LegalTech and Coud Computing

Katarzyna Biczysko-Pudełko

1. Introduction

When R.Susskind's book The Future of Law: Facing the Challenges of Information Technology was published in 1996, in which he made a bold claim that in the future lawyers would communicate with their clients via e-mail, for many this thesis was abstract, just like the technology and the very concept of cloud computing. It was not until 1996[1] that the latter appeared for the first time in the document[2] .

However, less than a quarter of a century later, the fact that lawyers use e-mail is already undisputed, which also makes the thesis about the use of cloud computing services, i.e. computing in the cloud, undisputed. The level of interest in cloud computing services among the representatives of le-

1 In 1996, two Compaq specialists, G.Favaloro and S. O'Sullivan, came to the conclusion that in the near future both software, storage and computing power of computers will be accessed through actions undertaken on the Internet, the above phenomenon describing in more detail within the framework of a business plan prepared for their form and calling it cloud computing.Nozar Daylami, 'The origin and Construct of Cloud Computing' (2015) 9, 2 International Journal of the Academic Business World, 39; Suryanarayanan Srinivasan, *Cloud Computing Basics*, (Springer 2014,4); 'The era of cloud computing'<https://www.matillion.com/cloud-computing-era> accessed 13 January 2021.

2 It should be noted that in scientific studies devoted to the origins of the very concept of cloud computing there are also such views, according to which the term was used for the first time by Professor R. Chellappa from the University of Texas in his publication entitled "Intermediaries on cloud computing". Intermediaries on cloud computing". In resolving this dispute, it should be pointed out that in the case of Compaq specialists, we were dealing not so much with a scientific publication as with an internal document of the company in the form of a business plan. Thus, none of the above events should be depreciated and both Compaq specialists and Professor Chellappa should be credited with influencing the concept of cloudcomputing. Antonio Regaldo, 'Who Coined "Cloud Computing"?', (*MIT Technology Review*, 31 October 2011) <https://www.technologyreview.com/s/425970/who-coined-cloud-computing> accessed 9 March2021.

gal professions is perfectly illustrated by a survey conducted in 2020[3] by The International Legal Technology Association (ILTA), in which as many as 89 % of lawyers[4] declared that they would consider using cloud computing services[5]. The above trend is also followed by Polish representatives of the legal industry, where as recently as in 2013 there were discussions whether to include the issue of using cloud computing technology in the rules of ethics[6], but already today: "using cloud computing is like breathing. We just don't think about it. From the users' point of view, current solutions are almost transparent"[7].

However, it would be insufficient to say that lawyers are using cloud computing quite extensively today, because as cloud technology itself evolves, so does the way it is used. While initially the use of cloud computing was limited mainly to email, currently, there is a growing trend towards greater interest among lawyers in more complex and technologically advanced solutions offered by cloud computing - which is directly related to the desire to optimie costs and working time, but is also a natural consequence of the development of the IT industry. Therefore, just as in the case of LegalTech we can talk about a division into three levels, i.e. LegalTech 1.0, 2.0 and 3.0, so it seems justified - at least for the purposes of this analysis - to distinguish cloud computing 1.0, 2.0 and 3.0, each of which, reflecting the individual stages of its development, will imply various doubts as to the admissibility of its use, in the context of personal data processing[8], by lawyers within their organisations. The following part of the work will therefore signal those aspects that are of the most sensitive nature with regard to particular cloud tools - in the context of personal data protection law.

---

3 ILTA's, '2020 Technology Survey' <www.iltanet.org/resources/publications/surveys/2020ts?ssopc=1> accessed 9 March 2021 r.

4 The survey involved 470 entities representing over 103,000 lawyers and 208,000 users.

5 Latest ILTA Survey Suggests Security Has Taken a Back Seat to Productivity in Firms. Here's How to Fix it, (*Netdocuments*, 23 November 2020) <https://www.netdocuments.com/blog/latest-ilta-survey-suggests-security-has-taken-a-back-seat-to-productivity-in-firms-heres-how-to-fix-it> accessed 9 January2021.

6 Katarzyna Żaczkiewicz-Zborska, 'Kancelaria w chmurze obliczeniowej naraża na szwank tajemnicę zawodową', <www.prawo.pl/prawnicy-sady/kancelaria-w-chmurze-obliczeniowej-naraza-na-szwank-tajemnice,175923.html> accessed 9 March2021.

7 Anna Klimczuk, 'Chmura jak powietrze: cyfrowa transformacja kancelarii prawnej Magnusson'<news.microsoft.com/pl-pl/2016/12/13/chmura-jak-powietrze-cyfrowa-transformacja-kancelarii-prawnej-magnusson/> accessed 9 March2021.

8 More on the concept of personal data in part IV chapter 5.

2. Cloud Computing 1.0

The concept of cloud computing, for which the term "cloudcomputing" or "cloud computing" is used alternately in the literature as well as in everyday speech, has not yet been reflected in a single commonly used definition. However, the one most often quoted is the one proposed by the US National Institute of Standards and Technology (NIST), according to which cloud computing is a model enabling ubiquitous, convenient and on-demand network access to shared computing resources (i.e. network, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management or provider intervention[9].

According to another, slightly more simplified definition, cloud computing "allows access to data from any device, anywhere, as long as there is an Internet connection"[10].

In practice, the use of cloud computing by a lawyer, as referred to above, will include within its conceptual scope the possibility to use electronic mail, file storage and processing (e.g. Dropbox, Google Drive), or even online office packages (e.g. Microsoft Office 365), i.e. services that are already common today, both in the case of large legal corporations and individual entities. This state of affairs is not surprising, if we take into account a number of benefits that cloud computing brings (can bring), i.e. from cost minimisation, through flexibility (which in practice works out to automatic access to resources of almost unlimited scale), to increased work efficiency.

Nevertheless, cloud computing also poses a number of challenges of various types, with one of the biggest threats being that related to the broadly understood security of data[11], including personal data stored and

---

9 Peter M. Mell and Timothy Grance, 'The NIST Definition of Cloud Computing Recommendations of National Institute of Standards and Technology', (2011) No. 800-145 Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, ,2, <csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf> accessed 9 January 2021,Commission 'Unleashing the Potential of Cloud Computing in Europe', (Communication) COM (2012) 529 final, 2, https://eur-lex.europa.eu/legal-content/pl/TXT/?uri=CELEX%3A52012DC0529 access: 9 March 2021); Kenneth L. Bostick, 'Pie in the Sky: Cloud Computing Brings an End to the Professionalism Paradigm in the Practice of Law', (2012) 60, 5 Buffalo Law Review, 1375.

