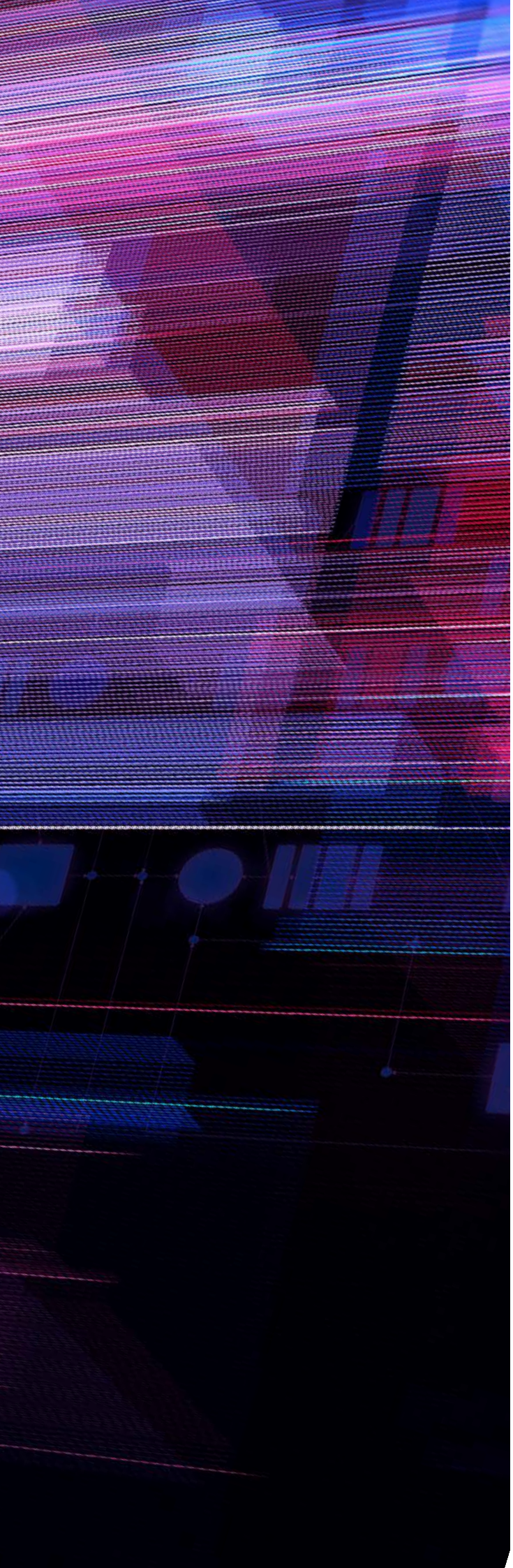
Baker McKenzie.

Regulatory Impact on Cloud Services' Application in Ukraine

Contents



Foreword

Banks seem to face difficulties in implementing their digital transformation projects due to the regulatory restrictions directly or indirectly applicable to cloud computing. In particular, applicable regulation often applies the so-called "perimeter-based" approach whereby banks are required to build their security systems within their own "perimeter." Moreover, applicable regulation may be interpreted as preventing banks to process data outside of their jurisdiction. This leads to difficulties in applying modern cloud computing services. Many financial institutions indicate that a lack of bespoke cloud computing regulation is a significant obstacle for high profile cross-border transformational projects.

This report aims to leverage **Cloud Survey 2020**, which indicates that nearly 60% of respondents consider cloud applications to create more operational efficiencies and 55% said it would drive business agility. Hence, this report shall analyze the notion of cloud computing and cloud services and how these are used to assist financial institutions in their digital transformation efforts. It is further intended to assess the efficiency of local regulation pertaining to the use of such technology in four EMEA markets, namely South Africa, Turkey, UAE and Ukraine.

