EU DATA PROTECTION REFORM: CHALLENGES FOR CLOUD COMPUTING

Marina Škrinjar Vidović*

Summary: The EC adopted a strategy to unleash the potential of cloud computing, where it marked data protection legislation as one of the main barriers for the development and expansion of cloud computing in Europe. In light of the EC goal to ensure a stimulating environment for the development of cloud computing in the EU, this paper aims to assess the consequences of the new roles and responsibilities of cloud service providers and the new rights for individuals under the GDPR. The analyses show that, in line with the position of data protection in the EU as a fundamental right, the GDPR considerably raises standards of data protection in cloud computing, which faces EU cloud service providers with a more demanding position than their non-EU competition. Further analysis shows that by promoting privacy enabling technology and by the extraterritorial application of the GDPR, together with the hefty fines for non-compliance, the GDPR provides tools that might force non-EU service providers to adjust their business model to EU standards, thus rebalancing possible market disruption in cloud computing. The paper concludes that the GDPR provides tools that might result in raised standards of data protection globally and in cloud computing in particular.

1 Data protection reform in the context of cloud computing

The current EU Data Protection Directive[1] (DPD, Directive) was adopted in 1995 and came into effect on 25 October 1998. Since then, the DPD has been the principal legal instrument in the data protection field in the European Union.

---

* Marina Škrinjar Vidović, LLM (Utrecht). The author wishes to thank the anonymous reviewers for their comments and guidance.

[1] 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 [1995] OJ L281/31. The Data Protection Directive was transposed by the EU Member States and the three European Economic Area States: Iceland, Liechtenstein, and Norway by the Decision of the European Economic Area Joint Committee No 83/1999 Amending Protocol 37 and Annex XI (Telecommunications Services) to the EEA Agreement [2000] OJ L296/41. Switzerland has also implemented the Directive in the areas related to the Schengen Agreement: Annex B (Article 2(2)), Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's Association with the implementation, application and development of the Schengen Acquis [2008] OJ L53/52.

However, the data protection system has been among the most debated issues in the EU in recent years, and there are many different reasons for this. One of the most important changes was made with the entry of the Treaty of Lisbon[2] in December 2009, by which the Charter of Fundamental Rights of the EU[3] became legally binding and data protection was elevated to the status of a separate fundamental right (article 8). Consequently, this gave weight to the fundamental dimension of the DPD, which has been evident in the CJEU case law in recent years.[4] Further, the way in which data are collected, processed and accessed at present differs from the methods that were used around two decades ago. While the DPD provided a solid foundation for data protection, it was not equipped to handle the explosion in data collection and storage, and it did not specifically address the world of *cloud computing*,[5] which fell into a regulatory grey area. Another deficiency of the DPD is that it failed to produce the desired level of harmonisation of national legislations within the EU.[6] Rulings of the CJEU empowered national Data Protection Authorities (DPAs), which also had consequences for the different interpretation of the data protection rules.[7] This EU-wide disparity has

---

2 Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community [2007] OJ C306/01.

3 Charter of Fundamental Rights of the European Union [2012] OJ C326/391.

The Charter recognises the right to privacy in art 7 and the right to the protection of one's personal data in art 8.

4 In this regard, see M Brkan, 'The Unstoppable Expansion of EU Fundamental Right to Data Protection. Little Shop of Horrors?' (2016) 23(5) Maastricht Journal of European and Comparative Law 812.

5 According to C Millard, *Cloud Computing Law* (OUP 2013) 3, 'Cloud computing is a way of delivering computing resources as a utility service via a network, typically the Internet, scalable up and down according to user requirements'. According to Mell and Grance, the cloud model is composed of five essential characteristics (on demand self-service; broad network access; resource pooling; rapid elasticity; measured service), three service models (Software as a Service – SaaS; Platform as a Service – PaaS; and Infrastructure as a Service –IaaS), and four deployment models (Private cloud, Community cloud; Public cloud and Hybrid cloud). P Mell and T Grance, 'The NIST Definition of Cloud Computing' (2011) National Institute of Standards and Technology, US Department of Commerce (Special Publication 800-145) <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf> accessed 16 May 2016.

6 See Peter Hustinx, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation' 26-27 <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/ Documents/EDPS/Publications/Speeches/2014/14-09-15_Article_EUI_EN.pdf> accessed 16 May 2016, and the Commission's First Report on the Transposition of the Data Protection Directive <http://ec.europa.eu/justice/data-protection/document/transposition/index_en.htm> accessed 16 May 2016.

7 Eg, according to Case C–230/14 *Weltimmo* EU:C:2015:639, a company might be subject to multiple data protection authorities; in Case C-362/14 *Schrems* EU:C:2015:650, national data protection authorities are empowered to decide on a case-by-case basis whether a particular data transfer meets all the relevant requirements prescribed under the national legislation and EU directive.

in turn become a costly administrative burden for businesses.[8] Finally, the Snowden revelations of mass unauthorised surveillance operations of several countries have raised concern about privacy protection among EU citizens, which has given impetus to the reform of the data protection framework.

At the same time, in its digital agenda, the EC adopted the objective to unleash the potential of cloud computing. Estimations envisage that the cumulative economic impact of cloud computing in the EU could be up to EUR 940 billion and 3.8 million jobs for the period 2015–2020.[9] However, the EC has marked data protection legislation as one of the main barriers for the development and expansion of cloud computing in Europe.[10] In particular, the Commission emphasised that 27 diverging national legislative frameworks disenable a cost-effective cloud solution at the level of a digital single market, and, in particular, that there is a need for clarification of regulations of international data transfers in cloud. Other concerns emphasised were the need for increased transparency of data processing, and the need for the determination of the relevant location of a cloud provider.

The data protection working party, the so-called Article 29 Working Party (WP29)[11] adopted an Opinion on cloud computing on 1 July 2012.[12] In its Opinion, the WP29 outlined how the wide-scale deployment of cloud computing services can trigger a number of data protection risks, mainly a lack of control over personal data, as well as insufficient information with regard to how, where and by whom the data are being processed/sub-processed. The Opinion gives a list of recommendations on how to apply the present EU Data Protection Directive, which, although not obligatory, the Commission has welcomed.[13]

It seems that the development of cloud computing has shown all the shortcomings indicated by the DPD. The ability of data to move rapidly within the cloud and the lack of transparency about its physical location have presented problems for policy makers. While EU legislation is all

---

[8] See Commission, 'Data Protection' (2015) Special Eurobarometer 431/ Wave EB83.1 – TNS opinion & social, Summary, 2 <http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_sum_en.pdf> accessed 10 May 2016.

[9] Commission, 'Unleashing the potential of Cloud Computing in Europe' Communication COM(2012) 529 final, 8, quoting IDC (2012) 'Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Take-up' <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF> accessed 21 October 2016.

[10] ibid.

[11] The Article 29 Working Party is set is up under the Directive 95/46/EC. It is composed of representatives from all EU Data Protection Authorities, the EDPS and the European Commission. It has advisory status and acts independently.

[12] WP 29 Opinion 05/2012 on Cloud Computing, adopted on 1 July 2012.

[13] Commission (n 9) 9.

about keeping control over data and relies on the assumption that the controller has entire control of data processing, the use of cloud computing results in reducing the level of direct control. Additionally, most cloud computing contracts limit the liability of cloud processors to a level that is not equivalent to the potential risk for data subjects.

Following the challenges of the new technologies and the abovementioned shortcomings of data protection within the present Directive, in 2009 the European Commission announced it had started a procedure of data protection reform in the EU, and, finally, after years of intensive negotiations, in April 2016 the European Parliament adopted the long-awaited General Data Protection Regulation (GDPR, Regulation).[14] The Regulation will replace the current Data Protection Directive and will be directly applicable in every EU Member State. Still, the DPD remains the main legal instrument regulating this area of law in the EU until the GDPR comes into force on 24 May 2018. The Regulation itself does not deal specifically with cloud computing, but sets out to be technology neutral. This means that the rules of the GDPR apply regardless of the means used to process personal data. Nevertheless, it will have specific consequences for cloud computing due to the nature of data processing that takes place in the cloud.

The CJEU took an active role in shaping the GDPR during the tripartite negotiations between the European Parliament, the European Commission and the Council of Ministers, as the final text of the GDPR was highly influenced by its decisions adjudicated during the negotiations of the GDPR. In 2014, the Court issued a landmark ruling in the case *Digital Rights Ireland*[15] by which it invalidated the 2006 Data Retention Directive, which required private providers to retain for a considerable period electronic communication metadata for law enforcement purposes. The CJEU held that the EU legislature had exceeded the limits of the principle of proportionality in relation to certain provisions of the EU Charter (articles 7, 8 and 52(1)), thus placing EU citizens' privacy and data protection rights as a fundamental law on the centre stage. The *Google Spain* case[16] is of utmost importance, not only because the Court recognised the 'right to be forgotten' but even more because of its analysis of issues such as whether an internet search engine should be considered to be a data controller or a data processor; the territorial application of the EU data protection law; and the extension of data protection rights to the internet.

---

[14] 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) [2016] OJ L119/1.

[15] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* EU:C:2014:238.

[16] Case C-131/12 *Google Spain and Google* EU:C:2014:317.

Finally, in *Schrems*,[17] the Court invalidated the Safe Harbour adequacy decision for the transfer of data between the EU and US, stating that it does not offer a level of data protection equivalent to the level of protection in place in the EU. In particular, the Court found that the access enjoyed by the US intelligence services to the transferred data interferes with the right to respect for private life and the right to protection of personal data of EU citizens, thus enhancing the status of data protection as a fundamental right. Additionally, the decision enhanced the position of the DPAs as they gain the power to evaluate and counter EC adequacy decisions.