10 Kenneth L. Bostick, (n 9) 1382.

11 While understanding the essence of this technology, one cannot help but ask a number of questions concerning not so much the technological processes of data processing in a computing cloud, but their security, bearing in mind the

processed in it, which in the case of representatives of the legal industry, as those obliged to maintain professional secrecy, seems to be even greater. Therefore, as rightly indicated in the documents prepared by the Council of Bars and Law Societies of Europe (CCBE), i.e. in 2012 Guide - Electronic Communications and the Internet[12] and the Guidelines on the Use of Cloud Computing Services by Lawyers[13] , when considering the possibility to use cloud computing technology, a lawyer should first examine whether the laws and rules of professional ethics in force in his or her country allow the storage of data off-site. In the case of investigating the possibility to process personal data in cloud computing, the answers to the above questions, in relation to a huge number of lawyers, will be shaped by the provisions of GDPR.

First of all, a lawyer using cloud computing tools must be aware that as a rule - in the light of the provisions of the above mentioned GDPR - he acts as a data controller, i.e. as the one who alone or together with others determines the purposes and means of the processing of personal data, while the provider of services in cloud computing as a processor. The consequence of the above will be, therefore, the requirement for the lawyer to fulfil a number of duties, as well as the scope of his or her responsibility

Often, it is worth emphasizing that the EU legislator, when regulating the scope and distribution of controllers' duties, relied on two concepts that significantly differ from the hitherto rigid and non-relative protection frameworks, i.e. the risk-based approach and the concept of technological neutrality of the regulation.

The first concept, i.e. risk-based approach, assumes that a legal decision regarding the processing is based on a risk assessment of the processing, which is nothing more than a regulation based on shaping the controllers' obligations *ad casum* through the prism of a risk assessment[14]. This assessment should take into account the state of the art, the cost of imple-

---

whole spectrum of threats, from the so-called "data leakage", through data loss, to unauthorised access to data.

12 CCBE, 'Komunikacja elektroniczna i Internet –przewodnik CCBE' (2013) 142 Radca Prawny Dodatek Naukowy 5D.

13 Council of Bars and Law Societies of Europe, 'CCBE Guidelines on the Use of cloud Computing Services by Lawyers', (*CCBE*, 7 September 2012), <http://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Position_papers/EN_ITL_20120907_CCBE_guidelines_on_the_use_of_cloud_computing_services_by_lawyers.pdf> accessed 21 January2018.

14 Dominik Lubasz, in: Edyta Bielak-Jomaa *and* Dominik Lubasz (eds), *RODO. Ogólne Rozporządzenie o Ochronie Danych. komentarz* (Wolters Kluwer 2017) 586.

menting security measures, the nature, scope, context and purposes of the processing and the risk of violation of the rights or freedoms of natural persons with varying degrees of probability and seriousness arising from the processing

On the other hand, the second concept, i.e. the technological neutrality of the GDPR, boils down to the lack of indication in its provisions of specific technical or IT solutions that the controller should implement to ensure compliance. Indeed, as stated in Recital 15 of the GDPR, in order to prevent a serious risk of circumvention, the protection of individuals should be technologically neutral and should not depend on the techniques used. Thus, the data protection regime should be tailored to risks of varying likelihood and relevance to the rights and freedoms of individuals and linked precisely to a risk assessment by a lawyer and a data protection impact assessment, while the instruments should be adequate and chosen by the controller itself.

In the spirit of the concepts referred to above, a lawyer must fulfil a number of individual obligations imposed on him/her by the provisions of GDPR, i.e. both those provided for in the content of Chapter IV and those resulting from the need to guarantee natural persons the implementation of their rights provided for in Chapter III of GDPR. In particular, it is important that a lawyer, when selecting a cloud computing provider, should be guided by the content of Article 28(1) of the GDPR, i.e. use only services of such entities that provide sufficient guarantees of implementing appropriate technical and organisational measures so that the processing meets the requirements of the GDPR and protects the rights of data subjects. In this context, as pointed out in the CCBE Guide mentioned earlier, it seems indispensable to examine the experience, reputation and credibility of such a provider, but also to verify whether the provider operates under procedures compliant with international IT risk management standards, such as e.g. ISO 27001:2005.

Inseparably connected with the above obligation is also the issue of appropriate construction of the contract concluded with the cloud computing provider and ensuring the possibility to control the performance of contractual obligations by the provider[15]. In addition to determining the law applicable and the competent court for resolving disputes, the

15 Fédération Suisse des Avocats, 'Indications et recommandations de la FSA pour la sous-traitanceinformatique et l'utilisation de services cloud' <https://<www.sav-fsa.ch/fr/documents/dynamiccontent/190408-sav-guidelines-outsourcing_f-(4).pdf> accessed 9 January 2021.

contract should also contain provisions on data ownership and the exclusive right of access, on the prohibition to use subcontractors without the prior consent of the recipient, on the physical location of the servers, on the right to control and audit compliance with the contract, on data processing rules in accordance with national requirements applicable to the recipient, on contractual penalties and on the recipient's liability in the event of a breach of confidentiality.

Moreover, in the context of ensuring compliance of the processing of personal data in cloud computing by a lawyer with the provisions of the GDPR the lawyer should take into account the issues related to the transfer of data to third countries, which due to the specificity of cloud computing is not an incidental situation. In the case of cloud computing, the phenomenon of cross-border data processing becomes particularly visible, which results, inter alia, from such factors as service providers' provision of services on the basis of servers located in the so-called third countries or the use of services of sub-processors not only not having their registered office or organisational unit in EU countries, but also performing processing in third countries. However, in accordance with the provisions of GDPR, the transfer of data to another country is permitted, provided that it belongs to the European Economic Area (EEA). However, when data is transferred outside the EEA, the possibility of such a transfer should be analysed individually and in accordance with Articles 45-49 of the GDPR.

In this context, the issue of data transfer based on the so-called standard contractual clauses that constitute part of the provider's terms and conditions deserves particular attention, due to the ruling of the CJEU of 16 July 2020, C-311/18 (Schrems II)[16]. In the framework of this ruling, the CJEU held that the transfer of data to the US on the basis of an EC decision called the "Privacy Shield"[17] is not possible, as this decision is invalid. Therefore, if a lawyer (acting as the data controller) processes data in computing resources located in the USA, it should always assess whether the standard contractual clauses ensure a sufficient level of personal data protection (a situation where the legislation of the country in which the data importer is located does not ensure a level of protection equivalent to the level set by the provisions of GDPR cannot be deemed as such).

16 Case C-311/18 *Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems* [2020] EU:C:2020:559.

17 Commission Implementing Regulation (EU) 2016/1250 of 12.7.2016 adopted pursuant to Directive 95/46 of the European Parliament and of the Council, on the adequacy of the protection provided by the EU-US Privacy Shield.

Therefore, it would be beneficial for the lawyer to limit the processing to the EEA.

3. Cloud Computing 2.0 - or Multi-Cloud in the Work of Lawyers.

Multi-cloud (in.multi-cloud computing), just like cloud computing, may be defined in various ways, and the variable in this respect is primarily the defining entity. It is obvious that a representative of the IT or business sector will have a different understanding of the term, while a user (client) will have a different one. For example, while for representatives of the first of the above-mentioned industries multi-cloud will be a kind of process of integration of IT resources, more precisely[18], for representatives of the business industry it will be a strategy[19]. On the other hand, individual (single) users of the multi-cloud will associate it either with the possibility to use multiple platforms provided and managed by different public cloud providers, or with the possibility to combine their own computing resources with those of external entities, or with the possibility of simultaneous use of the resources of a cloud.

