, technical means used by the data controller to process data and located in Poland, which will result in the application of Polish law, may also include cookie text files placed on the data terminal equipment of a user located in Poland (e.g. on a computer, tablet or smartphone) in order to store personal data.

The PDPA will apply to any data processor with its registered office in Poland to the extent of the regulations stated in Chapter 5, i.e. safeguards for personal data filing systems.

According to the Directive and the Opinion, where the data controller and processor are in different EEA States, the relationship between the data controller and processor is governed by the personal data protection law of the State of the data controller’s registered office. Additionally, personal data protection rules specified in the state of the processor’s registered office shall apply to the data processor.

Therefore, the PDPA also applies to the processor in situations (i) and (ii), although to a limited extent, i.e. only in relation to safeguards for personal data.

The scope of application of the PDPA may therefore be very broad. Similarly, the scope of application of other European acts based on the Directive may be equally as broad.

“Multi-regime compliance” of the cloud. In theory, the Directive determines a uniform level of personal data protection in the EEA and imposes a similar level of duties on entities processing data – in practice, discrepancies between individual legal systems in EEA countries are considerable.

Formally, it is the personal data security rules relevant to the registered office of the processor that will apply to the data processor.

In practice, however, the data processor is often obliged to fulfil not only the personal data security requirements of the data processor (where the duties are governed by the law relevant for its registered office), but additionally, in performance of the personal data processing agreement, it is obliged to fulfil the duties of the data controller, including with regard to the personal data security.

In this type of case, despite the position expressed in the Opinion as indicated above in regard to the application of the law of the country of the processor’s registered office governing personal data security duties, in practice a situation takes place in which the personal data processor is obliged to cumulatively apply safeguards indicated both in the law of the country of its registered office and in the country of the data controller’s registered office.

In particular, data controllers (cloud users) from Poland should expect that providers of a cloud located in other EEA countries will meet the duties specified in the PDPA, including personal data security. In theory, the personal data protection method guaranteed by legal systems of other EEA countries should be sufficient. However, due to the regulations imposed on cloud users from Poland (e.g. the obligation to provide IT system functionality, thanks to which the system records who and when has access to data, and who modifies data, when and to what extent), it will often be necessary for the cloud provider to ensure the compliance of the cloud with Polish requirements with regard to personal data security.

Similarly, the data processor (cloud provider) based in Poland or using technical means to process personal data in Poland, addressing its services to data controllers (cloud users) based in different EEA countries may be forced to adapt the personal data processing terms to meet the requirements of all of the involved Member States.

1.1 Duties of the data controller and cloud computing

In order for the personal data processing to be compliant with law, the data controller (cloud user) must fulfil a number of duties resulting from the PDPA and the Regulation, including (i) ensuring particular care in data processing (i.e. ensuring that data are processed for a specific, defined purpose, and that they are substantively correct (accurate, complete and up to date), and adequate for the purpose of processing, and that they are processed no longer than necessary to achieve the purpose of processing), (ii) processing personal data pursuant to specific legitimising prerequisites, (iii) ensuring appropriate information for the data subject, (iv) registering the data filling system, (v) appropriately securing personal data.

Those duties may be performed directly by the data controller or, as has been mentioned above, the data controller may outsource the performance of parts of these duties to a processor (e.g. the duty to provide appropriate information to data subjects).

The data controller is responsible for the processing of data in accordance with law, including the meeting of all statutory duties / supervision over fulfilment of all duties. That is why the data controller should have ongoing control over the conditions in which personal data is processed. This must include control of the entities that receive personal data under its administration, where and how such data is processed, and whether the data is adequately secured.

1.2 Personal data protection duty in the PDPA

The duty to secure personal data in accordance with the PDPA and the Regulation may turn out to be particularly problematic in the case of the processing of personal data in a cloud (especially if personal data will be processed by a provider outside Poland).

Polish regulations are among very few in the EEA which describe appropriate technical and organisational safeguards which should be applied to adequately protect personal data in such detail.

As an example, it may be indicated that a Polish data controller (processor) should have and implement in its organisation a written security policy and an IT system management instruction, as well as records of IT system users. Those documents should determine among other things places in which the data are processed (i.e. places in which the processing of personal data takes place physically), functionality of the IT system (for example, whether the system ensures the recording of who enters data into the system and when, and also when they are modified, as well as to whom they are forwarded and when).

If the personal data have been outsourced or forwarded to third parties to a “cloud,” it may be problematic to identify places in which the data under administration are located in the security policy. As it seems, all locations of data centres belonging to the cloud should be indicated. Additionally, the data controller must meet requirements in terms of IT system functionality, such as the requirement that clear reports are drawn up indicating the data source, information about any objections, cases of data availability together with dates and scope to which they were made available.

Where a personal data controller submits personal data to a cloud provider whose centre of business is located in Poland, the meeting of the above duties should not be a problem because the cloud provider is obliged by the PDPA and the Regulation to apply them in its own organisation.

Where a data controller (cloud provider) submits data to a cloud provider outside Poland, it should particularly ensure that the cloud provider secures data adequately.

1.3 Cloud computing as personal data processing outsourcing

A question appeared in the literature as to whether the computing cloud constitutes outsourcing of the processing of personal data. This question has been posed in the context

of cloud computing consisting exclusively in the provision of infrastructure access intended for data storage, for example, hosting.

According to the Article 29, Working Party, in their view expressed in Opinion 1/2010 of 16 February 2010 concerning the terms of “data controller” and “processor”, state that as a rule, hosting constitutes the outsourcing of personal data processing to a data processor.

Part of this doctrine questions such qualification of the cloud as a data processor in the situation where the cloud provider does not have access to data because they are encrypted by the cloud user. It seems, however, that as long as personal data storage is one of the operations constituting the processing of personal data within the meaning of the PDPA, outsourcing even no more than cloud user’s personal data storage operations to another entity (cloud provider) in fact constitutes outsourcing of the personal data processing.

The General Inspector for Personal Data Protection (hereinafter the “GIODO”) expressed an interesting opinion at https://edugiodo.giodo.gov.pl/file.php/1/INF1/INF_R05.html. It says that “where we are dealing with the outsourcing of data processing within the meaning of Article 31 of the PDPA, meaning that the entity providing access to the IT infrastructure has knowledge as to the nature of data processing, it shall be subject to its regulations to the extent of Article 36-39 (personal data security), despite the fact that it is not the personal data controller. However, if the entity providing access to the system does not know the nature of data processed, then it is subject to provisions of Article 12-15 of the APSEM”.

In practice, however, any infrastructure provider citing lack of knowledge about the nature of data processed as an excuse will not be credible.

1.4 Personal data processing outsourcing agreement

A properly drawn up agreement guaranteeing constant maintenance of the appropriate personal data processing method may be a remedy for most of the above problems related to ensuring adequate control over the rules of processing and securing personal data.

In the case of a private or hybrid cloud, the cloud user has an opportunity to individually shape contractual provisions in a manner ensuring appropriate securing of data processing processes in the cloud. In the case of a public cloud, a cloud user will have little or no possibility to negotiate an agreement and influence its shape, and therefore the cloud provider’s responsibility will be to develop such an agreement that an institution of public trust, like a bank or other financial institution, has the possibility of accepting the proposed terms.

The PDPA orders that the outsourcing of personal data processing to a processor by the data controller takes place on the basis of a personal data processing outsourcing agreement. A provision of the PDPA states that such agreement should be concluded in a written form. The absence of the written form may result in negative consequences for the data controller under administrative law, and the GIODO may issue a decision ordering the conclusion of such an agreement in the written form. Theoretically, it may also result in penal liability for inadequately securing personal data.

The personal data processing outsourcing agreement should determine the purpose and scope of the processing of personal data to at least a minimum extent. As has been shown above, the data controller – user of services in a “cloud” – is responsible (before the GIODO and the data subject) for meeting all obligations imposed on it, even if the processing of data has been outsourced to a processor.

The processor, in turn, is as responsible before the GIODO for securing personal data in relation to personal data entrusted to it as the data controller. The processor has a responsibility to the data controller for compliance of data processing with the agreement concluded.

In Poland, it is in fact sufficient to rely on the personal data processing outsourcing agreement on provisions of the PDPA and the Regulation because they provide a sufficient level of security. However, in the case of the outsourcing of personal data to a cloud provider in another EEA country (particularly if that provider conducts business in a legal system which does not ensure detailed statutory regulations with regard to securing data), such contractual regulation of data security will play the fundamental role.

It is, therefore, necessary to carefully describe in the agreement all details of the processor's obligations, as well as to establish the controlling authorities of the data controller, regulation of the method of returning or destroying personal data in the event of termination of the agreement and specification of places in which the data will be processed. In this way, the data controller may acquire a contractual guarantee that personal data in the cloud are properly secured.

1.5 Sub processing of personal data

The cloud provider who would like to subcontract part of the service provided in the cloud to another contractor (e.g. a company from the group) should remember about the implications of such subcontracting from the point of view of personal data. Subcontracting constitutes the sub processing of personal data, which, unlike the outsourcing of data processing, is not regulated directly in the PDPA.

According to the GIODO, sub processing is compliant with law where (i) the data controller enters into the outsourcing agreement directly with the sub-outsourcing entity or (ii) the agreement between the data controller and the data processor contains an explicit authorisation to sub process personal data.

This means that (i) the cloud provider should enter a clause on personal data sub processing into the personal data outsourcing agreement with the cloud user or (ii) the cloud user should conclude an agreement directly with the sub processor.

The first possibility seems more optimum from a practical point of view, however the sub processor should be identified. A general indication of the sub processor may be insufficient.

It is assumed that requirements must be met concerning the personal data outsourcing agreement indicated by the Act, i.e. the obligation to conclude a written agreement, indication of an objective and scope of data processing, securing of personal data by the sub processor also apply to the sub processing agreement/clause.

1.6 Exporting of personal data

Exporting of personal data is a jargon term used to describe the transfer of personal data outside Poland. Obviously, in the context of the Internet, legal institutions and concepts based on the Directive of 1995 (which was created before the Internet era) do not fully correspond to the existing reality and, out of necessity, force artificial territorial divisions.

Having that assumption in mind, the key factor which should be examined in the case of data exporting is the location of the cloud, i.e. determination of whether the cloud is within the territory of the EEA or outside. The exporting of data within the EEA (as ensuring the same level of protection under the Directive) does not require meeting additional requirements. Therefore, placing personal data in a cloud located within the EEA is treated as using the services of a Polish cloud.

Outside the EEA. Exporting data to a third country outside the EEA does not require meeting additional obligations if that country's law ensures adequate protection of personal data. If the exporting of personal data is to take place to a third country that does not provide adequate personal data protection, it is necessary to meet additional requirements.

The European Commission, in the form of a decision, has indicated only 10 countries so far (including Canada, Australia and Israel), which meet the requirements of adequate

protection, and thus exporting data to these countries does not have to be guarded by special requirements.

The United States, as a rule, does not ensure an adequate level of protection. However, some American business entities, which have acquired the Safe Harbour scheme certificate through participation in that scheme, guarantee an appropriate level of personal data protection. It should be remembered, however, that American entities have the possibility of selectively acceding to the Safe Harbour scheme, e.g. only in relation to their own employee data.

