IEEE CLOUD COMPUTING

VOLUME 5, NUMBER 6 NOVEMBER/DECEMBER 2018

Reengineering Cloud Data Centers

IEEE
IEEE computer society
IEEE ComSoc IEEE Communications Society
www.computer.org/cloud

IEEE CLOUD COMPUTING

November/December 2018
Vol. 5, No. 6

www.computer.org/cloud

TABLE OF CONTENTS

Cloud Computing and the New EU General Data Protection Regulation

Barbara Russo, Laura Valle, Guido Bonzagni, and Davide Locatello
Free University of Bozen-Bolzano

Marta Pancaldi
University of Manchester

Davide Tosi
University of Insubria

Disclosing personal data for a purpose not known by data subjects is a practice that the 2018 European Union General Data Protection Regulation (GDPR) is supposed to prevent. This article gives an overview of the major aspects of GDPR related to provision, use, and maintenance of cloud services and technologies.

The European Union (EU)'s new law on data protection, the General Data Protection Regulation (GDPR),[1] now has a direct effect on all EU member states (as of May 2018). Unlike the previous EU legal framework, Data Protection Directive 95/46/EC (DPD),[2] no national transposition is needed, and the regulation soon comes into force in all member states, including the United Kingdom (UK). It is therefore of paramount importance to understand the effects that the regulation has on use and management of technologies concerned with data protection in the EU, such as cloud computing. GDPR aims at clarifying concepts and procedures for data protection in today's connected world that drastically amplifies risks of data breach.[3] Compliance with GDPR is a tough task, as European companies use an average of 608 cloud apps.[4] Hence, an analysis of the effects of GDPR should be performed with particular attention to IoT, big data, and cloud computing.[5]

One of the major novelties of GDPR that is relevant for cloud computing is its scope of application (referred to as extra-territorial applicability). Unlike DPD, which applied to organizations established in the EU or that use equipment situated in the EU, GDPR also applies to non-EU organizations that process or monitor personal data of subjects who are in the EU. Organizations operating in cloud computing are often based outside the EU (such as Google[6]) but typically process data of subjects who are all over the world. Therefore, GDPR applies to most of them.

A second aspect of GDPR is the new responsibility given and shared by processors and controllers of personal data. Under GDPR, the cloud service provider (CSP) will have to take responsibility of what is processed and how its service, platform, or infrastructure is deployed and utilized by the customer.[7] Additionally, a CSP must gather a non-passive consent from the customer regarding how and by whom the data is processed (for example, with additional explicit consent on subcontractors). This may increment the diversification of the contractual agreements

Copublished by the IEEE CS and IEEE ComSoc
2325-6095/18/$33.00 ©2018 IEEE

between the provider and the single customer that, for big players with many customers (such as Amazon), may make the service as-is impossible to manage. Therefore, big players in the cloud-computing industry are implementing codes of conduct or new terms of service that serve as transparent frameworks for decisions on data protection under GDPR.

In this paper, we explore GDPR's impact on cloud computing. We discuss its effects in comparison with DPD and the UK Data Protection Act 2018 (DPA).[8]

GDPR OVERVIEW

GDPR is supposed to prevent and punish cases such as the UK-based consulting firm Cambridge Analytica's unauthorized possession of Facebook users' personal data. Under GDPR, such unauthorized possession may be punished with a hefty administrative fine. What makes Facebook exposed to GDPR? Facebook provides social-networking services over the Internet that share personal data within networks of connected users. As such, Facebook is a CSP. Any CSP that manages customers' data over the cloud needs to be careful not to incur risk of infringement of GDPR. To shed some light on the problem, the following sections review the key aspects of GDPR that eventually affect the provision, use, and management of cloud computing.

