Regulatory Impact of Data Protection and Privacy in the Cloud

Sakshi Porwal*, Srijith K. Nair**, and Theo Dimitrakos

Security Futures Practice, BT Innovate & Design,
Martlesham Heath, Ipswich IP5 3RE, United Kingdom
{sakshi.porwal,srijith.nair,theo.dimitrakos}@bt.com

Abstract. The use of cloud computing services has developed into a new method for deploying software and services and hosting data. The model has provided enormous social and economic benefits but at the same time it has also created potential privacy and security challenges for businesses, individuals and the governments. For example, the use of shared compute environment, data storage and access via internet has made information vulnerable to misuse, and thus, has made privacy a major concern for organisations adopting cloud services for storage and computation purpose. Generally, each country maintains their own laws and regulations to prevent frauds and protect their citizens from harm, including the potential dangers of data privacy, essential when internet and related technologies are involved. The European Union, for example, follows the overarching governmental regulations while the United States prefers the Sectoral Approach to Data Protection legislation, which relies on the combination of legislation, regulation and self regulation. This report discusses data protection issues related to cloud computing and identifies privacy laws enforced in the EU that can be applied to this model. Moreover, it also provides recommendations that cloud service providers can consider to implement in order to provide enhancements to their services and to demonstrate that they have taken all necessary measures to comply with the data protection principals in place.

Keywords: cloud computing, data privacy, data protection, regulations.

1 Introduction

Privacy of digital data has always been a critical concern of the IT industry. It occupies a central concern in the cloud computing service delivery model due to its unique multi-tenanted and resource-shared nature. Its richness in functionalities has exacerbated the concerns of individuals, organisations and government as there is a greater perceived probability of compromise of the privacy of personal data.

Many elements of regulations related to the traditional IT industry can be applied in order to protect information in a cloud environment, with little or no specialized provisions. However, the cloud model introduces additional complications in order to

* Work carried out during internship at BT.
** Corresponding author.

I. Wakeman et al. (Eds.): IFIPTM 2011, IFIP AICT 358, pp. 290–299, 2011.

comply with some of these regulations. In addition, different nations have varying views on the regulation needed to protect data and private information and to whom these laws apply. One of the major reasons for this difference across countries is due to the fundamental difference in the role and relationships of government and the commercial sector.

While the European Union (EU) and the United States are each other's largest trading partners, they follow vastly different approaches to protect their personal information. In the EU, government actively participates along with the major industries to achieve public tasks. Moreover, it discusses regulatory and public interests, objectives and strategies to attain them. In contrast, US decision makers follow a more laissez-faire approach to corporate governance and emphasize on the role of private sectors in resolving challenges [1].

Cloud service providers, like any other IT service providers, have to architect their system in such a way as to obey their country specific laws and regulations. In the EU, the European Union Data Protection Directive is the central pillar of data privacy and in the US, several sector specific laws and regulations are collectively set forth to protect the privacy of cloud service consumer's personal data.

This paper looks at the data protection and privacy issues associated with the cloud computing model and goes on to examine the EU privacy laws related to this area with the aim of providing recommendations, with special emphasis on the point of view of cloud providers, in order for them to comply with country specific regulations. The structure of this paper is as follows: Section 2 provides a brief introduction of the cloud computing service model and identifies various areas that need special consideration from a regulatory point of view. The next section describes data protection and privacy laws applicable in the EU and with the help of different cloud scenarios discusses their applicability. Section 4 attempts to provide generic legal and regulatory recommendations distilled from the earlier section for cloud providers to consider in order to comply with their country-specific laws. The last section concludes the paper.

2 Cloud Computing

Cloud computing has emerged as a promising and challenging model for deploying software and services and hosting data. It utilizes two separate technological pillars-utility computing and service oriented architecture principles, to provide cloud service consumer with highly scalable, economic and everything-as-a-service delivery model. Cloud computing is rich in features such as scalability/elasticity, shared resource pooling, multi-tenant environment, ubiquitous network access and pay-as-you-go pricing. Its characteristics for providing faster, agile, robust and economic solution makes it a very attractive service delivery model from the customer's perspective.

The major players of the cloud computing ecosystem are Cloud Service Providers (CSP) that provides cloud services and Cloud Service Consumers (CSC) which makes use of (consumes) these cloud services. The CSC can be an individual, SME or a bigger enterprise.

