Leibniz University in Hannover

Cloud Computing and Reform of the Data Protection in European Union

Changes and new duties for cloud service providers

Gabriela Sváčková

Supervisor: Ioannis Revolidis, LL.M.

EULISP 2015/2016

Date of submission: 29 August 2016

Declaration of Authorship

I hereby affirm that this Master thesis is my own work and effort and that it has not been submitted anywhere else for any award. Where other sources of information have been used, they have been duly acknowledged.

In Prague, 29th August 2016

Gabriela Sváčková

1 Table of content

2 List of Abbreviations

Art.	Article
Board	European Data Protection Board
CJEU	Court of Justice of European Union
CSP	Cloud Service Provider
Charter	Charter of Fundamental Rights of the European Union
Directive 95/46/EC	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
EU	European Union
FTC	U.S. Federal Trade Commission
IP	Intellectual property
Para.	Paragraph(s)
GDPR or General Data Protection Regulation	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)
The WP29	Article 29 Working Party

3 Introduction

The area of modern technology has experienced an unprecedented growth in the last decades. This growth will not definitely stop in the coming years, more like the exact opposite. The world has become digital and information and data are the objects for trade. People are mobile and want access their data without taking any memory device with them. They do not have to, because cloud service providers provide us with enough space for our data.

Nevertheless, the law is rigid and legislative procedures are so slow that they cannot keep the step with the development in this area. Therefore, basic human rights have become endangered. Especially one of the fundamental rights - right to the protection of personal data enshrined in article 8 of the Charter of the Fundamental Rights of the European Union (hereinafter referred as "Charter") in connection to right to respect for one's private and family life, home and communications.[1]

The basis of the right to the protection of personal data concerning an individual lays in the principle, that personal "data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law." Moreover, according to the Art. 8 of the Charter, "everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified." And the compliance is to be controlled by the independent authority.[2]

The 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 (hereinafter referred as "Directive 95/46/EC") is based on the principles enshrined in the Charter and it has worked for 14 years than the work on new regulation began in 2009.[3]

Meantime, the Court of Justice of European Union (hereinafter referred as „CJEU") gave us several major indication, that the protection of personal data in the European

[1] Art. 7 of the Charter of Fundamental Rights of the European Union. OJ C 326, 26.10.2012, p. 391–407.
[2] Art. 8 of the Charter.
[3] Paul de Hert, Vagelis Papakonstantinou. The new General Data Protection Regulation: Still a sound system for the protection of individuals? Computer Law & Security Review 32, 2016. Page 181.

Union is not to be a mere phrase, but quite the contrary. The broad interpretation of the terms “processing” and “controller” followed by the establishing of “right to be forgotten” and invalidation of Safe Harbor Framework for EU –U.S. transfer of the personal data let people know that in Europe the right to privacy is one of the most important human right that deserve the high level of protection, especially in the online environment of the medium as Internet.

Because of this approach and development, soon it became clear that the Directive 95/46/EC has to be replaced as insufficient mean of protection. Thus, the 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 (hereinafter referred as „GDPR“ or „General Data Protection Regulation”) should be technology neutral and this seems to be the good direction of legislative process.

The GDPR contains several provisions that will have significant impact on the Cloud Service Providers (hereinafter referred as „CSP”), for instance by the extending of the obligations of processors or one-stop-shop mechanism.

The goals of this master thesis is to analyse new General Data Protection Regulation, identify the changes for CSP and assess whether the changes provide better protection of individuals with regard to the data they upload to the cloud.

To achieve these goals, I will firstly briefly define the used terms and explain the differences between controller and processor (since the role of CSP reflects to its obligations). In the main part of the thesis I will go through the GDPR provisions and detect the changes in comparison with the Directive 95/46/EC. For the sake of clarity, my thesis contains references to the provisions of the selected CSP Privacy Policy or of the Terms of Service directly in the respective chapter or sub-chapter.

Further, since the issuance of judgement in the Lindquist case, the processing of data is very broad when the sole operation of loading personal data on an internet page must be considered to be processing in the meaning of the Directive 95/46/EC.[4] The general approach of the CJEU and EU institutions in the last few years was to

[4] Case C-101/01. *Bodil Lindqvist*. [2003 I-12971]. Para 25.

broaden overall the protection of individuals with regards to their data. Therefore, the responsibility of stakeholders grows and is burdened with more burdensome sanctions. I discuss this fact in the last chapter of this master thesis.

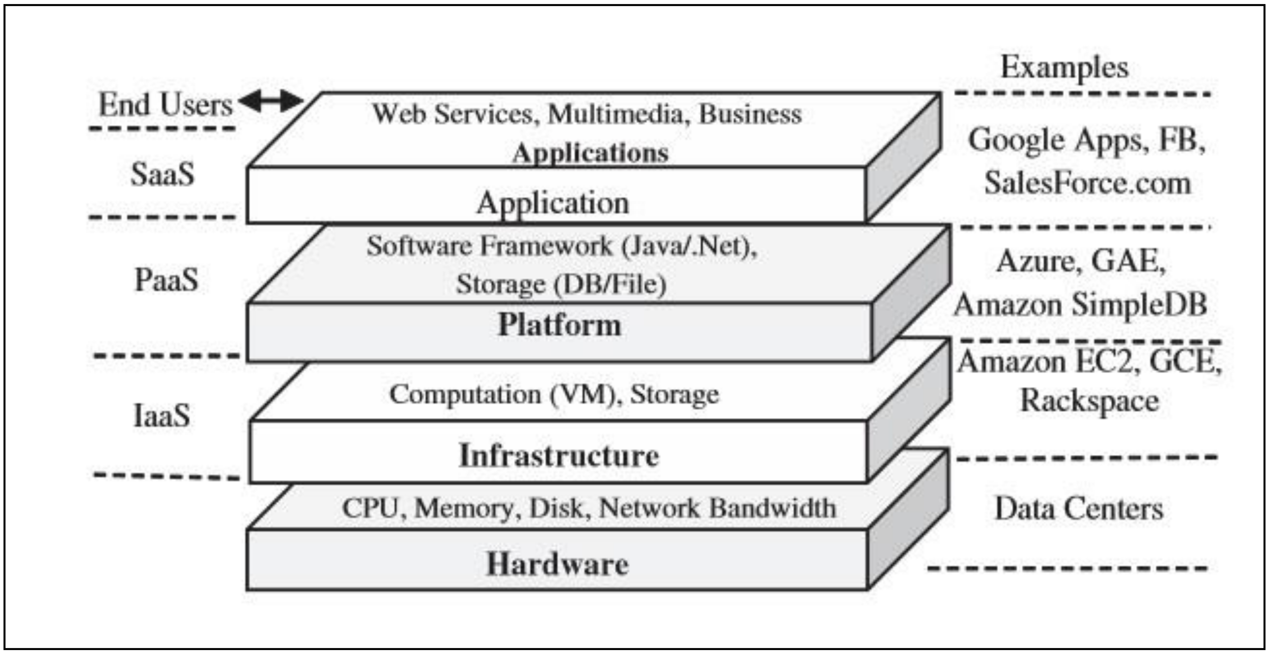
Finally, I provide the conclusion of my findings at the end of the thesis.

4 Cloud Computing

4.1 Cloud Computing in general

Cloud computing is defined in International Standard ISO/IEC 17788:2014(E) Information technology as a paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.[5]

According to the provided services and cloud architecture stakeholders initially distinguished three basic categories of cloud services: Software as a Service, Platform as a Service and Infrastructure as a Service. The following picture clearly represents the differences and provides for the examples of CSP.



Picture No. 1 Cloud Computing Architecture[6]

[5] International Standard ISO/IEC 17788:2014(E) Information technology — Cloud computing — Overview and vocabulary. Page 4.

[6] Md Hasanul Ferdaus, Manzur Murshed. Energy-Aware Virtual Machine Consolidation in IaaS Cloud Computing in Zaigham Mahmood (ed.) *Cloud Computing. Challenges, Limitations and R&D Solutions.* Springer 2014. Page 183.

4.2 Cloud service categories

Soon, it was clear that the needs of the market are much bigger and the development gave the clause to the creation of new categories of cloud services. Therefore, the International Standard ISO/IEC 17788:2014(E) currently describes following categories:

A) “Communications as a Service (CaaS): A cloud service category in which the capability provided to the cloud service customer is real time interaction and collaboration;

B) Compute as a Service (CompaaS): A cloud service category in which the capabilities provided to the cloud service customer are the provision and use of processing resources needed to deploy and run software;

C) Data Storage as a Service (DSaaS): A cloud service category in which the capability provided to the cloud service customer is the provision and use of data storage and related capabilities;

D) Infrastructure as a Service (IaaS): A cloud service category in which the cloud capabilities type provided to the cloud service customer is an infrastructure capabilities type;

E) Network as a Service (NaaS): A cloud service category in which the capability provided to the cloud service customer is transport connectivity and related network capabilities;

F) Platform as a Service (PaaS): A cloud service category in which the cloud capabilities type provided to the cloud service customer is a platform capabilities type;

G) Software as a Service (SaaS): A cloud service category in which the cloud capabilities type provided to the cloud service customer is an application capabilities type.”

The CSP will always have to consider very carefully, which of the above described scenarios apply in the respective relationships, as the privacy risks differ in each context. Moreover, the assessment has to include not only the role of the CSP, but also what types of data he does process; while some categories require more protection than others in the wording of the GDPR according to Art. 9 of the GDPR (the same apply already the Directive 95/46/EC).

In this master thesis I focus mostly on the Software as a Service relationship, as it is the most common one. When another scenario is discussed, it is clearly stated in relevant subchapter.

4.3 Cloud deployment models

For the purpose of the further analysis, I have to describe also cloud deployment models. These represent how cloud computing can be organized based on the control and sharing of physical or virtual resource, what has effect also on the responsibilities of the individual stakeholders. The cloud service community recognizes:

A) Public cloud: "Cloud deployment model where cloud services are potentially available to any cloud service customer and resources are controlled by the cloud service provider. A public cloud may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud service provider. Actual availability for specific cloud service customers may be subject to jurisdictional regulations. Public clouds have very broad boundaries, where cloud service customer access to public cloud services has few, if any, restrictions".

