Cloud Security and Privacy in the Light of the 2012 EU Data Protection Regulation

Andreas Kronabeter and Stefan Fenz

Vienna University of Technology,
Institute of Software Technology and Interactive Systems,
Favoritenstraße 9-11, 1040 Wien, Austria

Abstract. The essential characteristics of cloud computing such as elasticity or broad network access provide many economic benefits for their users, but with these benefits also many security and privacy risks come along. These risks can be generally classified into legal and technical risks. The upcoming general data protection regulation by the European Commission (COM (2012) 11) strengthens the consumer's rights with changes like a single set of European rules and more data protection obligations for organizations. Once the general data protection regulation becomes effective, organizations will have to fulfill more requirements to comply with the law, especially in situations of security breaches or issues about the life cycle and the processing of data. In this paper we describe a framework for the evaluation of cloud service providers in regard to the upcoming EU data protection regulation. The framework shall help service providers to comply with the new regulation, and shall enable consumers to evaluate the security and privacy competencies of cloud service providers.

Key words: cloud computing, European Union data protection regulation, security, data protection, privacy, evaluation framework

1 Introduction

Security and privacy issues which come along with cloud computing have grown in significance. The rapidly technological progress makes it difficult for legal regulations, laws and security provisions to be up to date. Virtualization, multitenancy, and outsourcing raise many questions according to how a provider runs his security policy and how he is handling security issues as well as the responsibilities of the user. Relevant work about cloud security risks and recommendations was published by Gartner [5], the National Institute of Technology (NIST) [6], the Cloud Security Alliance (CSA) [7] and the European Network and Information Security Agency (ENISA) [8]. According to Gartner the seven cloud computing security risks users have to face are: (i) privileged user access, (ii) regulatory compliance, (iii) data location, (iv) data segregation, (v) recovery, (vi) investigative support, and (vii) long-term viability. NIST defines trust, multi-tenancy, encryption and compliance as the key issues of cloud computing [9].

In this paper we present an evaluation framework which should help future as well as current users/providers of cloud computing services to comply with the upcoming EU data protection regulation (COM (2012) 11) [2]. In the following, we (i) introduce the upcoming European data protection regulation (COM (2012) 11) and the legal key changes for data protection in Europe (Section 2), and (ii) present the actual evaluation framework and describe how it supports user/providers at identifying/providing secure cloud services (Section 3).

2 EU Data Protection Regulation - COM (2012) 11

At the beginning of 2012 the European Commission presented their proposal for a comprehensive reform of the EU's 1995 data protection rules. The key changes of the *"Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)"* are [10]:

- Single set of rules applicable across the EU.
- "Right to be forgotten": If the user no longer wants his data to be processed and the provider has no legitimate reason to keep it, the data shall be deleted.
- "Right to data portability": The user can transfer, without any problems, personal data from one service provider to another one. This is important to avoid vendor and data lock-in.
- Easier access to personal data.
- Clear rules on when the EU law applies to data controllers outside the EU.
- European Data Protection Board as a new supervisory body.
- Obligatory notification of data breaches within 24 hours
- Increased responsibility and accountability for those processing personal data
- More transparency about data handling with a better information policy.
- The right for an individual to refer all cases to their home national data protection authority is claimed.
- The rules of the general data protection regulation will also apply to organizations not established in the EU, if their services are offered in the EU.

2.1 Definitions in the context of the EU Data Protection Regulation

"Controller" means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions and means of the processing of personal data; where the purposes, conditions and means of processing are determined by EU law or Member State law, the controller or the specific criteria for his nomination may be designated by European Union law or by Member State law.

"Representative" means any natural or legal person established in the European Union who, explicitly designated by the controller, acts and may be addressed by any supervisory authority and other bodies in the EU instead of the controller, with regard to the obligations of the controller under this regulation.