Making synergy between the rules of data protection as a human right and ensuring an environment for the development of the cloud market in the EU is challenging in many aspects. Considering that the Commission intends to promote the establishment and operation of cloud service providers in the European Union, and on the other hand aims to reassure EU citizens that their data in the cloud are safe and under their control, the questions explored in this paper aim to determine whether the GDPR will make these compliance issues easier for the EU cloud service providers in order to ensure for them an enabling environment. Therefore, the paper analyses new roles and responsibilities of cloud service providers under the GDPR. The impact of the new obligations will be analysed with regard to the scope of their implementation. This includes the provisions on encryption, extraterritoriality and trans-border data flow. Considering the topicality of cloud computing developments in the recent decade, reference is made in this paper to a number of scholars dealing with the most important insufficiencies of data protection rules in the complex cloud environment. The intention is not to analyse the technical aspects of cloud computing, although its most important aspects will be mentioned in order to analyse the final provisions of the GDPR and their impact. This paper does not attempt to provide any form of comprehensive economic analysis of the GDPR on cloud computing. It has a more limited purpose to merely highlight the potential impacts of and to caution against the potentially burdensome measures of the GDPR.

The paper concludes that the GDPR significantly raises standards in line with the position of data protection as a fundamental right, thus putting EU cloud service providers in a more demanding position than their non-EU competition. However, possible marked disruption might be rebalanced by applying privacy enabling technology and through the extraterritorial application of the GDPR, which will force non-EU service providers to adjust their business model to EU standards. This might result in raising data protection standards on the global cloud market.

[17] *Schrems* (n 7)

2 New responsibilities for cloud providers

The GDPR imposes a number of new obligations for cloud providers in two different ways: by introducing contractual responsibilities of data processors as well as by introducing new measures with the aim of enforcing the rights of data subjects. Both will be discussed in the following paragraphs.

2.1 Changes in the data controller and data processor relationship

Under the European data protection law, a distinction between the data controller and data processor is crucial in order to properly allocate responsibility and liability, and to determine applicable law. In this regard, the two main roles in cloud computing are cloud client and cloud service provider, where the cloud client will probably be considered as a data controller, and the cloud service provider as a data processor. However, in cloud computing sometimes it can be very difficult to establish whether the service provider is the data processor or the data controller. In reality, an individual (data controller) using a cloud computing service is unlikely to specifically determine the purpose and means[18] of how the personal data he/she controls is processed. In cloud databases, data are stored among servers and other storage equipment across the cloud that will be reunited and delivered to a user logging in with the right credentials.[19] Information and personal data are rapidly transferred from one data centre to another and the customer has no control over the 'means' with which the data are processed. Additionally, there are many consumer-oriented cloud services where users are provided with free services, while the cloud providers use the collected personal data (eg for targeted advertising) to help pay for them; in this case, the cloud service providers would be data controllers. Given this, the role played by cloud computing providers should be determined on a case-by-case basis in view of the nature of the cloud services.[20]

Under the current Data Protection Directive, cloud providers which act as data processors have few direct responsibilities,[21] and these are

---

[18] DPD (n 1) art 2; GDPR (n 14) arts 4(7) and 28(10).

[19] Millard (n 5) 9.

[20] P Hustinx, 'Data Protection and Cloud Computing under EU Law' (speech at the Third European Cyber Security Awareness Day, BSA, European Parliament, 13 April 2010) 3 <www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2010/10-04-13_Speech_Cloud_Computing_EN.pdf> accessed 10 May 2016.

[21] Therefore, in *Google Spain and Google* (n 16) the CJEU found that the definition of 'data controller' should be broadly construed, in order to provide 'effective and complete protection of data subjects'. Given this, it decided that the operator of a search engine is to be considered a data controller rather than a data processor. The search engine operator determines the purposes and means of that activity and thus of the processing of personal data that it itself carries out within the framework of the activity and is thus a controller.

mainly to ensure security of processing.[22] In this regard, the WP29 in its Opinion on the concepts of controller and processor[23] 'recognises the difficulties in applying the definitions in a complex environment where many scenarios can be foreseen involving controllers and processors, alone or jointly, with different degrees of autonomy and responsibility'. It has emphasised that there is a need to 'allocate responsibility between controller and processor in such a way that compliance with data protection rules will be sufficiently ensured in practice'. Therefore, with the aim of readjusting the definition of actors and roles, in some areas of the GDPR responsibilities are now placed on data processors directly, together with considerable fines for non-compliance, which will substantially change the position of the data processor in the cloud environment. This means that service providers now run the risk of direct enforcement action by a supervisory authority in the event of non-compliance with their new obligations.

In this regard, under the GDPR, cloud service providers will be required to comply with a number of new **specific obligations**, including to maintain adequate documentation of all their data processing activities,[24] implement appropriate security standards,[25] carry out routine data protection impact assessments,[26] appoint a data protection officer,[27] comply with the rules on international data transfers,[28] and cooperate with the national DPA.[29]

Presently, large cloud service providers (such as Google, Facebook, and Apple) which act as processors have standard, non-negotiable terms of service. Based on the popularity of these cloud providers, companies accept their take-it-or-leave-it contracts, and therefore are less in control of the data than they should be as controllers. This is why one of the key provisions affecting cloud computing services is article 28 GDPR, as it lists the **obligatory contractual terms** between processor and controller. This contract will now define how the processor carries out data processing on behalf of the controller, and presents a key tool for the transfer of responsibility between the controller and processor. In this regard, the contract between the controller and processor will now have to define the subject matter and duration of the processing, the nature and purpose of

[22] Arts 16 and 17 DPD (n 1).

[23] WP 29 Opinion 1/2010 on the concepts of 'controller' and 'processor', adopted on 16 February 2010.

[24] GDPR (n14) art 30.

[25] ibid, art 32.

[26] ibid, art 35.

[27] ibid, art 37.

[28] ibid, art 44.

[29] ibid, art 31.

the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.[30] However, more important are additional specific contractual obligations for processors which include their obligation: to ensure that the processor's staff are committed to confidentiality; to take adequate security measures to protect the data from loss, alteration or unauthorised processing; to engage a sub-processor only with the prior permission of the controller; to agree with the controller the necessary technical and organisational requirements for the fulfilment of the data subjects' rights in accordance with the Regulation; to assist the controller in meeting his/her obligation to notify the supervisory authority and the data subjects of a data breach; to hand over all personal data after the end of the processing or the termination of the service agreement; and to make information available to the controller and supervisory authority in certain circumstances.

Still, the Regulation maintained the current system under the Directive whereby **controllers are responsible** for the acts of processors. Moreover, the Regulation stipulates that where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the Regulation and ensure the protection of the rights of the data subject. This provision raises standards for cloud providers, and at the same time creates the obligation for the customer to test and examine the solution it is buying.[31]

Processors are obligated to act only on the **instructions of the controller**. If the processor makes its own decisions on personal data, rather than following the controller's instructions, that processor is treated as a controller in respect of that processing activity and is subject to the full compliance obligations of a controller in relation to that processing.[32] Here it must be noted that this provision is not appropriate for application to cloud service providers in IaaS. In this situation, it is generally the controller itself that processes data using the provider's resources, rather than the provider actively processing data for the controller, so it makes little sense to refer to the controller instructing the processor in relation to the processing of data in IaaS.[33] Considering that the GDPR tends to be technology neutral, it fails to correspond to the reality in which the technology works.

---

[30] ibid, art 28 (3).

[31] See Mark Weber, The GDPR's Impact on the Cloud Service Provider as a Processor (2016) 16(4) Privacy & Data Protecton.

[32] GDPR (n 14) art 28 (10).

[33] K Hon, J Hornle, C Millard, 'Data Protection Jurisdiction and Cloud Computing: When Are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing, Part 3 (2012) 26(2-3) International Review of Law, Computers & Technology 129, 152.

Another new requirement was added to the GDPR in order to resolve responsibilities between different roles and to ensure implementation of the guaranteed rights of data subjects. This concerns the obligation of **joint controllers** to stipulate in an arrangement their respective responsibilities, in particular their duties to allow individuals to exercise their rights to their personal data and to provide notice to individuals.[34] Joint controllers are each liable for the entire damage caused by the processing.[35]

In order to ensure effective implementation of the GDPR, all the foregoing has led to the introduction of a new liability scheme through which processors may be jointly and severally liable with controllers. Both controllers and processors will be subject to **administrative fines** under the GDPR, up to a maximum of EUR 20 million or 4% of the total worldwide turnover, whichever is higher.[36] It is of huge significance that processors will now be directly liable to those whose data they process. Individuals will have powers to seek a judicial remedy and claim compensation against a processor for infringing their rights as a result of the processor's non-compliance with the GDPR. Moreover, according to the rules of extraterritoriality of the Regulation, proceedings can be brought against a non-EU processor in the courts of the Member State where the individual resides. However, the processor is liable for the damage caused by its processing activities only where it has not complied with the obligations under the GDPR that are specifically directed to processors, or where it has acted outside or contrary to the lawful instructions of the controller. In this situation, the processor will be exempt from liability if it can demonstrate that it is not responsible for the damage.

Controllers and processers have until now defined their roles and obligations by contracts. However, the proposed new provisions will cause substantial changes in future contracting.[37] For example, the GDPR fundamentally changes the relationship between processors on one side and controllers, individuals and the DPA on the other. Under the present Directive, processors had no direct interaction with the DPA. However, now the DPA will have investigatory powers over processors and will be able to obtain access to all the personal data that the processor holds. It will have the right to access the processor's premises, issue warnings, order compliance, ban processing and ultimately issue fines. As previously noted, pro-

---

[34] GDPR (n 14) art 26 (1).

[35] ibid, art 26 (3)

[36] ibid, art 83

[37] See also the analysis by V Hordern, 'The EU General Data Protection Regulation: A Brave New World for Processors' (2016) World Data Protection Report, 16 WDPR 02, available at <www.hldataprotection.com/files/2016/03/Hordern-Art-16WDPR02.pdf> accessed 10 December 2016.

cessors (which employ more than 250 employees) are subject to the new obligation of maintaining records of processing activities in order to provide, upon request, the recorded information to the DPA. This is likely to require significant investment by processors in record-keeping functions.