Moreover, to support the report with empirical knowledge, it is contemplated to conduct a market survey in each of the above jurisdictions to identify key regulatory obstacles from the market perspective. It is finally proposed to work on the proposals of how best to approach the above findings in terms of specific steps working with the local competent authorities based on the available market precedents.

In particular, we highlight the following noteworthy guidance:

(i) the international standards (e.g., **ISO27036-4**, accessible **here**) and

(ii) national and/or regional legislative initiatives (e.g., OCC Statement on Security in a Cloud Computing Environment, accessible **here**, and EBA guidelines on outsourcing arrangements, accessible **here**).

Cloud services v. Digital Transformation

Our **Cloud Survey 2020** indicates that every business needs to make technology an integral part of its business strategy in order to survive and thrive. Hence, it explores the importance of cloud computing within a digitalization program of a business. The survey was conducted in August 2020 among seven sector groupings, including the financial institutions. This report aims to leverage the insights of this survey conducted globally, but primarily relies upon a separate survey conducted within some of the EMEA banking sectors.

Thus, as regards Ukraine, when asked about areas of importance for their technology strategies, 64% of respondents selected cloud computing as one of the top three most important elements to their technology strategy. Survey results reveal a definite trend in banks moving toward the use of private cloud, which possibly highlights an increase in concerns over data security (which includes cyber security) and disaster recovery. This has been further accelerated by the adoption of remote working among businesses due to COVID-19 lockdowns. From an industry perspective, financial institutions are the companies most likely to adopt private cloud.

This is probably not surprising, but regardless of the above benefits, respondents indicated that there are regulatory obstacles to cloud migration. What is more worrying though is that 100% of respondents (who provided full or partial responses) responded affirmatively when we asked whether they considered them a deal breaker. Moreover, some of the respondents seem to be convinced that they are not able to store any restricted data in the cloud (such as data falling into banking secrecy, personal data categories). Some of the respondents also suggested that they have not been able to proceed with their digital transformation projects due to the above restrictions. Given these rather drastic insights, the below chapters seek to analyze in a bit more detail the regulatory restrictions on migration into the cloud and potential solutions to the same.

Control over data, security, compliance

These insights are supplemented by further concerns that banks have with respect to cloud migration. It appears that control over data and data security are among the top concerns, which supports the above insight.

Cost reduction, flexibility of business model and functionality

The greatest impact of cloud was cited as cost reduction (38%), flexibility of business model (31%) and functionality (25%). Given the complex internal structure of many financial institutions, our survey highlights a key benefit of cloud being a cost reduction for the FI sector. Flexibility of business model, functionality, scalability, security, reduced infrastructure requirements, ROI, instant connectivity and commercial goals (e.g., competitiveness, improving customer experience etc.) followed as perceived benefits in that order.

Data Ownership v. Data Control

Data processing seems to be the key aspect of cloud computing application from the customer's perspective. In practice, data management arrangements between a financial institution and a cloud services provider constitute a major part of a technology transaction. This chapter seeks to establish what impact cloud computing application may have on the "ownership" rights vis-à-vis the customers' data.

Property rights vis- à-vis- data generated outside of cloud

In most cases, it is unlikely that any question of private property rights arises vis-à-vis data placed in the cloud.[1] So, ownership rights may generally be found in three areas of law: intellectual property; confidential information and trade secrets; and contract law. Below we analyze whether placing the data in the cloud would affect such ownership rights.

It is noteworthy that the Law of Ukraine No. 2657-XII "On Information" dated 2 October 1992 used to provide for private property rights vis-à-vis information.[2] However, it was clarified recently that "information" couldn't be regarded as an object of material world. Hence, the law now provides for a concept of the "right to information," which may include the rights to use, dispose and possess the information. Moreover, the "right to information" can be transferred to a third party pursuant to a contract.[3]

Regarding the intellectual property rights vis-à-vis information, Civil Code of Ukraine recognizes that these subsist in data bases and trade secrets.[4] Moreover, it recognizes that author's rights subsist in data bases, provided these constitute the result of intellectual activity. Hence, minimal effort is required to ensure that respective information is protected.[5] Regarding protection of trade secrets, Ukrainian law seems to follow the approach taken in Article 39(2) of the Agreement on Trade-Related Aspects of Intellectual Property Rights.[6]

Based on the above, we can conclude that certain amount of the information placed in the cloud by a bank may be protected by author's rights. However, it seems that a substantial portion of such information may not qualify for protection due to its factual nature The owner of these rights is likely to be the bank itself, subject to any contractual terms.