"Processor" means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

"Main establishment" means the controller's place of establishment in the European Union where the main decisions as to the purposes, conditions and means of the processing of personal data are taken; if no decisions as to the purposes, conditions and means of the processing of personal data are taken in the European Union, the main establishment is the place where the main processing activities in the context of the activities of an controller's establishment in the EU take place. The processor's 'main establishment' means the place of its central administration in the EU.

"Processing" means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction.

2.2 Territorial Scope

The EU regulation will apply on the processing of personal data in the context of activities of an establishment of a controller or a processor in the EU. It also applies on the processing of personal data of data subjects residing in the EU by controllers not established in the EU, where the processing activities are related to:

- The offering of goods or services to such data subjects in the EU, or
- the monitoring of their behavior.

3 Evaluation Framework

This section presents an evaluation framework for organizations which decide to outsource part of their IT to a cloud service provider. The framework should help to decide if a cloud provider can be assumed as reliable. The areas of relevance are based on the provided information from widely accepted institutions such as NIST or the Cloud Security Alliance. The concerns and risks of these areas are linked with the upcoming EU data protection regulation to understand what a company and provider has to mind and implement to comply with the proposed regulation. The framework highlights the responsibilities for both provider and user.

The different areas of relevance have been already analyzed in the literature. NIST summarized security and privacy issues and recommendations an organization should follow in their "Guidelines on Security and Privacy in Public Cloud Computing" [9]. The different areas are Governance, Compliance, Trust, Architecture, Identity and Management, Software Isolation, Data Protection, Availability, and Incident Response.

The Cloud Security Alliance published their security guidance for critical areas regarding cloud computing with the focus on governing and operating issues [3]. The governing part includes Governance and Enterprise Risk Management, Legal Issues, Compliance and Audit, Information Management and Data Security, Interoperability and Portability. The operating part includes Traditional Security, Business Continuity, Disaster Recovery, Data Center Operation, Incident Response, Application Security, Encryption and Key Management, Identity, Entitlement, Access Management, Virtualization, and Security as a Service.

The Australian Government provides with their Cloud Computing Security Considerations [11] a checklist of questions, according to security issues an organization has to deal with when using cloud computing.

The described approaches enumerate what an organization has to consider in regard to security and privacy. With our evaluation framework we combine these approaches and further consider the upcoming EU data protection regulation. We provide a checklist for general security and privacy considerations as well as for legal and organizational requirements according to the upcoming EU data protection regulation.

3.1 Legal and Organizational Requirements

Legal and organizational requirements cover governance, service level agreements, support and information, and compliance.

Governance includes the accountability, responsibility and transparency of an organization. To fulfill these requirements certifications and audits are used. Certifications and audits on which users can rely on are important since users are not able to get a complete insight of all security relevant issues. Hence, the provider should provide information about certification such as PCI DSS, ISO / IEC 27001, etc. and audit standards like SAS70 Type II. Third party audits should be a vital part of any assurance program.

Service Level Agreements are a contract between a provider and a user on the level of the provided service. SLAs and Terms of Service are essential to a reliable cloud provider. Service Level Agreements should contain:

- Adequate system availability (uptime, response time)
- Credits in case of outages
- Adequate compensation for a breach
- Notification in cases of failure or critical situations

Support and Information should be made available in a transparent and easily accessible way by the provider. The user should get as much information as possible. Therefore support and documentation by the provider is necessary. The following points should be made available:

- Frequently Ask Questions (FAQ)
- Help Lines and Wikis

– Reaction time on requests
– An extensive documentation about security
– Information about the billing system and the business continuity strategy

Compliance to laws and regulations is the base of every service provider to become reliable. It refers to the organization's responsibility to comply with regulations, laws and standards to assure secure services. With Audits it can be shown that a standard of security is reached but contractual obligations to protect personal information are essential for security and privacy issues. Laws and regulations can change depending on where the data is stored and processed. Legislative obligations (excerpt):

– Health Insurance Portability and Accountability Act (HIPPA)
– Gramm-Leach-Bliley Act (GLBA)
– Federal Information Security Management Act (FISMA)
– Sarbanes Oxley Act (SOX)
– Safe Harbor
– EU Data Protection Directive 95/46/EC

