Cloud Computing and the new EU General Data Protection Regulation

Marta Pancaldi
Free University of Bozen-Bolzano, Italy

Davide Tosi
Università degli Studi dell'Insubria. Italy

Davide Locatello
Free University of Bozen-Bolzano, Italy

Guido Bonzagni
Free University of Bozen-Bolzano, Italy

Laura Valle
Free University of Bozen-Bolzano, Italy

Barbara Russo
Free University of Bozen-Bolzano, Italy

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

The new law on data protection of the European Union (EU), the General Data Protection Regulation (GDPR)[GDPR2018], has a direct effect on all EU member states from May 2018. Unlike the previous EU legal framework (Data Protection Directive 95/46/EC, (DPD) [EU_DPD1995]), no national transposition is needed and the Regulation soon comes into force in all member states including 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 EU, like Cloud Computing. The GDPR aims at clarifying concepts and procedures for data protection in the today connected world that drastically amplifies risks of data breach [FernquistEtAl2017]. Compliance with GDPR is a tough task when European enterprises use an average of 608 Cloud apps [Netskope2015]. Hence, an analysis of the effects of the GDPR should be performed with particular attention to IoT, Big Data, and Cloud Computing [Fabiano2017].

One of the major novelties of the GDPR that is relevant for Cloud Computing is its scope of application (referred to as *extra-territorial applicability,* Article 3). Unlike Directive 95/46/EC, which applied to organisations established in the EU or that use equipment situated in the EU, the GDPR also applies to non-EU organisations that process or monitor personal data of subjects who are in the EU. *Given its ubiquitous nature, organisations operating in Cloud Computing are often*

based outside EU (e.g., Google [GoogleGDPR2018]) *and typically process data of any subject all over the world. Article 3 of the GDPR on territorial scope may then apply to them*.

A second aspect of GDPR is the new responsibility given and shared by processors and controllers of personal data. Under the GDPR, *Cloud Service Provider (CSP) will have to take responsibility in what is processed and how its service, platform, or infrastructure is deployed and utilised by the customer* [Webber2017]. Additionally, a CSP must gather a *non-passive consent* from the customer for processing data and how and by whom the data is processed (e.g., with additional explicit consent on sub-contractors). This may increment the diversification of the contractual agreements between the provider and the single customer that for big players with many customers (e.g., Amazon) may make the service as-is impossible to manage. Therefore, *big players of the Cloud Computing industry are implementing code of conducts or new terms of service* that serve as transparent framework for decisions on data protection under the GDPR.

In this paper, we explore the impact on Cloud Computing of the GDPR. We discuss its effects also in comparison with the previous European Directive DPD [EU_DPD1995] and the United Kingdom (UK) Data Protection Act 2018 (DPA) [UK_DPA2018].

GDPR OVERVIEW

The fact that a researcher had sold to Facebook data collected via a personality quiz to the consulting UK-based firm Cambridge Analytica in 2014 and the consequent unauthorized possession of personal data of Facebook users is an exemplar case that, if proved true, the GDPR is supposed to prevent and punish. Under the GDPR, such unauthorized possession may be punished with a hefty administrative fine. What makes Facebook exposed to the GDPR? Facebook provides social networking services over the Internet that share personal data within networks of connected users. As such, Facebook is popular example of CSP. As Facebook, any CSP that manages customers' data over the cloud needs to pay attention not to incur in the risk of infringement of the GDPR. To shed some light on such problem, the following sections review the key aspects of GDPR that eventually affect the provision, use, and management of Cloud Computing.

Key Elements of the GDPR

A first element of distinction of the GDPR is the specification of new types of data in what is referred to as personal data. *Personal data* is any information relating to an identified or identifiable data subject; a *data subject* (e.g., Cloud service subscribers) 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 to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal data is any information relating to an identified or identifiable data subject; a data subject (e.g., Cloud service subscribers) 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 to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person [GDPR2018]. The GDPR explicitly qualifies as personal data, types of data concerning the *identifier* like IP address or Internet cookies and the *genetic nature* like the 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 the Directive 95/46/EC and accommodate new types of data produced by the new technologies. An example that illustrates this evolution is the case of Mr. Patrick Breyer/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 the GDPR, Cloud services that regularly manage such types of data need to be designed to address privacy concerns (i.e., *privacy by design*), allow processing only the data that is absolutely necessary for systems' operations (i.e., *data minimization*), and limit the access to the data only to people involved in the processing [Macauly2018]. They also need to implement policies and tools to give data subjects

the right to move their personal data to other providers and finally delete their data (i.e., *right to be forgotten*) when they no longer need to be processed.

