Vol. IV, Issue 3
June 2014

Cloud Computing - Compliance with Regulatory Prescribed Data Protection Measures in Bosnia and Herzegovina

Author: **Hamidović Haris**, Mcf Eki Sarajevo, University Džemal Bijedić of Mostar, Sarajevo, Bosnia And Herzegovina, haris.hamidovic@eki.ba

The rapid emergence of cloud computing has raised concerns about its legal and regulatory implications. Issues of data protection and security are among the concerns most frequently mentioned by potential cloud customers. If sensitive company data are stored, processed or transmitted in a cloud environment, data protection and other laws will apply to that environment too. The allocation of responsibility between client and provider for managing security controls does not exempt a client from the responsibly of ensuring that their sensitive data is properly secured according to applicable law requirements. In this regard, it is necessary to get appropriate assurance that cloud service provider information security management system covers the security of the computers and computing environment that it uses in processing sensitive company data. This paper addresses the issues of compliance with regulatory prescribed data protection measures in Bosnia and Herzegovina in cloud environment.

Keywords: *Cloud Computing, Data Protection, Information Security, Compliance, Bosnia and Herzegovina.*

Introduction

In its simplest sense, e-business is the use of Internet technologies to improve and transform key business processes. Most companies understand this and have begun the evolution from traditional business practices to e-business. [1]

Recognizing that:

- only information societies, where know-how and timely, encompassing and correct information happened to be basic governing resources can ensure a progress and future for all the citizens,
- a divide between a level of development between societies, social groups and individuals is in a direct proportion with the divide about the level of application of information and communications technologies (digital divide),
- Bosnia and Herzegovina must act proactively and quickly towards a decrease of technological and development discrepancy, because the process of transition from industrial into information societies in the developed countries has already gained impetus and is in at an advance stage.

The Council of Ministers of Bosnia and Herzegovina passed in 2004. the document *Policy for Development of the Information Society of Bosnia and Herzegovina* as the framework and basis document, in accordance with which the future legislation, acts and other regulation will be passed in the process of building and development of information society, and also upon which the future decision will be taken on the development directions, action plans and priorities at the level of Bosnia and Herzegovina ant its entities.

Policy for Development of the Information Society of Bosnia and Herzegovina states that network and information security is important and indispensable for functioning of information society, and particularly in the e-business segment. [2]

Adoption of the Law on electronic document in the Federation of Bosnia and Herzegovina in July 2013 established a legal basis for administrative bodies, local authorities, business enterprises, institutions and other legal entities and individuals to accept and use electronic documents for their needs, as well as for business relationships and other interactions with other entities. [3]

The Law is fully harmonized with the EU legislation, as well as the current best practice in the world, and its adoption is in line with the directives of the European Union, according to which Bosnia and

Herzegovina has to create all preconditions for electronic access to information and e-commerce. [4]

Law prescribes the penal provisions and fines for legal entities and natural persons for conduct contrary to the provisions of this law, such as:

- Prevention verification of authenticity and integrity of electronic documents;
- Archiving of electronic documents in such form and with such technologies and procedures that do not provide a reasonable guarantee of their authenticity and integrity for the entire storage time;
- Application of information systems with inadequate protection of personal data in accordance with the provisions of the law governing the protection of personal data, etc.

According to the Law, any available and usable information-communication technology can be used.

Innovation in the realm of information technology continues its rapid pace, with cloud computing representing one of the latest advances. Significant improvements in the capacity to process transmit and store data are making cloud computing increasingly important in the delivery of public and private services. As Governments, enterprises and other organizations in the developing world consider whether to migrate some or all of their data and activities to the cloud, they need to assess the potential advantages and risks of such a move. The rapid emergence of cloud computing has raised concerns about its legal and regulatory implications. Issues of data protection and security are among the concerns most frequently mentioned by potential cloud customers in both developed and developing countries. [5] This paper addresses the issues of compliance with regulatory prescribed data protection measures in Bosnia and Herzegovina in cloud environment.

Cloud computing definition

As with any new technology, the definition of cloud computing is still evolving and may mean different things to different people.