3.2 Legal and Organizational Requirements According to the Upcoming EU Data Protection Regulation

For a controller to comply with the EU data protection regulation in the matter of legal and organizational requirements it is important to consider the following points:

– The Controller needs to designate a representative, which can be any natural or legal person established in the EU. The representative can be addressed by a supervisory authority instead of the controller.
– Article 22 "Responsibility of the controller" contains the implementation of appropriate measures and strategies as well as the adoption of policies so that the processing of personal data is in compliance with this regulation. The measure shall include:
  – According to Article 28 "Documentation"; the controller and processor and, if any, the controller‘s representative, shall maintain documentation of all processing operations. The documentation should be available, on request, to the supervisory authority.
  – Implementation of data security requirements according to Article 30 (described in the data protection section).
  – According to Article 33 "Data protection impact assessment"; the controller or the processor acting on the controller's behalf has to perform an assessment of the impact of the envisaged processing operations, in case that the processing operations present specific risks.
  – According to Article 34 (1) and (2) "Prior authorization and prior consultation"; the controller or the processor has to obtain an authorization from the supervisory authority prior to the processing of personal data.

  - According to Article 35 (1); the controller and processor shall designate a data protection officer, if the processing is carried out by a public authority or the processing is carried out by an enterprise with 250 employees or more.

  To ensure the effectiveness of these measures the controller has to implement mechanism for the verification. The verification shall be carried out by independent internal or external auditors.
- According to Article 24 "Joint Controller"; if a controller decides to determine the purpose, conditions and means of processing personal data jointly with others, the joint controllers have to determine the respective responsibilities to comply with the regulation.
- According to Article 26 "Processor"; a controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organizational measures as well as procedures in such a way that the processing will comply with the regulation. The processing shall be governed by a contract for binding the processor to the controller, in particular the processor shall:
  - act only on instructions from the controller;
  - employ only reliable staff;
  - implement all required measures according to security of processing;
  - support the controller in complying to the data security obligations of the regulation;
  - hand over all results after the end of the processing;
  - make available all information necessary to control compliance.

The controller and the processor have to document the controllers instructions and the processor's obligations listed above. Important to mention is that if a processor processes the data different than instructed by the controller, the processor will be considered as controller according to that processing and has to be applied to Article 24 "Joint Controllers". Moreover, the controller and the processor and, if any, the representative of the controller, shall co-operate, on request, with the supervisory authority in the performance of its duties.

3.3 Data Protection

The protection of data is a vital issue to make a cloud environment secure. A service provider should possess the following points to fulfill data and information protection requirements:

Data Center: A high standard of protection requires the access to information about data centers and the mechanism that are used to secure a data center. The following points about data centers should be considered:

- Quantity. Organizations should provide information about how many data centers are used to store and process data.
- Physical Security. Information about the physical provisions to secure the data centers should exist.

- Data Backup and Data Redundancy. It should be possible to backup and store data in several locations. The user should get information regarding backup procedures.
- Information about the location of the data centers should be provided. In the best case the user can choose where the data will be stored and processed.
- Data loss. The case of data loss should be stated in a contract, SLA or terms of service.
- Data isolation. Due to multi-tenancy and his complexity it is important how data will be isolated.

Data Security:

- Data sanitization techniques should be implemented.
- Auditing and Certifications should be verifiable.
- Data Encryption, Key Management. Techniques like PKI, PKCS, KEYPROV (CT-KIP, DSKPP) or EKMI should be implemented.
- Data/Vendor Lock-in. Exit strategies and other options should be stated in a contract.
- Data ownership. It should be clear who possesses the data and who is responsible for it.
- Identity and Key Management. Evidence for the access and authentication is necessary.
- Implementation of incident response strategies.
- Monitoring of data security.
- Implementation of network security strategies.