However one defines the term it is important to distinguish mulit-cloud from hybrid cloud. As pointed out in the literature, in the case of multi-cloud all its components are unique cloud computing systems, not methods of implementation, as it is the case under hybrid cloud[20]. Moreover, in the case of hybrid cloud, unlike within multi-cloud, there is also interference of the hardware layer.[21] Furthermore, multi-cloud is sometimes mistakenly identified with a virtual IT environment that is based on different operating system platforms, i.e. with the so-called multi-cloud platform.

For the purposes of this study, however, the term multi-cloud should be understood as the serial or simultaneous use of multiple data processing

---

18 Ana Juan Ferrer, Davi García Pérez, Román Sosa González, 'Multi-Cloud Platform-as-a-Service Model' (2016) 97 Functionalities and Approaches Procedia Computer Science 65.

19 Alan R. Earsl,'Multi-cloud strategy', <https://<searchcloudcomputing.techtarget.com/definition/multi-cloud-strategy> accessed 9 March 2021.

20 Jianngshui Hong, Thomas Dreibholz, Joseph Adam Schenkel, Jiaxi Alessia Hu, '*An Overwiew of Multi-Cloud Computing*'in Leonard. Barolli, Makoto Takizawa, Fatos. Xhafa, Tomoya Enokido (eds), *Web, Artificial Intelligence and Network Applications. Proceedings of the Workshops of the 33rd International Conference on Advanced Information Networking and Applications* (WAINA-2019) 7.

21 Ibid.

and storage services provided by different providers in a public or private cloud, and integrated within a single IT environment (architecture).

To illustrate the above in the context of LegalTech, we can use an example where a lawyer, for the purposes of his daily work, will simultaneously use computing resources made available by provider "X" (e.g. for document storage) and others made available by provider "Y". (e.g., for document storage), while at the same time using computing resources provided by provider "Y" (for data processing) (for data processing), and others by provider ,"Z" (e.g. for data analysis). As you can imagine, the use of multi-cloud by a lawyer can bring many benefits and be a great tool to facilitate daily work.

First multi-cloud allows for optimisation of labour costs and improvement of effectiveness, for example by providing lawyers with tools that can significantly streamline billing processes and reduce the working time associated with administrative tasks. Another unquestionable advantage of using this solution is the high availability of computing resources and services tailored to the individual needs of an organisation[22]. In addition, multi-cloud, as indicated in the literature, creates better conditions than classic cloud computing for the possible recovery of IT resources and data in the event of failure or other unforeseen events[23]. Finally, what fundamentally distinguishes multi-cloud from classic computing cloud is the fact that it allows avoiding the phenomenon of vendor lock-in, i.e. dependence on a single provider of this type of service.

The above, just an example of the benefits that the use of multi-cloud can bring, seem to highlight the circumstance why this technology has already been evaluated as a solution worthy of attention and use by lawyers. However, quite understandably, alongside a number of advantages and potential benefits, multi-cloud is also a whole new set of challenges and risks, which, although they find their origin in the technological dimension, ultimately also lead to a number of different types of legal challenges, including those focused on data protection, and in particular personal data processed in multi-cloud.

First making some general remarks with regard to the challenges created by the multi-cloud already at the IT level, it should be noted that the very implementation of the solution in question may prove problematic in

22 Giuseppe Di Modica, Antonella Di Stefano, Giovanni Morana, Orazio Tomarchio, 'On the Cost of the Management of user Applications in a Multicloud Environment', (7th International Conference on Future Internet of Things and Cloud (FiCloud), Istanbul, 2019).

23 Hong, Dreibholz, Schenkel, Hu. (n 20) 6.

practice, i.e. the collection of data processed so far under a classic cloud, and then their integration with the environment of another computing cloud, so that from a functional point of view, it is possible to create one coherent multi-cloud infrastructure[24]. Another challenge may turn out to be the skilful management of complex infrastructure and the implementation of consistent rules for the management of data processed by several cloud computing providers simultaneously, so that the multi-cloud potential is not lost in the form of increased efficiency in comparison to classic cloud computing. Incompetent use of multi-cloud solutions may also lead to the problem of duplication of data in the computing resources of individual providers, which, apart from the risk of increasing the costs of such processing, may negatively affect the level of data security[25]. The issue of data security is undoubtedly one of the biggest challenges in mutli-cloud solutions. While in the case of classic cloud computing ensuring security required a number of measures and the development of a certain methodology, in the case of multi-cloud this task becomes even more complicated. Each provider of cloud services, which constitute the "components" of the multi-cloud, implements its own security policy and information flow, which directly implies potential problems in terms of ensuring the integrity of the security policy for the entire multi-cloud architecture. Moreover, in the case of multi-cloud it is very likely that one process running in a particular computing cloud will be inextricably linked with a process already running in another provider's infrastructure. This in turn, as indicated in the literature, makes the use of a single access control mechanism impossible and creates a potential risk in the area of data transfer from the resources of one computing cloud to another, which often takes place on a large scale and in an automated manner[26].

These general remarks on the potential challenges of multi-cloud technology may, in the reality of everyday work of lawyers, boil down to the need to find answers to a number of individual questions, i.e. in

---

24 Faction,'What is Multi-Cloud? Everything You Need to Know', <https://www.factioninc.com/blog/what-is-multi-cloud/> accessed 28 December 2020.

25 CIO, 'Defining your data strategy for a multi-cloud world' <https://www.cio.com/playlist/the-cloud-control-room/collection/cloud-operations-and-management/article/defining-your-data-strategy-for-a-multi-cloud-world <https://www.cio.com/playlist/the-cloud-control-room/collection/cloud-operations-and-management/article/defining-your-data-strategy-for-a-multi-cloud-world> accessed 18 December 2020.

26 Piotr Waszczuk, 'Trend Micro: W jaki sposób zapewnić bezpieczeństwo infrastruktury IT w modelu multicloud? ', <https://www.itwiz.pl/trend-micro-jaki-sposob-zapewnic-bezpieczenstwo-infrastruktury-modelu-multicloud/> access 8 December 2020.

particular: where is the data (including personal data) located today and will it be located in the resources of the same provider in the future? How to manage a multi-cloud environment while maintaining full control over data processing? How to minimise the risk of data security breaches, which may increase especially when transferring data from one provider's resources to another's infrastructure? The search for answers to the last of these questions also seems to be complicated by the fact that often the interoperability of the individual computing clouds that make up the multi-cloud architecture must be coordinated and automated, which is often done using an additional IT tool (platform), the use of which may imply further questions about data security.