Thus, if a cloud is also located in a place outside of the EEA that ensures an adequate level of protection or if the cloud provider has acceded to the Safe Harbour scheme – the cloud user is protected from additional obligations.

GIODO's consent to data exporting. Theoretically, in accordance with the PDPA and GIODO's guidelines, a data exporter should conduct an independent evaluation as to whether the state to which it intends to export data provides adequate personal data protection.

In practice, such evaluations would be extremely difficult because this would require that all data transfer circumstances be taken into account, including the knowledge of law of another country and its practice of application. Additionally, the evaluation should allow for the influence on the adequacy of the intended export of such elements as nature of data, purpose and duration of the intended data export, as well as the country of origin and country of final destination of the data. The data exporter would also incur the risk of a wrong assessment of adequacy of another legal system (in the form of administrative or even penal liability).

That is why it is assumed, in practice, that only exports of data to third countries accepted by the European Commission or belonging to Safe Harbour ensure an adequate level of protection and not do require additional obligations.

In order to obtain the GIODO's consent, the data exporter must ensure that the data importer guarantees appropriate protection of privacy, as well as of the rights and freedoms of the person to whom the data refer. Most frequently, an appropriate agreement between the data exporter and the data importer will constitute such guarantee.

The European Commission has developed two mechanisms of ensuring adequate data protection, i.e.

- (i) standard contractual clauses (a set of appropriate model contractual provisions);
- (ii) binding corporate rules (the possibility of adopting data protection rules binding for companies within the given corporation – as a result of acceptance of those rules and their approval by appropriate personal data protection bodies – in Poland GIODO – a corporation is treated as a safe data processing area in which personal data are protected at the level required by the European Union, and

From a practical point of view – the GIODO's consent is granted for a specific instance of data exporting, to the extent indicated in the application – data categories that are to be submitted, persons to whom data refer, and purpose of data processing after handover must be specified in detail. The GIODO does not grant general consent for the exporting of all data categories without their detailed specification. Therefore, if a data exporter would like to extend the range of data exported (e.g. due to the extension of the cloud provider's offer), it must reapply to the GIODO for its consent.

Other grounds for data exporting. Hypothetically, exporting data to a country which does not provide an adequate level of protection may be also conducted without the GIODO's consent on the basis of one of the following exceptions, e.g. (i) with the written consent of the person about whom the data refer (the written form has not been observed if the consent has been expressed via the Internet), (ii) where it is necessary to perform an agreement between

the data controller and the person about whom the data refer, or undertaken at that persons request, (iii) data are generally available. However, these prerequisites would have to refer to every piece of data exported, i.e. they would have to refer to all data and each of the individual persons whose data were to be placed in the cloud. In practice, it is of little probability that any of those prerequisites would be relied on with regard to all personal data (and thus all data subjects) that could be placed in the cloud.

By way of an example, let us consider a cloud user who would like to base the submission of personal data to a cloud located outside the EEA on the consent of data subjects (quite apart from the need to obtain a written consent, which in the context of entities operating pursuant to banking law could potentially be valid when acquired in the electronic form due to Article 7 of the Banking Law).

Consent must be voluntary to be valid. Moreover, the data subject may revoke its consent at any time (which could have future implications). This means that if even one person did not express his or her consent to export data to a country outside the EEA or revoked consent, the cloud user would be forced to withdraw that person's data from the cloud and process it only within the territory of the EEA or obtain the GIODO's consent for the exporting of those data.

This model of personal data export based on the consent of the person to which the data refer by its very nature would not be complete, i.e. it would not concern all persons whose data are in the given filing system. Therefore, it is not appropriate for ensuring legality of exporting personal data contained in a entire, complete filing system.

Thus, exceptions from the obligation to acquire the GIODO's consent to data exporting are of marginal relevance for the forwarding of data to a cloud.

1.7 Sanctions

For the failure to observe regulations on personal data protection, in particular at the time of the processing of personal data in a cloud or outsourcing of them to a cloud, the following sanctions may be imposed: (i) administrative, (ii) penal, or (iii) civil.

The GIODO may demand the reinstating of a status compliant with law, on the basis of an administrative decision, e.g. by applying additional safeguards with regard to the personal data collected, suspension of the forwarding of data to a third country. In the case where the infringing entity fails to execute the decision, the GIODO may impose a fine in order to force the entity to execute the decision – up to PLN 50,000 in a single fine, and jointly up to PLN 200,000.

The consequence of a number of violations of the PDPA is also penal liability. For example, in a situation where the data controller violates the obligation to secure data in a cloud, even unintentionally, it is guilty of an offence according to the provisions of the PDPA, subject to a fine, restriction of freedom or imprisonment for up to two years.

Privacy and personal data are also covered by civil law protection. The failure to observe personal data protection rules may result in the infringement of personal rights of the data subject. Such a person may demand the abandonment of the infringement and removal of its consequences, payment of an amount as compensation for harm suffered, or indemnity for damage caused.

1.8 Summary

The model of the processing of personal data in a cloud is encompassed by the current personal data protection model.

The processing of data in a cloud is legal if the cloud user meets all obligations imposed on it with regard to personal data protection. From a practical point of view, this means that the cloud provider must ensure for the cloud user (who is responsible for the personal data

processed in the cloud) that the processing of personal data in the cloud will be in accordance with the principles binding for the cloud user.

The key issue is the appropriate agreement between the cloud user and provider. It should guarantee appropriate personal data processing rules and a mechanism of verification of these rules.

Additionally, if the cloud location were to extend beyond the European Economic Area, it is necessary to ensure a legal basis (usually, the GODO's consent) of the exporting of data to the cloud provider.

Considering the multi-entity and multinational nature of cloud processing, the binding corporate rules mentioned above may turn out to be a convenient method of proving a cloud's compliance with the European personal data protection regime.

The European Commission, wanting to address any difficulties or doubts related to the processing of data in a cloud and to ensure appropriate protection of data processed in a cloud outside the EEA, is currently preparing a strategy concerning cloud computing. This strategy may affect the interpretation of regulations concerning personal data in a cloud, as well as further legislative changes in that respect.

Outsourcing in the Financial Sector

2. Outsourcing in the Financial Sector

Norms and the resulting regulations concerning the outsourcing of operations are the main concern in cases when the particular operation or process to be outsourced is critical to the organisation (i.e. whether the problem with the execution of such operation or process makes it impossible or significantly hinders the pursuance of the organisation's core activity).

Regulations, in principle, focus on operations or processes critical to the organisation, leaving non-critical operations outside the area regulated by administrative law, i.e. within the domain of civil law and the freedom of contract principle. The assessment of the relevance of the (outsourced) operation to the organisation is left by regulations to the sphere of practice, with one significant exception – operations related to the access of legally protected information deemed to be critical / subject to regulations. In accordance with this logic, the restrictions refer to operations that result in access to data (information) covered by the obligation to observe secrecy imposed by law, and other operations critical to the organisation.

In the case of critical operations and processes, regulations are generally based on the following assumptions:

(i) **Responsibility.** *He who can destroy a thing, controls a thing* (Paul Atreides, Dune, Frank Herbert). *With great power comes great responsibility* (Uncle Ben, Spiderman). As it seems, the Polish legislator must be a follower of both of those rules. In consequence, in the regulation of outsourcing, Polish law generally does not permit the provider of the critical service to restrict its liability for damages caused by the improper performance of such service.

(ii) **Security of information.** European regulators, including Polish, expect the financial institution to know and control its operating risk, including, in particular, the provision of the security of its legally protected information. The condition for ensuring security and informed risk management is knowing the risk. In internal processes, the assumption is made that risk is known. The organisation and its managing personnel encounter individual risk factors on a daily basis – processes, personnel, infrastructure. The need to institutionalise the risk monitoring process appears when we lose sight of a process – i.e. when we outsource it. Relying on this observation, the legislator and the regulators expect that the organisation, even when it has outsourced a particular operation, will in fact continue to monitor the related risk without restricting itself to the sphere of legal obligations, or warranties.

As regards the assurance of security, which is explained later in this paper, the question arises as to whether cloud computing actually ensures lower security of information than outsourcing, or even insourcing. It seems that the answer to such a question is – no. As a rule, cloud computing does not generate higher risk regarding information security than outsourcing or maintaining the process within the organisation. In the case of cloud computing, the same security and data separation methods apply as in the case of outsourcing/insourcing. Possibly, one of the advantages is additionally (from the point of view of data security) physical separation, because the largest threat for an organisation is always the activity of its employees.

However, the answer to the question of whether a specific cloud provider under a given solution ensures the level of information security we expect depends on the actual situation, about which the cloud user should obtain sufficient assurance.

(iii) **Business continuity.** Business continuity is one of the aspects of information security – security from the point of view of access to information. Regulators expect the assurance of business continuity for the same reasons described in the previous two sections.

It is possible that in the cloud computing model, economies of scale may facilitate the assurance of business continuity. The provider should be more committed to ensuring the business continuity of its service where it services many entities with the same infrastructure. At the same time, considering the size of the basic infrastructure, the cost of possible repairs or necessary redundancy may turn out to be relatively lower when compared to solutions on smaller scales, with the assurance of the same level of reliability.

3. Bank Outsourcing

The banking law, similar to other regulations currently in force, does not regulate cloud computing directly. However, legal requirements for the outsourcing of banking operations, specified in the Banking Law Act of 29 August 1997 (Journal of Laws No 02.72.665) (hereinafter the “**Banking Law**”), in particular in Article 6a-6d, shall apply to cloud computing.

Banks may outsource the performance of various legal or actual operations to another entrepreneur. The outsourcing of data processing, a type of which is cloud computing, is an actual operation within the meaning of the Banking Law. Thus, further analysis will focus on restrictions on the outsourcing of data processing by banks (outsourcing of a type of IT services).

The legislation imposes a number of obligations on banks related to the outsourcing of actual operations concerning banking operations.

IT services are subject to bank outsourcing restrictions.

These restrictions cover actual operations “related to banking activity”, i.e. related to banking operations (Article 5 of the Banking Law) and other operations undertaken by the bank within its activity and within the authorisation to undertake activity specified by the Banking Law (Article 6 (1) of the Banking Law) or other Acts (e.g. Insurance Intermediation Act).

In accordance with the position of the General Inspectorate of Banking Supervision (GIBS) (letter of 21 December 2004, NB-BPN-I-022-70/04), operations related to banking activity may be deemed to be only those which are directly and functionally related to such activity, i.e. partial operations (components) of operations indicated in Articles 5 and 6(1) of the Banking Law, or ones without which it is impossible (due to the essence or nature of the given banking operation or operation under Article 6(1) of the Banking Law) to perform the agreement the subject of which are the operations mentioned in Articles 5 and 6(1) of the Act.

Transposing this position to the area of information technology, GIBS includes such operations which involve access to “sensitive” information related to the banking activity of the outsourcing bank, in particular to data covered by banking secrecy and to actual operations related to banking activity. An important, determining factor is also the purpose of operations performed on behalf of the bank. Those operations whose importance is fundamental in ensuring continuous and undisturbed operation of IT systems used to directly perform banking activity (e.g. e-banking systems, systems used to record banking operations) are also deemed to be “in relation” to banking activity.