It is clear from this explanation, that public cloud is the most fragile concerning data privacy threats. But it is very popular among the customers particularly because of the lower price. Cloud service is available for large number of customers, which does not require specific performance as in the private cloud.

However, before the customer decides to use this deployment model, he has to determine, whether this deployment model is the best for "his" data, especially, when he act as the data controller and CSP acts on his behalf as the processor. For instance, sensitive data[7], data leakage and loss of privacy are of particular concern to users when sensitive data is processed in the cloud. When the CSP process these kinds of data, public cloud deployment model is not the proper one to use. The customer acting as the

[7] See to this effect art. 9 of the GDPR.

controller of the data, has to comply with all his obligations as provided in the data protection law. So, even though the public cloud is the most commonly used model, because of the money saving issue, “relying on a CSP to manage and hold one’s data in such an environment raises a great many privacy concerns.”[8]

B) Private cloud: “Cloud deployment model where cloud services are used exclusively by a single cloud service customer and resources are controlled by that cloud service customer. A private cloud may be owned, managed, and operated by the organization itself or a third party and may exist on premises or off premises. The cloud service customer may also authorize access to other parties for its benefit. Private clouds seek to set a narrowly controlled boundary around the private cloud based on limiting the customers to a single organization.”

The advantage of this cloud deployment model is more control in the hands of customer. The customer sets the rules about access to the cloud and privacy policy. This luxury usually increases the price.

C) Community cloud: “Cloud deployment model where cloud services exclusively support and are shared by a specific collection of cloud service customers who have shared requirements and a relationship with one another, and where resources are controlled by at least one member of this collection. A community cloud may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises. Community clouds limit participation to a group of cloud service customers who have a shared set of concerns, in contrast to the openness of public clouds, while community clouds have broader participation than private clouds. These shared concerns include, but are not limited to, mission, information security requirements, policy, and compliance considerations”;

D) Hybrid cloud: “Cloud deployment model using at least two different cloud deployment models. The deployments involved remain unique entities but are bound together by appropriate technology that enables interoperability, data portability and application portability. A hybrid cloud may be owned, managed, and operated by the organization

[8] Siani Pearson. Privacy, Security and Trust in Cloud Computing in Pearson Siani, Yee George (ed). *Privacy and Security for Cloud Computing.* Springer, 2013. Page 15.

itself or a third party and may exist on premises or off premises. Hybrid clouds represent situations where interactions between two different deployments may be needed but remained linked via appropriate technologies. As such the boundaries set by a hybrid cloud reflect its two base deployments."[9]

This last cloud deployment model provides the possibility to combine the requirements of the customer available in different deployment models. It is very convenient for the customer, as the final model meets all his needs. But it also puts the burden of responsibility on parties regarding the proper settings about privacy. Where they enable sharing of the data, the proper measures must be taken in order to fulfil their obligations as data controllers/processors.

[9] International Standard ISO/IEC 17788:2014(E) Information technology — Cloud computing — Overview and vocabulary. Page 6 and 7.

5 Cloud Service Providers

Every one of us uses cloud services in our everyday life. It starts with email and ends with backup of pictures, documents, etc. The general definition of Cloud Service Provider is “a party which makes cloud services available”[10].

5.1 Controller or Processor

The obligation set for the service providers differ at some aspects according to the fact, whether the service provider acts as a controller or processor of data. The different level of responsibility then applies. [11]

The GDPR provides the definitions of both terms in Art. 4. So, the ‘controller’ means “the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law”, whereas the ‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller”.

Nevertheless sometimes it could be very difficult and problematic to determine the real role of the CSP, when and for which purposes he acts as the data controller and when as data processor. In most common situations, CSP usually behave as data processors, which process personal data on behalf of data controller (who is its customer). However, is case the “providers process data for their own purposes, they would be or become data controllers. Regulators also treat cloud providers as data controllers when they provide social networking services.”[12]

[10] International Standard ISO/IEC 17788:2014(E) Information technology — Cloud computing — Overview and vocabulary. Page 3.

[11] Opinion 1/2010 on the concepts of "controller" and "processor” of Article 29 Data Protection Working Party, No. 00264/10/EN, WP 169, adopted on 16 February 2010. Available:< http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf > Last accessed July 10, 2016.

[12] Dimitra Kamarinou, Christopher Millard and W. Kuan Hon. *Cloud privacy: an empirical study of 20 cloud providers’ terms and privacy policies—Part I.* International Data Privacy Law, 2016, Vol. 6, No. 2. Page 81.

The Directive 95/46/EC imposes the direct statutory obligations only to controllers. Thus, in case CSP acts as a processor via a contract with the controller, he shall be held liable only for breach of such contract. However, the Directive 95/46/EC sets no statutory obligation on processor, national laws can do so. For instance, Slovak data privacy act. [13] Czech data privacy act[14] impose sanctions to the processors as well as the controllers. These sanctions are fines according to the seriousness of the administrative delict.

On those examples, it is possible to observe how differently the Directive has been implemented into national laws. In Slovakia, controllers are obliged to create a security project in accordance with the requirements set for in Decree of the Office for Personal Data Protection of the Slovak Republic.[15]

The project shall be really detailed and contain information about physical, as well as virtual security measures. Adoption of the security project is an expression of the objective of the Controller's company management to meet regulatory requirements and to protect the legitimate interests of stakeholders in any activity at which the processing of personal data take place. Moreover, Controller usually intends to ensure stable, controllable and manageable security in processing of personal data in accordance with the Data Protection Act to the greatest possible extent possible in the conditions of the Controller's company.

The existence and regular update of the security project is regulated by the law and regularly subject to control from the Office for Personal Data Protection.

Whether CSP is processor or controller will depend on the type of cloud service provided. In order to fulfil all obligations requested by GDPR, CSP must first determine how he acts in respective relationship. For instance, Apple clearly states in its Privacy Policy:

[13] Act No. 122/2013 Coll. on Protection of Personal Data and on Changing and Amending of other acts, resulting from amendments and additions executed by the Act. No. 84/2014 Coll. Accessible at: < http://www.dataprotection.gov.sk/uoou/sites/default/files/kcfinder/files/Act_122-2013_84-2014_en.pdf > Last accessed: 14 May 2016.

[14] Act No. 101/2000 Coll., on the Protection of Personal Data and on Amendment to Some Acts, as amended. Accessible at: < https://www.uoou.cz/en/vismo/zobraz_dok.asp?id_ktg=1107 >. Last accessed: 14 May 2016.

[15] Decree no. 117/2014 which amends Decree no. 164/2013 of the Office for Personal Data Protection of the Slovak Republic on an extent of a safety measures documentation.

“Please note that personal information, including the information provided when using iCloud, regarding individuals who reside in a member state of the European Economic Area (EEA) and Switzerland is controlled by Apple Distribution International in Cork, Ireland, and processed on its behalf by Apple Inc. Personal information collected in the EEA and Switzerland when using iTunes is controlled by iTunes SARL in Luxembourg and processed on its behalf by Apple Inc.”[16]

[16] The Apple Privacy Policy. Available at: < https://www.apple.com/uk/privacy/privacy-policy/>. Last accessed: 24 August 2016.

6 General comments on Privacy Policies of CSP

While I was reading the Privacy Policies of Selected CSP for the purposes of this thesis, I have noticed that all of them are trying to make them understandable for users, who are not data privacy experts. This is of course plausible approach, after all, it is a part of the transparency principle to communicate with data subjects in clear and plain language[17], but it can also have negative consequences. From the wording of these texts, it could be perceived that when users/individuals make any information publicly available, for instance by posting, they lost control over them and everybody can do what they want with it. But nothing, not even public disclosure, change the status of personal data.

According to the definition in Art. 4 of the GDPR „'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

Once the data fulfil this definition, it gets the protection with all the principles of data protection law applicable. The understanding of what constitutes personal data is more or less clear between the CSP – they refer to identification of the person.

What I find as a shortcoming in all of the Privacy Policies I have come across so far, is that they do not provide any information what happens in the situation where two or more information that themselves do not lead to identification of individual, but in combination they do. Of course, all data privacy principles will apply including the purpose limitation principle. So in the above case, the CSP may use the data only for the purposes the original (non-identifiable) data were obtained.

Moreover, as some of other scholars observe, in the line of education public with the data privacy awareness, I would appreciate the CSP (and all other controllers/processors) to include in their privacy policy the clause explaining, that making the personal data available publicly "does not affect the statutory right under data protection law". It would be considered a good "practice in the spirit of consumer protection law" too.

[17] See recital 39 of the GDPR.

For instance, Google says: “Many of our services let you share information with others. Remember that when you share information publicly, it may be indexable by search engines, including Google.”[18] Likewise, explaining to the customers that if they use the personal data collected online, that are personal data, they are obliged to follow applicable data protection law, in case they are acting as data controllers.[19]

[18] Information you share. Available at: <https://www.google.com/intl/en/policies/privacy/>. Last accessed 24 August 2016.

[19] Dimitra Kamarinou, Christopher Millard and W. Kuan Hon. Cloud privacy: an empirical study of 20 cloud providers’ terms and privacy policies—Part I. International Data Privacy Law, 2016, Vol. 6, No. 2. Page 86.

7 The GDPR analysis

7.1 The Scope

In comparison with Directive 95/46/EC the territorial scope has been extended in the GDPR. Even bigger emphasis is given to the data subject and therefore, pursuant to Art. 3 the GDPR applies to the non-EU controllers or processor if (i) they solely monitor the behavior of data subject taking place in the EU or if (ii) they offer their goods or services to the data subject in the EU. Furthermore, without respect whether the payment of the data subject is required.[20]

7.2 Lawfulness of processing

Art. 6 of the GDPR did not change the conditions for assessment whether the processing is lawful.[21] Thus, the processing of personal data is considered lawful only in case "(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

7.2.1 Consent of the data subject

CSP usually rely on the consent of data subject given during the registration process or during the entering into the contract (litera a) or b)). But GDPR now provides specified conditions for data subject consent in Art. 7. This article should be read with the recital 42

[20] See also recitals 22, 23 of the GDPR.
[21] Compare also recitals 42-47 of the GDPR.

in mind: “Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC[22] a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.“

In accordance with the wording of the recital 42, the data subject shall have the right to withdraw his or her consent at any time without more effort than when the consent was given. Moreover, in case the consent as written declaration constitutes an infringement of the GDPR, it is not binding for the data subject pursuant to Art. 7 (2).