Paraphrasing the words of P. Miller, in order to summarize the above, it can therefore be said that a lawyer, before using a multi-cloud, must map its complexity before it becomes impossible to map it[27]. Doing so may increase the likelihood of satisfying legal requirements which, as mentioned above, in the case of multi-cloud environments seem to revolve particularly around data protection law. Since already today a large part of the legal profession uses a classic computing cloud for data processing, including data of a personal nature, this will undoubtedly also be the case in the multi-cloud, with the difference that in the case of the latter the legal challenges will both multiply, and completely new ones will appear, directly implied by the complexity of the multi-cloud environment.

In principle, one can risk a claim that all those obligations, which a lawyer identified (as it was established earlier) as a data controller in the light of the provisions of the GDPR must fulfil when using a classic computing cloud, will be obliged to fulfil also in the case of a multi-cloud, i.e. from the obligation to carefully select providers of individual services, through the appropriate risk assessment, to at least the implementation of data subjects' rights.

In the context of the obligation to carefully select providers of particular services, it seems particularly important, apart from the need for the provider to ensure an adequate level of availability of the service, as well as an adequate level of security assurance, to verify whether the cloud computing provider meets the conditions for the legality of its service, including the provisions of the General Regulation on the protection of personal data, which in turn involves, for instance, the need to analyse the content of particular cloud computing service contracts. Thus, a lawyer wishing to use multi-cloud in his or her everyday activity faces a challenge

27 CIO (n 26)

in the form of familiarising himself or herself with the content of individual contracts for the provision of services in computing clouds concluded with individual providers in order to ensure the compliance of each of the contracts with the requirements specified in Article 28 of the GDPR, which on the one hand is a challenge due to the lack of standards or commonly applied best practices in this respect, and on the other hand, may prove to be problematic in the context of the practical possibility to select individual cloud computing service providers who ensure not only an adequate, but also similar level of services. In practice, the above will involve, for example, the necessity to analyse Service Level Agreements (SLA), under which the minimum level of service is defined, starting with issues related to its availability or performance, and ending with provisions concerning the level of provider support. If, in a multi-cloud environment, at least one of the providers does not provide sufficient guarantees that appropriate technical and organisational measures are implemented to ensure that the processing complies with the requirements of the GDPR, a lawyer should not be able to include the services of this provider in the multi-cloud architecture being developed. In this context, the obligations that a lawyer as a data controller should fulfil will thus multiply in relation to those whose fulfilment is related to the use of the classic computing cloud.

On the other hand, the obligation of a lawyer, as a data controller, to exercise the data subject's right to erasure may be regarded as a completely new challenge, which will be directly implied by the multi-cloud character. It should be reminded that pursuant to Article 17 of GDPR the data subject has the right to demand from the controller immediate erasure of data relating to him/her, and the controller is obliged to erase such personal data without undue delay, if one of the circumstances indicated in the aforementioned Article 17 of GDPR occurs. As it has already been indicated above, one of the "derivatives" of multi-cloud use may be the phenomenon of duplication of the same personal data in the resources of various cloud computing providers, which - as it is not difficult to imagine - may later be connected to the challenge of exercising the right to erasure. Undoubtedly, whether the data controller will be able to meet this obligation will depend on whether it has sufficient knowledge as to where, i.e. in the resources of which provider personal data of a given data subject have been and are being processed.

However, for the same reasons as in the case of exercising the right to erasure, it may turn out problematic to fulfil the obligation to notify the data subject about the personal data breach, which is provided for in Article 34 of the GDPR. In case of a personal data breach under

circumstances which indicate that the breach may result in a high risk of violation of rights or freedoms of natural persons, the controller shall notify the data subject of the breach without undue delay. In the case of multi-cloud, the fulfilment of the above obligation will be possible, if the lawyer has knowledge as to which personal data of which subjects were actually processed in the particular computing cloud, where the breach occurred. Mere knowledge about a possible security incident within the resources of a specific computing cloud, without the possibility to identify whose data were processed in its resources, may turn out to be insufficient for the fulfilment of the above obligation.

An analogous challenge, i.e. connected with the controller's lack of knowledge as to whose data were processed exactly in the resources of the computing cloud in which the breach has occurred, will also appear in the situation of the necessity to notify the personal data protection breach to the supervisory authority, to which the data controller is obliged by Article 33 of the GDPR.

As a kind of countermeasure to minimise the risk of controller's failure to meet the obligations described above, the literature, following a proposal made earlier by L. DalleMulle and T.H. Devenport in Harvard Business Review[28], suggests that in case of willingness to use a multi-cloud solution, a "compromise" between defensive and offensive data strategies should be considered. In the case of an offensive strategy, the priority would be to support business objectives, e.g. increasing the efficiency and profitability of the business, and thus to process the data that could be used to achieve these objectives within the computing resources of a single provider. A defensive strategy, on the other hand, would boil down to processing within a computing cloud offered by another provider those data which are of a personal nature and are covered by legal protection. Subsequently, the computing resources provided by the various cloud computing providers should be integrated in a single virtualised and automated platform that will facilitate and simplify the management of data in the various clouds[29].

The above strategy, however interesting, in certain situations, especially when the processing operations concern large amounts of data and the resources of which increase rapidly, may turn out to be an insufficient tool to minimize the risk of personal data breach. That is why it is commonly

28 Leonardo. DalleMulle and Thomas H. Devenport, 'What's Your Data Strategy? The key is to balance offense and defense', < https://www.hbr.org/2017/05/whats-your-data-strategy> accesed 18 December 2020.

29 CIO (n 26).

suggested in the literature[30] that in the case of multi-cloud data processing personal data should be encrypted. It should be noted that pursuant to Article 32 of the GDPR, encryption of personal data was indicated as one of the technical and organisational measures which may contribute to ensuring an appropriate level of security of processing.

The very notion of encryption is a process of converting data into an unreadable sequence of characters without the knowledge of the relevant key and - so far - has not been reflected in a single legal definition. The provisions of the GDPR do not provide any further guidance as to the details and requirements of the process, but in practice there are certain variables that should be taken into account when implementing encryption processes - also by lawyers - and which may largely affect the level of data security.

Above all, it is important that encryption covers both so-called "data at rest" and data "in transit", i.e. during transmission, as well as data in use.

The first category includes data stored in databases, files or mass storage infrastructure. They usually constitute a certain logical whole and structure, hence gaining access to them for unauthorised persons seems to be particularly desirable and attractive, while for a lawyer (as an administrator) particularly dangerous. Meanwhile, statistics show that only 9 % of the 12,000 cryptographic service providers encrypt data at rest[31]. For this reason, it is important for lawyers wishing to use this security measure to recognise the need to select a provider that will provide encryption of data at rest - which can prove to be quite a challenge.

Moreover, it is equally important to adequately encrypt the second of the indicated data categories, i.e. data "on the move", i.e. during its transmission, movement through any network. In this case, however, apart from the encryption itself, it seems inevitable to implement robust and adequate security control mechanisms for the network through which the data are transmitted, such as firewalls, network access control, etc[32].

---

30 Ramya Srikanteswara and others 'Data security using encryption on multi-cloud' (2018) 5, 6 International Research Journal of Engineering and Technology 2969 HYTrust, 'Protecting sensitive data and achieving compliance in a multi-cloud world', <https://www.hytrust.com/uploads/Compliance-in-a-Multi-Cloud-World_WP.pdf> accessed 11January 2021.