3.4 Data Protection According to the Upcoming EU Data Protection Regulation

Important to mention for the security of data is again Article 26 which states that a controller has to choose a processor providing sufficient guarantees about the implementation of all technical measures so that the processing will comply with the EU data protection regulation. The processing shall be governed by a contract. In other words the controller has to protect himself legally with a contract otherwise he may be responsible for data breaches.

Data Loss / Data Breach: According to Article 30 "Security of processing"; controller and processor have to ensure with appropriate technical measures an adequate level of security. Both shall take these measures to protect personal data against unlawful or accidental destruction or accidental loss and have to prevent unlawful forms of processing. In particular any unauthorized disclosure, dissemination, access or alteration of personal data.

- Incident Response / Notification: According to Article 31 "Notification of a personal data breach to the supervisory authority"; the controller has to notify the personal data breach to the supervisory authority without undue delay and where feasible within 24 hours after getting aware of it. The processor has

to alert and inform the controller immediately after the establishment of a personal data breach. According to Article 32 "Communication of a personal data breach to the data subject"; the controller has to notify the data subjects after informing the supervisory authority without undue delay.
- Sanctions: A breach could result in a fine up to 1.000.000 EUR or in case of an enterprise up to 2% of its annual worldwide turnover. The fines will be imposed by the supervisory authority.

Data / Vendor-Lock in: According to Article 18 "Right to data portability"; a data subject has the right to obtain from the controller a copy of data that is undergoing processing in an electronic and structured format which is commonly used. That means if a controller is choosing a provider the controller is responsible for the provision of those data, this should be stated within a contract.

Data Lifecycle: According to Article 17 "Right to be forgotten and to erasure"; a data subject has the right to obtain from the controller the erasure of personal data relating to them. Further the controller has to implement mechanisms to ensure that the time limits established for the erasure of personal data or for a periodic review of the need for the storage of the data are observed.

Data Location / International Transfer: The transfer of personal data to third countries or international organization is stated within chapter five of the EU data protection regulation. A controller has to consider the following points:

- According to Article 40 "General principle for transfers"; any processing of personal data to a third country or to an international organization is just permitted if the controller and the processor comply with the conditions of the proposed regulation.
- According to Article 41 "Transfers with an adequacy decision"; if the commission states that the third country, territory or the international organization has an adequate level of protection the transfer may take place. Therefore, the commission publishes in the "Official Journal of the European Union" a list of those countries, territories and international organizations with an adequate level of security and a list of those which don't have an adequate level of security.
- Article 42 "Transfer by way of appropriate safeguards"; discusses the scenario if the commission has taken no decision. In that case the controller or processor has to adduce appropriate safeguards in a legally binding instrument. These safeguards can be provided by
  - binding corporate rules which shall specify according to Article 43 "Transfer by way of binding corporate rules"; their legally binding nature; the structure and contact details of the group of undertakings; the data transfer and the type of processing as well as purpose; the general data protection principles; the acceptance by the controller or processor established on the territory; the mechanisms for verification of compliance with the rules; or
  - standard data protection clauses adopted by the commission and by a supervisory authority; or

– contractual clauses between the controller or processor and the recipient of the data.

Some exceptions for the transfer of personal data, if the above described points do not exist are stated in Article 44 "Derogations".

Figure 1 summarizes the described evaluation framework. Providers/consumers can use it to review if the legal and technical requirements are given and fulfilled by the provider and consumer. The framework is applicable on all service models and all deployment models of cloud computing. It shall be used by screening the provider and the contractual relationship according to the listed points, and further to check if the own organizational provisions comply with the upcoming EU data protection regulation.