According to the regulator, however, operations concerning IT systems not used directly for banking activity purposes (i.e. in particular the sphere of internal processes, such as human resources management, internal materials administration, logistics and procurement management), acquisition of hardware, acquisition and installation of software, engineering, development and modification of licensed software, servicing of computer hardware or standard operating/system software are not covered by the statutory banking outsourcing regulations.

Distinguishing whether a particular actual operation or business process is related (specifically) to banking activity or not (division into critical and non-critical operations) is, therefore, important in determining the requirements constituting a condition for admissibility of outsourcing of data processing related to this type of operation or process.

3.1 Contents of banking outsourcing restrictions.

The entire banking outsourcing process is subject to active control by the Polish Financial Supervision Authority (hereinafter the “**PFSA**”). Under its authority, the PFSA (earlier its predecessor – the Banking Supervision Authority), through the General Inspectorate of

Banking Supervision (hereinafter the “GIBS”), also participates in the establishment of standards concerning the implementation of statutory requirements by issuing executive regulations (Resolution No 379/2008 of the Polish Financial Supervision Authority of 17 December 2008 concerning the determination of the list of documents relating to the activity of a foreign entrepreneur who is to perform operations outsourced by the bank, specified in Article 6a(1) of the Banking Law Act (hereinafter the “Resolution”), but also recommendations, interpretations and guidelines concerning the application of regulations related to banking outsourcing which, together with the statutory regulation itself, in practice create an integral regulatory body for the banking sector. This is why certain conclusions or information presented below allow for the position of the PFSA (GIBS) or regulations issued by the PFSA to fully present the essence of the problem.

3.2 Formal requirements

In order to outsource IT processes of critical importance (in particular client data processing) to a cloud (generally outside the organisation), the Bank must ensure that the following requirements have been met:

- 1) the bank and the cloud provider must have business continuity and disaster recovery plans (BCDR) covering the process / operations outsourced
- 2) the bank must conduct an analysis of the impact of outsourcing on the bank’s activity in terms of its influence on: (i) compliance with law; (ii) conservative and stable bank management; (iii) efficiency of internal control; (iv) possibility of bank audit; (v) information security (protection of secrets) – the outsourcing is possible if the impact analysis does not show negative consequences of outsourcing of operations
- 3) the bank includes the risk of outsourcing of operations in the risk management system
- 4) the bank records outsourcing contracts; and moreover

if the service provider or sub-provider is based outside the territory of the European Economic Area or outsourced operations are to be carried out outside the EEA

- 5) the bank must obtain the permission of the PFSA to conclude an agreement.

The outsourcing of operations by the bank may take place pursuant to an agreement concluded in writing. The bank should include the following items in the agreement with the service provider:

- 1) the need for the service provider to have a business continuity plan;
- 2) the provider’s undertaking to present a description of technical solutions used to provide services, ensuring security of information and efficient provision of services;
- 3) undertaking to provide services within the territory of the EEA or making the effectiveness of the agreement dependent on the PFSA’s consent to the performance of services or a service provider from outside the EEA;
- 4) terms of sub-contracting operations by the provider (sub-outsourcing), including (i) obligation to obtain the bank’s consent for permanent sub-outsourcing, (ii) obligation to do sub-outsourcing outside the EEA or to an entity based outside the EEA dependent on the PFSA’s consent, (iii) obligation to further “transfer” the provider’s obligations to a sub-provider (in particular those which are the consequence of regulations);
- 5) no limitation of liability;
- 6) principles of monitoring the method of performance of the agreement and risk related to its subject;

- 7) method of cooperation with the bank's internal control and audit;
- 8) provider's undertaking to submit to the PFSA's control and authorising the PFSA's access to information about the agreement and its performance;
- 9) the bank's right to amend the agreement as a result of the PFSA's decision or recommendations;
- 10) provider's undertaking to present the provider's incorporation and registration documents.

Prohibition on limitation of liability. The limitation of liability of the service provider towards the bank for client damages as a result of non-performance or improper performance of the outsourcing agreement is prohibited – Article 6b(1) of the Banking Law. The prohibition on limitation of the provider's liability is correlated with the statutory prohibition on exclusion or limitation of the bank's liability towards its clients for damages as a result of non-performance or improper performance of an outsourcing agreement by the service provider.

The issue of liability is particularly important for cloud computing. The cloud computing service originated in the area of consumer services where the financial liability of the service provider was practically excluded. Polish regulation on bank outsourcing is the polar opposite – full liability of the provider. This requirement still causes huge controversies on the part of service providers (particularly foreign ones), in particular in the IT service sector where there is widespread use of the limited liability practice. However, with the appearance of the cloud computing business offer in the financial sector, it is difficult to expect that the Polish legislature will change its attitude easily.

Sub-outsourcing. Until recently, in the light of the interpretation of the Polish Financial Supervision Authority, sub-outsourcing was prohibited. Currently, the possibility of subcontracting operations covered by the outsourcing agreement has been formally accepted. Sub-outsourcing cannot cover all of the services included in the agreement (in order to avoid the construction of a so-called “shell”), and moreover (i) it should either be provided for in the outsourcing agreement and the bank should express its written consent to the specific subcontracting; (ii) or it may take place incidentally in order to reverse the consequences of a disaster or another event of force majeure. The same requirements in terms of direct outsourcing apply to sub-outsourcing (e.g. prohibition on limitation of liability, business continuity plans, ensuring the possibility of an effective control by the PFSA, requirement of the PFSA's consent to going outside the EEA). Also, regulations concerning banking secrecy have been amended in a manner adapting them to the institution of sub-outsourcing.

Similarly as in the sub-outsourcing of data processing, the issue of sub-outsourcing is relevant for cloud computing. The main service in cloud computing is the “cloud” and its resources. Cloud resources of data processing are usually under legal ownership and actual control of various entities. In our opinion, as a rule it does not prevent the use of the master agreement / sub-outsourcing agreements structure. However, both parties to the cloud computing agreement and the regulator will have to conduct the actual assessment on the basis of the circumstances of the specific case. Practice will certainly develop accepted structures and provisions. The use of transaction structures developed by the banking sector under the rule of the previous regulation will also be possible – allowing the conclusion of outsourcing agreements with “multi-entity” banking services providers, where in reality, services of most of service providers are of an auxiliary, i.e. supporting (supplementary) nature in relation to the services of the main provider. Typical structures of this kind include: a syndicate of providers, a special purpose vehicle of the provider and its subcontractors, a local agreement in order to perform the provisions of a global agreement concluded by parent companies (provider appears as a leading entity with subcontractors).

Supervision of the PFSA and the ban over outsourced operations. In accordance with the Banking Law and additionally the PFSA's (GINB's) guidelines, the bank should ensure for itself and for the PFSA rights including the right to inspect premises where

services are provided, service provider's documentation, including financial documents (also by the bank's statutory auditor) and other related to services provided at the level of the agreement with the service provider to the extent to which it is necessary to assess the quality of services, legal and financial situation of the service provider, and the service provider's ability to provide services in a proper and continuous manner.

The right to conduct physical inspections is also an important issue from the point of view of cloud computing. Considering that the use of a cloud is aimed at the effective use of IT resources, combined with the fact that the data of service users may be in each and every location of the cloud, an independent execution of the possible right to inspection by each of the clients could significantly hinder the operations of a cloud provider, resulting in the reduction of security. Both economic reasons and process quality reasons would, in our opinion, indicate that it is reasonable to have an independent third party conduct cyclical security audits with the right of direct inspection by the client in special situations.

Business continuity plans. The issue of provisions for actual and legal business continuity seems particularly important in the case of a process placed in a cloud. The issue of reliability of a cloud and the possibility of migrating the process serviced by the cloud to another environment must be verified before a decision is made to "enter the cloud", and then monitored.

Information/secretcy protection. Ensuring information security in a cloud is an important issue. The evaluation of possible and practical implementation of this security can be ensured by technical specialists. The use of appropriate standards by cloud providers and their submission to audits conducted by independent institutions will lead to a considerable increase in the transparency of the issue. General concern about the security of data in a cloud is sometimes expressed – in particular, about securing them against unauthorised access by e.g. other cloud users. It seems, however, in practice, the ensuring of data security in a cloud does not differ significantly from, e.g. ensuring security of data in the infrastructure of a provider of outsourcing services.

3.3 Sanctions

The PFSA may order the bank in the form of a decision to undertake activities aimed at amending or even terminating an outsourcing (sub-outsourcing) agreement (Article 6c(5) of the Banking Law). Such a situation may take place when:

- 1) the performance of the agreement constitutes a threat to the conservative and stable bank management; or
- 2) an entrepreneur or foreign entrepreneur party to the agreement loses the required authorisations necessary to perform the agreement.

Moreover, it should be remembered that the submission of an appeal by the bank against the PFSA's decision does not stop the execution of such a decision (Article 6c(5) of the Banking Law). The lapse of the deadline appointed by the PFSA and the failure to execute the obligations imposed may result in the PFSA applying (without any prior notification) measures provided in Article 138(3) of the Banking Law (including (i) petition to dismiss the president of the management board of the bank, (ii) fine up to PLN 1,000,000).

3.4 Summary

The use of IT services by the banks in the cloud computing model should be verified from the point of view of statutory requirements concerning outsourcing in banking operations.

Where those services concern performance of operations connected functionally with banking activity conducted by the bank (direct application of the cloud in the performance of banking activity) or result in service provider's access to banking secrets, they will be covered by the regime of outsourcing regulations, with all consequences for preparatory operations

on the part of the bank, contractual terms of their provision, as well as possible obligations with regard to the PFSA (limited after the last amendment of the Banking Law mainly to the obtaining of a permission to outsource outside the EEA).

Recommendations of the
Polish Financial Supervision Authority

4. Recommendations of the Polish Financial Supervision Authority

Recommendations issued by the Polish Financial Supervision Authority include Recommendation D of 2002 (as updated) concerning management of risks accompanying IT and telecommunication systems used by banks and Recommendation M of 2004 concerning management of operating risk in banks refer to issues related to cloud computing.

Both documents basically contain recommendations which are pragmatic and compliant with good IT business practices, close to the requirements described above, which the Banking Law imposes on banks in the case of banking outsourcing (e.g. need to apply systemic and well-thought-out approach to IT solutions used by the bank – having an IT strategy, having a business continuity strategy, analysing and monitoring operating risk).

Industry Standards

5. Industry Standards

Cloud computing is a new business phenomenon in IT technologies. As a result, it sometimes arouses mistrust, and questions about the level of security in a cloud appear.

As it seems, from a technological point of view, cloud solutions differ from IT solutions applied so far mainly by their scale and the parallel use of cloud resources by different users (a so-called private cloud is deemed, as a rule, to be “ordinary” outsourcing). The above indicates that technological problems, in particular those concerning information security (confidentiality, integrity, accessibility, accountability) do not differ from “non-cloud” IT problems.

Considering the above, available industry standards may play a special role in the substantive evaluation of the cloud processing service. At the same time, considering the same concerns and points of interest of individual users and potential users of a cloud, the cloud provider should be interested both in the use of recognised standards, and authentication of its service through its certification and verification by independent specialists.

Below, we list international standards known to the authors of the report from the point of view of which technological and organisational solutions offered under cloud computing services may be evaluated.