Regarding the contract law, typically, local cloud service provider's terms of service (ToS) envisage that it is not liable for the customer's unlicensed software use or use in breach of license.[7] Also, ToS may impose the following on the customer obligations: (i) to keep secret any data and confidential information belonging to the customer and (ii) to ensure the security of its information, which is transferred through the internet and placed into the cloud. In addition, ToS exclude any vendor's liability for harm caused by any data breach.[8] Finally, It is curious though that ToS regard as confidential any data labelled as such by any party to a contract, in particular, customer's account number, personal data of the parties and data providing access to management panel without actually referring to data placed into the cloud and indicate that parties commit to maintain such confidentiality.

Given the above, one may think of the following to improve such typical ToS, particularly to add acknowledgment of IP rights that various participants own. Moreover, it may be appropriate to grant the licenses of IP rights necessary for cloud services work. Regarding the confidentiality, it would also be appropriate to agree on the confidentiality position following the termination of the contract.

Property rights vis-à-vis data generated inside the cloud by the customer

Ownership rights vis-à-vis data, which the customer generated in the cloud, will depend on both the type of information and, to some extent, on where it was generated.[9] The use of cloud computing makes it uncertain where the work was created.[10] This aspect, along with what type of data is produced in the cloud, may have an impact on IP rights. Below we analyze whether generating the data in the cloud would affect such ownership rights.

It is indicated on one of local provider's web page that it operates via a few data centers both in Ukraine and in other European jurisdictions.[11]

So, the recording of the customer's processing activities could take place outside of Ukraine in the EU. There is a view that a work is created where it is first recorded.[12] It appears that if the data base produced by a customer bank in the cloud is recorded on a server located in an EU Member State, it may fall under the protection of Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases **("EU Data Base Directive")**.[13] What if it is recorded on a server outside of EU? Given that most jurisdictions don't have a concept of computer-generated work, the question whether customer's copyright subsists in it will most likely depend on the local court's view.[14] This difficulties, however, should not, affect IP rights subsisting in the information generated within the cloud as well as its "confidential" status. Unfortunately, local ToS in Ukraine usually only indicate that provider is not responsible for the content produced by the customer using the cloud service.[15] Even if these would say that such data is protected by applicable IP rights this would unlikely have a legal effect vis-à-vis the third parties if, as a matter of law, this position would have been different under the law of the respective jurisdiction.

Cloud Computing v. Outsourcing

There are some prominent examples of cloud service regulatory treatment of cloud usage being subject to outsourcing requirements (e.g.,European Banking Authority's Outsourcing Guidelines **here**). Such treatment may not be in line with the mechanics of cloud computing. Regulation of cloud computing needs to take account how particular cloud technologies operate, and differences between cloud and traditional outsourcing.[16] This chapter seeks to identify the peculiar features of regulatory treatment in Ukraine.