7.2.2 Child’s consent

The GDPR further formulates the rule, that only at least 16 years old children can give necessary consent to process his/her data. Where the child is below the age of 16 years, the consent has to be given or authorised by the holder of parental responsibility over the child. The age limit for those purposes may be lower by the law of Member States but provided that the age is not below 13 years.[23]

I welcome this provision, as it covers the common situations where children do not perceive the consequences their actions online can have. Therefore, they need to be protected in bigger extent.

At this point it should be noted that many CSP already have in their Privacy Policy or terms of use different age limit for the use of their service. For instance, Google states age limit according to the country. If a user wants to own a google account, and comes from United States, he has to be at least 13 years old. Spanish or South Korean users have

[22] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, OJ L 095 , 21/04/1993 P. 0029 – 0034.

[23] Art. 8 of the GDPR.

to be at least 14 years old, whilst user from Netherlands at minimum 16 years old and users form all other countries 13 years old or older. [24] This policy reflects the age requirement imposed by the US Children's Online Privacy Protection Act (COPPA), which does not permit the online collection of personal information from children under the age of 13.[25]

Another example how to handle age limit gives Facebook with the possibility to report the user, which is under the age of 13. Facebook than investigates the Timeline of the user and can cancel the account.[26]

7.3 Information obligation

Both the Directive 95/46/EC and the GDPR impose the information obligation on the data controller. In order to use the service, users are usually required to provide some information, sometimes even the sensitive ones. But the mere information about the category does not make the processing lawful. It was common, that service providers often asked for data they did not really needed for the proper functioning of the service, despite the principle of purpose limitation, which basically prohibits it. Aware of this fact, the authorities came up with more principles and obligations of service providers, which are to be followed to ensure adequate protection of data and CSP has to bare them in mind.

7.3.1 Information to be provided where personal data are collected from the data subject

The information obligation pursuant to Art. 10 and 11 of the Directive 95/46/EC has been extended in the Art. 13 of the GDPR. Now, excerpt for the identity of the controller and his representative, should be provided also contact details of controller and (where applicable) data protection officer. Further, the purposes of the processing for which the data are intended, and newly also legal basis for the processing shall be given. In case

[24] Age requirements on Google Accounts. Available at: <https://support.google.com/accounts/answer/1350409?hl=en >. Last accessed: 23 August 2016.

[25] Dimitra Kamarinou, Christopher Millard and W. Kuan Hon. Cloud privacy: an empirical study of 20 cloud providers' terms and privacy policies—Part I. International Data Privacy Law, 2016, Vol. 6, No. 2. Page 83.

[26] Report an Underage Child. Available at: < https://www.facebook.com/help/contact/209046679279097>. Last accessed 23 August 2016.

processing is based on point (f) of Article 6(1) of the GDPR, the legitimate interests pursued by the controller or by a third party have to be provided. Further, the information about the recipients or categories of recipients of the personal data, if any (in Directive 95/46/EC this obligation was imposed only in situation where data have not been obtained from the data subject).

The CSP providers usually fulfil this obligation in “With whom (we share your data)” sections of the Privacy Policies. For instance Dropbox says: “Dropbox uses certain trusted third parties to help us provide, improve, protect, and promote our Services. These third parties will access your information only to perform tasks on our behalf and in compliance with this Privacy Policy.”[27]

Sometimes, CSP think also about the changes in company structure, such Facebook did: “If the ownership or control of all or part of our Services or their assets changes, we may transfer your information to the new owner.”[28]

At last, where applicable, the fact that the controller intends to transfer personal data to a third country or international organization and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

Moreover, to comply with the fair and transparent processing principle, the additional information according to paragraph 2 are to be provided. For instance, the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.

The most of the CSP do not inform the data subject about the exact period of time, because they simply cannot determine it in advance. For instance Apple says: “We will

[27] Others working for Dropbox part of the Dropbox Privacy Policy.

[28] New owner part of The Facebook Data Policy.

retain your personal information for the period necessary to fulfill the purposes outlined in this Privacy Policy unless a longer retention period is required or permitted by law."[29]

Dropbox uses similar wording: "We'll retain information you store on our Services for as long as we need it to provide you the Services. If you delete your account, we'll also delete this information. But please note: (1) there might be some latency in deleting this information from our servers and back-up storage; and (2) we may retain this information if necessary to comply with our legal obligations, resolve disputes, or enforce our agreements." [30]

Further information to be provided include: (b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability; (c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal; (d) the right to lodge a complaint with a supervisory authority; (e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; (f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

It is clear that every controller is now forced to review its terms of service to make sure, that he provides all the information required by the GDPR. My online research shows that almost no CSP fulfils this extended information obligation now. CSP have

[29] Integrity and Retention of Personal Information in the Apple Privacy Policy. Available at: <https://www.apple.com/uk/privacy/privacy-policy/>. Last accessed: 24 August 2016.

[30] Retention in The Dropbox Privacy Policy. Available at: < https://www.dropbox.com/privacy>. Last accessed 25 August 2016.

time to make their terms compliant till 25 May 2018, when it shall apply in the whole EU.[31]

7.3.2 Information to be provided where personal data have not been obtained from the data subject

In comparison with the situation where the personal data are obtained directly from the data subject, in case they are obtained from third person, the controller must in addition provide the data subject with the information about the categories of personal data concerned.[32]

7.4 Accountability

The principle of accountability was specified and expanded. While Directive 95/46/EC did not use the word accountability, when it stated "it shall be for the controller to ensure that paragraph 1(defining principles) is complied with", the GDPR uses more accurate and clear wording: "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."[33]

The principle goes through the GDPR and with more responsibilities on processors, it applies now also and directly to them. For instance, processors (as well as controllers) must now maintain written records regarding all categories of personal data processing activities carried out on behalf of a controller. These records must be available to the supervisory authority on its request.[34]

Moreover, the controller and also the processor (and, where applicable, their representatives) shall cooperate, on request, with the supervisory authority in the performance of its tasks. The processor, prior to processing personal data, may need

[31] Art. 99 of the GDPR.

[32] Art. 14 (1) (d) of the GDPR.

[33] Art. 5 (2) of the GDPR.

[34] Art. 30 (2) and (4) of the GDPR. To be precise, pursuant to paragraph 5 of this article, this obligation shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

to consult the supervisory authority in certain cases to ensure actual and effective protection of the rights and freedoms of data subjects.[35]

7.5 Sub-processors

The GDPR remembers also to the practical situation, where processor entail to its tasks another processor without given notice or any information at all to the data subject. Therefore now, pursuant to Art. 28 (2) of the GDPR before doing so, the processor would need “prior specific or general written authorisation of the controller” to engage another processor.

In practise, such approval will be provided in contract, but where the contract between controller and processor contain the general approval of entailing other sub-processor, the processor will be obliged to inform the controller “of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.“

Moreover, the liability of the processor who really engages another processor for carrying out specific processing activities on behalf of the controller is much stricter as described in paragraph four of the art. 28 of the GDPR. Because in such cases, “the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.”

7.6 Data security

The emphasis on data security has grown significantly in the GDPR. For instance, even processors must now have appropriate technical and organisational measures to

[35] Art. 31 and art. 36 (1) of the GDPR.

ensure a level of security appropriate to the risk. Processors will need a comprehensive understanding of their systems, the type of categories of data it processes. When it entails sub-processors, these must also implement necessary technical and organisational measures to ensure data integrity and security.

The Facebook in its word promotes safety and security: "We use the information we have to help verify accounts and activity, and to promote safety and security on and off of our Services, such as by investigating suspicious activity or violations of our terms or policies. We work hard to protect your account using teams of engineers, automated systems, and advanced technology such as encryption and machine learning. We also offer easy-to-use security tools that add an extra layer of security to your account. For more information about promoting safety on Facebook, visit the Facebook Security Help Center."[36] Furthermore, Facebook provide tips for its users how to make the account safer.[37]

When reading and implementing the GDPR, CSP should always remember to read the recitals at the beginning. Despite the fact, that the recitals are not legally binding, they provide decent guide on how the GDPR should be interpreted. For instance, when implementing security measures, recital 83 provides: "In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage."

[36] Promote safety and security in Facebook Privacy Policy.
[37] Facebook Security Help Center. Available at < https://www.facebook.com/help/379220725465972> . Last accessed 28 August 2016.

This lead to the obligation of conducting the impact assessment process as described later in this thesis. Another consequence is that the obligation to notice the data subject about any security breach.

7.7 Data Breach Notification

The art. 33 of the GDPR obliged the controller to notify the personal data breach to the supervisory authority not later than 72 hours after having become aware of it. The notification is not necessary in case this personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

Further, also processors must notify the controller without undue delay upon becoming aware of a data breach. This is for reason, that the controller must additionally communicate the breach to the data subject without undue delay. This obligation should "not be required if any of the following conditions are met: (a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; (b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise; (c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner."

These obligations should be described in agreed on in the contract between the controller and processor, to avoid any drawbacks in communication which could at the end lead to the violation of this provision.

7.8 Impact assessment

The new obligation for the controllers is adopted in art. 35 of the GDPR. The controller shall when "a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.”

Although paragraph 7 of the art. 35 provides the basic information about the content of such impact assessment (for instance description of the envisaged processing operations, purposes of processing, assessment of the necessity and proportionality of the processing and risks and measures safeguards, mechanisms to ensure the protection of the data subject rights), after reading may remain some doubts.