While cloud computing has been characterized as one of the most game-changing IT models to emerge in recent years, its adoption carry a number of risks and threats,

the general discussion of which is however beyond the scope of this papers. Here we concentrate on the data protection and privacy issues associated with the model.

Some aspects of cloud computing demands special attention because of the strong privacy concerns and legal requirements surrounding its use. To exemplify, data of various users is stored in a shared infrastructure environment, where faulty access control mechanisms can lead to unauthorised access to confidential data. Therefore, special mechanisms are needed to protect the sensitive data from such unwanted access. In order to secure their services, cloud providers have to comply with the legal and regulatory standards. Grey areas exist in the regulatory sphere. Concerns have been raised as to how the data will be transferred from the user's domain to the cloud and the associated legal issues if the cloud provider is based in a different country. Also, in the cloud model, providers have to provide assurance to their customers that they will respect the confidentiality of their data and integrity of their computation. In addition, the protection of intellectual property is another concern for service providers who provide flexible environment to cloud consumers to deploy their applications. Other issues which cloud providers have to consider in order to provide effective services to their customers includes risk allocation, privileged user access, data leakage, data recovering methods and key management.

Thus we see that there are several data protection and privacy issues that have to be considered by both the CSPs as well as the CSCs. In the next section we discuss the conceptions of privacy with respect to cloud computing model in the context of EU.

3 EU Perspective

The EU follows a single overarching privacy law which claims privacy as the fundamental right of a human being. It is the responsibility of the government in the EU to protect an individual's right to privacy and to actively participate with industries to achieve public tasks and discuss the regulatory and public interests, objectives and strategies. Furthermore, in the EU, use of personal data is proactively regulated which is refrained in the US [2, 3].

The Data Protection Directive [4] forms an important component of the EU privacy and human rights law and applies to the processing of information in electronic as well as manual forms and addresses both personal data and personally identifiable information. Its main purpose was to harmonize the privacy laws that existed in the different member states of the EU and to provide a basic standard on privacy protection. It consists of 32 articles, setting requirements on handling personal data and mandating the countries of the EU to implement them.

The EU directive is applicable to cloud providers that are established in the EU or "act as processor for a controller established in the EU." In other words, any cloud provider based in the EU or serving companies based or operating in the EU has to abide by its clauses. These include both the cloud provider as well as other service providers that use cloud providers for powering their service, based in the EU. It is also applicable if the cloud provider uses equipment (such as servers) that is located within an EU member state or act as processor for a controller using such equipment.

Furthermore, the EU Directive assumes the existence of cross border data flows and attempts to protect the data privacy rights of EU regardless of where the data is

transferred or processed [5,6]. The Article 5 of the Directive mandates that participating states should ensure that the personal data of EU is protected with adequate level of protection when it is exported to and processed in countries outside EU.

The following legal and regulatory analysis covers the issues and solutions unique to cloud services with regards to data protection, confidentiality, intellectual property and outsourcing services and changes in control.

3.1 Data Protection

The services provided by cloud providers in a Software as a Service (SaaS) model generally consist of email, messaging, desktops, projects management, payroll, accounts and finance, CRM, sales management, custom application development, custom applications, telemedicine and billing., where personal data of the customer get processed[1]. This data may belong to a number of persons for example, employees, clients, suppliers, patients and, more generally, business partners.

From an analysis of Section 4 of the Data Protection Directive, it can be concluded that the place where the controller is established is relevant to the application of the Data Protection Directive, and the place of processing of the personal data or the residence of the data subject is less relevant. The Data Protection Directive will then apply if the Controller is established in the EU and also if the Controller is not established in the EU but uses equipment located in the EU for processing of personal data (e.g., data centers for storage and remote processing of personal data situated on the territory of a Member State, computers, terminals, servers), unless such equipment is used solely for the purpose of transit through the territory of the Community.

Once it is determined that the Data Protection Directive applies, the first question that needs to be clarified is the identity of the Controller and the Processor. The classification as a Processor or Controller greatly determines the very different compliance duties and obligations and related liabilities associated with the entity. In general, if the customer of the cloud provider determines the purposes and means of the processing of personal data, he is the Controller and if the cloud provider processes personal data on behalf of his customer, it is an External Processor. In this analysis it is assumed that the customer of the cloud provider is the Controller and the cloud provider an External Processor.

