Volume 18, Issue 4
December 2020

ISSN 1731-8297, e-ISSN 6969-9696
https://czasopisma.uni.opole.pl/index.php/osap

ORIGINAL ARTICLE
received 2020-11-07
accepted 2020-12-23

OPOLSKIE STUDIA ADMINISTRACYJNO-PRAWNE
THE OPOLE STUDIES IN ADMINISTRATION AND LAW

Liability within the scope of Cloud Computing services

Odpowiedzialność w zakresie usług Cloud Computing

KATARZYNA CHAŁUBIŃSKA-JENTKIEWICZ
Chief of Department of Cybersecurity Law and New Technologies Law,
Law Institute, War Studies University,
Director of Academic Center for Cybersecurity Policy The law advisor
ORCID: 0000-0003-0188-5704, k.jentkiewicz@akademia.mil.pl

Citation: Chałubińska-Jentkiewicz, Katarzyna. 2020. Liability within the scope of Cloud Computing services. *Opolskie Studia Administracyjno-Prawne* 18(4): 09–22. DOI: 10.25167/osap.3427

Abstract: The issue of acquiring large amounts of data and creating large sets of digital data, and then processing and analyzing them (Big Data) for the needs of generating artificial intelligence (AI) solutions is one of the key challenges to the development of economy and national security. Data have become a resource that will determine the power and geopolitical and geoeconomic position of countries and regions in the 21st century.[1]

The layout of data storage and processing in distributed databases has changed in recent years. Since the appearance of hosting services in the range of ICT services, we are talking about a new type of ASP (Applications Service Providers) – provision of the ICT networks as part of an application). Cloud Computing is therefore one of the versions of the ASP services. The ASP guarantees the customer access to a dedicated application running on a server. Cloud Computing, on the other hand, gives the opportunity to use the resources of a shared infrastructure for many users simultaneously (Murphy n.d.). The use of the CC model is more effective in many aspects. Cloud Computing offers the opportunity to use three basic services: data storage in the cloud (cloud storage), applications in the cloud (cloud applications) and computing in the cloud (compute cloud). Website hosting

[1] This article has been prepared as a result of cooperation at the realization of the research project entitled “The Polish cybersecurity system - a model of legal solutions“ The Agreement MON No. GB/4/2018/208/2018/DA] granted by Ministry of National Defence.

and electronic mail are still the most frequently chosen services in Cloud Computing. The article attempts to explain the responsibility for content stored in the Cloud Computing.

Keywords: data protection, personal data, digital content, digital heritage, intellectual property, new technology

Abstrakt: Kwestia pozyskiwania dużych ilości danych i tworzenia dużych zbiorów danych cyfrowych, a następnie ich przetwarzania i analizowania (Big Data) na potrzeby generowania rozwiązań sztucznej inteligencji (AI) jest jednym z kluczowych wyzwań dla rozwoju gospodarczego, ale także dla zapewnienia bezpieczeństwa narodowego. Dane stały się zasobem, który będzie decydował o miejscu oraz pozycji geopolitycznej i geoekonomicznej państw XXI wieku.

Zasady przechowywania i przetwarzania danych w ich rozproszonych bazach zmieniły się w ostatnich latach, a od czasu pojawienia się usług hostingowych w zakresie usług teleinformatycznych mówimy o nowym typie usług ASP (Applications Service Providers), które obejmują udostępnianie sieci teleinformatycznych w ramach aplikacji. Cloud Computing stanowi jedną z wersji usług ASP, która gwarantuje klientowi dostęp do dedykowanej aplikacji działającej na serwerze. Cloud Computing z kolei daje możliwość korzystania z zasobów wspólnej infrastruktury wielu użytkownikom jednocześnie. Zastosowanie modelu CC staje się coraz bardziej efektywne pod wieloma względami. Cloud Computing umożliwia korzystanie z trzech podstawowych usług: przechowywania danych w chmurze, tworzenia aplikacji w chmurze oraz przetwarzania w chmurze (chmura obliczeniowa). Hosting stron internetowych i poczta elektroniczna to nadal najczęściej wybierane usługi w ramach Cloud Computing. W artykule podjęto próbę wyjaśnienia reguł odpowiedzialności za treści przechowywane w chmurze obliczeniowej, przyjmując za kluczowe ustalenie zarówno cech podmiotów świadczących usługę, jak i charakter gromadzonych w niej treści.