<table>
<tr><th colspan="2">Legal and Organizational Requirements</th><th>Data Protection</th></tr>
<tr><td>Governance:
- Certifications
- Audits</td><td>Service Level Agreements:
- Adequate system availability (uptime, response time)
- Credits in case of outages
- Adequate compensation for a breach
- Notification in cases of failure or critical situations</td><td>Data Center:
- Number of data centers - Data location
- Physical security - Data isolation
- Data backup</td></tr>
<tr><td>Support and Information:
- Frequently Ask Questions (FAQ)
- Help Lines and Wikis
- Reaction time on requests
- Documentation about security
- Billing system
- Business continuity</td><td>Compliance (excerpt):
- Health Insurance Portability and Accountability Act (HIPPA)
- Gramm-Leach-Bliley Act (GLBA)
- Federal Information Security Management Act (FISMA)
- Sarbanes Oxley Act (SOX)
- Safe Harbor
- EU Data Protection Directive 95/46/EC</td><td>Data Security and Privacy:
- Data sanitization - Data ownership
- Audits and certifications - Identity and key management
- Data encryption - E-discovery
- Data/vendor lock-in - Incident response strategies
- Monitoring mechanisms - Network security strategies</td></tr>
<tr><td colspan="3">EU Data Protection Regulation Requirements</td></tr>
<tr><td colspan="2" rowspan="2">Responsibilities (Article 22):
- Implementation of Appropriate Measures:
- Documentation (Article 28)
- Data security (Article 33)
- Data protection impact assessment (Article 33)
- Prior authorization (Article 34)
- Data protection officer (Article 35)
- Documentation (Article 28)
- Mechanisms for verification</td><td>Vendor-Lock in:
- Right to data portability (Article 18)</td></tr>
<tr><td>Data Lifecycle:
- Right to be forgotten and to erasure (Article 17)
Data Location / International Transfer:
- General principle for transfers (Article 40)
- Transfers with an adequacy decision (Article 41)
- Transfer by the way of appropriate safeguards (Article 42)</td></tr>
<tr><td>Representative:
- Designation of a representative in the EU</td><td rowspan="2">Processor (Article 26):
- Chosen processor by controller shall:
- act only on instructions
- employ reliable staff
- implement required measures
- support controller in complying
- hand over all results after processing
- make available all information for compliance</td><td rowspan="2">Data Loss / Data Breach:
- Security of processing (Article 30)
- Notification to the supervisory authority (Article 31)
- Notification to the data subject (Article 32)</td></tr>
<tr><td>Joint controller (Article 24)</td></tr>
</table>

Fig. 1. Cloud Security and Privacy Evaluation Framework

4 Conclusion

In this paper we analyzed the existing work and conditions for an evaluation framework to secure cloud computing in accordance to the upcoming data protection regulation by the European Commission. It is concluded that security and privacy are the major challenge customers and providers have to deal with when

using and offering cloud computing services. Due to the proposed data protection regulation an organization deciding to use cloud computing will have to deal with new significant and onerous obligations. Further, also the providers have to upgrade their policies and security implementations. The described framework will help organization as well as providers to comply with the obligations of the upcoming EU data protection regulation. As cloud computing will win on importance in the future, the proposal for a major reform of the European Union legal framework on the protection of personal data is an important step towards securing sensitive data in the cloud.

References

1. The NIST Definition of Cloud Computing - SP 800-145, National Institute of Standards and Technology (2011), http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
2. Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), European Commission, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
3. Security Guidance for Critical Areas of Focus in Cloud Computing V3.0, Cloud Security Alliance (2011), https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf
4. Nimis, J., Tai, S., Baun, C., Kunzem M.: Cloud Computing: Web-basierte dynamische ITServices. Springer-Verlag Berlin Heidelberg (2011)
5. Technology Research, Gartner Inc., http://www.gartner.com/technology/home.jsp
6. National Institute of Standards and Technology (NIST), http://www.nist.gov/index.html
7. Cloud Security Alliance (CSA), https://cloudsecurityalliance.org/
8. Securing Europe‘s Information Society (ENISA), http://www.enisa.europa.eu/
9. Guidelines on Security and Privacy in Public Cloud Computing - SP 800-144, National Institute of Standards and Technology (2011), http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf
10. Commission proposes a comprehensive reform of the data protection rules, European Commission, http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm
11. Australian Government (Department of Defense), Cloud Computing Security Considerations, http://www.dsd.gov.au/infosec/cloudsecurity.htm