To demonstrate compliance with the requirement to implement appropriate technical and organisational measures, processors may adhere to approved **codes of conduct or industry standards** drafted by associations or bodies representing both controllers and processors.[38] Such drafts must be submitted to the competent supervisory authority that will issue an opinion on the conformity of the draft to the Regulation, and, if favourable, will proceed to register it. These codes, once adopted as in compliance with the provisions of the Regulation, will certainly facilitate the drafting of future controller-processor contracts. In line with the activity envisaged in the EC Communication Unleashing the Potential of Cloud Computing in Europe, the EC established a Subgroup on the Code of Conduct for Cloud Service Providers within the Cloud Select Industry Group. The Code of Conduct was submitted to WP29 for its Opinion[39] according to which, at the time of writing this paper, the Code still does not meet the minimal legal requirements, and some substantial concerns remain (eg the definition of roles; the transparency of data processing; the applicability of the EU definition of personal data; reference to data portability; the requirement for international transfers, etc). Following the received WP29 Opinion, the Code of Conduct for Cloud Service Providers is currently being finalised. Considering that the GDPR is technologically neutral, once adopted, the Code will certainly be useful for cloud service providers in helping them align with the new provisions of the Regulation, but according to the specific environment of the cloud industry.

Both the Directive and the GDPR exclude a number of activities that, while they constitute the processing of personal data, are outside the scope of the EU data protection law. One of the debated exemptions connected with cloud computing is **household exemption**. Considering that there is a tendency for cloud providers to offer cloud computing services to individuals and end users, there was ambiguity about whether the cloud provider would be covered by the EU data protection framework, and hence whether individuals' data would be properly protected. In this regard, the GDPR expressly states that this Regulation

> does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commer-

[38] GDPR (n14) art 28 (5) in conjunction with art 40.

[39] WP29 Opinion on C-SIG Code of Conduct on Cloud Computing, adopted on 22 September 2015.

> cial activity. Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities.[40]

With the insertion of the last sentence, the Regulation fills the gap in household exemption and enters an explicit requirement which binds cloud providers to the same requirement as regular data processors when providing a service to a natural person whose processing falls into the scope of household exemption.

New obligations for processors under the GDPR have been criticised as inappropriate and burdensome when applied to a commoditised service, such as cloud infrastructure services or as a platform as a service model (IaaS/PaaS).[41] The problem is that considering the wide definition of personal data and the new roles of the processor, the cloud infrastructure service falls under the remit of the GDPR, although processors merely provide resources to cloud users and do not have knowledge of the nature of the data stored and/or lack the practical ability to access such data. Their position and business model will be substantially changed in order to meet the requirements imposed by the GDPR.

Another burden for cloud providers is the previously mentioned requirement for prior specific or general **written consent of the controller to another (sub) processor**.[42] Cloud services are generally provided by using subcontractors in various constellations.[43] However, because a typical cloud scenario may involve a larger number of subcontractors, the risk of processing personal data for further, incompatible purposes is quite high.[44] Now, according to the GDPR, when engaged, subprocessors must ensure the same data protection obligations as the one set out in the contract between controller and processor; in particular, they must provide sufficient guarantees to implement appropriate technical and organisational measures in such a way that the processing meets the requirements of the GDPR. Where the subprocessor fails to fulfil its

---

[40] GDPR (n14), recital 18.

[41] See Kuan Hon, 'GDPR: Killing Cloud Quickly? (*Privacy Perspectives*, 17 March 2016) <https://iapp.org/news/a/gdpr-killing-cloud-quickly/> accessed 15 December 2016.

[42] In line with WP 29 Opinion (n 12).

[43] See in this regard, EU Expert Group on Cloud Computing Contracts' 'Discussion Paper on Subcontracting', 25 March 2014 <http://ec.europa.eu/justice/contract/files/expert_groups/expert_group_subcontracting_discussion_paper_en.pdf> accessed 15 December 2016.

[44] WP 29 Opinion (n 12) 11.

obligation, the initial processor remains fully liable to the controller for the subprocessor's acts. As Hon emphasises,[45] there is a higher probability that only the big (US) players in the cloud industry that control their supply chain will be able to pass the GDPR obligations onto the subprocessors' chain of liability, while small SaaS providers will have difficulties in negotiating with Amazon, Google or Microsoft to get them to accept these extra obligations. This, she predicted, will leave the larger players to dominate Europe's cloud market.[46] Unbalanced negotiating positions were also acknowledged by the WP29 which urged the Commission to provide for a more proactive role for consumer and business interest organisations in order to negotiate more balanced general terms and conditions from big cloud computing providers.[47] At the same time, the WP29 states that 'this imbalance in the contractual power of a small controller with respect to large service providers should not be considered as justification for the controllers to accept clauses and terms of contracts which are not in compliance with data protection law'.[48] The Regulation does not have transitional arrangements with regard to the existing contracts, so all service providers who handle personal data, whether or not cloud based, will have to renegotiate contracts with data controllers to make sure liability is properly allocated according to the GDPR provisions.

2.2 Measures for enhancing the rights of individuals

As stated by the legislators,[49] the very aim of the Regulation is to put control of their data back into the hands of the data subjects. In line with this, the Regulation enhances existing and at the same time creates two new individual data protection rights: the rights to erasure and the right to data portability, which will have a direct effect on cloud providers and thus are analysed in more detailed below.

The right to erasure builds on and expands the so-called 'right to be forgotten' recognised by the CJEU.[50] According to the adopted pro-

---

[45] See Kuan Hon's series of publications on the GDPR influence on cloud computing <www.kuan0.com/publications.html> accessed 15 December 2016. See particularly Graeme Burton, 'Costs and Administrative Burdens of GDPR Will Help US Companies Dominate the EU's Cloud Computing Market' (*V3*, 27 October 2016) <www.v3.co.uk/ v3-uk/ news/2475499/costs-and-administrative-burdens-of-gdpr-will-help-us-companies-dominate-the-eus-cloud-computing-market> accessed 15 December 2016.

[46] However, see the contrary opinion of P Bindley cited in N Ismail 'Capability and Not the Size of Cloud Service Providers Will Determine Which of Them Thrive Under the GDPR' (*Information Age*, 14 November 2016) available at <www.information-age.com/size-matter-cloud-post-gdpr-123463175/> accessed 20 December 2016.

[47] WP29 Opinion (n 12) 23.

[48] ibid 14.

[49] See Commission, 'Protection of Personal Data' (*European Commission: Justice*) <http://ec.europa.eu/justice/data-protection/> accessed 15 December 2016.

[50] *Google Spain Google* (n 16).

vision of the Regulation, controllers must erase personal data without undue delay if: the data are no longer necessary in relation to the purpose for which they were collected; the data subject withdraws consent or there is no other legal ground for processing; the data subject objects to the processing; personal data have been unlawfully processed; personal data have to be erased in accordance with national law; personal data have been collected in relation to the offer of information society services directly to a child. Following criticism[51] that the right to erasure conflicts with other fundamental rights, the final text of the GDPR stipulates that the right to erasure has to be balanced against the freedom of expression and the right to information, compliance with a Union or Member State legal obligation, the performance of a task of public interest or the exercise of official authority, public interest in health, scientific and historical research, and the exercise or defence of legal claims.

The GDPR reinforces the right to erasure by clarifying that organisations in the online environment which make personal data public should take 'reasonable steps' to inform other organisations that process the personal data to erase links to, copies or replication of the personal data in question.[52] The Regulation does not define 'reasonable steps', as these will depend on available technology and the cost of implementation, but taking into consideration the possibility of a massive transfer of data in the cloud environment, and that the location of specific data may be difficult to determine in the cloud due to fragmentation, as well as the open question about who the original controller is and how the original controller will be able to identify other controllers it needs to notify in the complex cloud environment, it can be presumed that the right to erasure will present a substantial burden for cloud providers.[53]

However, the main deficiency of this provision is that data controllers will now be tasked with the role of judge and jury when considering requests for the erasure of data.[54] There is a high possibility that data controllers will not risk high administrative fines (again up to EUR 20,000,000 or 4% of the total worldwide annual turnover, whichever is

---

[51] See V Reading, 'The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age' (speech held at the DLD Conference in Munich, 22 January 2012) <http://europa.eu/rapid/press-release_SPEECH-12-26_hr.htm> accessed 1 December 2016.

[52] GDPR (n 14) art 17(2) in conjunction with recital 66.

[53] In that regard, see ENISA, 'The Right to Be Forgotten – Between Expectations and Practice' (*European Union Agency for Network and Information Security*, 20 November 2012) <www.enisa.europa.eu/publications/the-right-to-be-forgotten> accessed 20 September 2016.

[54] In this regard, see eg G Francoise, 'The Right of Erasure or Right to be Forgotten: What the Recent Laws, Cases, and Guidelines Mean for Global Companies (2015) 18(8) Journal of Internet Law 1, 8; ML Rustad and S Kulevska, 'Reconceptualising the Right to be Forgotten to Enable Transatlantic Data Flow' (2015) 28(2) Harvard Journal of Law & Technology.

higher) and that they will generally erase data following the data subject's request, which could subsequently have an impact on achieving a balance with freedom of speech and the right to information regardless of the imposed safety provisions. Considering that the right to erasure presumes conducting a balancing test between different fundamental rights which was until now done by the CJEU itself, it is unrealistic to expect cloud service providers to be qualified for this exercise. Therefore, very precise instructions on the application of the right to erasure should be provided, preferably by the WP29,[55] and the role of national DPAs should be enhanced as an advisory body in regard to the enquiries on the application of right to erasure.