Słowa kluczowe: ochrona danych, dane osobowe, treści cyfrowe, dziedzictwo cyfrowe, własność intelektualna, nowa technologia

1. Introduction

The European Commission perceives the role of data sharing and the benefits of AI development in one of its documents, on the basis of which it can develop an artificial intelligence ecosystem that provides the benefits of this technology to the entire European society and economy: "As digital technology becomes an ever more central part of every aspect of people's lives, people should be able to trust it. Trustworthiness is also a prerequisite for its uptake. This is a chance for Europe, given its strong attachment to values and the rule of law as well as its proven capacity to build safe, reliable and sophisticated products and services from aeronautics to energy, automotive and medical equipment" (European Commission 2020). To this end, the Parliament and the Council of the EU have published Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on the Framework for the Free Flow of Non-Personal Data in the European Union.

This Regulation applies to data processing in the broadest sense, encompassing the usage of all types of IT systems, whether located on the premises of the user or outsourced to a service provider. It should cover data processing of different levels of intensity, from data storage (Infrastructure-as-a-Service (IaaS)) to processing of data on platforms (Platform-as-a-Service (PaaS)) or in applications (Software-as-a-Service (SaaS)). Under these conditions, the issue of liability for cloud-based data storage is of particular importance.

2. Analysis

The first services of this type were launched by Amazon – one of the largest e-commerce companies in the world. The CC model cannot be treated as a new type of service, because many solutions used in its area are taken from the already existing ones. However, this model has many characteristic elements that make it unique in comparison to other similar services. These features include: outsourcing, i.e. one of the management strategies, multi-tenancy, sharing resources among many recipients at the same time. R. Marchini indicates that an important multi-tenancy operation is the use of the same copy of the software, run by many users at the same time (Marchini 2010: 8). The problem of multiple-tenancy is very important when constructing contracts. The supplier, due to the multitude of recipients and their dispersion, is forced to unify their pattern as much as possible so that it meets the needs of all the users, while meeting economic and business expectations. Contract templates are often inflexible and usually do not provide for exceptions in the case of individual users. Therefore, a customer who decides to sign such a contract must face certain restrictions. It is then an accession rather than a commission agreement. Another feature is scalability. According to J. Rosenberg and A. Mateos (2011: 36), scalability is "about the cloud platform being able to handle an increased load of users working on a cloud application." The entity using Cloud Computing does not have to report additional demand for resources, as they will be allocated automatically. Another very important term associated with this feature is flexibility. J. Rosenberg and A. Matos mention one more element, that is the main technological factor of cloud computing – virtualization. It is a technology that allows applications to run on many operating systems, running on the same specific physical server at the same time. It allows one to use the full computing power and server resources. It also allows one to quickly create operational systems ready for work in the virtual space. Although this model is mainly used in commercial enterprises, its potential has also been noticed by state authorities and international institutions. To countries, using the solutions offered by the CC model gives the opportunity to not only develop digital business of the state, but can also significantly reduce the costs associated with communication and information technologies (European Commission 2012: 2).