Data protection impact assessment drafted by The Cloud Accountability Project (or A4Cloud for short)[38] may help the CSP (and also other controllers) to deal with this obligation. Also, the compliance with the approved code of conduct (as discussed earlier) should be taken into account during the impact assessment process.

7.9 Data protection officers (DPOs)

In certain circumstances processors will now have to designate a DPO (for instance, where the processing is carried out by a public authority or body, where the processing requires regular and systematic monitoring of data subjects on a large scale, or the core activities consist in processing large scale of special categories of personal data). The DPO can be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract. This contract however is subject to publication and the details shall be communicated to the supervisory authority. [39]

I find very interesting, that the Slovak Data Protection Act, already contains the possibility to appoint DPO. In the Slovak regime, DPO is a natural person who has the full legal capacity, is irreproachable and has a valid confirmation of passing the exam by the Office for Personal Data Protection. Statutory body or the body entitled to act in the name of the statutory body of the controller or the processor may also be designated

[38] Data protection impact assessment. Available at: <http://www.a4cloud.eu/sites/default/files/Data%20Protection%20Impact%20Assessment.pdf >. Last accessed 19 August 2016.

[39] Art. 37 of the GDPR.

as the DPO. There may be one or several DPOs and also external person may be designated as the DPO.[40]

7.10 Code of conduct

Directive 95/46/EC itself and also GDPR encourage the Member states to exhort the creation of codes of conduct. Pursuant to recital 81 of the GDPR, the adherence of the processor to an approved code of conduct may be used as an element to demonstrate compliance of the controller with the obligations. The GDPR then further puts reference to the approved code of conduct in several places.

The C-SIG (Cloud Select Industry Group on Code of Conduct) sub-group on the Data Protection Code of conduct was set up in April 2013[41] and since then it is working on the Code of conduct for CSP (hereinafter referred as the "Code").

The first version of the Code was criticized by the Article 29 working party in its opinion on Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing.[42]

Therefore, the new wording of code was published on 22 June 2016. In this wording the concerns of Working Party has been processed.[43] The Code now clearly states that adherence does not make a CSP immune to change in the EU law.[44]

Although the Code is aimed at CSPs who process personal data on behalf of their customers (and therefore act as data processors for those customers), also other CSPs may

[40] Data Protection Officer by Slovak Office for Personal Data Protection. Available at: <http://dataprotection.gov.sk/uoou/en/content/data-protection-officer>. Last accessed: 20 August 2016.

[41] The C-SIG (Cloud Select Industry Group on Code of Conduct) sub-group on the Data Protection Code of conduct. Available at: < https://ec.europa.eu/digital-single-market/cloud-select-industry-group-code-conduct>. Last accessed: 28 August 2016. The group was established for reason provided in The Communication "Unleashing the Potential of Cloud Computing in Europe" which states that the Commission will work with industry to agree on a code of conduct for cloud computing providers.

[42] Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing, No. 2588/15/EN, WP 232, adopted on 22 September 2015. Available at: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp232_en.pdf> Last accessed 10 July 2016.

[43] Code of Conduct for CSP. Available at: < https://ec.europa.eu/digital-single-market/en/news/data-protection-code-conduct-cloud-service-providers>. Last accessed 28 August 2016.

[44] Code of Conduct, page 6.

adhere to the Code. Those, who process such personal data for their own purposes (and therefore act as a data controller or as a joint data controller). [45]

It is advisable that the CSP go through the Code and publicly declare the adherence to it, if he complies with the principles and clauses stipulated there. As previously mentioned, such adherence may be helpful within the cooperation with supervisory authorities, as well as to build trust in the services from the data subject, or other customers.

7.11 Right To Be Forgotten

7.11.1 Google Spain Case

The GDPR provides in Art. 17 the provision stating the popular right to be forgotten or right to erasure. The Directive 95/46/EC also includes this right in case of the incomplete or inaccurate nature of the data.[46] The GDPR describes this right in detail and in accordance with the judgment of the CJEU case C-131/12 *Google Spain SL and Google Inc. vs Agencia Española de Protección de Datos (AEPD) a Mario Costeja González.*

Mr. Gonzales requested Google Spain to erase the link to the information about his insolvency problems that were no longer truth. The CJEU ruling provides two important outcomes. Firstly, although the Google Spain is the subsidiary of the Google Inc. it has to process the request of Mr. Gonzales, because "operator of a search engine is liable to affect significantly the fundamental rights to privacy and to the protection of personal data when the search by means of that engine is carried out on the basis of an individual's name, since that processing enables any internet user to obtain through the list of results a structured overview of the information relating to that individual that can be found on the internet — information which potentially concerns a vast number of aspects of his private life and which, without the search engine, could not have been interconnected

[45] Ibid. Page 6. The scenario of the service (SaaS, PaaS, IaaS, etc.) provided in different deployment models (public, private or hybrid clouds) imply services of different nature which may have different related obligations. Customers should be provided with information necessary to understand the nature of the service. Guidance documents can further help users understand the nature of the service type and the obligations related to it. Ibid. Page 4.

[46] Art. 12 (c) of the Directive 95/46/EC.

or could have been only with great difficulty — and thereby to establish a more or less detailed profile of him."[47]

Secondly, the CJEU confirmed that in EU the right to be forgotten exists. It considered the information regarding Mr. Gonzales in this case to be "inadequate, irrelevant or no longer relevant and therefore, excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine, the information and links concerned in the list of results must be erased."[48]

7.11.2 Consequences

Since the judgement, resp. since the launch of the official request process on 29 May 2014, the total URLs that Google has evaluated for removal reached 1,645,087. The Transparency Report available online provides information about requests according to countries.[49]

In the light of the decision, the Art. 17 of the GDPR now provides the right of data subject "to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay" if the specified grounds applies.

For instance, (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; or (b) the data subject withdraws consent on which the processing is based […]and where there is no other legal ground for the processing; or (c) the data subject objects to the processing pursuant to Article 21 […] or (d) the personal data have been unlawfully processed; (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1)."

[47] Case C-131/12 *Google Spain SL and Google Inc. vs Agencia Española de Protección de Datos (AEPD) a Mario Costeja González*. Para 80.

[48] Ibid. Para 92-94.

[49] European privacy requests for search removals. Available at: < https://www.google.com/transparencyreport/removals/europeprivacy/?hl=en-GB>. Last accessed 23 August 2016.

Then the second paragraph provides the obligation of the controller who has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, to "take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data."

Paragraphs 1 and 2 shall not apply pursuant to paragraph 3. to the extent that processing is necessary for specified reason like right of freedom of expression and information or for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject, the public interest or in the exercise of official authority vested in the controller, etc.

Google acquiesced to the verdict, but it has removed the disputed results only from the search results on its web sites with European domains such as Google.fr for France. Another solution, according to Google, would create a dangerous precedent in terms of the territorial scope of national laws. In February, the company began to remove search results across all its domains, but only when people viewed the page of Google in the country from which the requirement to remove the reference came from.

The French Office for Personal Data Protection (CNIL) imposed on Google in March in amount of 100,000 euros for the fact that it does not perform these erasures comprehensively. According to CNIL, the imposing of fine is the only way how to promote the right of Europeans to privacy. Google has appealed against the decision to the Supreme Administrative Court, whose function in France is performed by the State Council.

CNIL argues that the right to privacy should not depend on where the person is located. Extending the right to be forgotten for all versions of Google then allegedly does not interfere with the freedom of expression, because the content is not essentially erased, it just does not appear in search results. [50]

[50] E-15. Czech news portal. Available at: < http://e-svet.e15.cz/internet/google-se-brani-pravo-byt-zapomenut-nema-podle-nej-platit-globalne-1296747#utm_medium=selfpromo&utm_source=e15&utm_campaign=copylink >. Last accessed 24 August 2016.

7.12 Data Portability

Another obligation for CSP acting as a controller is the right of the data subject pursuant to the Art. 20 of the GDPR to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.

This provisions aims to the situations, where the customer was forced to stay in contractual relationship with one controller just because the format he used, was not readable by another without the bearing of big costs. The customer should be able to change the CSP without any problems or additional costs.

Of course, the controller can bind the processor in the contract to store the data he is processing on the behalf of the controller in a structured, commonly used and machine-readable format in order to prevent situations, where the processor causes the problems with transmission of the data. It is more than advisable to do so.

8 Transfer to the third countries

The transfer of personal data to the third countries was always a deeply discussed issue. While the Member State are not allowed to "neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1"(right of the data subject to privacy) [51], the transfer to the countries outside the EU that do not ensure the adequate level of protection for the data subject residing in EU is prohibited (unless derogations of art. 26 of the Directive 95/46/EC apply).

Thus personal information can however be transferred from any member state to any third country[52], if an individual has given his free consent, or model contracts have been signed (see further in this chapter) and in many instances approved by the country supervisory authority, or Binding Corporate Rules have been approved.[53]

8.1 Max Schrems Case

The actual consciousness of the public about the principles in transfer of personal data to the third countries occurred in large part because of the case C-362/14 - Maximillian Schrems v. Data Protection Commissioner that has been decided by the CJEU.

The brief factual background starts with Maximillian Schrems, an Austrian national that lodged the complaint to the Data Protection Commissioner by which he asked the latter to exercise his statutory powers by prohibiting Facebook Ireland from transferring his personal data to the United States because the law and practice in force in that country

[51] Art. 1 of the Directive 95/46/EC.

[52] Other than Canada and Argentina because transfers from other countries with national privacy legislation (e.g. Canada, Argentina) also require contractual agreement, see Pearson Siani, Yee George. Privacy and Security for Cloud Computing. Springer, 2013.

[53] At this place it is worth mentioning that some scholars do not consider these technics as adequate for CSP. See Pearson Siani, Yee George. Privacy and Security for Cloud Computing. Springer, 2013. "The first reason is due to regulatory complexity and uncertainty in cloud environments, especially due to divergences between the individual European member states' national laws implementing the European Data Protection Directive, 1995. The second reason is that these techniques are not flexible enough for cloud, because administering and obtaining regulatory approval for model contracts can result in lengthy delays: the notification and prior approval requirements for EU model contracts vary significantly across the EU but are burdensome and can take from 1 to 6 months to set up. BCRs are suitable for dynamic environments, but their scope is limited: they only apply to data movement within a company group, it may be difficult for SMEs to invest in setting these up and there are only a few BCRs to date, although it is a relatively new technique."

did not ensure adequate protection of the personal data.[54] This case raised the big wave of popularity. Suddenly, with reference to the Edward Snowden revelations, everyone was concerned about his/her data. In this respect, Schrems case was a grand contribution to improving general awareness of privacy threats on the Internet.