Another new burdensome measure is the **right to data portability**[56] which was adopted with the aim of solving vendor lock-in problems. The right to data portability requires data controllers to ensure that they can hand over the personal data they possess about the data subject in a usable and transferable format, when the data is provided and processed on the basis of consent or contract. Currently, most cloud providers do not make use of standard data formats and service interfaces facilitating interoperability and portability between different cloud providers.[57] For small and medium sized enterprises, this new right to transfer personal data between controllers creates a disproportionate and significant additional burden, requiring substantial investment in new systems and processes to ensure export and import mechanisms for the transfer of data.[58]

According to the EU Expert Group on Cloud Computing Contracts,[59] the migration of data should be considered as a chargeable extra service to be offered by cloud providers. However, this might create the risk of 'big' cloud providers increasing the transaction costs necessary to shift from one service to another, and in this way locking their users into their systems. This could be considered an abusive practice insofar as the cloud providers hold a dominant position in the market.[60]. Therefore, there is a policy recommendation that the rule of data portability should be com-

---

[55] In this regard, WP29 already adopted on 26 November 2014 the Guidelines on the implementation of the Court of Justice of the European Union judgment in Case C-131/12 *Google Spain SL and Google Inc v Agencia Española De Protección De Datos (Aepd) and Mario Costeja González*.

[56] GDPR (n 14) art 20.

[57] WP29 Opinion (n 39) 12.

[58] See P Swire and Y Lagos, 'Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique' (2013) 72(2) Maryland Law Review 335.

[59] EC Expert Group on Cloud Computing Contracts, Synthesis of the Meeting of 11/12 December 2014 <http://ec.europa.eu/justice/contract/files/7th_expert_group_synthesis_final.pdf> accessed 1 December 2016.

[60] P De Filippi and L Belli, 'Law of the Cloud v Law of the Land: Challenges and Opportunities for Innovation' (2012) 3(2) European Journal for Law and Technology 6.

plemented with the EU competition rules and policy.[61] In its Guidelines on the right to data portability issued on 13 December 2016, the WP29 emphasis that article 12 GDPR prohibits the data controller from charging a fee for the provision of personal data, unless the data controller can demonstrate that the requests are manifestly unfounded or excessive, 'in particular because of their repetitive character'. [62] Further, it states that, in fact, article 12 GDPR focuses on the requests made by one data subject and not on the total number of requests received by a data controller, and that, as a result, the overall system implementation costs should neither be charged to the data subjects nor be used to justify a refusal to answer portability requests. However, it remains to be seen how the cloud market will apply this recommendation.

2.3 Concluding remarks

Following the inclusion of the new measures for enhancing the right of individuals and for the new responsibilities of data processors under the GDPR, cloud service providers will have to substantially change the way they operate. Investment will be needed in policies, procedures, technologies, training and staff to ensure full compliance with the GDPR. For example, according to the ICO study on the expected costs for GDPR compliance,[63] the UK Ministry of Justice produced research of its own that concludes the cost to UK business could be as high as £320 million a year, and £2.1 billion over fourteen years.[64] All this can have a substantial influence on prices and might disrupt the market of cloud computing. In this regard, the EC might use the possibility to co-finance investments and provide free training through EU funds and programmes for supporting small service providers in meeting their new legal obligations.[65] Ad-

---

[61] Eg B Engels, 'Data Portability Among Online Platforms' (2016) 5(2) Internet Policy Review <https://policyreview.info/articles/analysis/data-portability-among-online-platforms> accessed 20 September 2016.

[62] WP29 Guidelines on the right to data portability, adopted on 13 December 2016, 12.

[63] See London Economics, 'Implications of the European Commission's Proposal for a General Data Protection Regulation for Business' (Final Report to the Information Commissioner's Office, May 2013) <https://ico.org.uk/media/1042341/implications-european-commissions-proposal-general-data-protection-regulation-for-business.pdf> accessed 20 December 2016.

[64] One responder to the survey predicted that GDPR would cost their company £5 million to become compliant, and £1 million a year to maintain it!

[65] The EU already promotes and supports the research and development of privacy enhancing technologies, privacy by design and privacy by default settings through research priorities in FP 7. In this regard, see Commission Staff Working Paper – Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and the Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, SEC(2012) 72 final, 95.

ditionally, the EC should provide additional measures in order to ensure more balanced general terms and conditions with regard to big cloud computing providers, as the GDPR fails to deal with this problem. Detailed instructions on the implementation of the right to erasure should be prepared, preferably by the WP29, and DPAs should be enhanced as an advisory body in this regard.

However, even in the case of a breach of GDPR obligations, big cloud players will be in a better position to 'afford' the fines, which is not true for start-ups and small service providers. Although the GDPR stipulates that there is joint liability between controllers and processors, it will be the customer's choice as to who they want the fines paid by, and it is then up to the data processor to be refunded from the responsible parties within the supply chain.[66] Therefore, a processor could be sued, perhaps because it is seen as bigger, even if the damage was caused by the controller.[67] If contracts between processors and controllers are not negotiated properly and are not detailed enough, the question of compensation might end up in court proceedings[68] during which the processor might lose its market position and its service might no longer be compatible with the other services on the market. In order to avoid this situation, small cloud processors should be empowered in negotiating contracts, as proposed by the WP29. A useful tool could be the Code of Conduct that is being finalised and which will reconcile the Regulation requirements to the specific environment of the cloud industry, and which should have more detailed provisions on determining responsibilities and the division of liability.

The new responsibilities of data processors and the rights of data subjects reflect the intention of the legislator to ensure the highest level of protection of personal data of EU citizens as a fundamental right. Obviously and justifiably, the scale is tipping towards ensuring the privacy and security of EU citizens on account of the enabling environment for cloud computing in the EU. This might result in market disruption in favour of the dominant non-EU cloud service providers. However, the real impact of the GDPR must be determined with regard to its scope of application. This includes rules on anonymisation, territorial application and trans-border data flows that are analysed further in the text.

---

66 Bindley (n 46).

67 Kuan Hon, 'Open Season on Service Providers? The General Data Protection Regulation Cometh…' (SCL – The IT Law Community, 4 August 2015) <www.scl.org/site.aspx?i=ed43376> accessed 1 December 2016

68 GDPR (n 14) art 82 (6).

3 Anonymisation and the re-indentification risk in the cloud environment

The Regulation defines personal data as any information relating to an identified or identifiable natural person, ie data subject.[69] Further, it states that an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier. The Regulation lists the identifiers;[70] however, the list is not exhaustive (it states 'such as'). The definition of personal data adopted in the GDPR leans heavily on one adopted in the DPD and it reflects the intention of the European lawmaker to embrace a wide notion of personal data that was also confirmed by WP29[71] and CJEU case law.[72] Even more, the Regulation broadens the list of identifiers to include online identifiers,[73] such as internet protocol addresses,[74] cookie identifiers or other identifiers such as radio frequency identification tags, as they 'may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them'. Accordingly, the wider the definition of personal

---

[69] ibid, art 4 (1).

[70] GDPR (n 14) art 4(1): Identifiers are: name, an identification number, location data, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of that natural person

[71] WP 29 Opinion 4/2007 on the concept of personal data, adopted on 20 June 2007.

[72] Eg Case C-101/01 *Bodil Lindqvist* ECLI:EU:C:2003:596: The name of a person in conjunction with his/her telephone number, and information about his/her working conditions or hobbies constitute personal data; Case C-212/13 *Rynes* ECLI:EU:C:2014:2428: The image of a person recorded by a camera constitutes personal data because it makes it possible to identify the person concerned; Case C-201/14 *Bara* ECLI:EU:C:2015:638: Tax data transferred are personal data, since they are information relating to an identified or identifiable natural person; Case T-259/03 *Nikolaou* ECLI:EU:T:2007:254: The information published in the press release was personal data, since the data subject was easily identifiable, under the circumstances. The fact that the applicant was not named did not protect her anonymity; Case C-582/14 *Breyer v Germany* ECLI:EU:C:2016:779: the ECJ stated that dynamic IP addresses held by a website operator constitute personal data as long as the operator has the legal means which enable it to identify the data subject with additional data which the [ISP] has about that person.

[73] GDPR (n14) recital 30.

[74] In line with the Case C-70/10 *Scarlet Extended* ECLI:EU:C:2011:771 and *Breyer* (n 72); as well as with WP29 Opinion 4/2007 (n 71) 16. Presently MSs have different views as to whether IP addresses constitute personal data that are subject to data protection laws. For example, courts in Sweden (*Antipyratbyran*), Spain (*Promusicae*) and Austria have all found that IP addresses are personal data in the context of such cases, taking a broad view of personal data as does the Article 29 Working Party. But in its decisions, courts in France (the *Limewire*, *Anthony G* and *Henri S* decisions) and Italy (the *Peppermint* case) have both found IP addresses not to be personal data. See detailed analyses: time.lex, 'Study of Case Law on the Circumstances in Which IP Addresses Are Considered Personal Data (Final Report, 2 May 2011) 209

<http://www.timelex.eu/frontend/files/userfiles/files/publications/2011/IP_addresses_report_-_Final.pdf> accessed 15 December 2016.

data, the greater is the chance that the services of the cloud providers will fall under the remit of the Regulation. The second precondition for the application of the GDPR is that personal data are being processed. While the definition of processing is in line with that adopted in the DPD,[75] it would probably include most of the operations that are likely to occur in the cloud, including simply the storage of data (IaaS).

However, the nature of cloud services conflicts with the EU data protection requirements. It is said that cloud services are natively 'data indifferent' or 'data blind'.[76] In particular, Infrastructure as a Service (IaaS) has not been designed around the processing of personal data. In these cases, the cloud service provider acting as a data processor typically does not identify the personal data on their service, in particular when they are not entitled under the service agreement to identify such personal data, or when the customer has deployed tools such as data encryption which prevent the cloud service providers from identifying the personal data on their service.[77] In fact, customers can encrypt their personal data before uploading to the cloud in a way that the cloud provider has no access to the decryption key, so that no privacy risks can arise.[78] Therefore, in the context of the data protection framework in the cloud computing environment, the important question is whether the processor, who is holding encrypted data without holding the keys and as such is not aware of the contents and nature of these data, is required to comply with extensive data protection requirements. In this respect, the main question for the cloud service provider is whether anonymised, pseudonymised and encrypted data before submission to the cloud provider by the cloud customer fall under the remit of the definition of personal data.