Key Elements of GDPR

GDPR designates new types of data as personal data. Personal data is any information relating to an identified or identifiable data subject. A data subject is anyone who can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.[1] GDPR explicitly qualifies as personal data IP address, Internet cookies, and genetic information such as DNA when they are used to identify a subject. Such explicit mention is needed to acknowledge the evolution of the national and European case law since DPD and to accommodate new types of data produced by new technologies. An example that illustrates this evolution is the case of *Patrick Breyer v. Bundesrepublik Deutschland* (C-582/14) on the use of the dynamic IP address. In its resolution, the EU Court of Justice stated that the dynamic IP address (which is linked to the single access) can help profile a person if aggregated to other data that a third party can legally obtain. Thus, to be compliant with GDPR, cloud services that regularly manage such data need to be designed to address privacy concerns (privacy by design), allow for processing of only the data that is absolutely necessary for system operations (data minimization), and limit access to the data to only people involved in the processing.[9] They also need to implement policies and tools to give data subjects the right to move their personal data to other providers and to delete their data (right to be forgotten) when they no longer need to be processed.

Data processing

In both DPD and GDPR, processing means any operation or set of operations that is performed on personal data or on sets of personal data, whether or not by automated means. According to Article 9 of GDPR, it is prohibited to process "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership," as well as "genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation." As a cascading effect, these rules also apply to subcontractors that process some personal data, and processors must obtain explicit consent from the data subjects to share the data with subcontractors.

Processors and controllers

Both in DPD and GDPR, the controller is a natural or legal person, public authority, agency, or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data; the processor acts on data on behalf of the controller. Under GDPR, for the first time, the processor is liable for the damage caused by the processing when it has not complied with GDPR obligations or the controller's instructions.

Under GDPR, the concept of joint controllers introduced in DPD is further detailed and enforced. Anytime two or more controllers jointly determine the purposes and means of data processing, responsibilities are transparently allocated to each of the controllers for the sake of the data subjects. For example, infrastructure-as-a-service (IaaS) providers, which only provide users with a managed hosting service, must now take the responsibility of processing data generated by their infrastructure (such as logs).[10]

Data Location and Transfer

GDPR extends its scope of application outside of EU borders; GDPR affects all organizations within the EU, but it also applies to organizations established outside the EU (third country) if they offer goods or services to, or monitor the behavior of, EU data subjects. Examples of such activities are tracking subjects over the Internet with the intent of profiling them (such as through cookies) or using a language or a currency (euro) of an EU country with the possibility of ordering goods and services in that language or currency.

GDPR uses the concept of transfer in a broader sense than DPD by also defining data transfer as by means of intermediary international organizations. GDPR also defines five safeguards to transfer data outside EU borders: adequacy decision (whether a country has an adequate level of data protection), binding corporate rules (BCR) (rules for internal transfer of data for multinational companies), standard contractual clauses (suitable for one-time transfer), approved code of conduct (for multiple transfer), and certification mechanisms (to certify that appropriate safeguards have been established). Except the first, all the safeguards have to be approved by the Information Commissioner Office, and the code of conduct must be further approved by the European Data Protection Board.

Of course, case law is needed to better define the practice of ascertainment for third-country organizations to fall into GDPR and to identify models of safeguards for data transfer. Given its ubiquitous nature, this is especially true for cloud computing.

Data Subject's Consent

Consent is any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which the data subject agrees to the processing of personal data. GDPR makes clear that consent requires a clear affirmative action by the data subject (meaning no pre-checked consent statements) who must be informed about the agreement details—such as the identity of the controller, the purpose of data processing, and the right to withdraw consent at any time. At any time, data subjects can withdraw their consent and request a complete erasure of the data (right to be forgotten) and conduct audits to verify the actual destruction of the data. GDPR encourages this whenever the processing does not require the identification of the data subject (Article 11).

EFFECTS OF GDPR ON CLOUD COMPUTING

Cloud computing is a set of technologies and service models that allow access to a scalable and elastic pool (provisioned and released on demand) of shareable computing resources (through a common access to the service provided separately for each user). The majority of distributions for cloud services in small and medium European companies are hybrid (a federation of public, private, or partner clouds), partner (owned and managed by a trusted partner), or public (owned and managed by an unrelated business); the smallest portion is private (owned and managed internally), as reported by the European Union Agency for Network and Information Security.

The architectures of a cloud service differ in the type of layer from which users can access services. IaaS provides computing resources and hardware infrastructures over the Internet in a virtualized environment (such as virtual machines, storage, and networking). The component providing access to IaaS resources is called the hypervisor. Examples include Amazon's Elastic

Compute Cloud, Google's Compute Engine, and Dropbox. In terms of data access, IaaS instances provide much more information than the platform-as-a-service (PaaS) and software-as-a-service (SaaS) models, such as the customer ability to install and set up the image for security analysis purposes and to execute snapshots of the virtual machine. Some problems may arise from the unclear situation regarding how the provider handles the termination of customer contracts and from the inability of the customer to verify that the personal data stored on a virtual machine has been deleted exhaustively.