Data processing

Both in Directive 95/46/EC and GDPR, processing means any operation or set of operations, which is performed on personal data or on sets of personal data, whether or not by automated means. According to Article 9 of GDPR, special categories of personal data are the ones for which it is prohibited data processing in case it reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership and for the purpose of uniquely identifying a natural person, like data concerning health or a natural person's sex life or sexual orientation (e.g., genetic data and biometric). As cascading effect, processing of personal data must be followed and explicit consent of the data subjects must be obtained by processors from subcontractors that process part of their data.

Processors and controllers

Both in Directive 95/46/EC and the GDPR, the *controller* is a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data, whereas the *processor* acts on data on behalf of the controller. Under the 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 the GDPR, the concept of *joint controllers* introduced in Directive 95/46/EC 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, IaaS providers, which only provide users with a managed hosting service, must now take the responsibility of processing data generated by their infrastructure (e.g., logs) [LeQuellenec2017].

Data Location and Transfer

The GDPR extends its scope of application outside the EU borders: the GDPR affects all organisations within the EU, but it also applies to organisations established outside the EU (*third country*) if they offer *goods or services to, or monitor the behaviour of, EU data subjects.* Examples of such activities are tracking subjects over the Internet with the intent of profiling them (e.g. through cookies) or using a language or a currency (Euro) of one EU countries with the possibility of ordering goods and services in that language or currency.

The GDPR uses the concept of *transfer* in a broader sense than the Directive 95/46/EC by also defining data transfer as by means of intermediary international organizations. The GDPR also defines five different *safeguards* to transfer data outside EU borders: Adequacy decision (i.e., whether a country has adequate level of data protection), Binding Corporate Rules (BCR) (i.e., rules for internal transfer of data for multinational companies), Standard Contractual Clauses (suitable for one-time transfer), approved Code of Conduct (for multiple transfer), 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 organisations to fall into the GDPR regulation and to identify models of safeguards for data transfer. Given its ubiquitous nature, this is especially true for Cloud Computing.

Data Subject's Consent

The *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. The GDPR makes

clear that consent requires a clear affirmative action by the data subject (e.g., no pre-checked consent statements) that must be informed about the agreement details, such as the identity of the controller, the purpose of data processing and the right to withdraw subject's consent at any time. Data subjects can anytime withdraw their consent and request for a complete erasure of the data (*right to be forgotten*) and conduct audits to check the actual destruction of data. The 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 (i.e., provisioned and released on demand) of shareable computing resources (i.e., computing resource through a common access to the service provided separately for each user). The majority of the distributions for Cloud services in European small and medium enterprises are hybrid (i.e., a federation of public, private, or partner Clouds), partner (i.e., owned and managed by a trusted partner), or public (i.e., owned and managed by an unrelated business); a smallest portion is also private (i.e., owned and managed internally) as reported by European Agency ENISA.

The architectures of a Cloud service differ in the type of layer from which users can access services. Infrastructure as a Service (IaaS) provides computing resources and hardware infrastructures over the Internet in a virtualised environment (e.g., virtual machines, storage, 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 PaaS and SaaS models (e.g., the ability of the customer to install and set up the image for security analysis purposes, to execute snapshots of 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.

Platform as a Service (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, Python, e.g.) or byte code (Java servlets, C#). Examples include Google App engine and Microsoft Azure. In terms of access to data, the core application is under the control of the customer. 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 like security checks.

Individual software packages are available at the application layer of the Software as a Service (SaaS). Applications range from email servers, document editors, to customer relationship management systems. SaaS services can often be accessed with a browser or a web services client. SaaS providers (e.g., the video streaming service Netflix) may run their applications on an IaaS (e.g., Amazon Web Services) or 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 in such processing. 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 and what data the provider wants to process on the infrastructure, in which countries, for what purposes and how it wishes to protect its data. In general, IaaS providers are unaware of how their infrastructure is being used and are unable to tailor their services to individual customers (e.g., 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 the GDPR that has significant impact on Cloud services is the new responsibility assigned to the processor [Webber2016]. To understand such implication, we recall the role of a provider in Cloud services in the following. A CSP offers Cloud services and, in particular, process data of its customers. As such, in the GDPR, the *CSP is a processor* [Wolters2017, Webber2016]. This implication consolidates concepts introduced in recent European directives (e.g., [NISDirective2016]) 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 authorised access at any time and from anywhere in the world through an Internet connection [Flint2017]. 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, being the role of controller a matter of fact (see for example, [C-2010]). Finally, the new forms of data generated by modern Cloud infrastructures and platforms (e.g., system logs) are ascribed to personal data as they can profile users and are in the hand of the CSPs. Therefore, PaaS/IaaS providers that, before GDPR, have almost no role on data protection, under the GDPR, are given some responsibility although still limited [Webber2016].