Presently, according to recital 26 of the Data Protection Directive, the principles of data protection do not apply to data rendered anonymous. However, the interpretation and application of anonymous data are not straightforward, especially when considering how to anonymise personal data sufficiently to take data outside the Data Protection Directive.[79] The Article 29 Working Party (WP29), in its Opinion on anonymisation techniques,[80] made a rigid interpretation of personal data that have been pseudonymised, strongly encrypted or anonymised, expressing doubts

---

[75] GDPR (n14) art 4 (2).

[76] This is true for the IaaS and PaaS service. See M Maggiore, 'Cloud Computing: Obligations under the Directive v GDPR' (June 2016) Data Protection Law & Policy. However in many consumer-oriented cloud services, users are provided with free services while cloud providers use collected personal data (eg for targeted advertising) to help pay for them.

[77] See WP29 Opinion (n 39) 7.

[78] See Kuan Hon, 'Dark Clouds?' (2016) 43(4) Intermedia Journal of the International Institute of Communications.

[79] Millard (n 5) 168.

[80] WP29 Opinion 05/2014 on Anonymisation Techniques, adopted on 10 April 2014.

on those techniques and suggesting a cautious approach. Moreover, in the same Opinion, the WP29 analysed the real risks of (re)identification in very abstract terms, stating that technology is changing and the risk of re-identification cannot be completely eliminated on account of future technological developments, particularly if there is the possibility of combining different data sets.

It is undisputable that advances in technology, by the recombination of separate databases and by building connections between items of data and thereby identifying the person to whom they relate, have helped the de-anonymisation or re-identification of individuals hiding in anonymised data.[81] However, scholars argue that following the WP29 Opinion on anonymisation, easy re-identification makes the EU data protection legislation too broad and hinders the development of IT services in general. It is said that 'a law that was meant to have limits is rendered limitless, disrupting the careful legislative balance between privacy and information flow and extending datahandling requirements to all data in all situations'.[82]

In practice, not all DPAs accepted the WP29's strict position on anonymisation. For example, the UK's DPA, the Information Commissioner's Office (ICO), in its code of practice on anonymisation states: 'The DPA does not require anonymisation to be completely risk free – you must be able to mitigate the risk of identification until it is remote ... 100% anonymisation is the most desirable position, and in some cases this is possible, but it is not the test the DPA requires'.[83] Therefore, the ICO, along with the Swedish DPA,[84] accepted a risk-based approach aimed at assessing the risk of identification and related harm to the data subject.[85] Accordingly, a service provider's obligation is to take reasonable care to preserve confidentiality, taking account of the state of the technology at the time. However, a wise provider will need to keep alert to new developments in re-identification, as a failure to adapt to new technologies

[81] Many scholars have analysed the re-indentification problem. Eg, see P Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymisation' (2009) 57 UCLA Law Review 1701. IS Rubenstein and W Hartzog, 'Anonymization and Risk' (2016) 91 Washington Law Review 703; D Nunan, M Di Domenica, 'Exploring Reindentification Risk: Is Anonymization a Promise We Can Keep?' (2015) 58(1) International Journal of Market Research 19.

[82] Ohm (n 81) 1741.

[83] Information Commissioner's Office, 'Anonymisation: Managing Data Protection Risk. Code of Practice (ICO 2012) <https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf> accessed 20 September 2016.

[84] See Swedish Data Protection Authority, 'Cloud Services and the Personal Data Act' <http://www.datainspektionen.se/in-english/cloud-services/> accessed 20 September 2016.

[85] See also the test for assessing the risk of identification proposed by Ohm (n 81).

can also amount to a failure to take reasonable care.[86] Accordingly, the intended storage period of information is also relevant, as, for example, anonymised data meant to be stored for a month might not be considered personal data, and there is less chance for re-indentification in one month than in a period of several years.[87]

The adopted text of the Regulation, in line with the DPD, similarly states that using data rendered anonymous in such a way that the data subject is no longer identifiable does not fall under the scope of the application of the EU regulatory framework on data protection.[88] This is in line with the status of anonymisation in the data protection framework, where it has become, in legal and regulatory terms, a marker of the boundary between public and personal data and thus a key part of data protection legislation.

Additionally, and in line with the technical developments in re-identification techniques, the Regulation introduces the new legal concept of pseudonymisation. The GDPR defines pseudonymisation as the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information. To pseudonymise a data set, the identifier must be kept separately and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable person. Like encryption, pseudonymisation is considered a security protection measure[89] and it is also explicitly mentioned as a 'data by protection by design and by default' or PbD technique.[90] The GDPR has incentives for controllers to pseudonymise the data that they collect. For example, in the event of a data breach affecting pseudonymised data, data subjects may not need to be informed if the *key* to allow re-identification was not compromised.[91] Additionally, controllers that pseudonymise their data sets will have an easier time using personal data for secondary purposes and for scientific and historical research,[92] as well as meeting the Regulation's data security and data by design requirements.[93]

Still, according to the GDPR, although pseudonymisation reduces the risks of processing, it is not intended by the Regulation to preclude

---

86 C Reed, 'Information "Ownership" in the Cloud' (2010) Queen Mary University of London, School of Law, Legal Studies Research Paper No 45/2010, 20.

87 K Hon, C Millard and I Walden, 'The Problem of "Personal Data" in Cloud Computing' (2011) 1(4) International Data Privacy Law.

88 GDPR (n 14) recital 26.

89 ibid, art 32.

90 ibid, art 25.

91 ibid, recital 29.

92 ibid, recital 156.

93 ibid, recital 78.

any other measures of data protection.[94] Still, much debate surrounds the extent to which anonymised and pseudonymised data can be re-identified. This issue is of critical importance because it determines whether a processing operation will be subject to the provisions of the Regulation, especially considering newly imposed obligations on processors that will have a strong impact on cloud service providers. The GDPR emphasis that the data controller should have in place appropriate technical and organisational measures to mitigate the risk of de-identification.[95] Further, distinguishing between pseudonymous data, which fall under the scope of the GDPR, and anonymous data, which do not, the GDPR acknowledges the DPD provision that in risk assessment account should be taken of all the means *reasonably likely to be used*, such as singling out, either by the controller or by another person, to identify the natural person directly or indirectly.[96] In assessing what means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and also technological developments. It seems that by acknowledging the objective standard of 'reasonable effort' as opposed to the currently very extensive WP29 approach to the risk of re-identification, there is good basis for the GDPR to provide greater flexibility concerning the applicability of anonymised and pseudonymised data.[97] For example, where the controller deletes the identification key, and where the remaining indirect identifiers pose little risk of identifying an individual, the controller may be able to argue that there is no reasonable risk of re-identification and that it does not fall under the GDPR obligations.

In this respect, the recent judgment of the CJEU in *Breyer*[98] is particularly significant. Although the CJEU did not expressly deal with the re-identification issues, in its decision the court recognises that there are two opposing views, ie 'objective' or 'relative' criteria, on whether someone is identifiable.[99] The Court ruled that dynamic IP addresses can constitute personal data when the data controller, according to national law, has the legal means to ask additional information from a third party in order to truly identify a person. One can conclude that if there are no available legal means under the respective local laws for the respective

---

94 ibid, recital 28.

95 ibid, recital 75.

96 ibid, recital 26.

97 See G Maldoff, 'Top 10 Operational Impacts of the GDPR: Part 8 – Pseudonymization (*The Privacy Advisor*, 12 February 2016) <https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-8-pseudonymization/> accessed 15 September 2016.

98 *Breyer* (n 72).

99 ibid, para 25.

party to identify an individual, the dynamic IP address may not constitute personal data. Therefore, although the CJEU does not directly consider the issue of the likelihood of identification, one can conclude from its ruling that it adopted the objective standard of 'reasonable effort' as defined by the GDPR.[100]

As scientific and research developments have made it more difficult to truly anonymise personal data and to guarantee anonymisation, and have made it easier to re-identify data subjects from anonymous data, more and more data may fall within the pseudonymous rather than anonymous category.[101] On the other hand, if the techniques that underlie the principles of anonymisation are shown to be broken, there are serious implications for those who rely on it to maintain trust.[102] While the concept of data protection through technology is a key component of modern data protection law, without mandatory requirements and legal incentives, there is the risk that developers and controllers will not provide privacy enhancing technologies to their respective customers.[103] This is in line with the finding of an analysis of the terms of services of cloud providers,[104] which found that the majority of the companies at issue do not mention encryption policies in their terms of services. While it is clear that using privacy enhancing technologies is an additional cost to companies, the accepted legal solution, ie the inclusion of incentives for pseudonymisation, as well as acknowledging the objective standard of 'reasonable effort' for re-identification, might encourage cloud providers to use anonymisation and pseudonymisation when processing personal data, and thus in fact raise the security of data subjects, especially taking into consideration the amount of data stored in the cloud service. In fact, by imposing objective criteria for de-identification, it could be concluded that the Regulation in essence provides the right balance between data protection as a fundamental right and ensuring an environment for the development of the cloud market in the EU. However, this again will depend on its implementation.

---

[100] See also the analysis of G Spindler and P Schmechel, Personal Data and Encryption in the European General Data Protection Regulation' (2016) 7(2) Journal of Intellectual Property, Information Technology and E-Commerce Law <www.jipitec.eu/issues/jipitec-7-2-2016/4440> accessed 15 September 2016.

[101] Kuan Hon and others, 'Cloud Accountability: The Likely Impact of the Proposed EU Data Protection Regulation' (2014) Tilburg Law School Legal Studies Research Paper Series, No 07/2014, 10.

[102] Nunan and Domenico (n 81) 22.

[103] G Hornung, Regulating Privacy Enhancing Technologies: Seizing the Opportunity of the Future European Data Protection Framework' (2013) 26(1-2) European Journal of Social Science Research 181, 181.

[104] K Stylianou, J Venturini, N Zingales, 'Protecting User Privacy in the Cloud: An Analysis of Terms of Service' (2015) 6(3) European Journal of Law and Technology 16.