5.1 ISO standards

PN-ISO/IEC 20000-1:2007 Information technology – Service management – Part 1: Specification

PN-ISO/IEC 20000-2:2007 Information technology – Service management – Part 2: Rules of conduct

ISO/IEC 20000-3:2009 Information technology – Service management – Part 3: Guidance on scope definition and applicability of ISO/IEC 20000-1

PN-ISO/IEC 27005:2008 Information technology, Security techniques, Risk management in information security

ISO/IEC 27001:2007 Information technology, Security techniques, Information security management systems, Requirements

The above-mentioned standards may be used to develop rules for service delivery (business continuity management, security assurance, optimisation) by the cloud provider, as well as for the bank’s evaluation of solutions concerning business continuity, developed and presented to the bank by the cloud provider. Organisations may obtain certification with regard to ISO 20000 and 27001.

ISO/IEC 31000:2009 – Risk management, Principles and guidelines, and ISO/IEC 31010:2009 – Risk management, Risk assessment techniques. Standards, in accordance with their titles, contain principles, guidelines and methods of assessing various risks, and may be useful at the stage of analysis of the impact of forwarding the processing to a cloud, and in the further risk assessment. Standards are of general nature – they are not specifically addressed to “IT” risks.

5.2 British Standards Institution standards

BS 25777:2008 Information and communications technology continuity management – Code of practice. Similar to the ISO standards mentioned above, this code of practice with regard to information and communications technology continuity management may be used to develop business continuity management rules by the cloud provider and by the bank, and

for the bank's evaluation of business continuity solutions developed and presented to the bank by the cloud provider.

Also, BS 25999-1:2006 Business continuity management. Part 1. Practical rules and BS 25999-2:2007: Business continuity management. Part 2. Specification.

5.3 SAS70 Standard and SSAE16 Standard

Both the SAS70 Standard and the SSAE16 Standard currently in force were created by an American organisation, American Institute of Certified Public Accountants (AICPA) to audit the operation of service companies, i.e. providers of outsourcing services.

The SAS70 Standard has been replaced by AICPA with two new standards: (i) a standard with regard to reporting SSAE16 (Statement on Standards for Attestation Engagement No. 16), (ii) a standard with regard to an audit for clients (SAS Audit Considerations Relating to Entity using a Service Organisation).

SAS70 was a standard in the field of audit, designed to enable an independent auditor to evaluate and issue an opinion about the existence, but not the contents and main elements of a service provider's control system. However, the fact that the service provider could identify itself and present an auditor report compliant with SAS70 to the client did not result in the client having greater knowledge about the current control of security applied by the service provider.

AICPA decided to divide the SAS70 standard into two standards: (i) one with regard to standards applicable to service providers (SSAE16) and (ii) another one applicable to financial statements of clients using services of external providers (Audit Consideration Relating to an Entity Using a Service Organisation). Thus, the SSAE16 standard shall be of key relevance to IT services.

The SSAE16 standard introduces two types of reports by an auditor of service provider.

- **Type 1** – concerns the provider's service with regard to an accurate description of security measures for specific data, together with the auditor's opinion as to whether the given description is presented fairly and is appropriate for the achievement of the declared objectives.
- **Type 2** – containing the same range of the report as Type 1, and additionally an opinion of the auditor as to whether the security systems of the service provider have operated at least to a minimum extent for the last six months.

It seems that the cloud user (its internal audit department or external auditors) becoming acquainted with the SSAE16 T2 report may provide it with knowledge about the scope of data security applied by the cloud provider, and their actions in practice.

5.4 ITIL 2011

ITIL is a set of good IT service management practices. ITIL standards originally constituted a British Government standard. ITIL standards have become the basis for the development of the ISO 20000 standard, and thus their application may facilitate the implementation and certification of that standard.

On 29 July 2011, a new set of ITIL standards was published, containing fragmentary references to cloud computing. ITIL 2011 provides, among other things: (i) a definition of service structure in a cloud, (ii) a description of the strategy of provision of such services, (iii) issues concerning implementation of various types of services in the cloud environment – however without the proposal of any specific or complex solutions.

Other Financial Sector Regulations

6. Other Financial Sector Regulations

6.1 Cloud Computing in regulations concerning the investment fund sector

Similar to the case of the banking sector, also in relation to the investment fund sector, statutory regulations enable an investment fund company or the fund directly to outsource certain operations related to the functioning of an investment fund to external entities.

The Act on Investment Funds of 27 May 2004 (Journal of Laws No 04.146.1546, as amended) (hereinafter the “AIF”) directly mentions specialised entities, such as a depositary (with regard to keeping a register of assets of an investment fund) or a transfer agent (with regard to keeping a register of fund participants). The Act is silent about other operations which an investment fund company or an investment fund may outsource to external entities. An analysis of provisions of the Act indicates, however, that it provides the possibility to outsource also other operations necessary for efficient and unbroken operation of the fund. Such operations include advertising, marketing, bookkeeping, or IT services.

Similar to the case of the Banking Law, in the case of the investment fund sector, there are also detailed regulations concerning the observance of secrecy. Those regulations may affect the terms of provision of IT services, including cloud computing, in the situation where under the services provided the cloud computing service provider has the possibility of accessing data covered by professional secrecy pursuant to the Act on Investment Funds.

Professional secrecy is regulated in Articles 280-284 of the AIF. In accordance with Article 280 (2), professional secrecy is a “secret including information obtained in relation to the on-duty activities undertaken under employment, contract of mandate or another legal relationship of a similar nature, concerning legally protected interests of entities performing activities related to the operations of an investment fund or a collective securities portfolio, in particular with deposits and the register of fund participants or the collective securities portfolio, or other activities under operations regulated by the Act, covered by the supervision of the Polish Financial Supervision Authority or a foreign supervisory authority, and concern activities undertaken as part of the performance of such supervision.”

Professional secrecy is, therefore, presented broadly in the AIF, encompassing all information obtained in relation to activities concerning a broadly understood operation of investment funds, and concerning “legally protected interests of entities performing activities related to the operations of an investment fund or a collective securities portfolio”. Thus, this will be both information concerning the particular investment fund, the company managing it, and other entities through which the fund conducts its operations (including information concerning the contents of legal relationships binding the parties, or information constituting company secrets), as well as information concerning clients of the fund (participants and potential participants) or of the collective securities portfolio (including both personal data and all strictly investment-related information, concerning transactions).

The catalogue of entities obliged to maintain professional secrecy is provided by Article 280 (1) of the AIF. In accordance with Article 280 (1)(1)(f) of the AIF, the following persons are, among others, required to maintain professional secrecy: persons who are members of governing bodies and employees of entities related to the investment fund company or the fund basing on a contract of mandate or remaining with the abovementioned entities with another legal relationship of similar nature. These may be, for example, entities providing IT services, also under cloud computing.

From the point of view of a cloud computing agreement, the relevant provision is Article 284 (2) of the AIF, in accordance with which persons obliged to observe professional secrecy are liable for damages resulting from the disclosure of such information and its use that is not in accordance with its purpose. This provision, therefore, introduces statutory unlimited liability of persons who are members of governing bodies and employees of the outsourcer for the disclosure of information constituting professional secrecy or its unauthorised use. It should be pointed out at the same time that the AIF does not provide a direct answer to the

question about the scope of the possible damage and the “harmed person”. It should be assumed, due to the broad statutory definition of the professional secrecy itself, that the liability mentioned in that provision will encompass all damages suffered by “entities performing activities related to the operations of the fund or the collective securities portfolio” (an example catalogue has been indicated above) to which the information covered by the disclosed professional secrecy referred.

Summary. Considering the regulations discussed above relating to the professional secrecy, it should be stated that the provision of IT services with the use of a cloud model for the benefit of entities from the investment fund sector is permitted. Due to the meaning that AIF gives to professional secrecy, regardless of the scope of outsourced activities (category of services in a cloud provided to an investment fund company or a fund), entities to which the services have been outsourced, or rather in the light of the wording of Article 280 of the AIF – employees and persons under a contract of mandate or another civil law relationship of a similar nature are obliged to maintain professional secrecy with all of its consequences (discussed above). In practice, therefore, the use of the services of “cloud computing” by investment fund companies or investment funds will involve the need to appropriately regulate the issue of confidentiality of information to which the service provider may have access under the services provided, as well as the responsibility of persons directly performing services on principles provided for in the Act.

6.2 Cloud Computing in regulations concerning the pension fund sector

Regulations of the pension fund sector are analogous with regulations concerning the investment fund sector described above. Similar to the AIF, the Act on Organisation and Functioning of Pension Funds of 28 August 1997 (hereinafter the “AOFPF”) allows the pension fund company to outsource certain operations related to the functioning of the pension fund to external entities. Also, the AOFPF indicates only specialised entities in that respect (depository bank or transfer agents or sales representatives), not mentioning other entities and operations. The analysis of provisions of the AOFPF allows, however, a justified statement that there is the possibility to outsource other operations necessary for efficient and uninterrupted operation of a pension fund, including IT services performed in the form of cloud computing.

Similarly as in the case of operations regulated by Banking Law and the AIF, the AOFPF contains detailed regulations concerning professional secrecy. In the case where, under services provided to a pension fund, the cloud computing service provider has the possibility to access data covered by professional secrecy, those regulations must be taken into account.

Pursuant to Article 49 of the AOFPF, among others, persons related to the pension fund company or fund based on a contract of mandate or remaining with the abovementioned entities with another legal relationship of similar nature and employees of entities remaining with the pension fund company or fund with such a relationship, are obliged to observe professional secrecy with regard to operations of the pension fund.

This provision, therefore, will also apply to the cloud computing service provider and all of its employees. Professional secrecy, however, is regulated in the AOFPF to a narrower extent than in the AIF. This is because professional secrecy, within the meaning of the AOFPF, covers “information connected with a fund’s deposits, the register of fund members, instructions of fund members in the case of death, and statements mentioned in Article 83 [about property relationships between the fund member and that fund member’s spouse], which if disclosed could infringe upon the interests of fund members or the interest of market participants on the regulated market within the meaning of the Act on Trading of Financial Instruments of 29 July 2005.

It should also be indicated that the AOFPF, similar to the AIF, provides liability for disclosing or using information constituting a professional secrecy. In accordance with Article 220 (1), such behaviour is subject to a fine up to PLN 1 000 000 or imprisonment for up to 3 years, and if the disclosure or use of the professional secrecy was for the purpose of achieving

financial or personal gain, a person committing such an act is subject to a fine up to PLN 5 000 000 or imprisonment for up to 5 years.

Summary. Considering the regulations discussed above, it should be stated that the provision of IT services using a cloud model for the benefit of entities from the pension fund sector is permitted, and the performance of such operations should allow AOPPF's requirements concerning the observance of a professional secrecy.

6.3 Cloud Computing in regulations concerning operations of investment firms

Outsourcing of operations of an investment firm. The issue of outsourcing in the operations of an investment firm is regulated in Article 81a-81g of the Act on Trading in Financial Instruments of 29 July 2005 (consolidated text in Journal of Laws No 10.211.1384, as amended) (hereinafter the "**Trading Act**"). These provisions were added to the Trading Act on 21 October 2009, when the amendment to the Act, implementing provisions of the following two Directives, came into effect:

- Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments amending Council Directives 85/611/EEC and 93/6/EEC and Directive 2000/12/EC of the European Parliament and of the Council repealing Council Directive 93/22/EEC, and
- Commission Directive 2006/73/EC of 10 August 2006 implementing Directive 2004/39/EC of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive (hereinafter the "**MiFID**").