The European Commission, in the document issued in 2012, *Unleashing the Potential of Cloud Computing in Europe*, estimates that harmonization of the digital market based on operating in a public cloud model would increase the GDP by Euro 250 million in 2020. However, it can only be done with the assumption of well-functioning strategies enabling the CC model to operate. The lack of operation in this area implies an increase by only Euro 88 million. The difference is therefore substantial. In addition, it is estimated that the development of this field would create nearly 2.5 million new jobs (European Commission 2012: 7). Apart from the obvious benefits resulting from the development of cloud computing, this process also raises many doubts resulting, for example, from a very high dynamics of change, which involves, among others, the need to adjust legal solutions. Since the provision of services in this model is carried out on an outsourcing basis, this means that the entities involved in the supply chain (data controller, processing, sub-processing) are in most cases subject to other legal regulations regarding, e.g. data protection or have their headquarters in different jurisdictions (Skibińska-Mamzer 2013: 2). Given the pace of CC development in 2012, the Working Group on Data Protection in Telecommunications (Berlin Group) has created a document called the Sopot Memorandum on the processing of data in the cloud. It identified the most important issues that may involve the following examples of risk in the process of Cloud Computing development: continuous technology development; lack of standardized international terminology; huge number of data collected in the clouds; global scope of data processing; cross border and unlimited range of technology; lack of transparency regarding the practices of the service provider, processes and procedures, including whether the service providers entrust subcontractors with any processing and, if so, on what terms; lack of transparency regarding suppliers which causes difficulties in proper risk assessment; too much emphasis on economic issues related to data processing, which may consequently lower their standards (International Working Group on Data Protection in Telecommunications 2012: 2).

The conditions presented above may carry many undesirable actions, such as: committing acts that violate the provisions and principles of data protection and privacy, data may fall under the jurisdiction that does not provide them with a sufficient degree of protection, the administrator may not notice breaches of confidentiality and data security, the administrator may lose control of the data, the possibility of blurring responsibility in the long supply chain (International Working Group on Data Protection in Telecommunications 2012: 3). In the Sopot Memorandum, its authors give recommendations which, in their opinion, may contribute to minimizing the risks arising from the use of services in the Cloud Computing model. These include, among others: care for maintaining high standards of data protection stored and processed in the cloud;

commitment of data controllers to assess the impact on privacy protection and threat assessment, before taking activities in the CC space, standardization of data protection technologies; undertaking efforts for third-party testing and certification; continuous monitoring and assessment of the adequacy of the existing legal framework, which allows data to be transferred across borders and includes protection of the data in the CC model (International Working Group on Data Protection in Telecommunications 2012: 3). At CC, the service provider is not able to provide the user with guarantees regarding the place of data storage. This is due to the fact that the servers on which the data are stored are extensively distributed (Marciniak 2009: 1).

The Cloud Computing model is considered the next stage in the evolution of service delivery methods. It cannot be said that this is a new type of service, because it has developed on the already existing processes and infrastructure. It is often referred to as ISP 5.0 (Internet Service Provider; ISACA 2011: 17). In the CC services, the data controller is of key importance in the context of liability for the stored data. It seems that in the course of data processing this is it that plays the greatest role and has the greatest responsibility. Although it is possible to entrust data to another entity under a contract for processing, this fact does not exclude the controller's liability. If the situation is unclear from a legal point of view, the controller may even incur criminal liability. It is crucial to state that the controller "is responsible for data processing." According to the position set out in Opinion 1/2010 of the Article 29 of the Working Group "the first and foremost role of the concept of controller is to determine who shall be responsible for compliance with data protection rules, and how data subjects can exercise the rights in practice. In other words: to allocate responsibility" (Article 29 Working Party 2012: 7). An entity that processes data completely according to the instructions cannot be considered a controller. It follows that the main criterion in recognizing an entity as a controller will be here independence while making decisions regarding the purposes and means of data processing (Barta, Fajgielski, and Markiewicz 2011: 24). At this point, the question arises whether, based on the principles of personal data protection, the service provider can be recognized as a controller at the same time, or is it only a data processor? Is a CC user such a controller? Answering these questions is extremely important because not only the issue of obligations, but also the responsibilities of the processor depend on it (Article 29 Working Party 2006).