PaaS offers a development and deployment environment in the cloud, representing the operating-system layer. Examples of applications running on these platforms are scripts (PHP and Python) and byte code (Java servlets and C#). Examples include Google App Engine and Microsoft Azure. In terms of access to data, the core application is under the customer's control. The customer has no direct control of the underlying runtime environment, though. Logging and encryption mechanisms can be implemented on the platform so that providers can collect and store diagnostic data that can be used by the customer for different purposes, such as security checks.

Individual software packages are available at the application layer of the SaaS. Applications range from email servers and document editors to customer relationship management systems. SaaS services can often be accessed with a browser or a web services client. SaaS providers (such as Netflix) may run their applications on an IaaS (such as Amazon Web Services (AWS)) or the PaaS of another provider. As such, clients do not have a deep view of the system and its underlying infrastructure.

In terms of data processing, SaaS and IaaS technologies are at the extremes of the same scale, and therefore their providers have different responsibilities and roles. An IaaS provider typically offers a software application service that is specifically intended to process personal data. As such, a SaaS provider can exercise a wide range of controls in relation to the data processed using its SaaS and how that data is processed. Therefore, it is able to provide its customers with technical and contractual commitments that are tailored to the specific SaaS it provides. On the other hand, an IaaS provider only provides virtualized hardware or computing infrastructure. In principle, its customers can choose how to use that infrastructure. In general, IaaS providers are unaware of how their infrastructure is being used and are unable to tailor their services to individual customers (such as providing the same level of security for any use).

Cloud Service Customer and CSP under GDPR

The CSP as processor

An element of novelty introduced by GDPR that has significant impact on cloud services is the new responsibility assigned to the processor.[7] To understand such an implication, we recall the role of a provider in cloud services in the following example. A CSP offers cloud services and, in particular, processes data of its customers. As such, in GDPR, the CSP is a processor.[7,11] This implication consolidates concepts introduced in recent European directives (such as DPD) in which CSPs are operators that make their infrastructure available for data processing. In other words, mapping provider as processor, and not as controller, derives from the nature of the activity carried out by the provider for cloud storage. In particular, the provider offers data retention and storage systems on behalf of the customer and makes those immediately available to anyone with authorized access at any time and from anywhere in the world through an Internet connection.[12] Notice that, in some cases, a CSP offering personal data processing services directly to data subjects such as Facebook or Dropbox is considered a data controller, as it determines the purpose and the means for such processing services.[13] Finally, the new forms of data generated by modern cloud infrastructures and platforms (such as system logs) are ascribed to personal data, as they can profile users and are in the hands of the CSPs. Therefore, PaaS and IaaS providers that, before GDPR, had almost no role in data protection, under GDPR, are given some responsibility (although still limited).[7]

Cloud customer as controller or processor

If a provider is a data processor, a customer of cloud services is generally considered a data controller of the data stored in the provider's servers.[10] This is typically the case for IaaS and PaaS services in which, in principle, the customer determines how the data is processed and the purpose for which it is processed. The customer is a processor if she or he is merely processing the personal data according to the wishes of a third party. This is typically the case of SaaS. GDPR assigns the responsibility for violations in the processing of personal data mainly to the cloud service customer, as a data controller, but adds a shared responsibility with the processor as joint controller when the customer does not have direct control of the data and its process.

Responsibilities of cloud service customer and provider as joint controllers

In a recent investigation of more than 20 CSPs, the extent of liability ascertained under DPD has been minimal (less than $500 USD).[12] Under GDPR, customers may have a better means to claim for compensation against the provider thanks to the introduction of the joint control between a provider and its customers. While maintaining the two distinct roles, acting as a processor would in fact establish a co-responsibility of the provider for any damage suffered by the individual to whom the data refers. Such obligations with its customers extend to the CPS's subcontractors.[12] For example, a data controller that has personal data processed by a SaaS (such as Netflix) whose software is on servers operated by an IaaS company (such as AWS) is required to approve the use of such an IaaS, as well. Both the SaaS and IaaS providers share the responsibility of the personal data processed for what is within each competence. The joint responsibility applies to many popular cloud services. For example, according to this principle, Google and a company that advertises its products on the Google platform each act as an independent controller of personal data. The risks of security breaches are therefore shared. Consequently, in some cases, big CSPs and their subcontractors may need to tailor security measures for hundreds or thousands of customers.