According to definitions proposed in April 2013 by the International Telecommunication Union (ITU) and the International Organization for Standardization (ISO), cloud computing is a paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with on-demand selfservice provisioning and administration. Cloud services are defined as services that are provided and used by clients on demand at any time, through any access network, using any connected devices that use cloud computing technologies. [5]

Three categories of cloud services commonly used to encompass the whole range of cloud service categories that are currently available are [5]:

- infrastructure as a service (IaaS),
- platform as a service (PaaS), and
- software as a service (SaaS)

The defining characteristic of each of these variations of the cloud is the type of computing or information technology (IT) facilities that is made available remotely to a cloud service customer, on a rental or subscription basis, by a cloud service provider.

In the case of IaaS, the cloud provider's processing, storage, networks and other fundamental computing resources allow the cloud customer to deploy and run or enterprise to access computing infrastructure in a flexible and timely manner.

In the case of PaaS, the cloud customer deploys its own applications and data on platform tools, including programming tools, belonging to and managed by the cloud provider.

With SaaS, the cloud customer takes advantage of software running on the cloud-provider's infrastructure rather than on the customer's own hardware. The applications required are accessible from various client devices through either a thin client interface, such as a web browser (for example, web-based email), or a program interface. [5]

Cloud services can also be deployed to users in a variety of ways, the most significant of which are summarized below [5]:

- Public clouds: open resources that offer services over a network that is open for public use. Many mass market services widely used by individuals, such as webmail, online storage and social media are public cloud services.
- Private clouds: proprietary resources provided for a single organization (for example, a Government or large enterprise), managed and hosted internally or by a third-party.
- Community clouds: resources/services provided for and shared between a limited range of clients/ users, managed and hosted internally or by a third-party.

- Hybrid clouds: a mix of the deployment models described above, for example, public and private cloud provision.

Some authors also state that the cloud computing is a new way of delivering computing resources, not a new technology. [6]

The National Institute of Standards and Technology (NIST) defines cloud computing as „*a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.*“ [7]

Information security legal requirements

„*There are a number of factors to be considered when migrating to cloud services, and organizations need to clearly understand their needs before they can determine if and how they will be met by a particular solution or provider. As cloud computing is still an evolving technology, evaluations of risks and benefits may change as the technology becomes more established and its implications become better understood.* “[8] As already previously stated, issues of data protection and security are among the concerns most frequently mentioned by potential cloud customer.

European Network and Information Security Agency – ENISA states that cloud computing poses several data protection risks for cloud customers and providers. For example, „*it can be difficult for the cloud customer (in its role of data controller) to effectively check the data processing that the cloud provider carries out, and thus be sure that the data is handled in a lawful way. It has to be clear that the cloud customer will be the main person responsible for the processing of personal data, even when such processing is carried out by the cloud provider in its role of external processor. Failure to comply with data protection law may lead to administrative, civil and also criminal sanctions, which vary from country to country, for the data controller.*“ [6]

Bosnia and Herzegovina's data protection law is based on the EU Data Protection Directive. [9] Data protection legislation in Bosnia and Herzegovina, as well as in many other countries, require that the data controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Such measures need to ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected. [10]

Cloud service providers may be new, but data protection legislation in Bosnia and Herzegovina, as is other countries, hold the user of the service ultimately responsible for the security and integrity of their corporate and customer data, even when it is held by the service provider.

Traditional service providers submit to external audits and security certifications, providing their customers with information on the specific controls that were evaluated. But, whether the certification according to ISO/IEC 27001 international standard is sufficient to meet the legal obligations in this regard? As a general rule applies *that „compliance with an international standard does not in itself confer immunity from legal obligations.“* [11] As regards Bosnia and Herzegovina it is necessary to take into account that Council of Ministers of Bosnia and Herzegovina adopted in 2009 Regulation on storage and specific technical measures of personal data protection. This regulation prescribes specific technical and organizational measures for protection of personal data in Bosnia and Herzegovina. [12]

Comparative analyses of 133 information security controls from Annex A of the International Standard ISO/IEC 27001 and the measures prescribed by regulation of the Council of Ministers of Bosnia and Herzegovina shows that, ISO/IEC 27001 standard meet minimum security measures mandated by the Bosnia and Herzegovina data protection law. But, ISO/IEC 27001 also states that any scope of information security management system implementation may cover all or part of an organization. *„It is possible to define the entire enterprise as a scope of the ISMS, or a part of organization division as a scope of the ISMS.“* [13] In this regard, it is necessary to get appropriate assurance that the cloud service provider (CSP) information security management system (ISMS) covers the security of the computers and computing environment that it uses in processing personal and other sensitive company data.