Cloud customer as controller or processor

If a provider is a data processor, a customer of Cloud services is in general considered a data controller of the data stored in the provider's servers [LeQuellenec2017]. This is typically the case for IaaS and PaaS services for which in principle the customer determines the purpose for which the data is processed and choses how it is processed. The customer is a processor if s/he is merely processing the personal data according to the wishes of a third party. This is typically the case of SaaS. The 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 on the data and its process*.

Responsibilities of Cloud service customer and provider as joint controllers

In a recent investigation on more than 20 CSPs, the extent of liability ascertained under Directive 95/46/EC has been minimal, i.e., less than 500 USD [Flint2017]. Under the GDPR, customers may have a better means to claim for compensation against the provider thank to the introduction of the joint control between a provider and its customers. While maintaining the two roles distinct, 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 CPS's sub-contractors [Flint2017]. For example, a data controller that has personal data processed by a SaaS (e.g., Netflix) whose software is on servers operated by an IaaS company (e.g., Amazon Web Services) is required to approve the use of such 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 the company that advertises its products on the Google platform each act as independent controller of personal data. The risks on security breaches are therefore shared. Consequently, in some cases, big CSPs and their sub-contractors may need to tailor security measures for hundreds or thousands of customers.

Data Subject's Consent for Cloud Services

Implementing data subject's 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 it aware of both processing via 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 the 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 / access to report it. In practice, only the processor has competence and knowledge of how data received through the controller (e.g., SaaS) or directly through its platforms (e.g., IaaS, 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 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 only provide services that do not manage data (e.g., networking functionalities for IaaS, or 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 (e.g., for data analytics services), the compliance with GDPR becomes more stringent including when they offer such services under sub-contracting. 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 sub-contracting in Cloud Computing establishes a chain of responsibilities for data protection that needs to be tracked and monitored.

Data Location and Transfer

The new geographical scope of application of the GDPR is particularly relevant for Cloud services with what concerns data location. The top ten data centres in the world are all located outside Europe [DataCenters2017]. 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 centre often does not correspond to the location of the provider's head quarter. This is specifically the case of IaaS providers whose servers are typically located outside EU. For example, since December 2014, Amazon Web Services operate on about 1.4 Million servers over 54 locations worldwide, including United States, Europe, Asia, Australia, and South America. Data location in the GDPR may also have significant effects on SaaS services like Microsoft Office 365, G suite, or 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 the GDPR. Such subjects are, for example, companies that provide SaaS for data protection or backups for other SaaS applications for business/enterprise use. Such companies are data controllers with respect to SaaS providers and processor with respect to single subscribers. In addition, SaaS providers (like the G suite of Google) need to ensure that their sub-contractors also located outside EU (like the Spanning products for data protection) adhere to the GDPR as well.

Crucial for Cloud Computing is also how to transfer data through EU borders (e.g., with US) and what safeguards need to be implemented to be compliant with the GDPR. Among the ones that have signed a BCR are banks or payments companies (like MasterCard or American Express) and Hotel chains (like Hyatt) as well as electronic commerce (like e-Bay). 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 [CoC_CSP2017], whereas big IaaS providers like Aruba, Amazon Web Services, and UpCloud undersigned a specific GDPR compliant Code of Conduct for IaaS providers [CoC_CISPE2017]. Google has instead opted for a GDPR compliant Terms of Service.