Data Subjects' Consent for Cloud Services

Implementing data subjects' consent for cloud services can be a challenge, as it is not always clear where the data is. It is essential to provide the data subject with a disclosure, to make the person aware of both processing through the cloud and parties to be contacted in case of violations. Namely, data subjects are entitled to claim for damages suffered as a result of a violation of GDPR, but the proof of consent often falls on the customer of cloud services as data controller, who typically does not have the technical competence or access to report it. In practice, only the processor has competence and knowledge of how data received through the controller (such as SaaS) or directly through its platforms (such as IaaS and PaaS) is effectively processed. Only the processor is able to retain proof of its subjects' consents and make it accessible to the interested parties through its IT tools.

Data Storage and Processing Policies

The requirements and policies concerning personal data must be agreed on between the CSP and the customer before the processing activity takes place. Typically, CSPs of IaaS and PaaS are partially involved or aware of the data storage and processing policies since they provide only services that do not manage data (such as networking functionalities for IaaS and development environments for PaaS), or they manage data in an aggregated way. When they offer services to store persistently or to elaborate sensitive or special data for SaaS services (such as for data-analytics services), the compliance with GDPR becomes more stringent—including when they offer such services under subcontracting. For example, a SaaS provider outsourcing its applications through a PaaS of a third party would be a processor, as well. Thus, the practice of subcontracting in cloud computing establishes a chain of responsibilities for data protection that needs to be tracked and monitored.

Data Location and Transfer

The top ten data centers in the world are all located outside Europe.[14] Thus, customers and providers must know and monitor where data is stored and used by cloud services, as the physical location of a provider's data center often does not correspond to the location of the provider's headquarters. This is specifically the case for IaaS providers whose servers are typically located outside the EU. For example, since December 2014, AWS operates on about 1.4 million servers in over 54 locations worldwide, including the United States, Europe, Asia, Australia, and South America. Data location in GDPR may also have significant effects on SaaS services like Microsoft Office 365, G Suite, and Salesforce. In this case, even if service subscribers and the SaaS applications are based in a non-EU location, there could still be data subjects that patronize subscribers that are located in the EU and therefore cause CSPs of SaaS to adhere to GDPR. Such subjects are, for example, companies that provide SaaS for data protection or backups for other SaaS applications for business use. Such companies are data controllers with respect to SaaS providers and processors with respect to single subscribers. In addition, SaaS providers (like Google's G Suite) need to ensure that their subcontractors located outside the EU (like the Spanning products for data protection) adhere to GDPR, as well.

Crucially important for cloud computing is how to transfer data through EU borders and what safeguards need to be implemented to be compliant with GDPR. Among the ones that have signed a BCR are banks or payments companies (like MasterCard and American Express) and hotel chains (like Hyatt), as well as electronic commerce companies (like eBay). Big cloud-computing players have preferred to adhere to a GDPR-compliant code of conduct; in 2017, the major CSPs like IBM, Alibaba, Oracle, and SAP undersigned a GDPR-compliant code of conduct for CSPs,[15] whereas big IaaS providers like Aruba, AWS, and UpCloud undersigned a specific GDPR-compliant code of conduct for IaaS providers.[16] Google has instead opted for GDPR-compliant terms of service.

Data Security and Breach

Controllers and processors must take adequate measures (such as pseudonymization) and countermeasures to prevent security issues such as data loss, data alteration, and unauthorized access. For a CSP, such measures depend on the type of cloud architecture and the way it processes data. For example, IaaS providers adhering to the code of conduct[16] explicitly decline responsibilities derived solely from customers' use of the infrastructure. Thus, an organization that allows employees to use personal cloud software (such as Dropbox) within the company's IaaS can be directly exposed to the consequences of GDPR's violations if the IaaS provider will not take any responsibility or measure.