The WP29, in its Opinion 02/2015 on the C-SIG Code of Conduct on Cloud Computing, adopted on 22 September 2015, required the inclusion of its high standards of anonymisation as defined in the above cited Opinion on anonymisation techniques in the final text of the Code. It will be interesting to see whether this requirement will be changed following the provisions adopted in the GDPR and recent case law.

4 The extraterritorial application of the GDPR

When considering the scope of application of the GDPR, we are talking about jurisdiction. The doctrine distinguishes three main types of jurisdiction: prescriptive (or legislative), judicial (or adjudicative) and enforcement jurisdiction. The terminology itself gives insights into their scope: prescriptive (or legislative) jurisdiction relates to the power to make law in relation to a specific subject matter; judicial (or adjudicative) jurisdiction deals with the power to adjudicate a particular matter; and enforcement jurisdiction relates to the power to enforce existing law (for example, arresting, prosecuting and/or punishing an individual under that law). All these forms of jurisdiction may be exercised in an extraterritorial manner.[105] The doctrine distinguishes the application of the extraterritoriality principle[106] in public international law and in the EU data protection framework. Accordingly, the concept of extraterritoriality in public international law aims to protect an individual who is not physically present in the territory that is party to a particular human rights treaty, and hence in principle it applies only in a vertical relationship. On the other hand, the EU data protection framework mainly seeks to protect the data subject residing in the EU territory but experiencing data protection violations from a controller established in a third county. The extraterritorial principle of the EU data protection framework is applicable in both vertical and horizontal situations, and protects data from both public and private controllers.[107]

However, not all jurisdictional claims are equally likely to be carried out in practice. Jurisdictions with no prospects of being exercised in reality are in doctrine described as regulatory overreaching. While a number of authors see regulatory overreach as a problem *per se*,[108] there are

[105] On the differentiation of extraterritoriality and territorial extension, see J Scot, 'Extraterritoriality and Territorial Extension in EU Law (2014) 62 American Journal of Comparative Law 87; and J Scott, 'The New EU "Extraterritoriality"' (2014) 51 CML Rev 1343.

[106] On the concept of extraterritoriality, see C Kuner, 'Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law (2015) 5(4) International Data Privacy Law 238.

[107] Brkan (n 4) 828-829.

[108] See C Kuner and others, 'The Extraterritoriality of Data Privacy Laws – An Explosive Issue Yet to Detonate' (2013) 3(3) International Data Privacy Law.

also opposite positions stating that even if jurisdiction is not enforceable, there is a positive impact of its enactment in the form of fear of a sanction in the case of non-compliance.[109] In cloud computing, it is difficult to determine at any given time the location of personal data and of the equipment being used, and therefore there is a need for clear guidelines on the applicable law in order to address new technological developments.[110] This is why the debate on extraterritorial enforcement jurisdiction is especially relevant when discussing the extraterritorial principle of the EU data protection framework and its application in cloud computing, more importantly taking into consideration the new responsibilities and measures imposed by the GDPR on cloud service providers.

4.1 Scope of the GDPR and its impact on cloud computing

The Regulation states that even the establishment of a controller or a processor in Member State territory will trigger applicability regardless of whether the processing takes place in the Union or not,[111] even if it processes personal data of only non-EU residents. This concept is in doctrine defined as the **country of origin approach**.[112] The Regulation defines territorial scope by reference to the processing of personal data in the context of the activities of an establishment in the Union. The provision 'context of activities' might lead to extensive judicial jurisdiction, and its implementation will depend on the national courts' interpretation that can lead to a different implementation of the Regulation contrary to the intentions of the legislator. Additionally, in order to eliminate present MS national law conflicts, the Regulation included the main establishment concept.[113] However, the provision of the main establishment concept is not straightforward in the context of cloud computing. For example, cloud providers might have a number of data centres located within different MSs where no main decision or main processing is made, with headquarters outside the EU, and the Regulation does not give guidance on which data centre would be the main establishment in this situation.[114] However, as long as a data controller (cloud client) or data processor (cloud provider) is located within the EU, all processing conducted by the said controller or processor would be subject to the GDPR, even if these activities are not actually conducted within EU territory or related

[109] See DJB Svantesson, 'The Extraterritoriality of EU Data Privacy Law: Its Theoretical Justification and its Practical Effect on US Businesses' (2014) (50)(1) SJIL 60.

[110] See WP29 Opinion 8/2010 on Applicable Law, adopted on 16 December 2010.

[111] GDPR (n 14) art 3(1).

[112] See K Hon, J Hornle and C Millard, 'Data Protection Jurisdiction and Cloud Computing: When Are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing, Part 3' (2012) 26(2-3) International Review of Law, Computers & Technology 129.

[113] GDPR (n 14) ref 36, art 4(16).

[114] See Hon, Hornle and Millard (n 112) 136.

to EU data subjects. Criticism has been made that, considering the strict provisions of the GDPR, this requirement may have the effect of deterring non-EU cloud providers from setting up or retaining any establishments in the EU, which may be said to be places of administration, such as EU offices, or from building or using EU data centres or EU sub-providers.[115]

Secondly, as regards prescriptive jurisdiction, the GDPR applies extraterritorially to any entity (data processor or a data controller) that offers goods or services to residents (data subjects) of the EU. This concept is in doctrine defined as the **targeting approach**. Therefore, if the service provider is established outside the EU but offers services within the EU, the Regulation will also apply following the location of people in the EU whose data is being processed. The Regulation also clarifies that offering goods or services to data subjects in the Union irrespective of whether payment is required, or monitoring the behaviour of data subjects as far as their behaviour takes place within the Union, will trigger applicability.[116] This provision has direct effect on cloud computing, as there are many consumer-oriented cloud services where users are provided with free services while cloud providers use collected personal data (eg, for targeted advertising) to help pay for them.[117]

Recital 23 of the Regulation lays out the criteria for determining whether a data controller is offering goods or services to data subjects in the EU. Basically, if it is apparent that the data controller is envisaging the offering of services to data subjects residing in one or more EU Member States, the legislation would apply. Thus, a website or application would become subject to the law only to the extent that it actively markets to the particular geographic area, but not if it merely provides a site or application that is available to individuals in a particular geographic area.[118] Additionally, if a company operates a service in the MS language[119] or currency of a MS country, or if it mentions customers of the MS, it could trigger the applicability of the GDPR. To determine whether individuals' behaviour is being monitored, it should be assessed whether individuals are tracked on the internet, including subsequent profiling, in particular for analysing or predicting their personal prefer-

---

[115] ibid 151.

[116] GDPR (n 14) art 3(2).

[117] See EC Expert Group on Cloud Computing Contracts, Synthesis of the Meeting of 30 April 2014, Overview of Current Terms Relating to the Use of Content, 1 <http://ec.europa.eu/justice/contract/files/final_synthesis_30_april_6th_meeting_en.pdf> accessed 10 December 2016.

[118] GDPR (n 14) recital 23; in line with the CJEU ruling in *Lindqvist* (n 72), where the CJEU suggested a territorial limitation to the EU rules for international data transfers, ie that they should not be interpreted as having universal application and apply to the entire internet.

[119] In line with the *Weltimmo* case (n 7).

ences, behaviours and attitudes.[120] Again, this provision is directly connected with social media networks that track individuals and sell their personal information for targeted advertising.

In line with the Directive, where these extraterritorial provisions apply, the controller or processor must appoint a representative.[121] The Regulation makes it clear that the representative must be established in *one* of the Member States in which the relevant data subjects are based (there is no need for a representative in each MS). However, the Regulation does not define criteria according to which the relevant MS would be defined when relevant data subjects are based in more than one MS nor does it detail the representative's responsibilities.[122] There is a limited exemption to the obligation to appoint a representative where the processing is occasional, is unlikely to be a risk to individuals and does not involve large-scale processing of sensitive personal data. But again, there is no guidance on the scope of occasional processing, and there are no provisions on who bears the burden of proof for occasional processing.[123] Still, the representative will have to be the subject of enforcement proceedings before the relevant supervisory authorities and accept liability for any breach of the Regulation.[124]

There is criticism that the targeting approach applied in article 3(2) can be misguided in that it focuses on the subjective intentions of the relevant party.[125] Although geo-location technologies might be a useful tool for clarity in the application of a targeting approach,[126] it will probably provide no certainty for the parties involved in the complex cloud environment, where a large number of parties is involved in the handling of personal data. Therefore, when considering the judicial jurisdiction of the GDPR provision in the cloud environment, courts will probably be in a position to conclude either that they target just about every country in the world or no countries at all.[127]

Provisions on extraterritoriality should be interpreted in line with the *Google Spain* decision that introduced a broad concept of establishment.[128] Accordingly, a minimal amount of economic activity, such as a US-based company using a single sales representative operating in an EU country, can be sufficient to trigger the establishment requirement

[120] GDPR (n 14) recital 24.

[121] GDPR (n 14) art 27.

[122] See Hon, Hornle and Millard (n 112).

[123] ibid 155.

[124] GDPR (n 14) recital 80.

[125] DJB Svantesson. 'Extraterritoriality and Targeting in EU Data Privacy Law: The Weak Spot Undermining the Regulation' (2015) 5(4) International Data Privacy Law 232.

[126] ibid.

[127] ibid.