31 HYTrust (n 31)

32 Nate Lord, 'Data Protection: Data In transit vs. Data At Rest', <https://<www.digitalguardian.com/blog/data-protection-data-in-transit-vs-data-at-rest> accessed 13 January 2021.

Finally, the third category, data in use, refers to information that is currently being updated, processed, deleted, accessed or read by the system. This type of data is not passively stored, but actively moves through elements of the IT infrastructure[33]. Here, in addition to encryption, important data protection measures such as user authentication at all stages, including data access monitoring (e.g. login history) should be implemented[34].

Although the above-described need to categorise data and include in the encryption process both data at rest and "en route" as well as data in use is an important element of security, encryption alone is nevertheless insufficient. In the context of the aforementioned concept of encryption, it seems indisputable that it is the above-mentioned key - to put it figuratively - which is the equivalent of the combination of a series of numbers opening a safe's combination lock, that is the most important element of the whole process. If an unauthorised person knows this combination of numbers, he will be able to open every safe, and thus - returning to the multi-cloud case - will gain access to data processed within the cloud computing resources. Hence, once encryption begins, the most important aspect becomes the organisation's ability to manage these keys, especially as this very management is often a process so operationally complex that it is sometimes referred to as the "Achilles‘ heel of encryption".

For a lawyer wishing to use a multi-cloud, it is therefore important not so much that he implements the encryption process itself, but that he manages the encryption keys in an appropriate way, which should be comprehensive and include the possibility to generate, distribute, store or revoke or destroy keys if necessary. Of course, in the case of a mutli-cloud environment, this key management seems to present a much higher degree of complexity than in the case of a classical cloud. In practice, the greater the amount of computing resources of individual providers used by a lawyer, the greater the number of keys in use and the more complex their management becomes. Hence, a certain remedy for this state of affairs may turn out to be the use of management solutions that allow for the automation of all critical tasks related to the key management cycle, and this without disrupting or affecting the daily processing[35].

33 Laura Fitzgibbons, ‘Data in use. Definition’, <https://www.whatis.techtarget.com/definition/data-in-use> accessed 15 January 2021.

34 ibid.

35 HYTrust (n 31).

Finally, apart from data encryption and key management, indicated earlier, a sine qua non condition for increasing the level of data security is also its control and, more broadly, ownership. Well, when data were processed within the entity's own IT structure, the question of key ownership did not raise any doubts. However, in the cloudcomputing environment, and even more so in the case of multi-cloud architecture, the question of ownership of the key is no longer so obvious. Indeed, even when data at rest are strongly encrypted, it is still necessary to avoid that the cloud provider has control over the key. Firstly, this reduces the risk of a data security breach, since - hypothetically - if an unauthorised person learns the user's credentials and gains access to resources stored in the computing cloud, he or she will gain access to data that will be nothing more than an incomprehensible string of characters. Secondly, the issue of key ownership may also play an important role in the context of enhanced data access monitoring.

In conclusion, in order for encryption to play its role, it must take an appropriate - i.e. actually ensuring an adequate level of security of the processing - form, and be perceived as a certain component of a broader process, in which, apart from the fact of encryption itself, what seems to be more important is the management and possession of encryption keys. Only an encryption process identified in this way may significantly affect the security level of data processed in a multi-cloud environment by a lawyer. At the same time, however, there should be no doubt that the encryption in question is, first and foremost, a method of securing data, and not a process leading to the deprivation of personal characteristics of the information, which further leads to the conclusion, which every lawyer using this method in the multi-cloud environment must remember, that encrypted data remains personal data, and encryption itself is not a method of performing only a specific operation on encrypted data within the scope of application of the GDPR.

4. Cloud Computing 3.0

4.1 General Remarks

Finally, when analysing issues related to the admissibility of the processing of personal data by a lawyer in a computing cloud, reference should also be made to the case of cloud computing 3.0, mentioned in the intro-

duction to this work, i.e. the one based on blockchain technologies[36]. A natural consequence of the constant expansion of both these technologies, i.e. cloud computing on the one hand and blockchain technology on the other, is their integration[37], especially that the latter turns out to be an excellent tool where cloud computing may fail, i.e. for example in terms of increasing the security of processing. This, in turn, makes it a legitimate conclusion that also in the work of lawyers using cloud computing technology, the percentage of such "cloud" processing based on blockchain will increase year by year, which, in addition to the undoubted benefits arising from it again - as in the case of classic cloud or cloud 2. 0 - will imply questions about the mutual relationship between personal data protection regulations, i.e. the GDPR in particular, and cloud computing 3.0. At the same time, it is necessary to underline the fact that compliance with the GDPR may be discussed not so much in relation to the technological solution itself, but the way it is used. Therefore, ultimately, the legitimacy of the methodologies applied should always be assessed by the lawyer through the prism of his or her own organisation, i.e. on a case-by-case basis[38].

36 Due to the fact that both the very notion of blockchain, as well as issues related to its use in the work of a lawyer have been discussed in more detail in part IV, chapter 6, the author will limit herself only to pointing out the problems that may arise in the case of use of cloud computing based on the said blockchain by a lawyer, and only in the context of the problems that may arise in this respect from the data protection law.

37 The purpose of this analysis is the use by lawyers of cloud computing, which is based on blockchain. However, it should be noted that in practice, in addition to the mentioned correlation, there may also be a correlation between cloud computing and the mentioned technology, in which the blockchain technology will be based on cloud computing. Simanta Shekhar 'Sarmah, Application of Blockchain in Cloud Computing' (2019) Vol. 8 Issue 12 International Journal of Innovative Technology and Exploring Engineering. 4968.

38 Ministerstwo Cyfryzacji, Grupa robocza ds. rejestrów rozproszonych i blockchain, 'GDPR a technologia blockchain', <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwj1rtT-scTvAhVmsYsKHcsTAC8QFjAAegQIARAD&url=https%3A%2F%2Fwww.gov.pl%2Fattachment%2Fd39a05b8-f04c-4e7c-93ac-3b5b9946ed0c&usg=AOvVaw2Ngh2B3Pcf1XAUCdeplnnC9> accessed19Ferbruaty 2021

In the case of assessing that the provisions of the GDPR, due to their territorial[39] and material scope[40], will apply to cloud 3.0[41] processing, a lawyer using it must be able to identify (in the light of the provisions of the GDPR) his status, i.e. whether he plays the role of a data controller or perhaps a processor[42]. The answer to this question, although quite clear in the case of cloud 1.0 or cloud 2.0, seems to require a bit more commentary.

According to the Commission Nationale Informatique & Libertés (CNIL), and therefore the French supervisory authority, those users who use blockchain and have the right to decide to transmit data and place it on the blockchain for validation should be considered as data controllers. In particular, the CNIL takes the position that a user will be a data controller when:

1) is a natural person and the processing operation is not strictly personal;
2) he/she is a legal person and enters personal data into the blockchain.