The regulation of outsourcing in the Trading Act refers to the principle of freedom of use of other entrepreneurs' services by the outsourcer, with the observance of outsourcer's liability towards its clients for damage caused and the entrepreneur's liability towards the outsourcer for damage caused to it (both types of liability cannot be excluded or limited). Moreover, the Trading Act requires that the outsourcer ensures ongoing supervision over the entrepreneur and conducts current assessments of the quality of performance of outsourced operations. The Trading Act, however, excludes the admissibility of conducting brokerage operations in a manner which results in the absence of an actual performance of the given brokerage activity operation by the investment firm. Similarly, it is forbidden to outsource services in a manner leading to the handover of representation, conducting company matters, or transfer management of an investment firm within the meaning of provisions of the Code of Commercial Companies.

The terms of conclusion of an outsourcing agreement have been indicated in the provision of Article 81 b (1)(1)-(10) of the Trading Act, in particular through the determination of the requirement that an entrepreneur to whom operations have been outsourced has the qualifications to perform operations covered by the subject of the agreement (if legal regulations stipulate the obligation to have such qualifications) or performs those operations professionally and has the necessary knowledge, experience, as well as ensures technical and organisational conditions necessary for the correct performance of the agreement, including financial situation guaranteeing correct performance of that agreement.

Those requirements do not refer to the so-called **insignificant outsourcing**, i.e. in accordance with the wording of the provision of Article 81 f (1) of the Trading Act, concerning operations which are of no material importance for the correct performance of duties specified in legal regulations by an investment firm, for the financial situation of the firm, or for the continuity or stability of brokerage activity by an investment firm. The Trading Act mentions, by way of an example, that insignificant outsourcing takes place where an investment firm outsources advisory services, employee training services, bookkeeping, personal or property security, standardised services, including services consisting in the provision of market information or information about listings of financial instruments.

It should be noted that the provisions of Article 81a-81g coming into effect led to the establishment of regulatory dualism with regard to the so-called banking outsourcing, which previously was subject to uniform regulation specified by provisions of Article 6a-6d of the Banking Law. This is because the activity of a bank, fulfilling the prerequisites specified in Article 69 of the Trading Act, excluding exceptions arising from the provisions of Article 70 (2) and (3) of the Trading Act, is of a brokerage activity type. In particular, accepting and forwarding orders to buy or sell financial instruments and offering financial instruments should be deemed to be the bank's brokerage activity if the financial instruments subject to those operations have been admitted for organised trading (e.g. shares or investment certificates issued by closed-end investment funds in organised trading). In such case, the bank is obliged to directly apply provisions of the Trading Act with regard to outsourcing. It should be noted, however, that in accordance with the provision of Article 70 (4) of the Trading Act, also with regard to exceptions indicated in provisions of Article 70 (2) and (3) of the Trading Act (i.e. with regard to the performance of operations mentioned in Article 69 (2) (1)-(7) of the Trading Act) provisions of the Trading Act concerning outsourcing apply to banks – in this case “accordingly”.

To sum up, a bank, when performing operations indicated in Article 69 of the Trading Act, is subject to provisions of the Trading Act regulating outsourcing, and not to provisions of Article 6a-6d of the Banking Law. It is accepted in the doctrine that provisions of the Trading Act have precedence in the situation described before the regulation of the Banking Law due to the application of generally accepted rules: priority of later regulations over earlier ones (provisions of Article 81a-81g of the Trading Act constitute “lex posterior” in relation to provisions of Article 6a-6d of the Banking Law), priority of regulations of specific nature in relation to general regulations (provisions of Article 81a-81g of the Trading Act constitute “lex specialis” in relation to provisions of Article 6a-6d of the Banking Law because they regulate only a fragment of the bank's activity), full and effective implementation of the MiFID directives.

The legal dualism described above leads to many problems with the application of regulations, in particular in the case where the service which is outsourced concerns both the bank's activity in the nature described in Article 69 of the Trading Act, as well as other activity, e.g. in the situation where IT system maintenance services are outsourced and such IT system is used by bank clients' both to perform operations on financial instruments, and to open deposits. In such a case, in the absence of an explicit position of the regulator in that respect, through caution banks may lean towards the application of a more restrictive outsourcing regime, regulated in the Banking Law.

Summary. Considering the above, it should be stated that provision of IT services with the use of a cloud model for investment firms is permissible. However, the classification of the given scope of services as related or unrelated directly to brokerage activity may prove to be problematic. The outsourcing of the latter activities, regardless of the model of service provision for the investment firm (i.e. also under cloud computing), will be covered by the outsourcing regime arising from the Trading Act. This will also refer to banks – to the extent in which operations that are to be subject of outsourcing are covered by provisions of the Trading Act.

6.4 Cloud Computing in insurance activity

As in the case of banking operations, investment firm and investment fund operations, the scope of insurance secrecy and legal discipline of outsourcing in the activity of insurance companies need to be discussed (for the purpose of clarity of our disquisition, we are omitting the specificity of operations of reinsurance companies).

a) Insurance secrecy

In accordance with Article 19 (1) of the Act on Insurance Activity of 22 May 2003 (Journal of Laws No 10.11.66) (hereinafter the “AIA”), *an insurance company and persons employed*

there or persons and entities through which the insurance company performs its insurance operations are obliged to observe secrecy concerning individual insurance agreements.

The AIA does not use a generally adopted term “insurance secrecy”, and the obligation to maintain secrecy is not referred to insurance operations (as is the case in Article 104 (1) of the Banking Law, which refers the obligation to maintain secrecy called “banking secrecy” to “all information concerning banking operations, obtained in the course of negotiations, during conclusion and performance of an agreement on the basis of which the bank executes the operation”). It is assumed, as a result of a teleological interpretation, that despite the fact that Article 19 (1) of the AIA talks about “observing secrecy concerning individual insurance agreements”, insurance secrecy has a wider scope and also covers:

- information concerning the conclusion of an insurance agreement with the given policy holder,
- all information constituting contents of the insurance agreement concluded,
- information obtained by the insurance company independently or from the policy holder in relation to the insurance agreement concluded (also in the course of its performance),
- information obtained by the insurance company from potential business partners in relation to the conclusion of insurance agreements by the insurance company, even where an insurance agreement is not concluded in the particular case (according to some, however, this case does not have *de lege lata* legal basis but should be postulated *de lege ferenda*).

The Act on Insurance Activity does not contain a provision, analogous to that contained in the Banking Law, permitting the disclosure of information covered by the insurance secrecy on the basis of consent granted to the insurance company by the entity to which the information refers. Although it may be argued this is permissible. This is indicated among other things by the position of the Constitutional Tribunal expressed in the judgment of 20 November 2002 (K 41/02), according to which the essence of the “information autonomy rule” comes down to giving each person freedom to determine the extent to which knowledge about them will be available to others. The source of authorisation to express the consent to the disclosure of information covered by the insurance secrecy may be also sought in the construction of personal rights, in particular the right to privacy, as it is assumed that the eligible person’s consent waives the unlawfulness of infringement of personal rights. Such arguments, however, do not remove all of the doubt as to the meaning of the consent of an insurance secrecy beneficiary to the disclosure of information covered by the secrecy to third parties as a prerequisite legalising such act of an insurance company.

When the statutory group of entities obliged to observe insurance secrecy is interpreted, particularly as regards persons employed in the insurance company, the comments presented previously with regard to the statutory determination in the banking law of entities obliged to observe banking secrecy remain valid.

Article 19 (2) determines a group of entities to whom, at their request, an insurance company may (and in some cases, as it should be understood, is obliged to) provide information covered by insurance secrecy. Apart from state bodies, authorised to demand such information from the insurance company to a statutorily defined extent, “sectoral entities” indicated by name – to the extent of competences allocated to them in the Act, and other insurance companies and reinsurance companies for purposes specified in the Act, as well as persons participating in the particular insurance relationship (i.e. policy holder, insured, beneficiary and eligible person), among entities which may be provided by an insurance company with information covered by insurance secrecy, the provision indicates:

- entities processing data concerning policy holders, the insured, beneficiaries and persons eligible under insurance agreements, as well as administrators of individual

accounts of share units in a unit-linked insurance fund, at the request of the insurance company (Article 19 (2)(23)). It should be assumed that a cloud provider is within that very category.

In accordance with Article 19 (3), “data processing and performing of operations by entities mentioned in paragraph (2) subparagraphs (23) and (24) does not limit the liability arising from the prohibition mentioned in paragraph (1)”. This is an imprecise statement – there is no indication of what type of legal liability and whose liability is meant. It is probably supposed to mean that despite the legally permitted disclosure of information protected by insurance secrecy to indicated entities, the insurance company will be liable for any possible damage arising from the data about whom the information refers. This is because as regards penal liability, the provision of Article 19(3) cannot be applied. Article 232 of IBA does not leave any doubts that the offence consisting in disclosing or using information constituting an insurance secret may be committed by anyone obliged to observe insurance secrecy (subject to a fine or imprisonment for up to 3 years, and if the aim of the act was to achieve a financial or personal gain – up to 5 years). Those obliged to observe insurance secrecy include also “persons and entities through which an insurance company performs its insurance operations” (Article 19 (1)).

The statutory identification of entities mentioned in Article 19 (2)(23) and (24) as entitled to obtain information covered by the insurance secrecy from the insurance company is strictly related to the issue of outsourcing in the operations of an insurance company.

b) Outsourcing in the operations of an insurance company

The regulation of outsourcing in the AIA is insufficiently clear with regard to the determination of operations which may be outsourced to external service providers. It is, at the same time, a much more general and much more liberal regulation than that contained in the Banking Law for outsourcing in the banking activity.

The AIA indicates that outsourcing of operations of an insurance company, if one omits activity conducted via authorised insurance intermediaries in accordance with the Act on Insurance Intermediation of 22 May 2003, may consist in the insurance company contracting out:

- 1) pursuant to Article 19 (2)(23) – data processing operations with regard to data concerning policy holders, the insured, beneficiaries and persons eligible under insurance agreements, and administration of individual share unit accounts in a unit-linked insurance fund;
- 2) pursuant to Article 26 (1) second sentence – services related to safekeeping of documents concerning the conclusion and performance of insurance agreements, drawn up on digital data media;

and moreover (which does not seem relevant for cloud computing):

- 3) pursuant to Article 3 (6) – insurance operations mentioned in Article 3 (4)(1)-(6) and Article 5, i.e.:
 - risk assessment in personal insurance and property insurance, and in insurance guarantee agreements,
 - payment of compensation and other benefits due under insurance agreements and insurance guarantee agreements,
 - takeover and disposal of items or rights acquired by the insurance company in relation to the performance of an insurance agreement or an insurance guarantee agreement,

- conducting control of observance by policy holders or insured of obligations and security rules with regard to items covered by the insurance cover stipulated in an agreement or general terms and conditions of insurance,
 - conducting recourse proceedings and recovery proceedings related to the performance of insurance agreements and insurance guarantee agreements,
 - investing insurance company's funds,
 - determining reasons and circumstances of contingent events,
 - determining the extent of losses and amount of compensation and other benefits due to persons eligible under insurance agreements or insurance guarantee agreements,
 - determination of the value of the object of insurance,
 - preventing the occurrence or mitigating effects of insurance incidents, or financing those activities from the prevention fund;
- 4) pursuant to Article 3 (9) – operations mentioned in Article 3 (3)(2), i.e. submission of declarations of intent in matters concerning claims for compensation or other benefits due under insurance agreements and insurance guarantee agreements;

The AIA says nothing about other operations which an insurance company may outsource to external entities. This should be understood in such a way that, as the insurance company may conduct only insurance activity understood as the “performance of insurance operations related to the offering and providing cover in the case of risk of occurrence of consequences of contingent events” (Article 3 (1)), and activity “directly” related to insurance activity (Article 3 (2)), the AIA does not contain a clear limitation of admissibility of outsourcing with regard to activity directly related to insurance activity, then such activity may be outsourced by the insurance company to external service providers. Such activity encompasses, among other things, advertising, marketing, and IT for insurance business.