Under the existing regulatory framework applicable to banks, the application of cloud services does not seem to be regarded as outsourcing. Thus, the NBU adopted a regulation dedicated to outsourcing and set out detailed requirements vis-à-vis the same.[17]

Thus, "outsourcing" is defined as instructing an outsourcer on a contractual and regular basis to carry out the functions of a bank to optimize the expenses and processes of a bank. Also, "outsourcer" is defined as an organization, individual-entrepreneur or individual carrying out an individual professional activity chosen by a bank to perform on the terms of outsourcing specific functions of a bank. A separate NBU regulation concerning the data protection system of a bank indicates that the NBU will adopt a separate regulation governing the application of cloud services.[18] Moreover, the NBU indicated in its FinTech Strategy 2025 that it would adopt a separate regulation on IT outsourcing and cloud services by 2022 and 2024 accordingly.[19]

That said, a number of cloud survey respondents answered affirmatively when we asked them whether they considered cloud services as a type of outsourcing. Moreover, some of the respondents referred to Article 61(3) of the Banking Law, which provides for the sharing of data constituting banking secrecy with an outsourcer or a service provider supporting banking activity and regarded such legal basis as problematic to be relied upon in the context of cross-border cloud services. Given this, the question seems to be rather open for now. We would, however, tend to take the view that at least "IaaS" and "PaaS" providers should not be regarded as outsourcers, because they don't typically perform any functions on behalf of a bank, but rather provide cloud computing resources to a bank to perform its functions there.

Cloud Computing & Data Security

As we discussed in the previous chapters, going into the cloud offers a financial institution a lot of operational efficiencies and fundamentally enables it to digitally transform its entire business. That said, reliance on a cloud service provider's resources carries risks. Thus, one of such risks typically raised in the context of the financial services industry is a decreased

user control and increased provider control of data in the cloud, particularly data security (confidentiality, integrity and availability).

Therefore, data security arrangements in practice often constitute one of the most heavily negotiated aspects of the cloud services offered to a financial institution. The reason is that a financial institution is typically subject to heavy regulatory requirements concerning security of its clients' data, e.g., a banking secrecy regime. In view of this, regulators tend to impose a high degree of data security requirements to be complied with by a regulated entity. There is also a growing body of legislation imposing cybersecurity requirements. This chapter seeks to analyze whether such requirements may create obstacles for a financial institution to process its clients' data in the cloud.

Thus, the law restricts access to **three broad categories of data:** confidential data (e.g., personal data), secret data (e.g., professional secrecy) and classified data. Moreover, some data categories, which are protected under the law (e.g., personal data, banking secrecy etc.), must be processed by an 'integrated data protection system' (IDPS) and requires a conformity certificate issued by the designated department of the Security Service of Ukraine (SSU). An IDPS is a combined instrument of an approved software and hardware devices enabling adequate protection of data and must comply with Ukrainian data protection standards.

Based on the above, we can conclude that most of the information placed in the cloud by a bank may be subject to the requirement to process the respective data in IDPS. This could be the reason why some of the survey respondents indicated that they could not place data falling into these categories into the cloud environment.

In addition, in 2010 the NBU started to implement the ISO/IEC 27000 series of standards[20] governing the management of information security.[21] From the formal legal standpoint, the implementing NBU regulation does not apply to the use of "cloud" services.[22] However, it includes certain provisions that may be viewed as incompatible with the "cloud" environment, because they seem to be expected to be implemented within the "perimeter" of the relevant banking organization rather than beyond.[23] This view is also supported by some of the responses to the cloud survey.

Nevertheless, on 24 September 2018, the National Standardization Authority (NSA) of Ukraine adopted ISO/IEC 27036-4 as the national standard security.[24] This standard comes from the same ISO/IEC 27000 series of standards and it provides guidelines for the protection of data by an organization, which engaged a cloud service provider. This document is intended to be used by all types of organizations (including financial institutions) that acquire and consume cloud services. Given this, the Ukrainian banks should be able to implement ISO/IEC 27036-4, if they wish to do so, without additional guidance from the NBU.

Cloud Computing & Data Privacy

Data privacy seems to raise concerns around cloud adoption. Ensuring data confidentiality for FIs is especially important. At the same time, it also seems that privacy laws (in particular, those following EU personal data protection regime) tend not to suit cloud computing mechanics (i.e., tend to treat infrastructure cloud service providers as "processors" by default **here**). This chapter is primarily concerned with the position of such providers in relation to personal data that its users choose to store on its hardware or otherwise process via its cloud services.