The analysis of the tasks of individual entities participating in the activities of CC, implies that it should be assumed that it is the client – the CC user – that meets almost all the prerequisites for recognizing it as the controller, because it has the power to make decisions regarding the purpose of processing its data. In this case, the supplier will act as the processor. There are situations in which the processing entity, i.e. ISP CC, determines what kind of data it will process, as well as the principles and methods of data processing. In such a situation, should it still be referred to as the data processor or already the data controller? This problem was raised by the Working Group (GR) Article 29 in Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT). Similarly to ISP CC, this entity deals with information exchange and brokerage in transactions between banks, brokerage houses and other financial institutions (Wikipedia n.d.).

Theoretically, it only deals with the processing of data on behalf of service providers. Despite this, SWIFT also sets the standards and rules for this processing itself (Article 29 Working Party 2010). Recognition of each supplier as a controller could significantly limit their field of activity (Marchini 2010: 47). Therefore, although in the Opinion 1/2006, the issue of the controller and the related responsibility is quite broadly discussed, it does not give unequivocal suggestions on how to distinguish the controller from the data processor in the case of services provided in the virtual space. This problem is clarified by a slightly different opinion GR No. 1/2010. According to it, the definition of the "purpose" of processing is sufficient to regard an entity as the controller. However, it may transfer the 'method' of processing in technical and organizational matters to another entity, and this will not change its status of the data controller (Article 29 Working Party 2010). Because determining elementary issues regarding compliance of the processing with the legal provisions also belongs to the data controller (Article 29 Working Party 2010). In practice, in the Cloud Computing, especially in the SaaS model, the customer manages its data and is primarily responsible for all decision-making processes. The decision on the security issues or server locations, however, rests on the ISP CC, which in consequence would allow it to be considered the data controller. It is extremely difficult to clearly define the data controller and the data processor. That is why it is so important for all parties which contract for cloud services to become acquainted with the exact scope of activities of individual entities in relation to the transmitted data. In the case of Cloud Computing services, there can be no unequivocal position that the service provider is a data processor and taking into account the dynamics of changes within cloud services, it would be necessary to create clear rules that would not leave ambiguities and room for abuse.

Since the spread of broadband Internet and wireless connections IT professionals have faced new challenges related to copyright protection. Until now, almost at every level of providing services and products, their authors have had the opportunity to control the recipients. Book authors, music creators and programmers have encountered copyright infringement, but the Internet has significantly intensified this practice. With the dynamic development of the network, in which the number of users is constantly growing, its control is almost impossible. Problems related to copyright apply to cloud computing on many levels. A very important issue is primarily one related to the conclusion of contracts between the service provider and the recipient. This requires clear rules ensuring that there is no room for any kind of abuse. It will also be very important to consider the issue of providing access to computer programs located in the Cloud Computing space. The same will apply to applications. They clearly require establishing rules for their use, but it should be done in a different way than traditional licensing. The SaaS model, i.e. software as a service, raises the biggest controversy in this respect. Lawyers argue whether the use of software located in the cloud results in concluding a license or whether concluding a license is necessary at all (Góra 2013: 1).

An important problem related to Cloud Computing is storage of data, the number of which is huge and is still increasing, due to the growing popularity of services offered in this model. In recent years we have been witnessing dynamic popularization of social networking sites. Some of them, like Facebook together with Instagram belonging to it, provide the user with the possibility of sharing and storing photos. However, a significant number of users do not realize that the photos become the property of the service provider, which often leads to violation of rights, including personal rights.