[128] See *Google Spain* (n 16) and *Weltimmo* (n 7).

and therefore the application of the EU data protection law. However, the *Google Spain* case revealed the practical question of the enforcement of extraterritorial jurisdiction: implementing a court decision locally might result in undermining the effectiveness of the CJEU ruling, while implementing the local requirement on a global scale can bring about unintended consequences, eg to constrain the freedom of expression.[129] Therefore, when considering enforcement jurisdiction, the doctrine proposes that national authorities should use a test of proportionality to balance the need for effective protection against undue intervention in a foreign State's policies.[130]

4.2 Cross-border data flows

Cross-border data flows are one of the biggest data protection issues in cloud computing, due to the fact that personal information processed in the cloud usually flows through – and is stored in – various jurisdictions across the globe.[131] The cloud service provider often does not provide information about where the data are stored.[132] On the other hand, the data protection laws of the country where personal data are processed or stored may differ from EU laws or may have an inadequate level of protection. This creates a risk that personal data may be without restriction and possibly misused, without individuals being able to exercise their data protection rights as they would under EU law. Concretely, law enforcement authorities may be able to bypass the individual and ask cloud providers who operate in their jurisdiction for access to EU personal data stored in the cloud. As the transfer of data to third countries raises the question of the jurisdiction of data stored by a cloud provider, the latter may then face conflicting legal obligations.[133]

---

[129] In that regard, see a thorough analysis by B Van Alsenoy and M Koekkoek, 'Internet and Jurisdiction After *Google Spain*: The Extra-Territorial Reach of the EU's "Right To Be Forgotten"' (2015) The Leuven Centre for Global Governance Studies, Working Paper No 152 – March 2015, 15.

[130] ibid 29.

[131] According to WP29 Opinion (n 39) 7.

[132] See European Commission Expert Group on Cloud Computing Contracts Discussion on Data Location and Data Security, 10 <http://ec.europa.eu/justice/contract/cloud-computing/expert-group/index_en.htm> accessed 1 December 2016.

[133] This question was highlighted in 2014 when US federal courts determined that customer email data stored in a Microsoft data centre located in Ireland are subject to US law and must be turned over to authorities under subpoena. In July 2016, the US Court of Appeals for the Second Circuit reversed a 2014 lower court order, and ruled that Microsoft is not required to hand over customer emails held overseas to the Department of Justice (DOJ). In April 2016 Microsoft sued the United States Department of Justice and asked a court to declare the government's secrecy orders as unconstitutional. The Opinion is available at: <http://cases.justia.com/federal/appellate-courts/ca2/14-2985/14-2985-2016-07-14.pdf?ts=1468508412> accessed 8 January 2017; see a copy of Microsoft's suit available at <http://online.wsj.com/public/resources/documents/microsoftcomplaint.pdf> accessed 8 January 2017.

Additionally, the global cloud market today is dominated by US companies. Out of the top 25 public cloud companies in Europe, 17 are headquartered in the US and they generate 83% of the revenue, 7 are headquartered in the EU and generate 14% of the revenue and one is in Norway.[134] Therefore special concern for cloud providers are rules on transatlantic data flows.

Transfer to third states in the GDPR is regulated in a similar way as in the Directive, although more comprehensively. Its Chapter V gives detailed rules on this important aspect. In essence, the Regulation imposes limits on transfers of personal data outside the EU unless an '**adequate level of protection**' is guaranteed, and the Regulation differentiates several different mechanisms for permitting transfer to third countries.

In line with the Directive, the GDPR allows data transfers to countries whose legal regime is deemed by the European Commission to provide an 'adequate' level of personal data protection (the so-called **adequacy decision**). However, provisions on the adequacy decision are strongly influenced and detailed by the findings of the Court in the *Schrems* case.[135] In this regard, recital 104 of the GDPR confirms that a Commission adequacy decision means that the third country or specified entity ensures an adequate level of protection '*essentially equivalent*' to that ensured within the European Union. It stipulates that the adoption of an adequacy decision presumes that the third country ensures effective independent data protection supervision and that it has cooperation mechanisms with the MSs' DPAs. Additionally, the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress. According to the Regulation, the Commission may determine that even a specific territory or sector within a third country offers an adequate level of protection. The adequacy decisions will be subject to periodic review, at least every four years.[136] Even more, the Commission is obligated to monitor white-listed countries[137] 'on an on-going basis'[138] to see if circumstances arise that would affect its adequacy decisions and it has full power to repeal, amend or suspend an adequacy decision at any time after giving the affected jurisdiction notice and an opportunity to respond.[139]

---

[134] EC DG CONNECT, Deloitte study on 'Measuring the Economic Impact of Cloud Computing in Europe' SMART 2014/0031, 13 <file:///C:/Users/s50mask/Downloads/EconomicimpactofCloudComputing inEurope.pdf> accessed 20 December 2016.

[135] *Schrems* (n 7).

[136] GDPR (n 14) art 45(3).

[137] See Commission decisions on the adequacy of the protection of personal data in third countries <http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm> accessed 15 June 2016.

[138] GDPR (n 14) art 45(4).

[139] ibid, art 45(5).

In the *Schrems* case,[140] the Court invalidated the Safe Harbour adequacy decision between the EU and the US, stating that the US does not offer an adequate level of data protection which is in place in the EU. In particular, the Court found that the access enjoyed by the US intelligence services to the transferred data interferes with the right to respect of private life and the right to protection of personal data of EU citizens. Following the *Schrems* ruling and the annulment of the Safe Harbour adequacy decision, there was great uncertainty for US businesses on the legitimate manner of private data processing, and the European Commission renegotiated a new legal framework with the aim of ensuring that personal information of citizens is protected to EU standards when it is sent to the US: the EU-US Privacy Shield[141] agreement. Considering the strict interpretation of privacy rights as a fundamental right in the recent CJEU case law,[142] there is considerable uncertainty about the future of the Privacy Shield. The WP29 has expressed serious reservations about the Privacy Shield on the grounds that transfers to the US are still subject to 'mass and indiscriminate surveillance' by US national security agencies, with some DPAs going further and suggesting that other transfer mechanisms, such as model contracts, appear to lack adequacy for data transfers to the United States, too.[143] As stated in the *Schrems* decision, national DPAs are responsible for monitoring compliance with the EU data protection law on their respective territories and are vested with the power to check whether a transfer of personal data from its own territory to a third country complies with EU law. DPAs must therefore hear claims made by individuals and, if they consider such claims to be well founded, they have the possibility to bring a case before the national courts. In light of this, there is a substantial likelihood that the Privacy Shield will be challenged in the CJEU and there is considerable risk that it could be annulled, which raises the problem of the legal uncertainty of transatlantic data flows.[144]

---

[140] See Statement of the Art 29 Working Party of 16 October 2015 <http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf> and

Position Paper of the German Data Protection Authority of Schleswig-Holstein <www.datenschutzzentrum.de/uploads/internationales/20151014_ULD-PositionPapier-on-CJEU_EN.pdf> both accessed on 29 April 2016.

[141] Commission Implementing Decision (EU) 2016/1250 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 (notified under document C(2016) 4176) (Text with EEA relevance) [2016] OJ L207/1

[142] Eg *Digital Rights Ireland* (n 15); *Google Spain and Google* (n 16).

[143] Position Paper of the German Data Protection Authority (n 140).

[144] See European Parliament: Transatlantic Digital Economy and Data Protection: 'State-of-Play and Future Implications for the EU's External Policies' (2016) Policy Department, Directorate-General for External Policies, EU, 28 <www.europarl.europa.eu/RegData/etudes/STUD/2016/535006/EXPO_STU(2016)535006_EN.pdf> accessed 29 April 2016.

In the absence of an adequacy designation, the GDPR provides other mechanisms for cross-border data transfers. The controller or processor might utilise **'adequate safeguards'** that have been approved by the Commission or by the national DPA.[145]

Unlike the Directive, the GDPR explicitly recognises binding corporate rules and standard data protection clauses as adequate safeguards. Moreover, it provides clear provisions on requirements and procedures for **binding corporate rules**. If the binding corporate rules meet the requirements set out in the GDPR,[146] the competent national DPA must give approval. This is likely to make the adoption of binding corporate rules easier and should significantly decrease the inconsistencies in its interpretation and implementation from one DPA to another, which is specifically important with regard to the possible annulment of the US Privacy Shield. Moreover, the WP29 acknowledged binding corporate rules as an efficient legal instrument for massive transfers made by a processor to subprocessors which are part of the same organisation acting on behalf and under the instructions of a controller.[147] In this regard, binding corporate rules might be applicable in cloud computing.[148]

The **standard data protection clauses** may be adopted by the Commission, or adopted by a supervisory authority and approved by the Commission, and these do not require any further authorisation from a DPA as they do under the Directive, which reduces the administrative burden. According to WP29, the present model clauses 2010/87/EC[149] are applicable in international transfers from an EU controller to a cloud service provider established outside the EU.[150] However, these model clauses do not apply in a situation when the cloud service provider is established in the EU. The Regulation has not changed this insufficiency.

---

[145] GDPR (n14) art 46.

[146] ibid, art 47.

[147] WP29 Explanatory Document on the Processor Binding Corporate Rules adopted on 19 April 2013 as last revised and adopted on 22 May 2015, 5. See also the WP29 Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, adopted on 6 June 2012 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf> accessed 1 June 2016.

[148] See also V Reading, 'Binding Corporate Rules: Unleashing the Potential of the Digital Single Market and Cloud Computing (speech held at IAPP Europe Data Protection Congress, 29 November 2011) 4.

[149] Commission Decision 2010/87/EU (and repealing Decision 2002/16/EC) <http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm> accessed 29 April 2016.

[150] WP29 Opinion (n 12) 18.

Finally, the Regulation introduces provisions on **codes of conduct**[151] and **certification**[152] as adequate safeguards, which provides greater flexibility to data controllers and data processors in selecting the data transfer mechanisms according to their needs. However, these provisions are not sufficiently detailed and their application will depend on further interpretation and implementation.

If there is no adequacy decision or appropriate safeguards, the Regulation defines an enumerated list of **derogations** permitting limited data transfers to non-EU countries.[153] The definition of **consent** was a stumbling block in negotiating the Regulation, as consent is seen as sometimes a weak basis for justifying the processing of personal data, and it loses its value when it is stretched or curtailed to make it fit situations it was never intended for.[154] The accepted provision on consent states that it should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement.[155] Following this, the Regulation explicitly states that silence, pre-ticked boxes or inactivity should not therefore constitute consent. For sensitive data, explicit consent is needed.[156] Given that cloud computing includes a high number of data subjects, that the purpose of processing is not always familiar to the cloud provider, and that the location from where the data may be processed evolves constantly, it is unlikely that consent can be used in cloud computing.[157] Further, the WP29[158] states that derogations should only apply to non-massive, non-recurrent and non-structural transfers, and therefore it appears almost impossible to generally rely on exemptions in the cloud computing environment.[159]

The GDPR provides that Member States can invoke **important reasons of public interest** to expressly set limits to the transfer of certain types of data to a third country or international organisation that has not received an adequacy decision. Such national provisions must be notified

---

[151] GDPR (n 14) arts 40 and 41.