Data Security and Breach

Controllers and processors must take adequate measures (e.g., pseudonymisation) and countermeasures to prevent security issues such as data loss, alteration or unauthorised access. For CSP such measures depend on the type of Cloud architecture and the way it processes data. For example, IaaS providers adhering to Code of Conduct [CoC_CSP2017] explicitly decline responsibilities derived solely from customer's use of the infrastructure. Thus, an organization that allows employees to use personal Cloud software (e.g., 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 (i.e., the release also unintentional of secure or private information to an untrusted party) are one of the key concerns of the GDPR for which a detailed notification of the breach including the cause of the incident must be reported no later than 72 hours after the organisation has become aware of it. Accuracy of breaches' report is essential to increase the awareness of security risks and, thus, prevent naïve management of Cloud services. Year 2017 has seen a rising number of security incidents due to misconfigured or poorly secured Cloud servers [CRN2017]. Two cases are striking in their naïve management of the service. One case concerns the access to data of about 14 million Verizon customers' 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 Deep Root Analytics. The database lacked any protection against access and could be downloaded by anyone with an 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 customer's data on its behalf as the customer is responsible of these actions. In other cases, the way to erase data is also a technical matter. For example, the community of Hyperlegend (an open source SaaS provider offering blockchain services and hosted at the Linux foundation) has conceived three different strategies to ensure the right to be forgotten in their blockchain services.

Blockchain plus DB with pseudononymization: Use blockchain to keep track of all transactions state changes and use the database to store personal data. All the blockchain data of a user is associated with a user pseudonym and the access of such key is only available to the use. If data deletion is requested, the record is irreversibly deleted from the database.

Blockchain with cryptographic features: Delete 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 the SaaS application won't be able to read the data.

Actually deleting the data: Edit the immutable blockchain. This is an extreme case although may be useful to accommodate legal and regulatory requirements of the 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 AND AMAZON WEB SERVICES

Big industrial players, both from EU and extra-EU, such as Google, Microsoft, SAP, and Amazon are working to define policies and a practical support for stakeholders to comply with the 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 Google Cloud platform [GoogleGDPR2018] and the code of conduct [CoC_CISPE2017] to which Amazon has declared full compliance for its services [AWS2018] supplemented with Amazon Navigation GDPR Compliance. All such documents entered into force on May 25th, 2018.

The strategies of GCP and AWS for GDPR compliance are different. The GCP service agreement is based on a set of instructions agreed with the individual customer and included in Data Processing and Security Terms, the instructions given by customer via the Admin Console and any subsequent written customer's instructions acknowledged by Google. The AWS' service agreement instead refers to the CISP code of Conduct undersigned by a group of IaaS providers [CoC_CISPE2017]. 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 centres. 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's 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 own purposes, including, in particular, data mining, profiling or direct marketing. Worth noticing here that GCP reserves the right to migrate customer's data to centres in a location not chosen by the customer.

Table 1: Strategies of compliance with GDPR

Concern	Google Cloud platform (GCP)	Amazon Web Services (AWS)
Governance	GCP is a processor of the customer personal data, while the customer is the controller (or processor) of such data. Google will only process customer personal data in accordance with the below-mentioned customers' instructions.	AWS provider is processor of the customer personal data, while the customer is controller (or processor) of such data. According to CISP Code Requirements, (1) customers provide and manage controls such as security policies, monitoring, malware; (2) provider provides and customers configure and manage controls such as key management, logging services, virtual private Clouds; (3) provider alone manages and audits controls related to standards (e.g., 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. Up to now only some of the services (e.g., Amazon EC2) are fully compliant

		(https://cispe.Cloud/publicregister). The provider will act as controller for customer's personal data concerning account information (e.g., billing information).
Security	Google maintains a set of security measures on its data centres (e.g., redundant infrastructure systems and Linux-based secure application environment), network and transmission (e.g., ephemeral elliptic curve Diffie-Hellman cryptographic key exchange signed with RSA and ECDSA), and site controls (e.g., biometric access control system), access control (e.g., unique user IDs, strong passwords, two factor authentication and carefully monitored access lists) and data storage (e.g., data and file system architecture are replicated between multiple geographically dispersed data centres).	Responsibility on security is shared according to the above-mentioned governance of the services. For example, the provider is responsible for security of the physical infrastructure and the surrounding environment and the customer is responsible of the configuration of the IaaS service. Worth notice here that the customer is also responsible to review 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 customer's instructions. Google Cloud Platform License Agreement is supplemented by the Data Processing and Security Terms, the instructions given by customer via the Admin Console and otherwise in its use of the Services and any subsequent written customer's 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	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	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's data either (a) as part of the

	sub-processors maintains facilities. If data are to be transferred out of the EEA, Google will (a) if requested to do so by Customer, ensure that the transfers are made in accordance with such contract clauses and/or (b) offer an alternative solution. Administrators can export customer data, via the functionality of the Google Cloud Platform services, at any time during the term of the agreement. Customers can additionally delete their data, via the functionality of the Google Cloud Platform services, at any time. When Google receives a complete deletion instruction from the customer (e.g., 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's personal data for any other purpose.	service, or (b) by enabling customers to design and deploy their own solutions using the service. No further assistance to the customer with data subject's request is provided. In respect of 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 the purposes of data mining, profiling or direct marketing.