Data breaches (the unintentional release of secure or private information to an untrusted party) are one of the key concerns of GDPR; a detailed notification of the breach, including the cause of the incident, must be reported no later than 72 hours after the organization has become aware of it. The accuracy of the report is essential to increase awareness of security risks and, thus, prevent naïve management of cloud services. The year 2017 has seen a rising number of security incidents due to misconfigured or poorly secured cloud servers.[17] Two cases are striking in their naïve management of the service. One case concerns access to data of about 14 million Verizon customer accounts. Data was left exposed and easily accessible by guessing a simple URL that led to the improperly configured cloud drive. A second case concerns the voting data of about 200 million people in a database owned by a US company called Deep Root Analytics. The database lacked any protection against access and could be downloaded by anyone with Internet access. The reports about the incidents were not clear on whether any hacker violated the data.

Data Erasure

The right to be forgotten can be implemented in different ways depending on the type of cloud service that processes the data. For example, an IaaS provider does not typically manage or choose to delete customers' data on their behalf, as the customer is responsible for these actions. In other cases, the way to erase data is also a technical matter. For example, the community of

Hyperledger (an open-source SaaS provider offering blockchain services and hosted at The Linux Foundation) has conceived three strategies to ensure the right to be forgotten in its blockchain services:

- *Blockchain plus database with pseudonymization* uses blockchain to keep track of all transaction state changes and uses a database to store personal data. All the blockchain data of a user is associated with a user pseudonym, and access to this key is only available to the user. If data deletion is requested, the record is irreversibly deleted from the database.
- *Blockchain with cryptographic features* deletes data by using cryptographic features to make the personal data in the blockchain unreadable. The SaaS application would display to the user that the data is not available in the sense that post-encryption of the SaaS application won't be able to read the data.
- *Actually deleting the data* means editing the immutable blockchain. This is an extreme case, although it may be useful to accommodate legal and regulatory requirements of GDPR. Through the use of secure private keys, it enables designated authorities to edit, rewrite, or remove previous blocks of information without breaking the chain.

IAAS IN COMPARISON: GOOGLE CLOUD PLATFORM (GCP) AND AMAZON WEB SERVICES (AWS)

Big industrial players from the EU and elsewhere—such as Google, Microsoft, SAP, and Amazon—are working to define policies and practical support for stakeholders to comply with GDPR. Two IaaS providers are compared in Table 1 in terms of governance (as processor/controller), security, service agreement, and data storage, transfer, and disposal. The comparison is based on the Data Processing and Security Terms 2.0 for customers of the GCP[6] and the code of conduct[16] to which AWS has declared full compliance for its services[18] supplemented with Amazon Navigation GDPR Compliance. All such documents entered into force on May 25th, 2018.

Table 1. Strategies of compliance with GDPR.

Concern	Google Cloud Platform (GCP)	Amazon Web Services (AWS)
Governance	GCP is a processor of customer personal data, while the customer is the controller (or processor) of such data. Google will only process customers' personal data in accordance with the customers' instructions.	AWS is a provider that processes customer personal data, while the customer is the controller (or processor) of such data. According to CISP code requirements, (1) customers provide and manage controls such as security policies, monitoring, and malware; (2) the provider provides and customers configure and manage controls such as key management, logging services, and virtual private clouds; and (3) the provider alone manages and audits controls related to standards (such as the Cloud Computing Compliance Controls Catalogue (C5) in Germany). A provider may choose to declare only some cloud infrastructure services as adhering to the code requirements. Right now, only some services (such as Amazon EC2) are fully compliant (https://cispe.cloud/publicregister). The provider will act as controller for customer personal data concerning account information (such as billing information).
Security	Google maintains a set of security measures on its data centers (such as redundant infrastructure systems and a Linux-based secure application environment); network and	Responsibility on security is shared according to the governance of the services. For example, the provider is responsible for security of the physical infrastructure and the surrounding environment,