In the scope of copyright, the choice of the applicable law and jurisdiction appears to be relevant when using cloud computing. The CC model solution providers have their headquarters in different parts of the world. Most of them are situated in the USA, China and India (Mejssner 2011: 1). This is tantamount to being subject to the jurisdiction of these particular states. Most contracts for the provision of such a type of services include a clause concerning the choice of law. To Polish users it means the need to use the services of foreign entities, and thus, conclude cross-border contracts. This is extremely important because in the event of any contentious issues, the costs of international litigations are enormous. Due to the fact that the largest disputes in this matter are pending in connection with the licensing of these services, Cloud Computing service providers use various tools in their service provision, inter alia, tools that are based on open source licenses. It is a free software element whose main purpose is to allow free access to software to all its users (http://evolpe.pl/open-source). Open source software offers fewer opportunities for abuse of any kind other than the one in which the source code is non-public. Undesirable effects may include the situation when a person who knows a concealed code can use software to track or obtain data. In addition to a publicly available source code, an open source software is also characterized by such elements as: freedom to create derivative works, freedom of re-distribution, non-discrimination of individual users or groups, and free distribution of licenses. In the case of software where the source code is publicly available, the license should include a reservation that the source code is not allowed to be modified, because such activity would result in blocking its open use.

According to J. Barta, P. Fajgielski and R. Markiewicz, an open source license is “a collective category covering various forms of contracts for computer programs, characterized by making the program available also in the source version (next to a ‘machine’ version), combined with the authorization to make modifications to the software and its further distribution under this license” (Barta, Figielski and Markiewicz 2011: 234). Therefore, the basic element of this type of license is “obliging the user to provide modification of the program (…) under the same conditions as specified in the license he/she has used (the so-called copyleft software)” (Traple 2010: 295). Sometimes a copyleft is also called a viral elect because a user who adds his intellectual contribution into a given program cannot license it based on traditional rules (Machała 2007: 33). In order to protect the license based on *an open source*, in 1985, thanks to Richard Stallman, Free Software Foundation (FSF) was established. It is this foundation that, at the time of rapid development of Cloud Computing services, introduced a new type of license GNU Afferro GPL (AGPL), created to prevent any acts restricting freedom on the Internet or aimed at collecting too much information about the users. This type of license assumes that if the user uses a program or application placed on the server, he/she must have access to the source code.[2] Apart from that, copyleft assumes that “anyone who distributes this type of software must at the same time transfer the right to its further distribution and modification” (Chałubińska-Jentkiewicz and Karpiuk 2015: 225).

In the article “Data Privacy in the Cloud: Dozen Myths and Facts”, Lotar Datermann discusses 12 most popular myths related to data security in the cloud. However, the risk of cloud computing continues to exist and becomes a challenge to data security and privacy policies. The danger is even associated with the fact that the customer’s location is often very distant from the location where the servers on which the data are stored are located. This often raises the problem of determining the place of processing the entrusted personal data. On the one hand, the data controller is at risk of losing control over the data, yet on the other one – there is a risk of transferring the data to a third country (Pudo 2015: 1). In the context of the global reach of Cloud Computing services, appropriate legal solutions should be found to help define jurisdiction clearly. The customer is not aware who and to what extent has access to his/her data. Thus, they expose themselves to the risk of poor data access management or simply to a hacker’s attack (Muszyński 2012: 1). There are situations where the Cloud Computing model service providers do not delete mass or operational memory after disconnecting with the user (Muszyński 2012: 1). Another problem

[2] License available at: http://www.gnu.org/licenses/agpl.html [accessed: 20.04.2020].

is also an adequate level of data security in terms of privacy and confidentiality. Part of the data is stored in an open form, which increases the risk of it falling into an unwanted possession (Muszyński 2012: 1).

R. Marchini, in his study, gives suppliers several solutions which, in his opinion, will minimize the risk of adverse events and their security effects. First of all, providers' priority should be to maintain an appropriate level of internal and external security. The latter mainly concerns such aspects as: server and network security, data storage method, their encryption and issues related to backup copy (data backup created in the event of loss or damage) (Marchini 2010: 4, 24–25). This also relates to one of the largest cloud service providers, that is Google. In 2012, the company issued the "Privacy Policy" document which deals with many questions related to data and information security. Although the document issued by Google is quite extensive, many IT professionals and market research analysts indicate that there is a lack of transparency in many places of it. This includes the use of the users' data between different services or the acquisition of the users' phone numbers by logging into Google using Android (Stowarzyszenie Bibliotekarzy Polskich 2012).