In addition, it should bear in mind guidelines of ARMA International, professional association and the authority on managing records and information, specifying that public cloud may not be appropriate when information is covered under specific regulatory requirements or when an internal risk analysis determines that the information's exposure would jeopardize the company. Information of this nature may be better managed in a private environment where the risk of access can be reduced or mitigated. [14]

Organizations must understand and address regulatory requirements regarding information security. Regulatory compliance regarding information security is a complex task. [15] Numerous authors [16] [17], as well as the international framework of good practice for information security [18] suggest the need for a formalized approach to address this issue.

Conclusions

Cloud computing is seen by many as the next wave of information technology for individuals, companies and governments. Like any new technology advancement, cloud computing also creates disruptive possibilities and potential risks. Issues of data protection and security are among the concerns most frequently mentioned by potential cloud customers in both developed and developing countries.

Cloud customers need assurance that providers are following sound security practices in mitigating the risks facing both the customer and the provider. They need this in order to make sound business decisions.

Some cloud providers do provide information on the data processing that they carry out. Some also offer certification summaries of their data processing and data security activities and the data controls they have in place, such as ISO/IEC 27001 certified providers.

The adoption of an externally validated, best-practice approach to information security might enable compliance with regulatory requirements focused on the confidentiality, integrity and availability of electronically-held information. ISO/IEC 27001 can provide just such a solution. It focuses on the confidentiality, availability and integrity of data and its key precepts and requirements all occur in the regulatory requirements.

ISO/IEC 27001 certification is no by itself guarantee of compliance with legal obligations in regards to information security measures, but it might be good starting point if ISMS is implemented taking into account all applicable legal or regulatory requirements in this regard.

References

[1]. Smith Brian R., Chatfield Veronica, Uemura hki, IBM @server iSeries e-business Handbook: A V5R1 Technology and Product Reference, International Business Machines Corporation, 2001

[2]. The Council of Ministers of BIH, Policy of Information Society in Bosnia and Herzegovina, 2004

[3]. *Law on Electronic Document*, Official Gazette of the Federation of Bosnia and Herzegovina, Year XX, No. 55, 17/07/2013, 2013

[4]. USAID/Sida Governance and Accountability Project, *Comments on Law on Electronic Document*, 2012

[5]. The United Nations Conference on Trade and Development (UNCTAD), *Information Economy Report 2013 - The Cloud Economy and Developing Countries (UNCTAD/IER/2013)*, 2013

[6]. European Network and Information Security Agency (ENISA), *Cloud Computing Security Risk Assessment*, 2009

[7]. NIST, Special Publication 800-145, *The NIST Definition of Cloud Computing*, 2011

[8]. Cloud Special Interest Group PCI Security Standards Council, *PCI Data Security Standard (PCI DSS) Version: 2.0*, 2013

[9]. European Union, *The Data Protection Directive, Directive 95/46/EC*

[10].The Parliamentary Assembly of Bosnia and Herzegovina, *The Law on Personal Data Protection*, Official Gazette of Bosnia and Herzegovina, no. 49/06, 2006

[11]. ISO/IEC 27001:2005, *Information technology—Security techniques—Information security management systems—Requirements*, Switzerland, 2005

[12].The Council of Ministers of Bosnia and Herzegovina, *Regulation on storage and specific technical measures of personal data protection*, 2009

[13].ISO/IEC 27003:2010, *Information technology -- Security techniques -- Information security management system implementation guidance*, Switzerland, 2010

[14].ARMA International, *Guideline for Outsourcing Records Storage to the Cloud*, 2010

[15].Hamidović Haris, *General model for information security legal compliance*, In proceeding of Third International Scientific

Conference Economics of Integration, on the theme: Using knowledge to move from recession to prosperity, At Faculty of Economics, University of Tuzla, Bosnia and Herzegovina, 6.-7.12.2013., 2013

[16]. Tashi Igli, *Regulatory Compliance and Information Security Assurance*., in 'ARES', IEEE Computer Society, pp. 670-674, 2009

[17]. Adler M. Peter, *A Unified Approach to Information Security Compliance*. EDUCAUSE Review, 41(5):46–48, 50, 52, 54, 56, 58, 60, september 2006., 2006

[18]. ISO/IEC 27002:2013, *Information technology -- Security techniques -- Code of practice for information security controls*, Switzerland, 2013