When his complaint was rejected, Mr. Schrems brought an action before the High Court challenging the decision at issue. The High Court decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:

'(1) Whether in the course of determining a complaint which has been made to an independent office holder who has been vested by statute with the functions of administering and enforcing data protection legislation that personal data is being transferred to another third country (in this case, the United States of America) the laws and practices of which, it is claimed, do not contain adequate protections for the data subject, that office holder is absolutely bound by the Community finding to the contrary contained in [Decision 2000/520] having regard to Article 7, Article 8 and Article 47 of [the Charter], the provisions of Article 25(6) of Directive [95/46] notwithstanding? '

The second referred question was: 'alternatively, may and/or must the office holder conduct his or her own investigation of the matter in the light of factual developments in the meantime since that Commission decision was first published?'[55]

One of the problems with Safe Harbour Framework was that according to Annex I to Decision 2000/520, it was applicable solely to self-certified United States organisations, which received personal data from the European Union. But United States public authorities were not required to obey its principles. Therefore, "'national security, public interest, or law enforcement requirements' have primacy over the safe harbour principles, primacy pursuant to which self-certified United States organisations receiving personal data from the European Union are bound to disregard those principles without limitation where they conflict with those requirements and therefore prove incompatible with them."[56]

[54] Case C-362/14 - *Maximillian Schrems v. Data Protection Commissioner* [2015]. Para. 28.
[55] Ibid. Para 30 and 35.
[56] Ibid. Para 82, 86.

The Decision 2000/520 lacked also the reference to the existence of effective legal protection against violation in the individuals' data privacy right. According to Advocate General Bot, "the private dispute resolution mechanisms and the FTC, owing to its role limited to commercial disputes, are not means of challenging access by the United States intelligence services to personal data transferred from the European Union" The role of the FTC is to ensure the unfair or deceptive acts and practices in commerce will be punished. Therefore, it cannot be compared to the European national supervisory authorities, because they were established for the exact purpose to protect and enforce the protection of the data privacy rights with respect to the individuals. The FTC does not have the capacity to ensure the protection of the individual right to privacy, "to intervene in the sphere of personal data protection procedures before the Federal Trade Commission — the powers of which, described in particular in FAQ 11 set out in Annex II to that decision, are limited to commercial disputes".

Moreover, "the private dispute resolution mechanisms concern compliance by the United States undertakings with the safe harbour principles and cannot be applied in disputes relating to the legality of interference with fundamental rights that results from measures originating from the State."[57]

The CJEU than observed, that "the United States authorities were able to access the personal data transferred from the Member States to the United States and process it in a way incompatible, in particular, with the purposes for which it was transferred, beyond what was strictly necessary and proportionate to the protection of national security. Also, the Commission noted that the data subjects had no administrative or judicial means of redress enabling, in particular, the data relating to them to be accessed and, as the case may be, rectified or erased. In particular, legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter."[58]

[57] Ibid, para. 89 and Opinion of Advocate General Bot delivered on 23 September 2015, C-362/14 - *Maximillian Schrems v. Data Protection Commissioner.* Para. 204-206.

[58] Joint cases C-293/12 and C-594/12. *Digital Rights Ireland and Others*. [2014]. Para 39.

"The first subparagraph of Article 3(1) of Decision 2000/520 must therefore be understood as denying the national supervisory authorities the powers which they derive from Article 28 of Directive 95/46, where a person, in bringing a claim under that provision, puts forward matters that may call into question whether a Commission decision that has found, on the basis of Article 25(6) of the directive, that a third country ensures an adequate level of protection is compatible with the protection of the privacy and of the fundamental rights and freedoms of individuals"[59]

With the reference to the above-mentioned considerations, it was concluded that the Decision 2000/520 is invalid.

This situation caused a lot of problems for companies, including CSP. Suddenly, they become incompliant with the legislation. The only way how to remedy this undesirable status was to enter into a contract with the customers, based on the standard contractual clauses formulated by the Commission with are used for third countries, that do not provide the adequate level of protection.

8.2 Model Contracts for the transfer of personal data to third countries

Depending on the relationship in particular case, the different decision of the Commission applies:

A) Transfer from (EU-)controller to (Non-EU/EEA-)controller

Commission Decision 2001/497/EC - Standard contractual clauses for the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to third countries which do not ensure an adequate level of protection (controller to controller transfers).

B) Transfer from (EU-)controller to (Non-EU/EEA-)processor

Commission Decision C(2010)593 Standard Contractual Clauses (processors) for the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to

[59] Ibid, para. 89 and Opinion of Advocate General Bot delivered on 23 September 2015, C-362/14 - *Maximillian Schrems v. Data Protection Commissioner.* Para 102.

processors established in third countries which do not ensure an adequate level of data protection.[60]

8.3 Negotiating the data transfer agreement

As the contract itself, the negotiations preceding it are of big influence on the further function of the whole relationship.

The issues of applicable jurisdiction or choice of cloud (which of the deployment models is most appropriate for the actual business), establishment and location of the data, processor and any third party (if any), alternative dispute resolution strategy, may be the cause of problems on the later stage, if not negotiated in advance.

What are often forgotten in contracts are the termination clauses. Measures taken to prevent cyberattacks may be applicable in some cases. Whether there are obligations according to the national law, for instance, disclosure to the Commissioner (if applicable and if any).

I would also recommend include the clause about the continuing training on data protection management and compliance at all level (not only regular employees, but also board of directors, executive committee, senior management, executives, supporting staff, vendor, partners and associates). [61]

From my experience as a junior lawyer, I have observed that many third country cloud service providers (independently) complement the Standard contractual clauses with own provisions or ask their customers to enter into the agreement they drafted, in such case the Standard contractual clauses form the appendix to this agreement. As I understood, the main reason for this is to make completely clear, that they (i) understand, that without the adherence to the Standard contractual clauses, the business could not be

[60] Model Contracts for the transfer of personal data to third countries. Available at: < http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm >. Last accessed: 20 August 2016.

[61] Noriswadi Ismail. Selected Technologies' Appraisal from the PDPA's Lens. Noriswadi Ismail, Edwin Lee Yong Cieh (Ed.) in *Beyond Data Protection, Strategic Case Studies and Practical Guidance.* Springer, 2013. Page 115. Note that the book relates to the Personal Data Protection Act from Malaysia. "Note that these lists are not exhaustive and it may be depending upon the business plan, model and execution of the proposed cloud-based application."

realized; (ii) they want to take the lowest allowed degree of responsibility, because they are “afraid” of the European DPAs.

The most problematic standard clause is no. 8 and regards the cooperation with data protection authorities. Pursuant to its second paragraph: “The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.” [62]

Moreover, the data importer obligation continues in the Clause 12 with the heading Obligation after the termination of personal data processing services, pursuant to which, he has to “return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so;” followed by the proclaimed warranty in second paragraph: “The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.”

But the end of the day, CSP got used to the model contracts even with the audit. They did not have a choice. Without these model contracts, the whole EU trade market would be closed for them. I believe, this is one of the reasons why the Privacy Shield Framework has been agreed in relatively short time.

8.4 Binding corporate rules

Pursuant to the definition part of the GDPR the ‘binding corporate rules’ means “personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of

[62] For the avoidance of the situation, where the CSP in third country would rely on the protection from its national law, the third paragraph of the same Clause states: “The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2 […].”

undertakings, or group of enterprises engaged in a joint economic activity"[63] and form the mean by which the appropriate safeguards may be provided for pursuant to Art. 46 (20 of the GDPR.

8.5 Authorisation by the national supervisory authority

The last option for transfer to the third country is to ask for permission from the national supervisory authority with accordance to the national law. For instance the conditions for the issuance of authorisation in Czech Republic are (and it is up to the controller to prove that):

(a) the data transfer takes place with the consent of, or on the basis of an instruction by the data subject;

(b) in a third country, where personal data are to be processed, has been created sufficient specific guarantees for personal data protection, e.g. by other legal or professional regulations and security measures. Such guarantees may be specified in particular by a contract concluded between the controller and the recipient, if this contract ensures application of these requirements, or if the contract contains contractual clauses for personal data transfer to third countries published in the Official Journal of the Office;

(c) the personal data concerned are part of publicly accessible data files on the basis of a special Act or are, on the basis of a special Act accessible to someone who proves legal interest; in such case the personal data may be disclosed only in the scope and under conditions provided by a special Act;

(d) the transfer is necessary to exercise an important public interest following from a special Act or from an international treaty binding the Czech Republic;

(e) the transfer is necessary for negotiating the conclusion or change of a contract, carried out on the data subject´s incentive, or for the performance of a contract to which the data subject is a contracting party;

[63] Art. 4 (20) of the GDPR.

(f) the transfer is necessary to perform a contract between the controller and a third party, concluded in the interest of the data subject, or to exercise other legal claims, or

(g) the transfer is necessary for the protection of rights or important vital interests of the data subject, in particular for rescuing life or providing health services.

„When considering the application, the Data Protection Office shall examine all circumstances related to the transfer of personal data, in particular the source, final destination and categories of personal data which are to be transferred, the purpose and period of the processing, with regard to available information about legal or other regulations governing the personal data processing in a third country. In the authorization to the transfer, the Data Protection Office shall specify the period of time over which the controller may perform the data transfers. If a change of the conditions under which the authorization was issued occurs, in particular on the basis of a decision of an institution of the European Union, the Data Protection Office shall alter or revoke this authorization.“[64]

8.6 Privacy Shield

8.6.1 First draft

After the declaration of invalidity of the Safe Harbour, the European Union and USA started negotiate about another document in order to minimize the negative consequences of a situation where the US it was considered a country without adequate protection. This was serious problem for many corporations and affected also CSP.