Some of the main duties and obligations for the Controller set forth in the Directive are:

a. Processing the personal data according to the principles of Fairness, Lawfulness, Finality, Adequacy, Proportionality, Necessity and Data Minimisation (Section 6 of the Data Protection Directive)
b. Processing the personal data after having provided the data subject with the necessary information (Section 10 of the Data Protection Directive);
c. Guaranteeing the data subject the rights laid down in Section 12 of the Data Protection Directive - e.g., to obtain confirmation as to whether or not data relating to the data subject is being processed, to obtain information on the purposes of the processing etc.

[1] Note that as far as the directive is concerned, storage is a form of process.

d. Implementing appropriate technical and organisational security measures to protect personal data against accidental loss, alteration, unauthorised disclosure or access and against all other unlawful forms of processing (Section 17 of the Data Protection Directive);
e. Choosing a Processor that provides sufficient guarantees with respect to the technical security measures and organisational measures governing the processing to be carried out, and ensuring compliance with those measures;
f. Transferring of personal data to 'third countries which do not ensure an adequate level of protection within the meaning of Section 25 (2) of the Data Protection Directive only in case the data subject has given the previous consent unambiguously to the proposed transfer or under the condition that other procedures are in place as per Section 26 (e.g., 'Standard Contractual Clauses' or – if the data are transferred to the United States – 'Safe Harbor Principles'[7,8]).

The data controller (cloud customer) should provide the data subjects (end-users of the cloud customer) with all the mandatory information related to data processing. The cloud customer will be required under the Directive to inform their customers about the circumstances of the transfer to the cloud provider, the quality of the cloud provider (external processor), and the purposes of the transfer. It is crucial that those who collect data subject to the Data Protection Directive ensure that they understand the application of the Directive to the use and transfer of that data. In this respect, controllers not currently engaging in cloud computing are advised to seek informed consent from the data subjects to data processing and transfer outside the European Economic Area. Those currently engaged in cloud computing are advised to ensure that this consent has been procured and that it adequately describes the nature and extent of processing and transfer. The alternative would be to have in place one of the procedures set forth in Section 26 (Standard Contractual Clauses or Safe Harbor Principles – if the data is transferred to the US and the cloud provider participates in such a program).

To apply the Data Protection Directive adequately, the availability and integrity of data are key, which leads the discussion to data security measures. There are unavoidable trade-offs here. More data security is likely to lead to reduced availability. The customer of the cloud provider may thus want to take a close look at the security measures the cloud provider has in place and the data availability guaranteed. It has to be born in mind that in most European countries there are mandatory data security requirements. The customer of the cloud provider needs to make sure that those measures are complied with.

It has to be clear at this point that the customer – when classified as sole data Controller - will be the entity responsible for the processing of personal data in relation to the data subjects. The customer will also be responsible for this data when such processing is carried out by the Cloud Provider in the role of external Processor. Failure to comply with the Data Protection Directive may lead to administrative, civil and also criminal sanctions, which vary from country to country, for the data controller.

Dealing with the issues

Various steps can be taken in order to deal with the various regulatory constraints imposed on the cloud provider and cloud customer by the EU directive. Here we discuss some of the prominent ones.

It is recommended that the Cloud provider use fine grained access control mechanisms that take into account location of data owner/ jurisdiction and also the organisational structure of customer.

At the Cloud consumer's side, it should look for the presence of Data Protection clause in the contract between them and the provider instead of ensuring themselves that the collected personal data is handled in compliance with Sections 7 and 10 of the Data Protection Directive. This clause should set forth the relevant parties' duties and obligations. The cloud provider should cooperate with the controller in order to assure that the latter can effectively guarantee the data subject's rights in accordance with Section 12 of the Data Protection Directive.

The cloud provider should also have in place adequate security measures pursuant to Section 17 of the Directive and it should promptly notify the controller of any breach of data security and cooperate swiftly to solve the problem.

The data protection clause between the provider and the consumer should be subject to negotiation. In addition, security measures may be addressed in annexes and SLAs. In addressing security issues, the parties should keep in mind that they may not be able to detail all security measures to be addressed. Because IT security is an ongoing race to deal with new issues, contract terms need to be free to develop accordingly.

It may also be advisable for the customer to negotiate adequate remedies for contractual damages should the Data Protection clause be breached. Also, if the cloud provider's breach is substantial it may be included in the list of instances which lead to unilateral termination of the agreement

In addition, if the cloud provider is in a country outside the European Economic Area and that country does not offer an adequate level of data protection, it is advisable to have in place procedures in accordance with Section 26 (e.g., 'Standard Contractual Clauses' or 'Safe Harbor Principles' – if the data are transferred to the United States and the cloud provider participates in such a programme), rather than basing the transfer on the consent of the data subject.