In accordance with Article 30 (1) of the AIA, the management board of an insurance company “is responsible for the development, introduction and functioning of internal regulations determining the method of performance of insurance business, in particular with regard to operations outsourced to other entities /.../”.

A supervisory authority may order an insurance company to terminate an agreement on the basis of which insurance operations have been outsourced to another entity within the specified deadline if it finds that the operations are performed in violation of law, have unfavourable impact on the conducting of insurance business by the insurance company in accordance with legal regulations, on the prudent and stable management of the insurance company, or on interests of policyholders, the insured, beneficiaries and persons eligible under insurance agreements (Article 210 (1)). In such a case, limitations concerning the possibility and deadlines for dissolution or termination of the outsourcing agreement, provided for in that agreement, shall not apply (Article 210 (2)). In the case where the agreement has not been terminated within the specified deadline, the supervisory authority, pursuant to Article 210 (3), may impose fines mentioned in Article 212 (1)(1) and (2), i.e.:

- on members of the management board or proxies of the insurance company – fines up to the amount corresponding to three average monthly salaries from the last 12 months;
- on the insurance company – fines up to 0.5% of the gross written premium obtained by the insurance company in the previous year, and in the case where the company insurance did not conduct activity or the gross written premium was below PLN 20 million – up to PLN 100,000.

c) Anticipated changes in the Act on Insurance Activity

To the extent that is interesting for us, changes will be forced by the need to implement the provisions of the Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance – Solvency II (OJ EU L 335/1 of 17.12.2009), into Polish legal system. In accordance with Article 309 (1) of the Directive, Member States shall transpose its provisions indicated in that article (including those concerning outsourcing) by 31 October 2012.

Significant changes in the Act on Insurance Activity may be expected with regard to outsourcing, currently regulated randomly and inconsistently in the AIA.

First and foremost, the Directive introduces a definition according to which “outsourcing means an arrangement of any form between an insurance or reinsurance undertaking and a service provider, whether a supervised entity or not, by which that service provider performs a process, a service or an activity, whether directly or by sub-outsourcing, which would otherwise be performed by the insurance or reinsurance undertaking itself” (Article 13 (28)). The transposition of that definition to the AIA may be expected.

In accordance with recital 37 of the Directive, supervisory authorities should be informed prior to the outsourcing of critical or important functions or activities, and it is necessary that supervisory authorities have the right to inspect the contractor fully with regard to the performance of activities which have been outsourced to it. The requirements for insurance outsourcing, in turn, should be consistent with the “current rules and practices in the banking sector”.

In accordance with Article 38 of the Directive, Member States shall ensure that insurance undertakings include the necessary steps to ensure that the following conditions are satisfied:

- the service provider must cooperate with the supervisory authorities of the insurance undertaking in connection with the outsourced function or activity;
- the insurance undertakings, their auditors and the supervisory authorities must have effective access to data related to the outsourced functions or activities;
- the supervisory authorities must have effective access to the business premises of the service provider and must be able to exercise those rights of access.

In the case of outsourcing provided by a service provider from a Member State other than the one in which the insurance undertaking is located, the Member State where the service provider is located shall permit the supervisory authorities of the insurance undertaking to carry out themselves or through the intermediary of persons they appoint for that purpose, on-site inspections at the premises of the service provider. The supervisory authority of the insurance undertaking may delegate such on-site inspections to the supervisory authorities of the Member State where the service provider is located.

In accordance with Article 49 of the Directive, the outsourcing of critical or important operational functions or activities shall not be undertaken in such a way as to lead to any of the following:

- materially impairing the quality of the system of governance of the undertaking concerned;
- unduly increasing operational risk;
- impairing the ability of the supervisory authorities to monitor the compliance of the undertaking with its obligations;
- undermining continuous and satisfactory service to policy holders,

and insurance undertakings shall notify supervisory authorities prior to the outsourcing of critical or important functions or activities, as well as of any subsequent material developments with respect to those functions or activities.

Considering the above provisions of the Directive, including the clear demand contained in recital 37, to subject insurance outsourcing to the discipline of banking outsourcing, one may be certain that outsourcing will soon be regulated in more detail in the Act on Insurance Activity in the direction adopted in the banking law.

Cloud Computing in Regulations Concerning Classified Information (State Secrets)

7. Cloud Computing in Regulations Concerning Classified Information (State Secrets)

The Act on Protection of Secret Information of 5 August 2010 (Journal of Laws No 10.182.1228) (hereinafter the “APSI”) specifies the basic rules of protection of classified information.

The Act in Article 1 defines classified information as any information the unauthorised disclosure of which would or could result in damage for the Republic of Poland or would be detrimental from the point of view of its interests, also in the course of development of the information and regardless of the method and form of its expression.

From the point of view of cloud computing, it is relevant that the provisions of the Act apply to undertakings intending to pursue or pursuing the conclusion of agreements related to access to classified information, or performing such agreements, or carrying out tasks related to access to classified information pursuant to legal regulations (Article 1 (2)(6) of the APSI). In that respect, the following principles are of relevance: (i) processing of classified information (Article 1 (1)(3) of the APSI); (ii) proceedings conducted in order to determine whether an undertaking covered by the proceedings provides conditions for protecting classified information (Article 1 (1)(5) of the APSI); (iii) organisation of inspections of the status of security with regard to classified information (Article 1 (1)(6) of the APSI); (iv) protection of classified information in ICT systems (Article 1 (1)(7) of APSI); (v) application of physical security measures with regard to classified information (Article 1 (1)(7) of the APSI).

The term ‘processing of classified information’ is understood by the legislation to include all operations performed in relation to classified information and on such information, in particular the production, modification, copying, classification, collecting, storing, forwarding or making available (Article 2 (5) of the APSI). At the same time, the APSI, with regard to the ICT system, refers to the APSEM, states that an ICT system is a set of cooperating IT hardware and software, ensuring the processing and storage, as well as sending and receiving data through telecommunication networks using a data terminal equipment appropriate for the given type of network. Data to which a specific secrecy clause has been appended (“top secret”, “secret”, “confidential”, “proprietary”) must be processed in conditions that make their unauthorised disclosure impossible in accordance with regulations determining requirements concerning security of ICT systems.

ICT systems in which classified information is to be processed are subject to ICT information security accreditation. Such accreditation is granted by the Internal Security Agency or the Military Counterintelligence Services for a period no longer than 5 years for an ICT system, the purpose of which is to process classified information with the “confidential”, “secret” or “top secret” clause. The confirmation of such accreditation is the obtaining of an ICT system accreditation certificate (issued i.e. on the basis of a system audit).

The condition for providing an undertaking with access to classified information in relation to the performance of services is the ability to protect classified information confirmed with an industrial security certificate.

Cloud Computing in Accounting

8. Cloud Computing in Accounting

The Accounting Act of 29 September 1994 (Journal of Laws No 09.152.1223) specifies basic accounting principles, procedures for the audit of financial statements by statutory auditors and principles of conducting activity with regard to bookkeeping services, which from the point of view of providers in a cloud seems to be the most important.

The Act does not provide directly for any regulations which could apply to cloud computing. However, based on certain norms contained therein, the direction which should be followed by a provider of services in a cloud may be identified. This Act accentuates first and foremost business continuity and ensuring information security.

Business continuity

In accordance with the Act, accounting information resources are deemed to be tantamount to books of accounts in the case of electronic bookkeeping. These must be organised in the form of (i) separate computer data sets, (ii) databases or their separate parts – regardless of the place of their creation and storage.

The condition for conducting this type of accounting is for the given entity to have software enabling it to acquire readable information in relation to entries made in such books. The legislator also requires for this type of bookkeeping to apply appropriate procedures and measures protecting against the destruction, modification or concealment of an entry.

Information security

The Act describes the principles concerning data protection very broadly, describing all books of accounts, bookkeeping vouchers, inventory documents and financial statements as “data sets”.

Books of accounts may be in the form of data sets recorded on digital data media, on condition that a provider of services in a cloud will use in this respect (i) data media resistant to threats, (ii) appropriate external protection measures, (iii) systematic creation of backup copies of data sets recorded on digital data media. Moreover, the provider has to ensure (i) durability of the accounting system information recorded, and (ii) ensure protection of computer programs and accounting IT system data through the application of appropriate programs and organisational solutions protecting against unauthorised access or destruction.

Additionally, in accordance with the Act, the contents of bookkeeping vouchers may be transferred to digital data media, enabling their keeping in a durable form. Documents concerning transfer of property rights to real estate, entrusting responsibility for components of assets, relevant contracts and other important documents are excluded from this possibility. The condition for the possibility of applying this method, however, is having hardware allowing the reconstruction of documents in the form of a printout.

Regardless of statutory requirements indicated above – the cloud service provider must also meet criteria indicated for entities providing bookkeeping service, e.g. accounting certificate.

Regulations with Regard to Cloud Computing in Individual European Union Member States

9. Regulations with Regard to Cloud Computing in Individual European Union Member States

Below, we present a brief discussion of cloud computing regulations with regard to personal data protection and in the financial sector in individual European Union Member States.