Within relatively short period of time, the draft of new document was issued. It is called “Privacy Shield” and this new framework should reflect the requirements set by the European Court of Justice in its ruling in Maximillian Schrem case. Moreover, “the U.S. authorities provided strong commitments that the Privacy Shield will be strictly enforced

[64] Czech Data Protection Act. Act No. 101/2000 Coll., on the Protection of Personal Data. Section 27 (3) and (4).

and assured there is no indiscriminate or mass surveillance by national security authorities."[65]

The main points that should assure the protection are "(i) strong obligations on companies and robust enforcement, (ii) clear safeguards and transparency obligations on U.S. government access (for the first time, the U.S. government has given the EU written assurance from the Office of the Director of National Intelligence that any access of public authorities for national security purposes will be subject to clear limitations, safeguards and oversight mechanisms, preventing generalised access to personal data, (iii) effective protection of EU citizens' rights with several redress possibilities (Complaints have to be resolved by companies within 45 days. A free of charge Alternative Dispute Resolution solution will be available. EU citizens can also go to their national Data Protection Authorities, who will work with the Federal Trade Commission to ensure that unresolved complaints by EU citizens are investigated and resolved), (iv) annual joint review mechanism monitoring the functioning of the Privacy Shield."[66]

8.6.2 Article 29 Working Party Opinion

On 13 April 2016 the Opinion of the Article 29 Working Party no. 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision was adopted. Although the WP29 notes "the major improvements the Privacy Shield offers compared to the invalidated Safe Harbour decision", the WP29 expressed the concerns about it and the asked for clarifications. The opinion is very detailed and Commission should resolve these worries, identify suitable solutions and provide the demanded clarifications in order to "improve the draft adequacy decision and ensure the protection offered by the Privacy Shield is indeed essentially equivalent to that of the EU."[67]

[65] European Commission - Press release - Restoring trust in transatlantic data flows through strong safeguards: European Commission presents EU-U.S. Privacy Shield, Brussels, 29 February 2016. Available at: <http://europa.eu/rapid/press-release_IP-16-433_en.htm>. Last accessed: 22 August 2016.

[66] European Commission - Press release - Restoring trust in transatlantic data flows through strong safeguards: European Commission presents EU-U.S. Privacy Shield, Brussels, 29 February 2016. Available at: <http://europa.eu/rapid/press-release_IP-16-433_en.htm>. Last accessed: 22 August 2016.

[67]Opinion of the Article 29 Working Party no. 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision. adopted on 13 April 2016. Available at: < http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf >. Last accessed: 22 August 2016. Page 5.

The absence of clear rules where the Shield organisation is acting as an Agent (i.e. on behalf an EU controller) imply a loophole and might prevent the EU controller to remain into control. A Shield organisation receiving the data as an Agent of an EU controller has to respect the EU controller's instructions. This should be expressly stated in the Principles in order to ensure that the non-respect of those instructions will not only lead to a breach of the contract (Annex II, III.10.a.ii) but also to a violation of the Privacy Shield principles.

The Accountability for Onward Transfers principle of the Privacy Shield is not limited to recipient data controllers, processors or Agents established in the U.S. Therefore, onward transfers to a third country could take place on the basis of the Privacy Shield, even if the third country has laws providing for public access to personal data, for example for purposes of surveillance. This puts EU data at risk of unjustified interferences with the fundamental rights protection. [68]

"The first concern is that the language used in the draft adequacy decision does not oblige organisations to delete data if they are no longer necessary. This is an essential element of EU data protection law to ensure that data is kept for no longer than necessary to achieve the purpose for which the data were collected.

Secondly, the WP29 understands from Annex VI that the U.S. administration does not fully exclude the continued collection of massive and indiscriminate data. The WP29 has consistently held that such data collection, is an unjustified interference with the fundamental rights of individuals.

The third point of concern regards the introduction of the Ombudsperson mechanism. Even though the WP29 welcomes this unprecedented step creating an additional redress and oversight mechanism for individuals, concerns remain as to whether the Ombudsperson has sufficient powers to function effectively. As a minimum, both the powers and the position of the Ombudsperson need to be clarified in order to

[68] Opinion of the Article 29 Working Party no. 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision. adopted on 13 April 2016. Pages 21 and 23.

demonstrate that the role is truly independent and can offer an effective remedy to non-compliant data processing." [69]

8.6.3 Final Framework and Principles

The criticism of the WP29 caused a little delay, but finally, the Privacy Shield Framework is working. The Commission adopted an implementing decision on the adequacy of the protection provided by the EU–U.S. Privacy Shield on 12th July 2016.[70]The joining will be voluntary, but once an eligible company makes the public commitment to conform with the Framework's requirements, the commitment will become enforceable under U.S. law.[71]

To make the summary, the EU-U.S. Privacy Shield is based on the following principles:

1) "Strong obligations on companies handling data"

   The regular updates and reviews of participating companies will be performed by the U.S. Department of Commerce, in order to be sure that companies follow the rules they declared to follow. In case companies do not comply in practice, the sanctions may be imposed, including the removal from the list. Moreover, "the tightening of conditions for the onward transfers of data to third parties will guarantee the same level of protection in case of a transfer from a Privacy Shield company."

2) "Clear safeguards and transparency obligations on U.S. government access"

[69] Opinion of the Article 29 Working Party no. 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision. adopted on 13 April 2016. Page 57.

[70] Commission implementing decision C(2016) 4176 final of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, available at <http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf.> Last accessed: 15 August 2016.

[71] Fact Sheet Overview of the EU-U.S. Privacy Shield Framework For Interested Participants from 12 July 2016 . Available at: <https://www.commerce.gov/sites/commerce.gov/files/media/files/2016/fact_sheet-_eu-us_privacy_shield_7-16_sc_cmts.pdf>. Last accessed: 22 August 2016.

What was real issue in Safe Harbour Framework, should be eliminated, because the "U.S. has given the EU assurance that the access of public authorities for law enforcement and national security is subject to clear limitations, safeguards and oversight mechanisms". To make this assurance real, the redress mechanisms has been launched in this area with redress possibility for the individuals through an Ombudsperson mechanism.[72]

3) "Effective protection of individual rights"

   Individuals shall have many options at their discretion to protect their data from misuse. The Privacy Shield scheme provides several accessible and affordable dispute resolution mechanisms. In the ideal case, the complaint will be resolved by the company itself, next the Alternative Dispute resolution (ADR) solutions are available. All of these shall guarantee that individual bares no costs in relation with solving his complaint. Moreover, the data subject may always turn on his national Data Protection Authorities, who will cooperate with the Federal Trade Commission "to ensure that complaints by EU citizens are investigated and resolved." The final option for the EU citizen is an arbitration mechanism (in case all the previous should fail). For the area of national security an Ombudsperson shall provide the proper redress.[73]

4) "Annual joint review mechanism"

   To ensure that all the commitments are fulfilled, the mechanism of monitoring the functioning of the Privacy Shield is effective. "The European Commission and the U.S. Department of Commerce will conduct the review and associate national intelligence experts from the U.S. and European Data Protection Authorities. The Commission will draw on all other sources of information

[72] "The U.S. has ruled out indiscriminate mass surveillance on personal data transferred to the US under the EU-U.S. Privacy Shield arrangement. The Office of the Director of National Intelligence further clarified that bulk collection of data could only be used under specific preconditions and needs to be as targeted and focused as possible. It details the safeguards in place for the use of data under such exceptional circumstances." See further: European Commission - Press release from 12 July 2016. European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows. Available at: <http://europa.eu/rapid/press-release_IP-16-2461_en.htm >. Last accessed: 14 August 2016.

[73] The Ombudsperson shall be independent from the US intelligence services.

available and will issue a public report to the European Parliament and the Council."[74]

8.6.4 Self-Certification

The U.S. Department of Commerce[75] started to accept the self-certifications for organization from the 1st of August. Since then several companies have self-certified. For example, Microsoft has already its certification, also for its affiliates.[76]

The U.S. Department of Commerce also issued a guide to the self-certification[77] stating the conditions and process for organizations how to join the Privacy Shield.

First step is the confirmation of the organization's eligibility to participate in the Privacy Shield. "Any U.S. organization that is subject to the jurisdiction of the Federal Trade Commission (FTC) or the Department of Transportation (DOT) may participate in the Privacy Shield."[78]

The second step is the developing of the Privacy Shield-Compliant Privacy Policy Statement and hand it to the Department of Commerce. Among other things, the privacy policy should describe how the personal data (information) are handled in practice and the choices the organisation offers individuals with respect to the use and disclosure of their personal information. The Guide emphasises that the policy has to follow the Privacy

[74] European Commission - Press release from 12 July 2016. European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows. Available at: <http://europa.eu/rapid/press-release_IP-16-2461_en.htm >. Last accessed: 14 August 2016.

[75] The mission of the U.S. Department of Commerce is to create the conditions for economic growth and opportunity. The U.S. Department of Commerce. Available at: < https://www.commerce.gov/page/about-commerce>. Last accessed> 22 August 2016.

[76] Privacy Shield List, available at: <https://www.privacyshield.gov/list>. Last accessed: 15 August 2016.

[77] Guide to Self-Certification by U.S. Department of Commerce, available at: < https://www.commerce.gov/sites/commerce.gov/files/media/files/2016/how_to_join_privacy_shield_sc_cmts.pdf> . Last accesses 22 August 2016.

[78] The FTC and DOT have both committed that they will enforce the Privacy Shield Framework. Generally, the FTC's jurisdiction covers acts or practices in or affecting commerce by any "person, partnership, or corporation." The FTC does not have jurisdiction over most depository institutions (banks, federal credit unions, and savings & loan institutions), telecommunications and interstate transportation common carrier activities, air carriers, labor associations, most non-profit organizations, and most packer and stockyard activities. In addition, the FTC's jurisdiction with regard to insurance activities is limited to certain circumstances. The DOT has exclusive jurisdiction over U.S. and foreign air carriers. The DOT and the FTC share jurisdiction over ticket agents that market air transportation. Guide to Self-Certification. Page 2.