	transmission (such as ephemeral elliptic curve Diffie-Hellman cryptographic key exchange signed with Rivest–Shamir–Adleman and Elliptic Curve Digital Signature Algorithm); and site controls (such as biometric access control system), access control (such as two-factor authentication and carefully monitored access lists), and data storage (such as data and file system architecture replicated between multiple geographically dispersed data centers).	and the customer is responsible of the configuration of the IaaS service. Note that the customer is also responsible for reviewing the information made available by the provider on the physical and environmental security. AWS offers encryption tools to secure data-at-rest, disk, and file system.
Service agreement	The service agreement is defined by a set of customers' instructions. The GCP License Agreement is supplemented by the Data Processing and Security Terms, the instructions given by the customer through the Admin Console and otherwise in his or her use of the services, and any subsequent written customers' instructions acknowledged by Google.	The service agreement and use by the customer of the features and functionalities made available by the provider as part of the service are the customer's complete and final instructions to the provider in relation to processing of personal data. In addition, customers are provided with additional parameters that are defined in C5 and serve to better evaluate the terms of security of their services.
Data storage, transfer, and disposal	The customer may select where certain data will be stored, and Google will store it there in accordance with the Service Specific Terms. If a location is not covered by the Service Specific Terms or a location is not selected by the customer, Google may store and process the relevant data anywhere Google or its sub-processors maintain facilities. If data are to be transferred out of the European Economic Area (EEA), Google will either (if the customer requests it) ensure that the transfers are made in accordance with such contract clauses or (b) offer an alternative solution. Administrators can export customer data through the functionality of the GCP services at any time during the term of the agreement. Customers can delete their data through the functionality of the GCP services at any time. When Google receives a complete deletion instruction from the customer (such as when an email is permanently deleted), either during term or on term expiration, Google will delete the relevant customer data from all of its systems within a maximum period of 180 days unless retention obligations apply. Google will not process customer personal data for any other purpose.	The IaaS provider provides the customer the ability to choose to use the service to store and process its data entirely within the EEA. The provider provides its customers with the ability to rectify, erase, restrict, or retrieve customer data either (a) as part of the service or (b) by enabling customers to design and deploy their own solutions using the service. No further assistance to the customer with the data subject's request is provided. In respect to data processed on behalf of a customer using the cloud infrastructure service, the provider will not (a) access or use such data except as necessary to provide the services to the customer or (b) process such data for the provider's own purposes, including, in particular, for data mining, profiling, or direct marketing.

The strategies of the GCP and AWS for GDPR compliance are different. The GCP service agreement is based on a set of instructions agreed on with the individual customer and included in the Data Processing and Security Terms, the instructions given by the customer through the Admin Console, and any subsequent written customer instructions acknowledged by Google. The AWS service agreement instead refers to the cloud infrastructure service provider (CISP) code of conduct undersigned by a group of IaaS providers.[16] It is worth noticing that only some of the AWS services are listed in the register of services compliant to the code of conduct by date.

In terms of governance, GCP delegates the control to the above-mentioned instructions, whereas in the CISP code, control depends on the pre-defined type of access to data the customer and the provider have. For AWS, security is again handled on the pre-defined access and the role that customer and provider have on data processing; whereas for GCP, security is monitored through specific tools to protect the data centers. The CISP code additionally requires the customer to review the security measures set up by the provider. Again, the approach to data storage, deletion, and disposal of GCP is based on customer strategies that can be performed through tools provided by the platform. The CISP code explicitly mentions the prohibition for the provider to use data for its own purposes, including, in particular, data mining, profiling, or direct marketing. It is worth noticing here that GCP reserves the right to migrate customer data to centers in a location not chosen by the customer.

BREXIT: HOW THE UK CONFORMS

> *The United Kingdom submitted on 29 March 2017 the notification of its intention to withdraw from the Union pursuant to Article 50 of the Treaty on European Union. This means that unless a ratified withdrawal agreement establishes another date, all Union primary and secondary law will cease to apply to the United Kingdom from 30 March 2019 ('the withdrawal date'). The United Kingdom will then become a 'third country.' In view of the considerable uncertainties, in particular concerning the content of a possible withdrawal agreement, all stakeholders processing personal data are reminded of legal repercussions, which need to be considered when the United Kingdom becomes a third country.*[19]

With this statement begins the European Commission Directorate-General for Justice and Consumers' notice to stakeholders on January 9th, 2018. The same communication underlines, though, that GDPR has also simplified the use of the tools for data protection and transfer with third countries. Thus, which law will apply in the UK in the coming years?