[152] ibid, art 42.

[153] ibid, art 49.

[154] WP29 Opinion 15/2011 on the definition of consent adopted on 13 July 2012 <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf> accessed 29 April 2016.

[155] GDPR (n 14) recital 32.

[156] ibid, art 9.

[157] See Expert Group on Cloud Computing Contracts, Discussion Paper on Data Transfer in the Cloud, 4 <http://ec.europa.eu/justice/contract/files/expert_groups/discussion_paper data_transfers_in_ cloud.pdf> accessed 29 April 2016.

[158] WP29 Opinion (n 155).

[159] WP29 Opinion (n 12) 18.

to the Commission. This clause runs the risk of producing fragmentation among the Member States with regard to their data transfer policies.

Another important provision on trans-border data considers situations with the **legal requirement from a third country.**[160] In this regard, the GDPR states that any judgment of a court or tribunal or decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data can only be enforced if it is based on an international agreement concluded between the EU and the requesting third country, such as a mutual legal assistance treaty (MLAT). In the absence of such an international agreement, data disclosures are only allowed if the data transfer conditions of the GDPR are met. The position under the GDPR on this point is unsurprising in view of the discussions within the EU since the Snowden revelations around transatlantic data transfers and access to data by government agencies.

It can be concluded that in line with the present provisions of the DPD and the CJEU case law, the provisions of trans-border data flow are restrictive and limit data export only to countries having the same data protection standard as the EU, thus broadening the application of the extraterritorial provisions under the GDPR.[161]

4.3 Concluding remarks on the extraterritorial application of the GDPR

In conclusion, considering that cloud computing by its nature has no boundaries, in order to ensure EU data subjects' rights, extraterritorial rules seem to be a justifiable regulatory option for the legislator. We can therefore conclude that the development of cloud computing is one of the reasons why the GDPR considerably expands the scope of the present extraterritoriality principle of the Directive, with the clear aim of ensuring that the processing of EU citizens' personal data is always subject to EU data protection standards, but even more to ensure a level playing field for EU and non-EU service providers.

Considering the international nature of cloud computing, the principle of extraterritoriality will have a substantial affect for cloud service providers. Taking into consideration that cloud processors are not currently under direct obligations under the current data protection regime, many non-EU companies who have targeted EU consumers but have operated on the basis that EU law does not apply to them, will now have to adapt to the strict provisions of the GDPR. There is criticism that given the

---

[160] GDPR (n 14) art 48.

[161] K Hon and C Millard, 'Data Export in Cloud Computing: How can Personal Data be Transferred outside the EEA? The Cloud of Unknowing, Part 4' (2012) 26(2–3) International Review of Law, Computers & Technology 129, 130.

costly administrative measures and obligations for processors, such rules should have been envisaged only for businesses that have a substantial presence on the European market.[162] Additionally, as cloud computing activities have effects in, and affect citizens of, multiple States, the extraterritorial principle brings up the issue of the conflict of jurisdictions of multiple laws (eg US v EU), which raises the question of enforcement jurisdiction.[163] Geographic overexpansion may lead to unenforceability, as this raises the problem of interference with the territorial sovereignty of other states. The Regulation fails to deal with all the mentioned challenges already recognised by the doctrine, and further widens its extraterritorial application, which will include considerably more cloud service providers that will fall within the remit of the new strict provisions of the GDPR.

However, by introducing the extraterritorial principle, the GDPR imposes a higher level of data protection on non-EU service providers, and thus in fact introduces measures for the prevention of market disruption. Considering that the EU presents a significant market and taking into consideration the imposed high fines for non-compliance with the GDPR, it can be expected that market subjects will make an effort to comply with the EU rules. Therefore, the extraterritorial rules might remove the imbalance between EU service providers that are committed to abiding by the strict rules of EU data protection and non-EU service providers that have a dominant position in the global cloud market.

5 Conclusion

It is commonly agreed that the current legal framework within the DPD does not give adequate data protection to individuals in a society ruled by technology and the internet. On the one hand, cloud providers say that data protection legislation is outdated and impossible to implement on technologies that create a new, virtual, globally connected world. On the other hand, outdated legislation causes anarchy and leaves individuals unprotected. Therefore, the GDPR presents an important step in the right direction for improved protection for individuals in the framework of personal data protection in the cloud environment.

After the GDPR enters into force, cloud service providers will be required to fundamentally change their attitude towards data protection

---

[162] Svantesson (n 125) 232.

[163] For an analysis of the extraterritoriality principle in DPD and GDPR, see M Taylor, 'Permissions and Prohibitions in Data Protection Jurisdiction' (2016) Brussels Privacy Hub Working Paper, vol 6 no 2 <http://www.brusselsprivacyhub.org/Resources/BPH-Working-Paper-VOL2-N6.pdf>; see, for different views in settling conflicts of law, C Ryngaert, 'Special Issue Extraterritoriality and EU Data Protection (*International Data Privacy Law*, 7 October 2015) <http://idpl.oxfordjournals.org/content/early/2015/10/07/idpl.ipv025.full#xref-fn-10-1> both accessed 10 May 2016.

and to include data protection considerations into the core of their business activities. Considering the status of personal data as a human right in the EU, and on the other hand given the amount of data in the cloud and the lack of control over them by the data subject, this shift of responsibility seems to be justified.

Generally, the Regulation leans heavily on the main concepts of the Directive, for example with regard to the definition of personal data, the division of roles, the scope of application and the rules on trans-border data flows. As noted through the text, these provisions are aligned with the findings of the CJEU as well as with the Opinions given by the WP29.

Despite criticism, the controller–processor roles remain within the Regulation, too, although the responsibilities have changed. In particular, processors can in certain circumstances now be held directly liable and be required to pay compensation to a data subject. The Regulation fails to exclude commoditised services (IaaS, PaaS) from its application, even though they do not have knowledge of the nature of the data stored and/or lack the practical ability to access such data. This seems to be inconsistent with the aim of the GDPR that attempts to locate the actor which truly controls the conditions of processing data.

The right to erasure will be a challenge for cloud providers to implement due to the massive transfers of data in the cloud environment and the unknown location of data. There will also be challenges in defining roles in the context of data protection in cloud computing. The controller has to evaluate whether a request for erasure is legitimate, but faced with huge fines, there is a high possibility that such a request for erasure will be approved, thus potentially conflicting with the rights to information and freedom of speech. The right to erasure imposes enormous responsibility on cloud service providers, and detailed instructions on its application should be prepared by the relevant authority. Provisions on data portability might be misused, as big cloud providers might raise the transition costs in order to lock in their users. These issues will have to be considered by competition rules as well.

All of these provisions will have direct effect on cloud service providers. Their roles and obligations will change substantially, as until now they have been outside the scope of data protection rules, or at least their obligations were marginal. As most of the contractual relationships between controller and processor are at present based on standard 'take it or leave it' terms, the Regulation introduces compulsory provisions on future contracts. New obligations on subcontracting will be very hard to negotiate for small cloud providers, thus putting the 'big players' in a much better market position. Some of the new contractual obligations present a new administrative burden for cloud providers, and aligning

with them will probably lead to higher prices of cloud services. Thus, it is to be expected that on the global market EU cloud providers will not be competitive with non-EU cloud providers.

Taking into consideration that cloud processors in general are not informed about the data they are storing, and that their service is not directed towards data protection, if encrypted data is exempted from data protection rules then cloud providers would be in a good position to be exempted from applying data protection rules. Unfortunately for cloud computing, the Regulation did not go so far, although the definition of pseudonymised data provides greater flexibility in assessing the risk of re-indentification, which has been supported by the recent case law.

In conclusion, it seems that the GDPR itself does not provide measures to unleash the potential of cloud computing in the EU, but considerably raises standards in line with the position that data protection is a fundamental right, thus putting EU cloud service providers in a more demanding position than their competition. However, this issue might be influenced by the extraterritorial effect of the GDPR.

In this regard, the scope of the Regulation has been expanded. It now applies to companies inside and outside the EU. Even if personal data are processed outside the EU by companies established outside the EU, as long as they are active in the EU market and offer their products and services to EU citizens, these companies will be bound by the EU data protection regime. Additionally, the GDPR continues to require that data may only be transferred to third countries if the EU legal standards apply to their processing, thus widening the extraterritorial application of the Regulation.[164] Provisions on the scope of the application and trans-border transfer of data will create inherent conflicts of jurisdictions, which will cause uncertainty for businesses. However, hefty fines, although in certain circumstances hard to enforce, might force the big non-EU cloud providers that dominate the market to raise their standards to comply with the GDPR.

Thus, it might be concluded that with the GDPR the EU is endorsing European standards of data security and privacy in a globalised economy that will especially influence the cloud computing market. The practical consequence of compliance might raise privacy standards both within and outside the European Union, thus producing the so-called 'Brussels effect' in raising privacy protection in cloud computing.[165]

---

[164] C Kuner, 'Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law (2015) 5(4) International Data Privacy Law 241.

[165] Or the 'ratcheting-up' effect. See M Rotenberg and D Jacobs, 'Updating the Law of Information Privacy: The New Framework of the European Union' (2013) 36 Harvard Journal of Law and Public Policy, 637.

From the EU Data Protection Regulation to the possible inclusion of data protection and electronic commerce in the upcoming US–EU trade agreement, as well as with international concerns about US security agencies' collection of personal information worldwide, data protection is a rapidly growing field in international law and policy. It seems that the Regulation seeks to provide the means for the application of a European privacy policy in international markets. However, time will tell how this will be enforced.