Shield Principles and should be written as “clear, concise, and easy to understand.” Moreover, the compliance to the Privacy Shield Framework has to be specifically declared in this policy in accordance with supplemental principle 6. This principle requires each organization that self-certifies to state in its relevant published privacy policy that it adheres to the Privacy Shield Principles. Finally, a hyperlink to the Privacy Shield website has to be added to the privacy policy.

Further, the company has to determine and describe in its Privacy Policy the “Independent Recourse Mechanism”, which is the result of the Privacy Shield’s recourse, enforcement and liability principle. That basically means that in the company’s privacy policy which is located and accessible on their website, a hyperlink to the website of the independent recourse mechanism must be incorporated. This mechanism shall be eligible to investigate unresolved complaints on the topic of the (in-)compliance with the Privacy Shield. No cost shall be applicable on data subject with relation to the complaint. The privacy policy itself has to be accurately located on the website and be available online at any time to ensure, that the customers will easily find it without any further effort. The web address (the link to effective the privacy policy) of the company is to be provided during self-certification process.

At this stage of the process, private sector comes to stage, as the guide clearly counts that private sector dispute resolution programs may operate as the independent recourse mechanism. Organizations from U.S.[79] or also the cooperation with the EU data protection authorities with respect to all types of data may be relied on, but the procedures outlined in Supplemental Principle 5 (The Role of the Data Protection Authorities) has to be bared in mind.

The next step is the ensuring that the company’s verification mechanism is working. According to the Supplemental Principle 7 (Verification), if the company

[79] According to Guide to Self-Certification by U.S. Department of Commerce, available at: < https://www.commerce.gov/sites/commerce.gov/files/media/files/2016/how_to_join_privacy_shield_sc_cmts.pdf> . Last accesses 22 August 2016, Council of Better Business Bureaus (BBB), TRUSTe, the American Arbitration Association (AAA), JAMS, and the Direct Marketing Association (DMA) have developed programs that assist in compliance with the Framework's Recourse, Enforcement and Liability Principle and Supplemental Principle 11(Dispute Resolution and Enforcement).

selfcertifies itself to the Framework, it is required “to have procedures in place for verifying compliance”. For the avoidance of doubt, the company is allowed to use the self-assessment or an outside/third-party assessment program to prove this compliance.

The final step is the designation of a contact within the organization regarding Privacy Shield -the contact person for the handling of questions, complaints, access requests, and any other issues arising under the Privacy Shield, for instance the obligation to respond to individuals (data subjects) within 45 days of receiving the complaint. This contact person may be for example the corporate officer (as it can be the case according to Slovak law).

8.6.5 The conclusions

The principles and mechanisms in the new Privacy Shield Framework seem to be much more detailed and elaborated. The self-certification process requires much more effort from the companies before they can start and the review mechanisms are also stricter then before.

On the other hand some experts are sceptical to the Privacy Shield Framework, arguing that the new Commission implementing decision C(2016) 4176 final repeats the same mistake as the invalidated Safe Harbour Decision, namely that the “Commission has failed again to provide an overall assessment of the US legal order and to find that the US as “a third country ensures an adequate level of protection” within the meaning of Article 25(2) of the directive “by reason of its domestic law or of the international commitments it has entered into [. . .] for the protection of the private lives and basic freedoms and rights of individuals”, pursuant to Article 25(6) of the directive.”[80]

As many annexes 1 to 7 to the decision imply, the Commission has relied on letters from various authorities of the US government but not on appropriate US law. “These letters may however not shield US law from the application of the findings made

[80] See to this effect: Xavier Tracol. EU–U.S. *Privacy Shield: The saga continues.* Computer Law & Security Review: The International Journal of Technology Law and Practice (2016), doi: 10.1016/j.clsr.2016.07.013. Page 2.

by the Grand Chamber in the Schrems judgment. The latter implies substantial changes to the US law.[81] The legal system of the US has however not changed. [82]

Whether or not the Privacy Shield Framework has the potential to operate properly with its annual control mechanism and more specified principles, will be sure in couple of years.

[81] Xavier Tracol, "'Invalidator' strikes back: The harbour has never been safe", Computer Law & Security Review, volume 32, issue 2, April 2016, p. 360.

[82] Xavier Tracol. EU–U.S. *Privacy Shield: The saga continues.* Computer Law & Security Review: The International Journal of Technology Law and Practice (2016), doi: 10.1016/j.clsr.2016.07.013. Page 2.

9 Control and consistency

9.1 Independent supervisory authorities

Although the GDPR shall apply from 25 May 2018, the CSP should not wait with reviewing its terms of service, safeguards and other documentations. The GDPR defines clearly the competence, tasks and power of the supervisory authorities and vests them with the investigative, corrective, authorisation and advisory powers.

The violation of provisions of the GDPR is subject to corrective powers of supervisory authority pursuant to Art. 58 (2) of the GDPR. These corrective power are very broad and vary from issuance of warnings or even reprimands to a controller or processor where processing operations have infringed provisions of the GDPR, the order to comply with the data subject's requests to exercise his or her rights or to bring processing operations into compliance with the provisions of the GDPR, or to communicate a personal data breach to the data subject.

Further, the authority may impose a temporary or definitive limitation including a ban on processing or order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19. Last but not least, the authority can withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met; Finally, it may order the suspension of data flows to a recipient in a third country or to an international organisation.

9.2 One-stop-shop Mechanism

One of the main objectives of the new Regulation is to achieve consistent and coordinated application across the EU.83 In ordert to achieve this gole, the GDPR created

[83] Marcus Evans and Adam Smith. *EU Proposes "One Stop Shop" for Data Protection Supervision and Enforcement*. Available at: < http://www.dataprotectionreport.com/2015/04/eu-proposes-one-stop-shop-for-data-protection-supervision-and-enforcement/>. Last accessed 28 August 2016.

the One-stop-shop Mechanism aiming at the situations where data controller or processor processes information relating to individuals in more than one EU Member States. The supervisory authority in one EU Member State would assume control of the controller's or processor's activities (so called :lead supervisory authority), and cooperate in accordance with art. 60 of the GDPR with the supervisory authority in other relevant EU Member States.[84]

9.3 Sanctions

In addition to, or instead of measures described above the direct administrative fines pursuant to Art. 83 may be imposed by the supervisory authority. I believe the high of these fines (depending of course on the circumstances of each individual case) is sufficiently deterrent, when the less serious infringement can be penalized by the fine up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher, (paragraph 4) for the more serious infringement, the fine can reach up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher (paragraph 5).

For the illustration, the less serious infringement may be the violation of the obligation of the controller or the processor regarding the child`s consent, notification of a personal data breach to the supervisory authority, or communication of the personal data breach to the data subject. On the other hand, the violation of any right of the data subject pursuant to Art. 12 to 22 constitutes more serious infringement, i.e. for instance right to information and access, rectification, erasure, restriction of processing, data portability and automated individual decision making, including profiling. For the more serious violation is perceived also the infringement of the basic principles for processing, including conditions for consent pursuant to Art. 5, 6, 7 and 9.

[84] See further to this effect recital 127 and 128 of the GDPR and art. 56 and 60 of the GDPR.

Moreover, Member states shall adopt other effective, proportionate and dissuasive penalties for violations that are not subject to the administrative fines and notify the Commission about this law also by 25 May 2018.[85]

This system of deterring means of remedy has a good potential for functioning and builds the sound backup if the regulation were not respected.

9.4 European Data Protection Board

The next strengthening element of the protection of individuals‘ personal data in the EU is the establishing of the European Data Protection Board (hereinafter referred as the “Board”) pursuant to art. 68 of the GDPR. It shall be composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor. In accordance with art. 69 the Board shall act independently.

The tasks of the Board are listed in art. 70 and 71 of the GDPR. It shall mainly ensure the consistent application of the GDPR, of course. For this purpose, it is competent to monitor the application of the GDPR even in cases w

Further, the Board should advise the Commission, issue guidelines, recommendations, and best practices on procedures related to the processing of personal data, and review the practical application of these guidelines, recommendations and best practices, encourage the drawing-up of codes of conduct. Least but not last, the Board shall maintain a publicly accessible electronic register of decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism, which will make them easily founded by the interested individuals.

Moreover, the Board shall draw up an annual report about the protection of natural persons with regard to processing mostly in the EU, but also, in relevant cases, processing in third countries and international organisations. The report shall be made public and review the application of the GDPR, the issued recommendations of the Board and binding decisions according to art. 65.

[85] Art. 84 of the GDPR.

I am personally very curious about the functioning of this Board and cooperation with the particular national supervisory authorities. The time will show us what effect the tasks and powers vested to it will have to the protection of individuals with regard to their right to privacy.

10 Conclusion

There is no doubt, that the data stored in clouds are endangered by many threats. To my delight the data protection law in the EU is not taken lightly and the on-going discussion about related issues as well as publishing the cases of CJEU arouse interest and public awareness of the threats to which individuals' data in the online environment are facing. The GDPR forms a good basis for the minimalizing the consequences if any of these threats become a real problem.

I find it very favourable, that the data subject got the bigger emphasis in the Regulation. Through the whole regulation I can see an effort to strengthen the position of the data subject and its bigger involvement in the protection of his/her personal data. The strengthening of the principles and more detailed explanations of the rights of data subjects are progressive elements of the GDPR.

Thus, the data subject may more easily enforce its rights regarding the protection of his/her data, for instance the right to erasure (to be forgotten) or right to lodge the complaint.

On the other hand, there are mechanisms to protect also the data subjects, which are not aware of the threats the online world brings or do not care about them. This approach does not mean though, that their data deserve less protection.

The CSP have to review their privacy policies and terms of use as soon as possible to ensure, that they will comply with all the requirements in the GDPR before it became effective on 25 May 2018. The new rules apply to the processors, including the sanctions for violation of the provisions. These may require some technical or organisational measures to be implemented. In some situations, the processor will be considered to act as a controller, when he infringes the GDPR by determining the purposes and means of processing.[86] Such responsibility will be new to many CSP who relied on their position of mere processor of personal data.