Transferring the above to the LegalTech area, by way of example, it may be pointed out that if a notary registers his client's property deed in a

39 According to Article 3, the GDPR will apply to the processing of personal data in connection with the activities of an establishment of the controller or processor in the EU, regardless of whether the processing takes place in the EU. Further, as stated in paragraph 2, the GDPR applies to the processing of personal data of data subjects residing in the EU by a controller or processor that does not have an establishment in the EU, if the processing activities involve: (1) offering goods or services to such data subjects in the EU, whether or not they are required to pay; or
(2) the monitoring of their behaviour, insofar as that behaviour takes place in the EU. Finally, according to paragraph 3, the GDPR applies to the processing of personal data by a controller that does not have an establishment in the EU but has an establishment in a place where the law of a Member State is applicable under public international law.

40 The GDPR applies to the processing of personal data by fully or partly automated means and to the processing otherwise than by automated means of personal data which form part of a filing system or are intended to form part of a filing system (Article 2).

41 Michèle Finck, 'Blockchain and the General Data Protection Regulation, Can distributed ledgers be squared with European data protection law? ', (2019) Study. European Parliament,

42 Luiz-Daniel Ibáñez, Kieron O'Hara, Eelena Simperl, 'On Blockchains and the General Data Protection Regulation' <www.eublockchainforum.eu/sites/default/files/research-paper/blockchains-general-data_4.pdf> accessed 9January 2021.

blockchain, he will be identified as the data controller[43]. At the same time, the literature on the subject does not lack the opinion that due to the decentralised nature of blockchain and activity based mostly on P2P relations, each user is a controller with regard to the data they enter. Resolving the above, it should be pointed out that the determination of who is the data controller in a given situation will require an individual assessment for each case[44].

In the situation when, within the framework of the assessment of a particular processing process in cloud computing 3.0, there will be grounds to consider that the provisions of the GDPR (due to their territorial and material scope) are applicable and, further, that the lawyer will play the role of a data controller, he will thus be obliged to fulfil a number of obligations that arise from the regulation in question and will further be held liable in the event of their breach.

With regard to the first of the above-mentioned implications, i.e. the necessity to meet the obligations imposed on the administrator, in the case of cloud computing 3.0 satisfying some of them, while not proving impossible, is certainly extremely difficult to achieve in practice. This is because cloud 3.0 will focus, as if through a lens, all those problems and challenges that, on the one hand, are characteristic of cloud 1.0 and, on the other, are characteristic of blockchain, and it is the latter that will be the subject of further considerations.

The first fundamental difficulty seems to be the ability of the lawyer (data controller) to comply with the principle of retention limitation resulting from Article 5.1.e GDPR, according to which data must be kept in a form which permits the identification of the data subject for no longer than is necessary for the purposes for which the data are processed. If this is combined with the feature of blockchain, which implies that data, once stored in blocks, cannot be deleted or modified[45], compliance with the aforementioned obligation seems doubtful. Furthermore, it is not clear how the 'purpose' of the processing of personal data should be understood in the context of blockchain, in particular whether this only includes the initial transaction or whether it also includes further processing of

43 CNIL, 'Blockchain:Solutions for a responsible use of the blockchain in the context of personal data' <https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf> accessed 11 December 2020.

44 Michał Dymiński, Dominik Ferenc, 'GDPR w łańcuchu bloków' (2020) 6 Przegląd Prawa Publicznego 202061.

45 See more: Part IV chapter. 6

personal data (such as their storage and consensus use) once it has been introduced in the chain[46].

In the light of the above statements, it seems obvious to assume that under cloud computing 3.0 it will be difficult to meet the data minimisation principle, which is set out in Article 5(1)(c) of the GDPR and further specified in Article 11. In accordance with them, data should be adequate, used and limited to what is necessary for the purposes for which they are processed. This principle is often associated with the need to quantitatively limit data collection, and in this sense it is difficult to assume that there is a possibility of its implementation in the case of cloud computing 3.0. Alternatively, however, it could be assumed that data minimisation is not so much about the quantity but rather about the quality of data, which means that it would be required that no special categories of data are processed unless absolutely necessary, and that data are pseudonymised or even anonymised whenever possible. However, the possibility of such an interpretation seems irreconcilable in light of Article 25(2) of the GDPR, which provides that the controller shall implement appropriate technical and organisational measures so that, by default, only those personal data are processed which are necessary for each specific purpose of the processing. This obligation relates to the amount of personal data collected, the extent of their processing, their storage period and their availability[47]

The possibility for a lawyer to exercise the right to rectify data referred to in Article 16 of GDPR should also be assessed in an analogous way. How, in the case of the processing of personal data in a computing cloud that operates on the basis of blockchain, would a lawyer exercise this right, since in blockchain it is practically possible to modify the information contained in the blocks? Well, a certain answer to this type of question may be the fact that in certain situations, private or public blockchains nevertheless allow for the possibility of modifying data by, for example, mixing blocks, which should be possible by appropriate technical configuration. Then each user has specific write rights and is entitled to add new blocks which should correct previously placed information[48].

Going further, similar concerns as before may also imply the need for the controller to satisfy the right set out in Article 17 GDPR, i.e. the right to erasure (right to be forgotten). Assuming that the prerequisites of Article 17 GDPR for the admissibility of exercising the right to be for-

46 Finck (n 42) II
47 ibid.
48 Dymiński, Ferenc (n 45)

gotten by the data subject are met, due to both the previously mentioned technical factors characterising blockchain and its governance structure, the possibility of its fulfilment comes into question[49].

Taking into account the above, only exemplarily indicated problems that, in the light of the provisions of the GDPR, may cause the use of cloud computing based on blockchain by a lawyer, it seems justified to pose the question of whether a lawyer should process personal data under cloud 3.0 at all, precisely due to these problems, at least with the implementation of data subjects' rights and, more broadly, compliance with the provisions of the GDPR? It seems that if possible, personal data should be processed off-chain. The chain itself should contain links (hashes) to the document, allowing to verify its authenticity and correctness[50]. This procedure allows avoiding difficulties with the use of dispersed databases in accordance with GDPR, and also simplifies the management of personal data, because the data processed off-chain are stored in a centralised database, which further facilitates the identification of the data controller, which will be the entity storing the data off-chain, or at least enables the rectification and erasure of personal data in the light of Articles 16 and 17 of GDPR. Importantly, such register still needs to comply with the GDPR and every lawyer should bear this in mind.

However, if the rights referred to in Articles 16 and 17 GDPR are exercised in the framework of centralised data outside the blockchain, the question of what status will be given to the remaining hash, which after all will still remain in the blockchain, is still open. In this regard, it will need to be determined whether this hash will fall within the category of personal data and enable the identification of the data subject. However, as indicated in the literature, determining the above is an extremely complicated process today. Therefore, until at least a guideline or recommendation is issued on this subject, a lawyer should be aware of the existence of this doubt[51].

Moreover, it should be noted that the previously mentioned possibility to store data off-chain does not apply to public keys.