9.1 Personal data protection

Country	Regulations relevant to cloud computing
Belgium	Not aware of any legislation that could prevent the development of cloud computing services.
Czech Republic	Not aware of any legislation that could prevent the development of cloud computing services. Under Czech law, the service provider would most likely be considered a data processor but that would depend largely on the nature of services.
Finland	No specific rules prevent the provision/use of cloud services in Finland. However, especially concerning public entities, there may be provisions regarding security restrictions which could have that effect.
France	Under the French Data Protection Act, controllers need to specify the exact third countries to which data are to be transferred in order to obtain an authorisation from the French Data Protection Authority. Note that a report from the French National Assembly dated 22 June 2011 (" <i>Rapport d'information sur les droits de l'individu dans la révolution numérique</i> ") suggests drafting a new legislation, where cloud computing solutions located outside the EU would be barred from processing sensitive data. Presently, there is no indication that this proposal will be turned into law.
Germany	Under German law, cloud providers are seen as data processors. Both the strict, impracticable German requirements for data processing agreements and the particular view of German data protection authorities on Safe Harbor are major issues for cloud computing. There are even opinions of German data protection authorities that cloud computing, in particular in non-EU/EEA-clouds are not legally possible at all
Hungary	Not aware of any specific legislation in Hungary preventing the use/provision of cloud computing services. The Hungarian Parliament passed a new Data Protection Act in July (effective 1 January 2012), but this does not contain any specific legislation on cloud computing either.
Italy	The Italian Data Protection Authority issued a general Resolution - published in the Official Gazette No. 153 of 4 July 2011 - outlining a new principle for the appointment of data processors by companies which outsource personal data to external agencies. Under the Resolution, companies which outsource work but 'maintain operational control' must formally nominate the agencies as 'data processors'.
Netherlands	Under the Dutch Data Protection Act, controllers need to specify the exact third countries to which data are to be transferred in order to obtain a permit.
Slovakia	In Slovakia there are no restrictions for the private sector in Slovak law in relation to providing/using cloud computing within the EU. However, state authorities may have issues with using cloud computing services located in other countries with regards to classified information.
Spain	Not aware of any specific restrictions preventing the use or provision of cloud services. In most cases, Spanish providers of cloud computing solutions will be defined as 'data processors'.

Country	Regulations relevant to cloud computing
Sweden	No specific rules prevent the provision/use of cloud services in Sweden. However, especially concerning public entities, there may be provisions regarding security restrictions which could have that effect.
UK	No specific rules prevent the provision/use of cloud services in the U. All the usual rules (need to assess and enforce security, data transfers, etc) apply.

9.2 Financial sector

United Kingdom

In the United Kingdom, the regulator of the financial service market is the Financial Services Authority (FSA). The FSA Handbook (auxiliary material published by FSA), which determines basic regulations and guidelines binding for financial institutions operating within the United Kingdom, is particularly relevant with regard to cloud computing.

Besides the FSA Handbook, there is also MiFID Connect – a joint project of various commercial organisations aimed at supporting the United Kingdom in the implementation of the Market in Financial Instruments Directive. Many guidelines found in this document, despite the fact it is not generally binding, are applied by companies from the sector and are taken into consideration by the FSA in the context of its supervision over entities.

The payment sector is also globally introducing standards developed by the PCI Security Standards Council. The PCI Security Standards Council is an entity managed by the 5 largest payment sector companies (American Express, Discover Financial Services, JCB International, MasterCard Worldwide, Visa Inc.) that defines security standards for banks and commercial entities using card payments.

Requirements from the above documents applicable to regulations concerning cloud computing in the United Kingdom are presented below.

Regulation/Standard	Requirements	Cloud computing
FSA Handbook	<p>The FSA Handbook sets out 11 principles with which regulated firms must comply.</p> <p>The 2nd principle states that “a firm must conduct its affairs with due skill, care and diligence”.</p> <p>The 3rd principle states that “a firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems”.</p> <p>The 5th principle states that “a firm must observe proper standards of market conduct”.</p> <p>The 6th principle states that “a firm must pay due regard to the interests of its customers and treat them fairly”.</p>	<p>Financial services firms must take account of these principles when determining whether a move to cloud computing is appropriate and which services or suppliers would be appropriate.</p> <p>Any move to cloud must not constitute an abdication of control contrary to the 3rd principle.</p> <p>Any financial benefits from moving to cloud computing will need to be weighed against any increased risk to customer data.</p>
	<p>The FSA Handbook also sets out a series of Senior Management Arrangements, Systems and Controls (SYSCs). A number of these have an impact on a firm’s IT provisioning but examples</p>	<p>Cloud services often involve a transfer of control over data to the service provider. This may be contrary to SYSC 4.1.1R.</p> <p>Many cloud providers do not allow</p>

	<p>include:</p> <p>SYSC 4.1.1R states that “a firm must have robust governance arrangements, which include a clear organisational structure with well defined, transparent and consistent lines of responsibility, effective processes to identify, manage, monitor and report the risks it is or might be exposed to, and internal control mechanisms, including sound administrative and accounting procedures and effective control and safeguard arrangements for information processing systems”.</p> <p>SYSC 6.2.1 requires a regulated firm, where appropriate and proportionate, to establish an independent internal audit function that can examine and evaluate the adequacy and effectiveness of the firm’s systems, internal control mechanisms and arrangements.</p> <p>SYSC 8.1.8R requires a firm outsourcing an important or critical function to ensure that:</p> <ol style="list-style-type: none"> 1) the service provider must have the ability, capacity, and any authorisation required by law to perform the outsourced functions, services or activities reliably and professionally; 2) the service provider must carry out the outsourced services effectively, and to this end the firm must establish methods for assessing the standard of performance of the service provider; 3) the service provider must properly supervise the carrying out of the outsourced functions, and adequately manage the risks associated with the outsourcing; 4) appropriate action must be taken if it appears that the service provider may not be carrying out the functions effectively and in compliance with applicable laws and regulatory requirements; 5) the firm must retain the necessary expertise to supervise the outsourced functions effectively and to manage the risks associated with the outsourcing, and must supervise those functions and manage those risks; 6) the service provider must disclose to the firm any development that may have a 	<p>customer audits. This will make it difficult to comply with SYSC 6.2.1 or point 9 of SYSC 8.1.8R.</p> <p>The use of a third party cloud service will in most circumstances constitute an outsourcing subject to SYSC 8.1. If it is a “material” outsourcing, financial services firms will need their service provider to comply with all of the requirements of SYSC 8.1.8R. Points 2, 3, 8, 9 and 11 are likely to be most challenging in the context of cloud computing.</p>
--	--	--

	<p>material impact on its ability to carry out the outsourced functions effectively and in compliance with applicable laws and regulatory requirements;</p> <ol style="list-style-type: none"> 7) the firm must be able to terminate the arrangement for the outsourcing where necessary without detriment to the continuity and quality of its provision of services to clients; 8) the service provider must cooperate with the FSA and any other relevant competent authority in connection with the outsourced activities; 9) the firm, its auditors, the FSA and any other relevant competent authority must have effective access to data related to the outsourced activities, as well as to the business premises of the service provider; and the FSA and any other relevant competent authority must be able to exercise those rights of access; 10) the service provider must protect any confidential information relating to the firm and its clients; 11) the firm and the service provider must establish, implement and maintain a contingency plan for disaster recovery and periodic testing of backup facilities where that is necessary having regard to the function, service or activity that has been outsourced. <p>SYSC 13.7 provides similar rules on outsourcing for insurers.</p> <p>[Note: The FSA Handbook defines an “Outsourcing” for the purposes of SYSC 8 as “an arrangement of any form between a firm and a service provider by which that service provider performs a process, a service or an activity which would otherwise be undertaken by the firm itself”.]</p>	
MiFID Connect Guidelines	The MiFID Connect Guidelines on Outsourcing specifically refers to SYSC 8 and offers examples of what compliance might involve.	<p>These guidelines should be reviewed and applied where appropriate by any financial services firm implementing cloud computing.</p> <p>Some of the guidance is difficult to apply in the context of cloud computing as opposed to more traditional outsourcing. For example,</p>

		agreeing quantitative and qualitative service levels, scheduling regular meetings with the service provider, imposing service credits or step-in in the event of problems.
United Kingdom Data Protection Act of 1998 (DPA)	<p>The DPA implements the Data Protection Directive (95/46/EC) in the UK.</p> <p>The 2nd principle requires that “personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.</p> <p>The 7th principle requires that “appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data”.</p> <p>The 8th principle requires that “personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data”.</p>	<p>Any transfer of data to a third party would need customer consent, particularly if the data was to be hosted outside of the EEA.</p> <p>For most cloud services, customers are not given sufficient access and information to determine whether a cloud service provider has put in place appropriate technical and organisational protections.</p>
PCI Data Security Standard (DSS)	The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This standard is intended to help organisations proactively protect customer account data.	Financial services firms will need to ensure any relevant applications or services in the cloud meet the PCI DSS in order to ensure they can continue to handle card payments.
BS 7858:2006	This British Standard gives recommendations for the security screening of individuals to be employed in an environment where the security and safety of people, goods or property is a requirement of the employing organisation's operation and/or where such security screening is in the public interest.	It is often unclear the extent to which cloud service providers undertake vetting of their staff.
ISO27001/ ISO27002	Standards concerning information security have been described in the earlier part of this document.	In the case of a lack of authorisation to conduct a direct audit of a cloud provider, cloud users often rely on the provider obtaining certification for independent standards, such as ISO 27001/27002
FSA Data Security in Financial Services Good	This report was published following a review by the FSA into how financial services firms in the UK are addressing the risk that their customer data may be	It is unclear how well-versed cloud providers are in the more detailed guidance familiar to financial services firms and therefore the extent to

<p>Practice (April 2008)</p>	<p>lost or stolen and then used to commit fraud or other financial crime. It is not formal guidance from the FSA but the FSA expects firms to use it to create a more effective assessment of the risk and put in place more effective controls as part of their obligation to meet principles 2 and 3 in the FSA Handbook (see above).</p>	<p>which they are compliant.</p>
<p>Regulation of Investigatory Powers Act (RIPA)</p>	<p>RIPA regulates the powers of public bodies to carry out surveillance and investigation, and covers the interception of communications. It was introduced to take account of technological change such as the growth of the Internet and strong encryption.</p> <p>RIPA can be invoked by government officials Act on the grounds of national security, and for the purposes of detecting crime, preventing disorder, public safety, protecting public health, or in the interests of the economic well-being of the UK.</p>	<p>Financial services firms need to ensure that any cloud deployment does not impact their ability to comply with RIPA.</p> <p>They should also ensure they are notified of any disclosure by a cloud provider or ISP under RIPA of data relating to them or their customers.</p>

France

Under French law, there is no specific rule regarding the adoption of Cloud Computing in the Financial Services Sector and neither regulators nor professional organisations or financial institutions have taken official position on the subject.

The French Data Protection Act of January 6, 1978 and the Regulation 97-02 of February 21, 1997 relating to internal control of credit institutions and investment firms as well as professional secrecy rules apply to the cloud.