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." With this statement, begins the "Notice to Stakeholder" of the European Commission Directorate of JUST of January 9th, 2018. The same communication underlines, though, that the 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, after May 2018 the GDPR applies to it. Form the withdrawal date, the data flow between the UK and the EU must be maintained as about 43% of the EU tech companies are UK-based and 75% of the UK's data transfers take place with the other EU members [Brexit2018]. Thus, in June 2017, the UK Department of Digital, Culture, Media and Sport issued the Data Protection Bill 2018 (DPB, ico.org.uk), which has been finalised in the 2018 DPA. The DPA entered into force on May 25th, 2018 and

updates the UK data protection laws and further supplement the GDPR by extending data protection to as-yet uncovered areas of application. The DPA also includes some exemptions to the GDPR that may also have effects on Cloud services. For example, some of the SaaS services (e.g., Facebook) are concerned with the age of consent that the DPA has lowered to 13.

Besides the DPA and its compliance with the 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 Artificial Intelligence. In her speech at the Alan Turin award in March 2018, Elizabeth Denham, the head of the UK Information Commissioner's Office, made it clear that the opaqueness of the algorithms used in processing large amount of data and the inferred data that such processes might derive put under serious risk the protection of personal data. 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 on information rights. Such strategy also foresees the establishment of a technological sandbox where new technologies will be deployed and tested for data protection (e.g., how fingerprints in smartphone easy access are processed).

OBSERVATIONS

The GDPR has some consequences on the provision, management, and use of Cloud services. The magnitude of such 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 (e.g., log data) are now ascribed to the personal sphere or new roles (e.g., 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 ground for GDPR compliance and updating the current UK law. Until Brexit is effective, the UK, as an EU member state, must comply with the GDPR. Thus, the DPA is designed to make this transition period the smoothest possible although few differences might need further attention at the application stage (e.g., age of consent).

The territorial scope in the GDPR is extended to non-EU countries as far as 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 Code of Conducts, defining Binding Corporate Rules for internal transfer across national borders, or updating Terms of Service contracts to align their procedures and policies to the GDPR. Differences in such agreements and contracts as in the case of the two IaaS CGP and AWS make it clear that *stakeholders in the Cloud computing business need case law to understand the real impact in both the provision and the use of such services in relation to the processing of personal data*.

REFERENCES

1. [GDPR2018] Regulation (EU) 2016/679 of the European Parliament and the Council (General Data Protection Regulation). http://eur-lex.europa.eu/eli/reg/2016/679/oj Last access: March 2018
2. [EU_DPD1995] EU Data Protection Directive, 1995. http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf Last access: March 2018
3. [FernquistEtAl2017] J. Fernquist, T. Fägström and L. Kaati, IoT Data Profiles: The Routines of Your Life Reveals Who You Are, In proceedings of the IEEE European Intelligence and Security Informatics Conference, 2017
4. [Netskope2015] Netskope Cloud Report 2015 EMEA edition. https://resources.netskope.com/Cloud-reports/autumn-2015-emea-Cloud-report Last access: March 2018.