Until March 2019, the UK will still be a member of the EU, and therefore GDPR applies to it. From the withdrawal date, the data flow between the UK and the EU must be maintained, as about 43 percent of EU tech companies are UK-based and 75 percent of the UK's data transfers take place with the other EU members.[20] Thus, in June 2017, the UK Department for Digital, Culture, Media, and Sport issued the Data Protection Bill 2018 (ico.org.uk), which has been finalized in the 2018 DPA. The DPA entered into force on May 25th, 2018 and updates the UK data protection laws and further supplements GDPR by extending data protection to as-yet-uncovered areas of application. The DPA also includes some exemptions of GDPR that may also have effects on cloud services. For example, some of the SaaS services (such as Facebook) are concerned with the age of consent that the DPA has lowered to 13.

Besides the DPA and its compliance with GDPR, the UK is also actively working on understanding the impact of the technological change on information rights. In particular, a great concern in the UK is how data is specifically processed by cloud services that make use of big-data analytics and AI. In her speech at the Alan Turing award in March 2018, Elizabeth Denham, the head of the UK Information Commissioner's Office, made it clear that the opacity of the algorithms used in processing a large amount of data and the inferred data that such processes might derive put the protection of personal data under serious risk. As such, her office has issued a technology strategy document for 2018/2019 that outlines how the UK will adapt to technological change as it impacts information rights. Such a strategy also foresees the establishment of a technological sandbox where new technologies will be deployed and tested for data protection (such as how fingerprints in smartphone easy access are processed).

OBSERVATIONS

GDPR has some consequences on the provision, management, and use of cloud services. The magnitude of such an impact does not only depend on the regulation itself, but also on special circumstances in which the regulation comes into force. Responsibility in processing personal data is overall increased for CSPs either because new types of data generated or available in cloud technologies (such as log data) are now ascribed to the personal sphere or new roles (such as joint controllers) are given to CSPs.

After Brexit, the UK will be a “third-party” country, making the provision of cloud services in principle more complex. To cope with this issue, the UK released the DPA 2018 that aims at providing the groundwork for GDPR compliance and updating the current UK law. Until Brexit is effective, the UK, as an EU member state, must comply with GDPR. Thus, the DPA is designed to make this transition period the smoothest possible, although a few differences might need further attention at the application stage (such as age of consent).

The territorial scope in GDPR is extended to non-EU countries where personal data of subjects who are in the EU are processed or monitored. As such, some big industrial players are taking proactive actions by undersigning codes of conduct, defining binding corporate rules for internal transfer across national borders, or updating terms of service contracts to align their procedures and policies with GDPR. Differences in such agreements and contracts, as in the case of GCP and AWS, make it clear that stakeholders in the cloud-computing business need case law to understand the real impact of both the provision and the use of such services in relation to the processing of personal data.

REFERENCES

1. “Regulation (EU) 2016/679 of the European Parliament and the Council (General Data Protection Regulation),” 2016; http://eur-lex.europa.eu/eli/reg/2016/679/oj.
2. “Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data,” 1995; http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.
3. J. Fernquist, T. Fägström, and L. Kaati, “IoT Data Profiles: The Routines of Your Life Reveals Who You Are,” *Proceedings of the IEEE European Intelligence and Security Informatics Conference*, 2017.
4. *Netskope Cloud Report*, EMEA edition, 2015; https://resources.netskope.com/Cloud-reports/autumn-2015-emea-Cloud-report.
5. N. Fabiano, “Internet of Things and Blockchain: Legal Issues and Privacy. The Challenge for a Privacy Standard,” *Proceedings of the IEEE International Conference on Internet of Things*, 2017.
6. “Google Cloud Platform, Data Processing and Security Terms (Customers),” 2018; https://cloud.google.com/terms/data-processing-terms.
7. M. Webber, “The GDPR’s impact on the Cloud service provider as a processor,” *Privacy & Data Protection Journal*, vol. 16, no. 4, 2016.
8. “UK Data Protection Act,” 2018; www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf.
9. T. Macaulay, *How to ensure GDPR compliance in the cloud*, 2018; www.computerworlduk.com/cloud-computing/how-ensure-gdpr-compliance-in-cloud-3663797/.
10. E. Le Quellenec, “Cloud Contracts: Impacts of GDPR on Joint Controllers,” 2017; https://Cloudprivacycheck.eu/latest-news/article/Cloud-contracts-impacts-of-gdpr-on-joint-controllers/.
11. P.T.J. Wolters, “The security of personal data under the GDPR: a harmonized duty or a shared responsibility?,” *International Data Privacy Law*, vol. 7, no. 3, 2017.
12. D. Flint, “Sharing the Risk: Processors and the GDPR,” *Bussiness Law Review*, no. 4, 2017, pp. 171–172.