If a provider is regarded as a 'controller,' it may be subject to relevant regulatory obligations and liability as such. If it is regarded as a 'processor,' then a separate set of requirements regarding processors may apply. This chapter seeks to argue that due to cloud computing mechanics, in many cases infrastructure cloud service providers should not be regarded as controllers or processors.

Ukraine "implemented" European Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and free movement of such data. Thus, the Law of Ukraine No. 2297-VI "On Personal Data Protection" dated 1 June 2010 ("Personal Data Protection Law") uses concepts such as "controller" and "processor" in relation to stakeholder roles vis-à-vis personal data. Given this, a Ukrainian bank is usually regarded as data controller, because it would typically define the purpose of processing vis-à-vis personal data it would collect from its clients. At the same time, there is no official guidance regarding treatment of a cloud service provider's status. Therefore, if a cloud service provider is not involved in "processing" of the respective personal data, it should not be regarded as data processor, so should not be subject to applicable requirements imposed by the Personal Data Protection Law (e.g., an obligation of a data controller and data processor to enter into a specific data processing agreement).

At the same time, in the cross-border context, engagement of the cloud service provider may be subject to conditions, because Article 29 of the Personal Data Protection Law imposes certain requirements on personal data "transfer" to a foreign entity related with personal data.[25] The law does not define the notion of the "transfer." However, it appears from the responses to the cloud survey that some of the banks regard this requirement as applicable in the cloud computing context. If so, in case of a transfer to a cloud service provider located outside of a "safe harbor," it might be a challenge for a bank to pick a suitable legal basis for such transfer. Given this, some of the respondents to our survey proposed to amend the law and provide for additional legal basis applicable in the cloud computing context.

Data Residency & Regulation

It seems that data residency requirements have become a trend globally. When such rule is introduced, there is often uncertainty as to the precise scope of the same. Foreign cloud providers tend to consider this as a matter of competition favoring local companies. Technically, physical access to a server containing data is not required to access data in an intelligible form. At the same time, the storing of data in a particular location does not automatically mean it is secure.[26]

This discussion may also be relevant in the context of the respective jurisdictions obligations undertaken after joining the WTO. For example, a data residency requirement could be interpreted as violating a specific commitment under Article XVI of the General Agreement on Trade in Services not to limit the ability of nonresidents to render the "data processing services" (CPC 483) and "data base services" (CPC 844) in the cross-border mode. Available expert analysis indicates that such commitments extend to, respectively, (i) a wide range of digital business and consumer services, **including cloud-based business-to-business services**,[27] and (ii) complex cloud computing services. So, the requirement to have an on-soil server may de facto limit cross-border trade in cloud services, because it seems to apply a 'zero quota' on the supply of cloud services by any means of cross-border delivery of the service.

As discussed in Chapter 3, some data categories, which are protected under the law (e.g., banking secrecy etc.), must be processed by an IDPS. NBU confirmed that this requirement also applies to banks.[28] The applicable standards pertaining to setting up the IDPS do not prohibit processing data in the cloud environment. However, from a practical perspective, the standards are drafted in a manner indicating that the IDPS should be created in Ukraine (please refer to the applicable standard in Ukrainian **here**, which indicates that the respective data center premises should be built on Ukrainian soil in accordance with the applicable building standards).

Moreover, under Section 5, Chapter I of the Accounting Regulation, the bank is required to carry out the processing and storage of banking transactions data on servers and/or other computer equipment that is physically located in the territory of Ukraine. Based on the formal reading of the Accounting Regulation, both processing and storage of banking transactions

data on a computer equipment located outside of Ukraine are prohibited. In view of this, the processing of the data controlled by a bank in the vendor's "cloud" outside of Ukraine could technically be regarded as a breach of the above requirement. Some respondents to the cloud survey also suggested that this requirement may have such impact.