However, it has to be stressed that the transfer of data within the territory of Member States is not without problems. Indeed, despite the fact that personal data can freely circulate within Member States, the laws are not consistent across countries. This inconsistency may create obvious difficulties in compliance and thus liability issues. As the Data Protection Directive is currently under revision, it is hoped that the Commission would take steps towards the standardization of minimum data protection requirements in Europe.

3.2 Confidentiality

Confidentiality concerns are also raised by the scenarios considered in this paper. As secret information and 'know-how' may be processed in clouds, any leakage of information caused by voluntary communication by the Cloud Provider or cloud's security breach may jeopardise the customer business/services. It is crucial to distinguish between processing of data as in computational operations over that data, and the storage or transmission of data without altering it, since processing in this sense usually requires the data to be in unencrypted form, at least during the computation stage.

There do not seem to be any European regulations applicable to such scenarios. European regulations regarding know-how, defined as a body of information that is secret, substantial and identified in any appropriate form, apply principally to licensing and activities involving the transfer and exploitation of information.

Dealing with the issues

Keeping regulations in mind, and in order to preserve the economic value of know-how and secret information in general, including research results, customer and project-related information, it is recommended that customers seek contractual terms covering this issue. In fact, parties' duties and obligations to preserve such value could be specifically addressed in a 'confidentiality/non-disclosure clause'. Particular attention should be given to the boundaries of the responsibilities of parties and related liabilities.

The potential customer of the cloud provider should carefully analyse the confidentiality/non-disclosure clause to determine whether the cloud provider offers sufficient guarantees to protect the customer's secret information and know-how that will be placed in the cloud.

It is also recommended that the parties negotiate a provision that reflects the damage a party may sustain should confidential or secret information be disclosed. If the disclosure is substantial, this breach may be included in the list of instances which allow the company to unilaterally terminate the agreement.

3.3 Intellectual Property

Intellectual property may also be at risk when used within a cloud environment. Although an entity outsourcing services to the Cloud Provider may protect and enforce its intellectual property rights by means of the relevant legislation, which is similar in all the European Member States, a breach of Intellectual Property rights may cause immediate damage which will never be fully restored in a legal proceeding.

Moreover, in the unlikely case that the interactions between the customer and the cloud provider may give rise to joint results which can be object of intellectual property rights, it is wise to determine who will own these rights prior to engaging in cloud computing activities, and further determine the use that the parties can make of the objects of such rights.

Dealing with the issues

Intellectual Property rights should be regulated through dedicated contractual clauses: "Intellectual Property Clause" and "Confidentiality/Non Disclosure Clause". The Intellectual property clause should be detailed enough that it covers all the issues related to the Intellectual Property right. It should be explicitly mentioned in the contract that who owns various parts of the process- the data, the application, the result of the computation etc.

In addition, the potential customer of the cloud provider should carefully assess the value of its intellectual property and the risks related to cloud computing services. Having done so, the customer should carefully review any clauses governing

intellectual property to determine whether the cloud provider offers sufficient guarantees and allows the customer appropriate tools to protect its information (e.g. through encryption of data), to protect the customer's assets. The cloud customer should ensure that the contract respects their rights to any intellectual property as far as possible without compromising the quality of service offered (e.g. the creation of backup copies may be a necessary part of offering a good service level).

It is also advisable that the customer negotiate a clause in which the cloud provider is penalized should the provisions governing intellectual property be violated. Substantial breaches by the cloud provider may be included in the list of instances allowing the company to unilaterally terminate the agreement.

3.4 Outsourcing Services and Changes in Control

The agreement between the company and the cloud provider is likely to be defined as a contract "intuitu personae". This contract is one in which a party chooses to contract with a company based on qualities that are unique to the company. For example, a customer may choose a particular cloud provider because of the services it offers, its reputation or professionalism, or its technical skills. As a result, the customer may be reluctant to see the cloud provider outsource all or part of the services to be provided to the customer.

Furthermore, the control of the cloud provider may also change and, as a result, the terms and conditions of the services provided by the cloud provider may change too.

Dealing with the issues

Cloud providers should explicitly state in the contract which of the processes it is outsourcing to a third party and maybe even allow the customer to choose from a list of potential outsourcing companies based on its preference.