Although storing personal data outside the blockchain seems to be a certain remedy for the previously mentioned potential risks of non-compliance with GDPR, it should be realised that this solution is not without its drawbacks. The consequence of applying this solution will be a situation

49 Fábio Coelho and George Younes, 'The GDPR-Blockchain paradox: a work around' (W-GCS'18 2018: 1st workshop on GDPR compliant systems, co-located with 19th ACM international middleware conference, Rennes, 2018).

50 Dariusz Szostek, Blockchain and the Law (1 ed., Nomos 2019)109-110.

51 Michèle. Finck (n 42) 32.

in which it is the personal data that will be centralised. Thus, if a failure occurs, the data may be irretrievably lost, as it will not be possible to reconstruct them on the basis of a hash. Moreover, the availability failure (intentional or not) may disrupt the entire data processing, bringing us back to the problem whose solution motivated the blockchain developers[52].

4.2. Smart Contract and Personal Data

The previously presented considerations concerning the processing of personal data in blockchain-based cloud computing would not be complete without reference to issues related to smart contract[53]. Indeed, the combination of blockchain and smart contract is the most classic model of their functioning[54]. This in turn, from a lawyer's perspective, implies questions about the correlation between the provisions of GDPR and the smart contract. And although, as rightly pointed out in Part IV, Chapter 7, for most lawyers dealing with the machine language in which the smart contract is written may involve the need to cooperate with programmers, nevertheless, the need to know what legal consequences - including those related to the protection of personal data - will be triggered by running an algorithm in a smart contract will be on the side of the lawyer. And these consequences are not lacking.

Above all, practitioners need to be aware that it is the European data protection framework shaped by the GDPR provisions that will be one of the decisive factors in determining the extent to which smart contracts can be used in the EU[55]. Although smart contracts have so far attracted the attention of legal practitioners mainly in the context of contract law, it should be noted that although a smart contract is not always a contract in the legal sense, it may - and this will be further analysed - more often than not involve the automated processing of data, including personal data, which directly raises various implications under the GDPR[56].

---

52 Luiz Daniel Ibáñez,Kieron O'Hara, Eelena Simperl (n 43)

53 More on smart contracts in Section Three 'Smart Contracts, Blockchain and Distributed Ledger Technology'
(DLT) in the Work of a Lawyer.

54 Marlena Pecyna, Adam Behan, 'Smart contracts — nowa technologia prawa umów?' (2020) 3 Transformacje prawa prywatnego 189.

55 Michèle Finck, 'Smart Contracts as a Form of Solely Automated Processing under the GDPR', (2019) 9(2) International Data Privacy Law 78.

56 ibid.

Article 22(1) of the GDPR provides that the data subject has the right not to be subject to a decision which is based solely on automated processing, including profiling, and which produces legal effects concerning him or her or significantly affects him or her in a similar manner. Thus, as aptly assumed by Ms Finck, in order to assess whether smart contracts are covered by this provision, it must be determined whether they are considered a decision based solely on automated processing and whether the decision produces legal effects on the data subject or otherwise significantly affects the data subject[57].

With regard to the question of understanding how - in the context of smart contracts and for the purposes of Article 22 GDPR - 'decision making' should be interpreted, the literature proposes two alternative possibilities. Firstly, the execution of a smart contract code following the occurrence of a predetermined event may be considered as a 'decision'. According to the nature of smart contracts, there is no human involvement at the 'decision' stage, which means that Article 22(1) applies in this situation. Secondly, it is also possible to consider that the concept of 'decision' will encompass a broader time scale and thus the initial decisions that led to the smart contract. Indeed, in many circumstances people will agree on the purpose and configuration of the smart contract. Sometimes a human will act as an , "oracle", giving the smart contract the inputs needed to make it work. In addition, a human agent is also needed to translate human intentions into computer code. When the smart contract is combined with a contract, the 'decision' can also be equated with preliminary contractual negotiations. Such an understanding of the concept of decision in the context of Article 22 GDPR would certainly be accepted by those who care about excluding the application of the said GDPR standard. However, this scenario is unlikely if one considers that Article 22(2) contains an explicit exemption from the prohibition in Article 22(1) where a smart contract is used for the performance of a contract. If human involvement in the development of the contract were to be taken into account for the purposes of paragraph 1, there would be no need for an explicit exemption to this effect in paragraph 2. Hence, taking into account the wording of Article 22 of the GDPR, it can be concluded that the , "decision" for the purposes of Article 22(1) is probably only the final execution of the code, which actually takes place without direct human involvement. It can therefore be concluded that smart contracts, at least in certain circumstances, fall under Article 22(1) GDPR. On the other hand,

57 ibid.

as regards the determination of whether the decision produces legal effects for the data subject or otherwise significantly affects the data subject, it is worth emphasising, on the basis of the meticulously conducted analysis by M. Finck, that such a scenario is not excluded either, if only when smart contracts decide whether an insurance premium is paid, consumer rights are enforced or payment for goods or services is made[58]. According to the author, this leads to the conclusion that smart contracts may not comply with the GDPR in this respect and that this fact should be taken into account when designing them.

Moreover, when analysing possible correlations between GDPR provisions and smart contracts, the lawyer should take into account the fact that the scope of application of these provisions will be determined by the ecosystem in which the smart contract operates. If we are dealing with an open ecosystem, the specificity of which is the transfer of data from external sources, then questions may arise in the context of personal data protection law, i.e. in particular whether an agreement on entrustment of processing should be concluded, subcontracting or perhaps we are dealing with co-management. Obviously, giving an unambiguous answer to this question seems to go far beyond the framework of this paper, and moreover, it depends on the factual circumstances, nevertheless, it is important for a lawyer to be aware of this type of coincidences

In the light of the above mentioned implications, which may arise at the junction of data protection law and smart contracts, the question of how a lawyer should find himself in this "reality" seems to be without a single exhaustive answer. Nevertheless, it seems interesting to draw attention to an idea presented by M. Corrales, P. Jurcys and G. Kousiouris, who proposed to apply the so-called smart disclosure strategy[59]. These authors point out that while a typical contract is written using natural language, smart contracts are written in computer code using special programming languages. Such languages use strict algorithms and can be very complicated for non-programmers, including lawyers. Therefore, as a solution, they proposed a pseudo-code process, which is an intermediate step between planning and programming. It is basically a step-by-step code outline that can later be rewritten into any programming language. The purpose of pseudo-code is to simplify operations, instead of using a real programming

58 ibid.

59 Marcelo Corrales, Paulius Jurčcys and George Kousiouris, 'Smart Contracts and Smart Disclosure: Coding a GDPR Compliance Framework' in Marcelo Corrales, Mark Fenwick and Helena Haapio (eds), Legal Tech, Smart Contracts and Blockchain (Springer 2019) 189.

language with a complex syntax. The proposed pseudocode follows a programming logic that allows the implementation of legal concepts in the user interface and related systems. It has been developed to comply with the requirements of the GDPR, as the pseudo-code project includes a set of specific legal and technical questions.