5. [Fabiano2017] N. Fabiano, Internet of Things and Blockchain: Legal Issues and Privacy. The Challenge for a Privacy Standard, In proceedings of the IEEE International Conference on Internet of Things, 2017
6. [GoogleGDPR2018] Google Cloud Platform Terms, Data Processing and Security Terms (Customers). https://cloud.google.com/terms/data-processing-terms Last access: June 2018
7. [Webber2016] M. Webber, The GDPR's impact on the Cloud service provider as a processor, Privacy & Data Protection Journal, 2016, Vol. 16, No. 4
8. [UK_DPA2018] UK Data Protection Act. http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf
9. [Macaulay2018] Macaulay T. M. How to ensure GDPR compliance in the Cloud, Computerworld UK. https://www.computerworlduk.com/Cloud-computing/how-ensure-gdpr-compliance-in-Cloud-3663797/ Last access: March 2018.
10. [LeQuellenec2017] Le Quellenec E. Cloud Contracts: Impacts of GDPR on Joint Controllers, https://Cloudprivacycheck.eu/latest-news/article/Cloud-contracts-impacts-of-gdpr-on-joint-controllers/ Last access: March 2018.
11. [Wolters2017] P. T. J. Wolters, The security of personal data under the GDPR: a harmonized duty or a shared responsibility?, International Data Privacy Law, 2017, Vol. 7, No. 3
12. [Flint2017] Flint, Sharing the Risk: Processors and the GDPR, Bussiness Law Review, Issue 4, 2017, p. 171-172
13. [C-2010] Case Law of the Court of Justice, C-2010 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH
14. [DataCenters2017] The biggest data centres in the world, where they are and who owns them, https://www.computerworlduk.com/galleries/infrastructure/biggest-data-centres-in-world-3663287/ Last access: March 2018
15. [CoC_CSP2017] Code of Conduct for Cloud Service Providers. https://eucoc.Cloud/fileadmin/Cloud-coc/files/European_Cloud_Code_of_Conduct.pdf Last access: March 2018
16. [CoC_CISPE2017] Code of Conduct for Cloud Infrastructure Service Providers. https://cispe.Cloud/wp-content/uploads/2017/06/Code-of-Conduct-27-January-2017-corrected-march-20.pdf Last access: March 2018
17. [CRN2017] Kuranda S. The 10 biggest data breaches of 2017 (so far). https://www.crn.com/slide-shows/security/300089736/the-10-biggest-data-breaches-of-2017-so-far.htm/pgno/0/10 Last access: March 2018
18. [AWS2018] AWS security blog: All AWS Services GDPR ready. https://aws.amazon.com/blogs/security/all-aws-services-gdpr-ready/ Last access: March 2018.
19. [Brexit2018] Brexit and Partnership with the UK. www.gov.uk/government/uploads/system/uploads/attachment_data/file/589189/The_United_Kingdoms_exit_from_and_partnership_with_the_EU_Print.pdf Last access:

Barbara Russo is an associate professor at the Faculty of Computer Science of the Free University of Bozen-Bolzano, Italy. She received a PhD in mathematics from the University of Trento, Italy. She was research fellow at the Max-Planck Institut für Mathematik in Bonn, Germany. She has written more than 100 papers in software engineering, information systems, and mathematics. Her current research interest focuses on monitoring and predicting vulnerabilities of software systems and services. Contact her at: barbara.russo@unibz.it

Laura Valle is associate professor of Private Law and she teaches Private Law, Contract Law and Contracts of the Public Administration. She is a Member of the Phd Program on Legal Instruments for SME at the University Suor Orsola Benincasa of Neaples. Her publication activity concerns mainly: contract law, standard contracts, unfair terms in contracts, consumer protection, European contract law, personality rights and fundamental rights, domain names, nonprofit organization law. Ongoing research projects are “Contract and Fundamental Rights”, “Trusted Cloud Computing for Europe 2020” and “Contract, Sustainability, Human Rights and the Corporate Social Responsibility”. 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 gradueted with honors at the Law Faculty of Alma Mater Studiorum-Bononia University and collaborates with prof. Laura Valle at the Faculty of Economics of 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 Maria Locatello graduated in 2016 at the University of Bologna School of Law with highest honour. His research interest includes contract law, family law and tort law. These studies led to the publication of some articles. Contact him at: davide.locatello2@unibo.it

Marta Pancaldi is a MSc student at the University of Manchester, UK. She studied in Italy, at the Free University of Bozen-Bolzano, and in the United States, at the College of Charleston (South Carolina). Her current research interest are 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 assistant professor of Software Engineering at the Università degli Studi dell’Insubria. He obtained his PhD in Computer Science in 2007 working on self-* Web Services. 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 has been scientist at Vodafone spa, H3G spa, and Reply. He is chairman of OpenSoftEngineering srl (a spin-off at Università degli Studi dell’Insubria and Chairman of Facedoor srl (startup). Formerly, he worked as a post-doc at the Department of Computer Science at the Università di Milano Bicocca. Contact him at: davide.tosi@uninsubria.it