Conclusions

Both our analysis as well as the results of the survey indicate that Ukrainian legislation does not as such prohibit banks' migration into the cloud environment. At the same time, the legislative and regulatory framework imposes a number of complex requirements, which may be difficult to comply with in such an environment. In particular, such difficulties may be faced in the cross-border context where a bank would seek to cooperate with a foreign cloud services provider (or even with a local one that has data centers outside of Ukraine).

In this context, it is useful to refer to an established view that national laws may not be a suitable mechanism for regulating cloud, because cloud computing typically disregards national borders. Moreover, it is very likely that national laws will differ and as such would never produce a coherent governance framework.[29]

Given these complexities, it may be suggested to the relevant regulators to consider a so called "light touch" approach towards application of cloud services by the banks. This approach seems to be applied in some of the prominent jurisdictions, e.g., in the USA whereby the regulator does not create any additional regulatory expectations vis-à-vis the regulated entities, but rather provides methodological guidance on how to consume cloud services in view of the existing regulatory requirements (i.e.,OCC Statement on Security in a Cloud Computing Environment, accessible **here**). The European Banking Authority seems to be following a similar approach in its **guidance outsourcing arrangements**. That said, some of the imposed requirements are more challenging in the context of cloud services.[30]

As discussed above, it appears that the NBU is now working on the draft regulation applicable to the application of cloud services. In view of the above, it would seem that a more balanced approach would be to avoid producing a new layer of regulatory requirements. Instead, the regulator could consider the adoption of methodological guidance on how to use cloud services in view of the existing (sometimes outdated) legal framework. As we discussed in Chapter 5, Ukraine implemented the relevant ISO standards, hence the general legal framework is already available. What seems to be missing though is the additional clear guidance to the banks on how to use it in the specific context of the banking industry. The lack of such legal certainty seems to create confusion and very different views on whether or not a bank could migrate into the cloud.

Appendix

1 Cloud Computing Law, OUP, 2013, edited by C. Millard, p. 144.

2 This regime was abolished back in January 2017 when the recast version of this law N 2938-VI was adopted.

3 Yarysh O.M., 'Regulation of civil law relationships relating to information,' (2014) Scientific Newsletter of the International Humanitarian University: Jurisprudence № 9-2, issue 1.

4 Article 420(1) of the Civil Code of Ukraine.

5 Article 433(1)(3) of the Civil Code of Ukraine.

6 Article 505(1) of the Civil Code of Ukraine provides that protection must be given to information, which:

- is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;
- has commercial value because it is secret; and
- has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

Moreover, under Article 505(2) of the Civil Code of Ukraine, information of technical, organizational, production and other nature is also protected unless is expressly excluded under applicable law.

7 Please, for instance, refer to para. 6.4.6 of GigaCloud ToS at: https://gigacloud.ua/uploads/0/added-contract.pdf. accessed [*]. 20 June 2021

8 Ibid, paras 8.2.3 - 8.2.4.

9 Ibid, p. 147

10 Cloud Computing Law, OUP, 2013, edited by C. Millard, p. 148.

11 https://gigacloud.ua.

12 Cloud Computing Law, OUP, 2013, edited by C. Millard, p. 148.

13 However, under Article 7(1) of the EU Data Base Directive a customer bank would need to show "qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents."

14 Cloud Computing Law, OUP, 2021, edited by C.Millard, p.163

15 Please, for instance, refer to para. 6.4.2 of GigaCloud ToS at: https://gigacloud.ua/uploads/0/added-contract.pdf.

16 Ibid, 64.

17 Section 47, Chapter I of the NBU Regulation on Organization of Risk Management System in Ukrainian Banks and Banking Groups, approved by the Resolution of the Board of the NBU No. 64 dated 11 June 2018.