Another example of a service provider is Facebook. It should be emphasized that in the last few years Facebook's privacy and security policy has been criticized by both users and other public cloud service providers. LinkedIn, like Facebook, is a social networking site which provides services in the Cloud Computing model. On its official website, as in the examples described earlier, we can find information on data security. Unlike Facebook, LinkedIn addresses the issue of its users' data security extensively. Such records constitute a kind of safeguard, which, however, is often perceived by users as the avoidance of the suppliers' liability for security breaches. In the security policy available on the official Google website, we can find information that "Google can be used in a variety of ways, e.g. for searching and sharing information, communicating with other people or creating new content. Thanks to the information obtained from users (e.g. when creating a Google account), we improve these services – we display more relevant search results and more relevant ads, we facilitate contacts with friends and offer faster and simpler ways of sharing content" (Google: 2018). The collection of information occurs in a twofold manner: directly from the user and when using the services offered by Google (e.g., watching YouTube videos). In the second case, data collection is independent of the user who is unaware of this process. The data that Google obtains in this way including location of the user, gives information about the equipment it uses, IP address or information about the mobile network and phone number (Google: 2018). According to the EU experts, Google also violates some of the findings of the "Safe Harbor" program regarding the exchange of personal data between the European Union and the United States and treats them very selectively. It is primarily about the aforementioned use of non-precise concepts, listing only selected confidential data or guaranteeing users the right to access data. Similar accusations were made towards Facebook when in 2014 it turned out that its privacy policy was changing. According to its creators, these were changes of only minor importance. However, they allow collecting even more data on its users. The first change is the introduction of the "Friends nearby" service, which will allow the user to download a signal from mobile devices and provide friends with the information of the user's location. Another is the "Buy" service, which allows the user to buy the advertised product without logging out of Facebook. The company reserves the right to collect location and transaction data. In addition, the website will collect information on the visited websites and used applications more accurately, aiming at adapting the offer as close as possible to our needs.

Directive 95/46/EC of the European Parliament and of 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 contained restrictions on the transfer of data intended for the prevention of control over them by natural persons. It should be noted that, in accordance with the provisions of the Directive, data transfers between Member States should be free and uninterrupted.

Similarly, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) emphasizes that "the economic and social integration resulting from the functioning of the internal market has led to a substantial increase in cross-border flows of personal data. The exchange of personal data between public and private actors, including natural persons, associations and undertakings across the Union has increased. National authorities in the Member States are being called upon by Union law to cooperate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State".

The situation is different when the entity to which we are sending data is based outside the EU. In the transfer of data outside the European Union, it is very important that many countries, including the United States, do not have an adequate level of protection. This situation required creation of legal regulations that would allow trade between market participants in the US and the EU. In order not to complicate trade relations, the European Commission and the US Department of Commerce created the already mentioned Safe Harbor Privacy Principles, which it is also called the Safe Harbor Principles (Generalny Inspektor Ochrony Danych Osobowych n.d.). The main assumption of the Safe Harbor is to enable the processing of data from the European Union to entities from the United States. The SLA provisions relating to maintaining the appropriate level of services are extremely important in cloud service contracts. These principles create a certain framework that determines the actual scope of services offered by it, they oblige it to maintain appropriate standards and the level of services it provides, and to make every effort to ensure that it does not change (Marchini 2010: 110). The elementary issues regarding the level of services provided, according to Marchini, should relate to: availability of the service, time of resolving problems, time of responding to inquiries, speed of delivery of resources requested by the customer (Marchini 2010: 114-115).