Regulation/ Standard	Requirements	Cloud computing
<p>French Data Protection Act of 6 January 1978</p>	<p>Under French law, a data controller is subject to an obligation of security. Indeed, according to article 34 of the Data Protection Act, the data controller shall take all useful precautions, with regard to the nature of the data and the risks of the processing, to preserve the security of the data and, in particular, prevent their alteration and damage, or access by non-authorized third parties. Furthermore in case of outsourcing, the processor shall offer adequate guarantees to ensure the implementation of the security and confidentiality measures. However, this requirement does not exempt the data controller from his obligation to supervise the observance of such measures.</p> <p>The contract between the processor and the data controller shall specify the obligations incumbent upon the processor as regards the protection of the security and confidentiality of the data and provide that the processor may act only upon the instruction of the data controller. This implies notably that contract shall provide processor shall not sub-contract any part of the processing without prior approval from controller.</p> <p>Furthermore, personal data transfer outside the EU or to a third country that does not ensure an adequate level of protection, is subject to a prior authorization of the French data protection authority (CNIL). In order to file the request for authorization, data controller must name all countries concerned, list all processors and data centres.</p>	<p>Financial services firms should take into account the obligation of security in the contract signed with the cloud computing provider. However, they will remain responsible for any loss, damage or disclosure of data in case of any breach of contract by the cloud computing provider. Also they should ask to the service provider to comply with high technical standards (such as ISO/CEI 27001 and ISO 27005 or PCI DSS).</p> <p>Service provider should provide a list of all data centres and contractors that will be used for the processing. If data centres/contractors having access to personal data are located outside the EEA this will imply conclusion of a data transfer agreement based on the SCC of the EC with each processor (including the processor's own contractors) and obtaining prior authorisation from the CNIL.</p> <p>Hence they should prefer a provider installed in a country that ensures an adequate level of protection.</p>
<p>Regulation 97-02 of February 21, 1997 relating to internal control of credit institutions and</p>	<p>Under the regulation 97-02, article 37-2, Banks and financial institutions must in case of outsourcing of essential services keep relevant expertise in order to ensure effective control of outsourced tasks or services and deal with</p>	<p>Audit and access requirements are often not compatible with cloud solutions based on the random dissemination of data on several servers.</p> <p>Financial service firms should ensure</p>

investment firms	<p>associated risks.</p> <p>In particular they must conclude a written contract with service provider that shall provide that service provider :</p> <p>enables them and competent authorities, whenever necessary, to access, if necessary onsite, to any information or service made available to them, in accordance with regulations on the disclosure of information,</p> <ul style="list-style-type: none"> • ensure a quality level ensuring usual functioning of the service and in case of incident • ensure protection of confidential information • put in place adequate continuity plans • cannot modify unilaterally and substantially the service unless duly authorised • comply with the financial institution's internal controls • enable when necessary access, including onsite, to any information on services • inform of any event that may seriously impact its capacity to perform service • accept that French financial regulator and any other equivalent foreign regulator access information including on site. 	<p>(by technical, organisational and contractual means) that the implementation of cloud computing respects regulation 97-02.</p> <p>In practice, this shall limit the number and location of data centres.</p>
Article 511-33 of the Monetary and Financial Code relating to banking secrecy	<p>Under article 511-33 of the Monetary and Financial Code, employee, Banks and financial service organizations are bound by professional secrecy. Accordingly, all measures (technical and contractual) must be taken in order to ensure the respect of professional secrecy.</p> <p>The sharing or transfer of data is strictly limited subject to a necessity test to cases listed by article 511-33 or by authorizations obtained from clients under express and informed consent.</p> <p>Under certain circumstances (private banking, specific reinforced confidentiality agreements), client authorization may be considered valid only if, at the time of consent, information has been provided to client relating to countries where data is processed.</p>	<p>Financial institutions shall ensure (by technical and contractual means) that the implementation of cloud computing respects banking secrecy in accordance with French law.</p> <p>Financial institutions shall ensure that they have obtained from clients all authorizations required.</p>

Authors



Maciej Gawroński
Partner
Head of Bird & Bird Poland
Head of IT practice
Attorney-at-Law
maciej.gawronski@twobirds.com

Report editor
and author of the following sections:
Outsourcing in Financial Sector (2)
Industry Standards (5)

He has been advising entrepreneurs since 1994. Maciej specialises in IT. Before becoming a head of Bird & Bird Poland, Maciej was a partner responsible for IT practice in an independent Polish lawyer office. Maciej also specialises in privacy and personal data protection, intellectual property, commercial negotiations, dispute resolution (litigation and arbitration), and banking & finance. He advises purchasers of technology in their back-office projects (such as IT implementations, outsourcing, data flows, or risk management procedures), regulatory matters and disputes, as well as designs, leads and manages negotiations and other communication processes. He is thought to be one of the top IT lawyers in Poland, not only by Bird & Bird's clients, but by our competitors as well. Due to his business experience, analytical approach, and focus on solutions, Maciej provides high value consultancy and fulfils the role of a trusted counsel.

Maciej studied law at the Jagiellonian University in Poland and at the Université de Tours in France.



Emilia Stępień
Head of data protection practice
Attorney-at-Law

Co-author of the following section:
Cloud Computing and Regulations
Concerning Personal Data
Protection (1)

Emilia joined Bird & Bird from the European Commission, DG Internal Market and Services, Industrial Property Unit.

Emilia specialises in privacy & data protection, intellectual property, e-commerce and new technologies, competition law, consumer law and corporate law.

Emilia studied law at the Warsaw University in Poland. In 2005, she completed a course of English and EU law organised by the University of Cambridge (2003-2005). In 2007, she completed training on Competition Law in the European Union - new entitlements of national courts conducted by the School of European Law in Warsaw. In 2009, Emilia completed the 7th Community Trade Mark Special Module at the University of Alicante, Spain within The Magister Lvcentinvs framework.

Emilia is lecturer on SAR University. She is the author of publications on intellectual property law and data protection, and a speaker at national and international conferences and seminars.



Izabela Kowalczyk
Associate

Co-author of the following section:

*Cloud Computing and Regulations
Concerning Personal Data
Protection (1)*

Izabela Kowalczyk has gained her professional experience in Polish law offices and in the Association for Competitive Technology in the US. Her main areas of legal practice cover intellectual property law, IT law, and personal data protection law and litigation, including arbitration.

Izabela is a graduate of the Faculty of Law and Administration at the University of Warsaw and a second year trainee at the District Chamber of Legal Advisers in Warsaw. She completed a course of American Law at the University of Warsaw. She also studied at the Katholieke Universiteit Leuven (Belgium).



Michał Balicki
Associate
**Head of debts and receivables
collection**

Author of the following sections:

*Bank Outsourcing (3)
Recommendations of the
Polish Financial Supervision
Authority (4)*

Michał studied law at the Adam Mickiewicz University in Poznań and he completed a course of Comparative Company Law with Law and Economics at the University of Bergen, Norway. Michał also completed postgraduate studies at the Warsaw School of Economics in Risk Management in Financial Institutions.

He has over three years of experience, and his main areas of legal practice include banking & finance, new technologies law, data protection and employment.



Katarzyna Otwinowska
Associate

Author of the following sections:

Cloud Computing in regulations concerning the investment fund sector (6.1)

Cloud Computing in regulations concerning the pension fund sector (6.2)

Cloud Computing in regulations concerning operations of investment firms (6.3)

Katarzyna specialises in company law, asset management and investment funds, banking and finance and contract law. She also provided ongoing assistance to several companies and acted as an independent project coordinator. She has also provided ongoing legal advice to a fund management company and its investment funds.

She is a graduate of the Faculty of Law and Administration of the University of Nicolas Copernicus in Toruń. In 2005, she completed a *Diploma in an introduction to English law and the law of the European Union* organised by the Institute of Continuing Education at the University of Cambridge.



Wojciech Marek
Attorney-at-Law

Author of the following section:

Cloud Computing in insurance activity (6.4)

Wojciech Marek has over 25 years of legal experience. Between 1990 and 2007 he was a member of the management board and the head of the legal department of BISE Bank, as well as a member of the Advisory Committee for Supervisory Regulations and the Banking Law Council at the Polish Banking Association. He also participated in proceedings as an ad hoc arbitrator and attorney at the Court of Arbitration of the Polish Banking Association. He has been an arbitrator of the Court of Arbitration at the Polish Chamber of Commerce in Warsaw since 2009.

Wojciech specialises in civil law, banking law, company law and insurance law.

Wojciech graduated from the University of Warsaw, Faculty of Law and Administration. He is also a Doctor of Law. Between 1971 and 1990 he was a lecturer of civil and insurance law at the Faculty of Law and Administration of the Warsaw University. Wojciech is a member of the Warsaw District Chamber of Legal Advisers and the co-author of Insurance Law (1983), as well as the author of over 40 articles and glosses on civil law, insurance law and banking law.

**Filip Łukaszewicz****Document operator****Author of the following sections:**

*Cloud Computing in Regulations
Concerning Classified Information
(State Secrets) (7)
Cloud Computing in Accounting
(8)*

Filip is a student of the Faculty of Law and Administration at the University of Warsaw. He has also completed a course of *Center of American Law Studies* (a joint initiative of the University of Florida Levin College of Law and University of Warsaw Faculty of Law and Administration).

Filip has over two years of experience. His main areas of practice include employment law, IT and new technologies law and civil proceedings law.

About Forum of Bank Technology
and about Bird & Bird

Forum of Bank Technology (FBT) at the Polish Banks Association was created on 14 April 2004 and it works within the Electronic Banking Council. It also associates technological firms (banking technologies providers) cooperating with banks and the Polish Banks Association (PBA) in the implementation of statutory PBA tasks. The main reason for establishing the FBT was the growing need for technology companies and banks to automate cash a turnover and to promote a non-cash turnover, as well as to introduce modern technology in the banking sector in Poland. The most important tasks of the FBT are to prevent electronic banking crime and to implement the modern banking products, which operate on the basis of the latest solutions.

The FBT includes recognized companies and leaders in their fields. The FBT Members have great achievements within the ongoing projects for banks and have undertaken initiatives for the information society, increasing the confidence in the electronic banking. FBT associates entrepreneurs with positively evaluated experience, verified within the cooperation with banks.

The FBT also gives impetuses for changes with effect on the economy and e-government in Poland. One of its main objectives is widely understood promotion of electronic economy, non-cash turnover, modern technologies, electronic identity and widely understood security.

Within the FBT we prepare reports, analysis and studies that initiate implementation of innovations. Good examples of our work are the documents relating to biometrics, identification and authentication, ensuring business continuity (BCM), transaction security, etc.

In the first phase of its activity, the FBT analused, promoted and helped to implement the standard of EMV chip cards, the multiplication of the card solutions, electronic transportation card, or electronic student cards or school cards with payment applications, electronic money and mobile banking. Many of these solutions were then implemented in practice.

The FBT is a formalized group, which aims at adopting legal solutions enabling the dynamic development of electronic economy.

The FBT as the name suggests is a place of exchange of ideas and information, as well as education, presentations and meetings with bankers.

It has its own structure and full autonomy.

The FBT conducts educational activities directed at the banking and its surroundings. It provides the information on the most modern technological solutions in banking and electronic business. It is an association open to cooperate and promote the beneficial development of the Polish banking and electronic economy solutions.

Bird & Bird is an international legal practice, comprising Bird & Bird LLP and its affiliated and associated businesses, including Bird & Bird Maciej Gawroński sp.k.

Bird & Bird was established in 1846 in London. Now there are 23 offices in 16 countries in Europe and Asia. Bird & Bird Maciej Gawroński sp.k. is the “Legal Expert to the Polish Chamber of Commerce” appointed by the Polish Chamber of Commerce, member of the Polish Information Technology and Telecommunications Chamber, member of the British Polish Chamber of Commerce, and cooperates with the Forum of Bank Technology. Bird & Bird advises to the entities of financial sector in transactions, regulations and back-office projects. Co-heads of Banking & Finance sector in Warsaw office are Aleksandra Widziewicz and Sławomir Szepietowski, Attorneys-at-Law, with a many years of experience in this sector. The head of TMT group (Technology, Media, Telecommunications) is Maciej Gawroński, Attorney-at-Law, who has been working for the financial sector since 1999. More information about Bird & Bird are on the website www.twobirds.com (the Polish version is under construction).