And it is the need to answer these questions that aims to , "intelligently disclose" the relevant information so that, in effect, cloud service providers make the necessary changes to SLAs and the underlying software, compliant with GDPR, which could further be used in the blockchain sphere as a piece of code along with the normal blockchain code. M. Corrales, P. Jurcys and G. Kousiourisza proposed a list of the following questions:

1) are personal data/special category data referred to in Article 9 of the GDPR subject to processing?
2) is the processing subject to encryption/authentication?
3) is it possible to choose the location where the data will be processed?
4) is the processing (e.g. within a SaaS service) dynamically configured to use IaaS/PaaS services?
5) are the "ownership" rights of the data or metadata clearly defined and explained in the contract/SLA?
6) does the provider undertake to notify if the terms of the contract change?
7) does the provider commit to notify in case its underlying PaaS/IaaS provider changes the terms of the contract?
8) does the provider enable "greater virtual control" of the data, ensuring data portability and interoperability within the cloud?
9) does the provider commit to exercise the right to erasure of data in the originally used service?
10) does the provider declare that its subcontractor offering PaaS/IaaS services applies standard contractual clauses?
11) does the provider apply measures to prevent data loss (regular backups, etc.)?
12) does the provider use its own resources to run the application?

4.2 Cloud Computing and Electronic Communications

The issue of using cloud computing services by a lawyer in his or her daily practice is inextricably linked with the subject of electronic communication. This is because cloud computing is an excellent tool for changing the mode of communication from "on paper" to electronic. While initially

the above was associated mainly with the use of electronic mail in the communication process, currently, due to the increasingly advanced communication tools based on cloud computing, there is a paradigm shift in this respect. If the subject of such communication is also personal data, and other prerequisites are met (e.g. territorial or substantive scope of the GDPR), then the provisions of the GDPR will be applicable, which will thus create obligations on the part of the lawyer, first of all, to identify in which role (in the light of the provisions of the GDPR) he/she acts, and further, what obligations, scope of responsibility, etc. he/she will have in connection with it. And the possible scenarios in this context can be multiplied.

As already mentioned in Part VI, Chapter 1, it is becoming more and more common to use cloud computing not for data transmission, but for making data available to authorised or entitled entities. Moreover, this is also increasingly taking place using cloud computing 3.0

Although the provisions of GDPR lack the legal definition of making available, there should be no doubt that it is one of the forms of personal data processing. The disclosure shall take place whenever the data are taken into possession by the data recipient, who then becomes the controller of personal data, whereas it is essential that the controller of data allows another person or entity, which will act as the data controller, to get familiar with such data. The very "making available" of the data shall be of a factual nature and may be effected in any way, as long as the result of the activity is to enable another entity to gain an actual access to and authority over the data[60].

Thus, in the case where, for example, between lawyers there will be a sharing of data just within the framework of electronic communication undertaken with the use of cloud tools, the lawyer (both the one who shares personal data and the one to whom the data have been shared) should consider the legal consequences of that. The lawyer who makes the data available must fulfil the obligation to have an appropriate legal basis to make the data available, verify whether the entity to which the data is made available has been specified within the information obligation referred to in Article 13 of the GDPR. Moreover, also the form in which such personal data will be made available should meet the requirements of personal data security referred to in GDPR, for example through the

60 Paweł Barta and Maciej Kawecki in Paweł Litwiński (ed), *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz* (C. H. Beck 2018) 202-203.

aforementioned encryption. On the other hand, the lawyer who gains access to such data and has 'authority' over it, will - in the light of the provisions of the GDPR - act as a personal data controller, with all the implications of this that have already been mentioned above, such as the need to fulfil a number of duties, or to guarantee the data subjects the exercise of their rights[61].

In the event that cloud computing tools are used by lawyers to communicate within the organisational structure of which they are a part, then there will be no sharing of personal data in the shape discussed earlier. Thus, if, for example, lawyers - employed in different departments, but within the same organisation - communicate with one another and share data under the cloud computing, then not they themselves, but their organisation will still act as a data controller. Moreover, the situation of transferring data to the entity to which the processing of personal data has been commissioned cannot be treated as sharing either, because in such a case it will be the processor. Therefore, with regard to the use of cloud computing by lawyers, it should be concluded that the provider of the services we are interested in will be the procesor.

The above scenario should be distinguished from the situation, where in the process of personal data processing there are involved at least two lawyers (from other organisations), who for the purposes of communication interact with each other and who jointly determine the purposes and means of the processing[62]. Then, in accordance with Article 26 of GDPR, we will be dealing with co-management of personal data - which will furthermore give rise to various legal obligations on their side, both in a purely internal relationship (i.e. between them) and in an external context (i.e. in relation to the data subject, but also to the supervisory authority)[63].

First of all, pursuant to Article 26 of GDPR, the lawyers should, by way of joint arrangements, clearly determine the scope of their responsibility for the performance of obligations under GDPR, as well as set out the principles for the exercise of data subjects' rights. And although the GDPR provisions do not provide guidance on the form of the arrangements in question, it is worth emphasising that the form should be such that the

61 ibid.

62 It is the joint formulation of the purposes and means of processing that will be the sine qua non for it to be possible to speak of co-management rather than entrustment of processing.

63 Katarzyna Witkowska-Nowakowska in Edyta Bielak-Jomaa and Dominik Lubasz (eds), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz* (Wolters Kluwer 2018) 612-622.

obligation to make the contents of those arrangements available to the data subject can be implemented. Therefore, it is reasonable to assume that it should be a written form, including an electronic one. On the other hand, the division of duties made by them - as postulated in the doctrine - should be as transparent and clear as possibile[64].

5. Summary

The analysis conducted above makes it necessary to conclude that just as it is natural nowadays for lawyers to use cloud computing solutions in their everyday activity, it should also be natural to identify the above with the provisions of the personal data protection law. And although it may also be assumed that in certain factual situations the aforementioned processing processes will not be covered by the provisions of GDPR, the very fact that such an assumption cannot be excluded a priori in relation to all situations requires the lawyer to be very careful when using these tools within his or her own activity. This task, as demonstrated earlier, appears to be difficult for at least two reasons. First and foremost, with the evolution of cloud technology itself, the challenges that any lawyer will face under data protection law have changed and, it is fair to assume, will continue to change. This is perfectly illustrated by the example of cloud computing 1.0 or 3.0.

Moreover, due to a number of different types of variables (such as the categories of personal data to be processed, the purpose of the processing, etc.) the legitimacy of the methodologies applied should always be assessed by the lawyer through the prism of his/her own organisation, i.e. on a case-by-case basis. This makes it impossible to indicate one "golden mean" in this respect.

It seems, however, that if a lawyer is familiar enough with the specificity of cloud computing technology to be able to identify the problems that its application may pose in the light of the GDPR regulations (as discussed above) and juxtaposes that with the methodology of implementing LegalTech solutions as such (as discussed in Part V), the risk of violating GDPR regulations, and thus being exposed to liability, will be lower.

64 ibid..