A very important part of the SLA that should be included in Cloud Computing contracts is to define the extent of a third party participation in the process of service provision and to clearly define their responsibilities. Under the Polish law, this issue is referred to in Article 738 Para 1 of the Civil Code, which states that the contractor of the order may entrust the execution of the order to a third party only if it results from the contract or from a custom, or when the existing circumstances force him/her to do so. In such an event, he/she is obliged to immediately notify the principal about the person and place of residence of his/her deputy and in the event of notification he/she is only responsible for the lack of due diligence in the selection of the deputy. The deputy is responsible for the execution of the order also to the principal. If the contractor of the order is liable for the activities of his/her deputy as for his/her own, their liability is joint and several.

According to the provisions of this article, subcontractors may be selected by the service recipient. This, however, may only occur with the consent of the customer (service recipient). Cloud Computing services often encounter this type of situation. This is due to the fact that as an outsourcing service it involves many subcontractors. If contractors fail to fulfil their obligations, service providers will do everything to demonstrate that they have made every effort to ensure that the service is provided at an appropriate level; however they are not able to control all subcontractors. Therefore, one has to take into account the risk of side effects, e.g. interruptions in the provision of Internet services, program errors, or unreliability of servers. These situations, although not common, result in consequences for several, and sometimes even several million users. In order to protect themselves from liability for such incidents, the recipients of the services, in the contracts they prepare, contain clauses that provide for the exclusion or limitation of their liability in the event of damage caused by system errors. For example, Google included in the regulations regarding the conditions of use of their services that "in no event shall Google, its suppliers or distributors be liable for any loss or damage which cannot be foreseen by reasonable measures" (Google: 2015). Possible damage concerns the mass number of users and not a single customer.

In the Polish law, this situation is permitted by Article 353 Para 1 of the Civil Code. It is also common for the service providers to determine the amount for damages below which they do not bear liability. In addition to the liability for damage presented above, an important issue is also related to the limitation of liability regarding damage caused by inappropriate data processing.

3. Conclusion

It is worth noting that in cloud systems there are not only data provided by the customer, but also data resulting from the use of the cloud. The boundary between customer data and machine data is thus blurred. The data is on the servers of the company which processes it on the basis of a contract with specific clients and is also its own resource. Cloud companies will defend themselves against the transfer of aggregated data, claiming that they are "not their data, but customers' or users'." In relation to the so-called own data "that it is our data because we incurred the costs of their production" and it is difficult to refuse them. It is not possible to limit processing to only one country.

Therefore, we can deal here with personal and non-personal data and – consequently – the question arises which of these data should, for example, be protected by Regulation (EU) 2016/679? Each type of data may be subject to other legal contractual regulations, as well as those resulting from generally applicable laws. It seems possible to create flexible legal solutions based on acts for safe entrustment of data in the model of "fiduciary management", but with a clear system of sanctions for breaking the rules.

Bibliography

Article 29 Working Party. 2006. *Opinion 10/2006 on the Processing of Personal Data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)*. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp128_en.pdf [accessed: 30.04.2020].

Article 29 Working Party. 2010. *Opinion 1/2010 on the Concepts of "Controller" and "Processor"*. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf [accessed: 30.04.2020].

Article 29 Working Party. 2012. *Opinion 05/2012 on Cloud Computing*. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf [accessed: 30.04.2020].

Barta, Janusz, Paweł Fajgielski, and Ryszard Markiewicz. 2011. *Ochrona danych osobowych. Komentarz* 5th ed. Warszawa: Wolters Kluwer Polska.

Chałubińska-Jentkiewicz, Katarzyna, and Mirosław Karpiuk. 2015. *Prawo nowych technologii: wybrane zagadnienia*. Warszawa: Wolters Kluwer.

Directive 95/46/EC of the European Parliament and of 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, OJ L 281, 23.11.1995, p. 31.

European Commission. 2012. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Unleashing the Potential of Cloud Computing in Europe"*, COM(2012) 529 final.

European Commission. 2020. *White Paper on Artificial Intelligence – A European Approach to Excellence and Trust*, COM(2020) 65 final.