13. "Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein. v. Wirtschaftsakademie Schleswig-Holstein GmbH," 2017; http://curia.europa.eu/juris/document/document.jsf?docid=195902&doclang=EN.
14. H. Williams, "The biggest data centres in the world, where they are and who owns them," 2017; www.computerworlduk.com/galleries/infrastructure/biggest-data-centres-in-world-3663287/.
15. *EU Data Protection Code of Conduct for Cloud Service Providers*, 2017; https://eucoc.cloud/fileadmin/cloud.../European_Cloud_Code_of_Conduct_1-7.pdf.
16. *Data Protection Code of Conduct for Cloud Infrastructure Service Providers*, CISPE, 2017; https://cispe.Cloud/wp-content/uploads/2017/06/Code-of-Conduct-27-January-2017-corrected-march-20.pdf.
17. S. Kuranda, "The 10 biggest data breaches of 2017 (so far)," *Cloud Computing and the new EU General Data Protection Regulation*; www.crn.com/slide-shows/security/300089736/the-10-biggest-data-breaches-of-2017-so-far.htm/pgno/0/10.
18. C. Woolf, "All AWS Services GDPR ready," *AWS Security Blog*, 2018; https://aws.amazon.com/blogs/security/all-aws-services-gdpr-ready/.
19. *Notice to stakeholders: withdrawal of the United Kingdom and EU rules in the field of data protection*, European Commission Directorate-General for Justice and Consumers, 2018; http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=611943.
20. *The United Kingdom's exit from and new partnership with the European Union*, 2017; www.gov.uk/government/uploads/system/uploads/attachment_data/file/589189/The_United_Kingdoms_exit_from_and_partnership_with_the_EU_Print.pdf.

ABOUT THE AUTHORS

Barbara Russo is an associate professor at the Faculty of Computer Science at the Free University of Bozen-Bolzano. She has a PhD in mathematics from the University of Trento. Previously, she was a research fellow at the Max Planck Institute for Mathematics. She has written more than 100 papers in software engineering, information systems, and mathematics. Her research focuses on monitoring and predicting vulnerabilities of software systems and services. Contact her at barbara.russo@unibz.it.

Laura Valle is an associate professor of private law at the Free University of Bozen-Bolzano. She publishes on contract law, standard contracts, unfair terms in contracts, consumer protection, European contract law, personality rights and fundamental rights, domain names, and nonprofit organization law. Contact her at laura.valle@unibz.it.

Guido Bonzagni is a legal trainee in a law firm specialized in ICT law, data protection law, and e-commerce law. He graduated with honors from the Law Faculty of University of Bologna and now collaborates with Professor Laura Valle at the Faculty of Economics at the Free University of Bozen-Bolzano. His interests involve civil, criminal, and tax liability in the digital society. Contact him at guido.bonzagni@gmail.com.

Davide Locatello is a scientific collaborator at the Free University of Bozen-Bolzano. He has a degree from the University of Bologna School of Law. His research interests include contract, family, and tort law. These studies led to the publication of some articles. Contact him at davide.locatello2@unibo.it.

Marta Pancaldi is a master's student at the University of Manchester. She previously studied at the Free University of Bozen-Bolzano and the College of Charleston. Her research interest is IT governance applied to cloud computing and software engineering, including its pedagogical aspects in teaching the subject. Contact her at marta.panc@gmail.com.

Davide Tosi is an assistant professor of software engineering at the University of Insubria. He has a PhD in computer science. His research interests include software testing and analysis, mobile agent systems, component-based systems, self-managed systems and services, open source quality and testing, and big-data analysis. He previously worked at Vodafone, H3G, Reply, and the University of Milano-Bicocca. He is chair of OpenSoftEngineering and Facedoor. Contact him at davide.tosi@uninsubria.it.