18 Para. 4, Chapter I of the NBU Regulation on Organization of Measures Ensuring Information Safety in the Banking System Approved by the Resolution of the Board of the NBU No. 95 dated 28 September 2017.

19 Available at the official NBU web page here: https://bank.gov.ua/ua/about/develop-strategy/fintech2025.

20 ISO/IEC 27001 and ISO/IEC 27002.

21 Resolution of the Board of the NBU No. 474 dated 28 October 2010 "On Implementation of Information Security Management Standards in the Banking Industry of Ukraine." It was replaced by the Resolution of the Board of the NBU No. 95 dated 28 September 2017.

22 Please refer to paragraph 4, Chapter I of the Resolution of the Board of the NBU No. 95 dated 28 September 2017.

23 For instance, please refer to paragraph 107, Chapter IV of the Resolution of the Board of the NBU No. 95 dated 28 September 2017.

24 Please refer to NSA Order No. 337 dated 24 September 2018.

25 In particular, under Article 29(3) of the Personal Data Protection Law, the transfer of personal data to a foreign entity may take place only if the third country in question ensures an adequate level of protection of such personal data. Signatories to Convention 108 are deemed to be providing sufficient level of personal data protection. In other words, the transfer of personal data to the EEA and other jurisdictions signatories to Convention 108 is regarded as transfer to the "safe harbor." The Cabinet of Ministers of Ukraine is expected to approve additional list of jurisdictions meeting this requirement, but this has not yet been done.
In case the transfer is envisaged to a jurisdiction outside of a "safe harbor," Article 29(4) of the Personal Data Protection Law provides for an alternative legal basis to transfer personal data outside of Ukraine - such transfer would be permissible in the following circumstances:

(i) the data subject has given consent to the transfer;
(ii) transfer is necessary for the discharge by the date controller (e.g., a bank) of a contract between the data controller and a third party — data subject executed in favor of another data subject;
(iii) transfer is necessary in order to protect the vital interests of the data subject;
(iv) transfer is necessary for the performance of a task carried out in the public interest, or for the provision, execution or facilitation of a legal aid; and/or
(v) transfer is necessary for the data controller (e.g., a bank) to ensure non-interference into the private life of the data subject(s).

26 "Forced Localization of Cloud Services: Is Privacy the Real Driver?" Christopher Millard.

27 Daniel Crosby, Analysis of Data Localization Measures under WTO Services Trade Rules and Commitments, p. 6, https://e15initiative.org/wp-content/uploads/2015/09/E15-Policy-Brief-Crosby-Final.pdf (visited 18 February 2021).

28 Regulation "On Organization of Accounting, Accounting Controls During Operational Activity of the Ukrainian Banks," approved by the Resolution of the Board of NBU No. 75 dated 4 July 2018.

29 Cloud Computing Law, OUP, 2013, edited by C. Millard, p. 469.

30 https://www.bakermckenzie.com/en/insight/publications/2019/10/eba-outsourcing-guidelines-come-into-effect.

Baker McKenzie Contacts:

Serhiy Chorny
Managing Partner
Serhiy.Chorny
@bakermckenzie.com

Maksym Hlotov
Senior Associate
Maksym.Hlotov
@bakermckenzie.com

The content of this document contains the initial results of the ongoing legal research carried out by the Kyiv office of Baker McKenzie, which does not constitute a legal advice. The results of a similar research carried out by Istanbul, Dubai and Johannesburg offices may be obtained from these offices upon request.

Baker McKenzie helps clients overcome the challenges of competing in the global economy.

We solve complex legal problems across borders and practice areas. Our unique culture, developed over 65 years, enables our 13,000 people to understand local markets and navigate multiple jurisdictions, working together as trusted colleagues and friends to instill confidence in our clients.

Renaissance Business Center
24 Bulvarno-Kudriavska St.
Kyiv 01601, Ukraine
Tel: +380 44 590 0101

bakermckenzie.com/ukraine