Generalny Inspektor Ochrony Danych Osobowych. n.d. *Co to jest safe harbor?*. http://www.giodo.gov.pl/317/id_art/1500/j/pl/ [accessed: 19.05.2015].

Google. 2015. *Terms of Service*. http://www.google.com/intl/pl/policies/terms/ [accessed: 25.05.2015].

Google. 2018. *Privacy Policy*. http://www.google.com/intl/pl/policies/privacy [accessed: 12.12.2018].

Góra, Jarek. 2013. *Technologie mobilne – wybrane aspekty praktyczne i prawne – część 2 IP Blog*. http://www.ipblog.pl/2013/02/technologie-mobilne-wybrane-aspekty-praktyczne-i-prawne-czesc-2/#more-1632 [accessed: 12.12.2018].

International Working Group on Data Protection in Telecommunications. 2012. *Working Paper on Cloud Computing. Privacy and Data Protection Issues – "Sopot Memorandum"*.

ISACA. 2011. *IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud*. Rolling Meadows, IL: ISACA.

Machała, Wojciech. 2007. *Licencja mieszana? Prawnoautorskie aspekty obrotu programami komputerowymi stworzonymi z wykorzystaniem oprogramowania o otwartym kodzie*. Zeszyty Naukowe UJ 1: 28–37.

Marchini, Renzo. 2010. *Cloud Computing. A Practical Introduction to the Legal Issues*. London: BSI.

Marciniak, Marcin. 2009. *Bliższe niż chmura*. http://www.computerworld.pl/artykuly/350736_4/Blizsze.niz.chmura.html [accessed: 13.02.2015].

Mejssner, Barbara. 2011. *Cloud computing: prawo w chmurze nieskuteczne*. *Rzeczpospolita*. https://www.rp.pl/artykul/724643-Cloud-computing--prawo-w-chmurze-nieskuteczne.html [accessed: 30.04.2020].

Murphy, Lincoln. n.d. *ASP vs SaaS – What's the Difference?*. http://sixteenventures.com/difference-between-asp-and-saas [accessed: 5.11.2018].

Muszyński, Józef. 2012. *Bezpieczeństwo w chmurze*. http://www.computerworld.pl/news/376996_2/Bezpieczenstwo.w.chmurze.html [accessed: 11.05.2015].

Pudo, Bartosz. 2015. *Ochrona danych osobowych a cloud computing*. http://mojafirma.infor.pl/mala-firma/pracownik-i-zus/707750,Ochrona-danych-osobowych-a-cloudcomputing.html [accessed: 11.05.2015].

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.05.2016, p. 1–88.

Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a Framework for the Free Flow of Non-Personal Data in the European Union, OJ L 303, 28.11.2018, p. 59–68.

Rosenberg, Jothy, and Arthur Mateos. 2011. *The Cloud at Your Service. The When, How, and Why of Enterprise Cloud Computing*. Greenwich: Manning.

Skibińska-Mamzer, Ilona. 2013. *Bezpieczeństwo informacji w cloud computingu – aspekty prawne*. http://www.twojbiznes24.pl/artykuly,10218,17176,bezpieczenstw o-informacji-w-cloud-computingu-aspekty-prawne,strona,2 [accessed: 2.01.2016].

Stowarzyszenie Bibliotekarzy Polskich. 2012. *Czy polityka prywatności Google jest zgodna z prawem UE?*. http://www.sbp.pl/artykul/?cid=6458&prev=540 [accessed: 13.12.2015].

Traple, Elżbieta. 2010. *Umowy o eksploatację utworów w prawie polskim*. Warszawa: Wydawnictwo Oficyna.

Wikipedia. n.d. *Society for Worldwide Interbank Financial Telecommunication*. https://en.wikipedia.org/wiki/Society_for_Worldwide_Interbank_Financial_Telecommunication [accessed: 18.05.2015].