[86] Art. 28 (10) of the GDPR.

The CSP who acts as the data controllers should also revise their policies and contracts, particularly these concluded with data processors, to ensure, that they will comply with their obligations.

In the area of trans border data transfer we have also detailed provisions, but the new U.S. Privacy Shield Framework has attracted all the attention. The good think is that the real launch of the Framework was delayed as proposed by the Article 29 Working party and therefore, its wording was compared and (hopefully) is in compliance with the provisions of the GDPR. Despite the comments, that the previous mistakes are repeated, now the Framework is in operation and till the new Max Schrems come to the stage, the stakeholders may rely on it.

The new rules are in my opinion broadly covered by the control mechanism, counting the new powers of national supervisory authorities, the one-stop-shop mechanism and the newly established European Data Protection Board with the Chair in the head. When the tasks will be fulfilled and the cooperation between the EU institutions and the Board and national supervisory authorities and the Board will be working, the protection of personal data under the GDPR shall have decent basis. Hopefully, it will not become the nice term without real influence.

I welcome also directly applicable sanctions, especially quite high administrative fines, which works as intimidating element.

To conclude, the GDPR will at first cause some wrinkles on the faces CSP representatives, but at the end of the day, the data subjects will get better protection regarding their personal data. And this is one of the main goals according to the recital 1 at the very beginning of the GDPR.

11 Bibliography

11.1 Literature

- Pearson Siani, Yee George. *Privacy and Security for Cloud Computing*. Springer, 2013.
- Noriswadi Ismail. Selected Technologies' Appraisal from the PDPA's Lens. Noriswadi Ismail, Edwin Lee Yong Cieh (Ed.) in *Beyond Data Protection, Strategic Case Studies and Practical Guidance.* Springer, 2013.
- Md Hasanul Ferdaus, Manzur Murshed. Energy-Aware Virtual Machine Consolidation in IaaS Cloud Computin. Zaigham Mahmood (ed.) in *Cloud Computing. Challenges, Limitations and R&D Solutions.* Springer, 2014.
- Massimo Felici, Siani Pearson. Accountability for Data Governance in the Cloud in Massimo Felici, Carmen Fernández-Gago (ed.) *Accountability and Security in the Cloud.* Springer International Publishing Switzerland 2015.
- Serge Gutwirth, Ronald Leenes, Paul de Hert (ed.) *Reforming European Data Protection Law*. Springer,

11.2 Legislation

- Charter of Fundamental Rights of the European Union. OJ C 326, 26.10.2012, p. 391–407.
- Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, OJ L 095 , 21/04/1993, p. 29 – 34.
- 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. 31–50.
- Commission implementing decision C(2016) 4176 final of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, available at <http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf.> Last accessed: 15 August 2016.
- Annexes to the Commission Implementing Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield C(2016) 4176 final from 12 July 2016. Available at: < http://ec.europa.eu/justice/data-protection/files/factsheets/annexes_eu-us_privacy_shield_en.pdf >. Last accessed: 15 August 2016.

- 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, 4.5.2016, p. 1–88.
- International Standard ISO/IEC 17788:2014(E) Information technology — Cloud computing — Overview and vocabulary.
- Commission Decision 2001/497/EC - Standard contractual clauses for the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to third countries which do not ensure an adequate level of protection (controller to controller transfers).
- Commission Decision C(2010)593 Standard Contractual Clauses (processors) for the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.
- Slovak Data Protection Act. Act No. 122/2013 Coll. on Protection of Personal Data and on Changing and Amending of other acts, resulting from amendments and additions executed by the Act. No. 84/2014 Coll. Available at:

  < http://www.dataprotection.gov.sk/uoou/sites/default/files/kcfinder/files/Act_122-2013_84-2014_en.pdf > Last accessed: 14 May 2016.
- Slovak Decree no. 117/2014 which amends Decree no. 164/2013 of the Office for Personal Data Protection of the Slovak Republic on an extent of a safety measures documentation.
- Czech Data Protection Act. Act No. 101/2000 Coll., on the Protection of Personal Data and on Amendment to Some Acts, as amended. Available at:

  < https://www.uoou.cz/en/vismo/zobraz_dok.asp?id_ktg=1107 >. Last accessed: 14 May 2016.

11.3 Case-law

- Case C-101/01. *Bodil Lindqvist.* [2003 I-12971]
- Case C-131/12. *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) a Mario Costeja González.*
- Case C-362/14 - *Maximillian Schrems v. Data Protection Commissioner* [2015]
- Opinion of Advocate General Bot delivered on 23 September 2015, C-362/14 - *Maximillian Schrems v. Data Protection Commissioner*.
- Joint cases C-293/12 and C-594/12. *Digital Rights Ireland and Others*. [2014]

11.4 Articles

- Paul de Hert, Vagelis Papakonstantinou. *The new General Data Protection Regulation: Still a sound system for the protection of individuals?* Computer Law & Security Review, Vol. 32, Issue 1, February 2016. Pages 179–194.
- Paul de Hert, *The cloud computing standard ISO/IEC 27018 through the lens of the EU legislation on data protection*. Computer Law & Security Review, Vol. 32, Issue 1, February 2016, Pages 16–30.
- Georg Borges. *Cloud Computing und Datenschutz. Zertifizierung als Ausweg aus einem Dilemma*. Datenschutz und Datensicherheit - DuD, Volume 38, Issue 3, March 2014. Pages 165–169.
- Dimitra Kamarinou, Christopher Millard and W. Kuan Hon. *Cloud privacy: an empirical study of 20 cloud providers' terms and privacy policies—Part I.* International Data Privacy Law, 2016, Vol. 6, No. 2. Pages 79-101.
- Xavier Tracol. *EU–U.S. Privacy Shield: The saga continues.* Computer Law & Security Review: The International Journal of Technology Law and Practice (2016), doi: 10.1016/j.clsr.2016.07.013.
- Xavier Tracol, *"'Invalidator' strikes back: The harbour has never been safe"*, Computer Law & Security Review, volume 32, issue 2, April 2016, p. 360.

11.5 Online sources

- Opinion 1/2010 on the concepts of "controller" and "processor" of Article 29 Data Protection Working Party, No. 00264/10/EN, WP 169, adopted on 16 February 2010. Available at: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf > Last accessed 10 July 2016.
- Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing, of Article 29 Data Protection Working Party, No. 2588/15/EN, WP 232, adopted on 22 September 2015. Available at: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp232_en.pdf> Last accessed 10 July 2016.

- Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, of the Article 29 Working Party, No. 16/EN WP 238, adopted on 13 April 2016. Available at: < http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf >. Last accessed: 22 August 2016.

- E-15. Czech news portal. Available at: < http://e-svet.e15.cz/internet/google-se-brani-pravo-byt-zapomenut-nema-podle-nej-platit-globalne-1296747#utm_medium=selfpromo&utm_source=e15&utm_campaign=copylink >. Last accessed 24 August 2016.

- Data protection impact assessment by The Cloud Accountability Project. Available at: <http://www.a4cloud.eu/sites/default/files/Data%20Protection%20Impact%20Assessment.pdf >. Last accessed 19 August 2016.

- Model Contracts for the transfer of personal data to third countries. Available at: <http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm >. Last accessed: 20 August 2016.

- Datenschutz-Zertifizierung für Cloud Computing. Bundesministerium für Wirtschaft und Energie. Available at:

  <http://www.bmwi.de/DE/Presse/pressemitteilungen,did=600746.html>. Last accessed: 20 August 2016.

- Data Protection Officer by Slovak Office for Personal Data Protection. Available at: <http://dataprotection.gov.sk/uoou/en/content/data-protection-officer >. Last accessed: 20 August 2016.

- European Commission - Press release - Restoring trust in transatlantic data flows through strong safeguards: European Commission presents EU-U.S. Privacy Shield, Brussels, 29 February 2016. Available at: <http://europa.eu/rapid/press-release_IP-16-433_en.htm>. Last accessed: 22 August 2016.

- The U.S. Department of Commerce. Available at:

  < https://www.commerce.gov/page/about-commerce>. Last accessed: 22 August 2016.

- Guide to Self-Certification by U.S. Department of Commerce, available at: < https://www.commerce.gov/sites/commerce.gov/files/media/files/2016/how_to_join_privacy_shield_sc_cmts.pdf>. Last accessed: 22 August 2016.

- Fact Sheet Overview of the EU-U.S. Privacy Shield Framework For Interested Participants from 12 July 2016. Available at:

  <https://www.commerce.gov/sites/commerce.gov/files/media/files/2016/fact_sheet-_eu-us_privacy_shield_7-16_sc_cmts.pdf>. Last accessed: 22 August 2016.

- Report an Underage Child. Available at:

  < https://www.facebook.com/help/contact/209046679279097>. Last accessed 23 August 2016.

- European privacy requests for search removals. Available at:

  < https://www.google.com/transparencyreport/removals/europeprivacy/?hl=en-GB>. Last accessed 23 August 2016.

- Marcus Evans and Adam Smith. *EU Proposes "One Stop Shop" for Data Protection Supervision and Enforcement.* Available at:

  <http://www.dataprotectionreport.com/2015/04/eu-proposes-one-stop-shop-for-data-protection-supervision-and-enforcement/>. Last accessed 28 August 2016.

11.6 Privacy Policies

- The Apple Privacy Policy. Available at: < https://www.apple.com/uk/privacy/privacy-policy/>. Last accessed: 24 August 2016.
- The Google Privacy Policy. Available at: < https://www.google.com/intl/en/policies/privacy/>. Last accessed: 24 August 2016.
- The Dropbox Privacy Policy. Available at: < https://www.dropbox.com/privacy>. Last accessed 25 August 2016.
- The Facebook Data Policy. Available at: < https://www.facebook.com/policy.php>. Last accessed 25 August 2016.
- Facebook Security Help Center. Available at:
  < https://www.facebook.com/help/379220725465972> . Last accessed 28 August 2016.