Moreover, the customer should determine in advance whether services will be outsourced by the cloud providers and whether the cloud provider issues some guarantees or warranties relating to the performance of the services outsourced. However, it is recommended that the customer look to be able to restrict the outsourcing of services by the cloud provider. It is also advisable that the contract be reviewed to determine how the cloud provider will communicate changes in control to the customer. The customer may also want to consider whether the contract includes the right to terminate the contract if a change in control occurs.

Furthermore, the customer may choose to require that the outsourcing of services by the cloud provider be subject to the customer's prior authorisation. To make this decision, the customer will need to be informed about the type of services that the cloud provider intends to outsource and the identity of the company to whom these will be outsourced. Even if the customer agrees to the outsourcing, it may want the cloud provider to issue some guarantees or warranties relating to the performance of the services outsourced. By the same line of reasoning, the customer may also want to have the chance to approve a change of control, or to terminate or renegotiate the contract in case of a change in the control of the cloud provider. Such options may be carefully specified in the contract between the company and the cloud provider by means of a 'third-party outsourcing' clause, a 'warranties and indemnification' clause, a 'change in control' clause, or a 'termination of agreement' clause – again depending on the bargaining power of the parties.

5 Conclusions

In this paper we took a close look at the European Union regulations that we consider will have direct impact on the use of cloud computing based services. We analysed these impacts and made specific observations on how the cloud service provider as well as the consumer can take steps in order to comply with the regulations.

Based on the discussions in the preceding section, we conclude the paper with the following high level regulatory recommendations

- **Data Protection:** Cloud provider should provide sufficient technical security measures and organisational measures governing the processing to be carried out, and provide to the customer evidence ensuring compliance with those measures.
- **Data Security:** Cloud provider should pay attention to mandatory data security measures that potentially cause either the cloud provider or the customer to be subject to regulatory and judicial measures if the contract does not address these obligations.
- **Data Transfer:** Cloud service provider should also pay attention to what information is provided to the customer regarding how data is transferred within the cloud, outside that cloud, and within and outside the European Economic Area or the US territory.
- **Confidentiality and Non-disclosure:** Cloud provider should provide assurance to their customers that they will not disclose customer's data to any third party.
- **Law Enforcement Access:** Cloud provider should make available information about the jurisdiction in which data may be stored and processed and evaluate risks resulting from the jurisdiction to the customer.
- **Intellectual Property:** Cloud providers should ensure that the contracts with the customer acknowledge and respect their rights to any intellectual property or original works as far as possible without compromising the quality of service offered.
- **Risk Allocation and Limitation of Liability:** When reviewing their respective contract obligations, cloud provider and all other parties should underscore those obligations that present significant risk to them by including monetary remediation clauses, or obligations to indemnify, for the other party's breach of that contract obligation. Furthermore, any standard clauses covering limitations of liability should be evaluated carefully. The review should include both the liability of the cloud provider and the liability of the customer for data storage or processing that is performed by the cloud provider or on cloud provider's premises / infrastructure on behalf of the customer.
- **Change of Control:** Transparency should be ensured, cloud provider should honor their contract obligations in the case of a change of control, as well as any possibility to rescind the contract.
- **Audit:** As customers have no visibility into the cloud, cloud provider should take specific measures to audit and monitor customer's data and processes in the cloud.

References

[1] Farrell, H.: Constructing the international foundations of e-commerce: The EU-U.S. safe harbor arrangement. International Organisation 57, 277–306 (2003)
[2] Fromholz, J.M.: The European data privacy directive. Berkeley Technology Law Journal 15, 461–484 (2000)
[3] Schwartz, P., Reidenberg, J.: Data privacy law: A Study of United States data protection. Michie, Charlottesville (1996)
[4] European Commission, "Data Protection Legislative Documents", http://ec.europa.eu/justice/doc_centre/privacy/law/index_en.htm#directive
[5] Movius, L.B., Krup, N.: U.S and EU Privacy Policy: Comparison of Regulatory Approaches. International Journal of Communication 3, 168–187 (2009)
[6] Schriver, R.R.: You Cheated, You Lied: the Safe Harbor Agreement and Its Enforcement By the Federal Trade Commission. 70 Fordham L. Rev. 2777, 2779 (2002)
[7] Dubois, P., Wiles, N.: Solutions for cross-border transfers of personal data from EEA. In: IP&IT, vol. 2 Data Protection (2006/2007)
[8] Kobrin, S.: Safe harbors are hard to find: The transatlantic data privacy dispute, territorial jurisdiction and global governance. Review of International Studies 20, 111–131 (2004)