EMCSR | 2014
Book of Abstracts | 596-600

ISSN 2227-7803
BCSSS

Evaluation criteria for cloud computing based on the upcoming European data protection regulation

Manfred Halper
Vienna University of Technology, Vienna, e0007821@student.tuwien.ac.at

Stefan Fenz
Vienna University of Technology, Vienna, stefan.fenz@tuwien.ac.at

Johannes Göllner
National Defence Academy of the Austrian Federal Ministry of Defence and Sport, Vienna, johannes.goellner@bmlvs.gv.at

Gerald Quirchmayr
University of Vienna, Vienna, gerald.quirchmayr@univie.ac.at

Abstract: The European Union released a proposal on the protection on individuals with regard to the processing of personal data and the free movement of such data. One goal of the Data protection Regulation is to form the statutory framework to facilitate the adoption of cloud technology by Small and Medium Enterprises and mitigate the risks stemming from introducing Cloud Computing Service Providers (CCSP) into their supply chain networks. The developed evaluation criteria stemming from the Regulation should help SMEs to assess CCSPs for compliance and their capability of handling modern security and privacy objectives.

Keywords: General Data Protection Regulation; Small and Medium Enterprises; Cloud, Security

1 Introduction

Today cloud computing technology and its various fields of application have reached a momentum and like every other, rather young technology service, the adoption and integration of cloud computing in the existing supply chains faces different problems and risks for small and medium-sized businesses. The European Union has identified cloud computing as a major future technology in the Information- and Communications Technology (ICT) sector and aims at enabling the economy to faster adopt and facilitate cloud computing through all sectors. The utmost important regulation for this cause is the upcoming European Data protection Regulation, as for the moment only available as an evolved proposal.

Information has become one of our utmost important resources in most industry branches, data has become a very liquid good that can easily be transported across sites, cities and borders and this generates a complete new challenge for SME's using or providing cloud computing services. The motivation is to distil evaluation criteria out of the regulation and security guidelines from the European Union to create a framework for SMEs that help them adopting cloud computing in their IT assets in a secure way.

2 Results

The first step in the assessment of a CCSP is to identify who holds which role. Regarding the Regulation there are the roles of controller, processor and the joint controller. Each role has its own set of rights and duties therefore the SME has to identify the role of every partner in the supply chain and evaluate their level of compliance in accordance to their role.

The key component of any cloud service nearly always revolves around data. The Regulation gives insight on the different classes of data and how to evaluate the CCSP regarding his implementation of security and organizational measures to protect this data. Especially personal data – any information relating to the data subject – and sensitive data have to be protected to prevent unlawful use.

Another criterion is given by the need of documentation due to the heavy impact on security. Documentation is important to demonstrate results that originate from selected security measures or controls and makes decisions traceable. In combination with the necessary authorization from the supervisory authority prior to the use of personal data and a detailed data impact assessment the Regulation establishes traceability in the relationship between SME and CCSP.

Every venture working with the personal data of data subjects (an identified natural person or a natural person who can be identified) has to establish procedures that enable the data subject to exercise his/her rights. Due to the new data centric business models the Regulation identifies the collection of personal data as a field that is in need of adjustment and therefore demands the provision of possibilities of rectification, erasure, access and objection for the data subject.

The Regulation also introduces the data protection officer that has to be established by every corporation that employs 250 people or more, that is a public authority or body, or if his core activity requires regular and systematic monitoring of data subjects. The data inspection officer has to be involved in all issues related to the protection of personal data and is responsible to keep the SME informed regarding his obligations to the regulation.

The regulation describes very precisely the circumstances under which data can be lawfully transferred to a third country or an international organization for further processing purposes and thereby reacts to the current uncontrolled cross border flow of data. It states four core scenarios that help to evaluate if a data transfer anywhere in the supply chain is legally.
Another criterion is the encouragement of codes of conduct that include commitments to fair and transparent data processing and to the lawful collection of data and a certification scheme that proves the proper application of the Regulation by the SME or CCSP. The development of certificates, certification mechanism, data protection seals and marks will help elevating the possibilities of the SME, to assess the level of data protection and compliance provided by the CCSP.
The European Union is well aware that especially the adoption of cloud technology by SMEs is a critical success factor to enable the cloud to reach its full potential and therefore has identified cloud-specific Key Actions in the Europe 2020 plan. One action is to cut through the jungle of standards by identifying and counteracting typical risks and challenges like the Availability of services and data, the current lack of data classification mechanism, integrity issues, confidentiality concerns, regulatory compliance, reputability, lack of forensic readiness, loss of control, responsibility ambiguity, lack of liability, migration problems and lock-in.
Since cloud services have special requirements regarding security and privacy objectives the European Union Agency for Network and Information Security developed a guideline that aims beyond the traditional IT infrastructure and security requirements and developed standards that elevate security and privacy objectives that are regarded major in the field of cloud computing, this includes protection of data from unauthorized access, disclosure and modification, the insurance of isolation, service availability, appropriate security provisions for cloud applications, security of connections and networks, enforcement of privacy policies and incident prevention, detection and response.
Every listed criterion can be used by the SME to assess current or future cloud service providers in his supply chain. The criteria focus on the view of the European Union well aware that there are several nongovernmental guidelines in the field of secure cloud computing.

3 Conclusion

There is a major need of regulation in the information market and SMEs are waiting for the upcoming Regulation to align their business strategy appropriately. Nonetheless a firm and solid security strategy pose as a competitive advantage in the fast developing cloud service market. It is beyond all questions that a SME sooner or later has to add cloud services to its infrastructure to stay competitive but the SME can choose how he integrates this technology in his business model and thereby influences if it will be successful or end in disaster. Not every criterion applies to any scenario; the SME has to verify where the criterions are applicable and if they are enforce them. The aggregation of evaluation criteria stemming from the Regulation also helps cloud service providers by identifying criteria that are applicable to their business model and giving them a competitive edge by implementing the regulatory criterions and thereby facilitating compliance, strengthen security and boosting customer confidence. Since the Regulation is still in progress the final version may change some details of the here presented criteria.

References

E. Union, “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),” 01 2012

ENISA, “Cloud computing. benefits, risks and recommendations for information security,” 11 2009.

N. I. of Standards and Technology, “The NIST definition of cloud computing,” 01 2011.

E. Commission, “Unleashing the potential of cloud computing in Europe,” 09 2012.

E. T. S. Institute, “Cloud standards coordination,” 11 2013.

E. T. S. Institute, “Cloud cloud private-sector user recommendations,” 11 2012.

About the Author

Manfred Halper: 2008 Bachelor degree in business informatics. Since 2007 working in administration/security of a service provider in the banking, big corporate sector.

Dr. Stefan Fenz (CISSP) is a researcher at Vienna University of Technology and SBA Research and founder of Xylem Technologies GmbH. From 2012 to 2015, Stefan is an appointed member of the European Network and Information Security Agency’s (ENISA) Permanent Stakeholder Group. In 2010, Stefan worked as a visiting scholar at Stanford Center for Biomedical Informatics Research at Stanford University (USA). From 2008 to 2012, Stefan lectured on information security at Peking University (Beijing, China), Beijing Jiaotong University (Beijing, China), Konkuk University (Seoul, Korea) and University of Applied Sciences Technikum Wien (Vienna, Austria). His primary research is on information security, with a secondary interest in semantic technologies and energy efficiency. Stefan received an MSc in software engineering & internet computing from Vienna University of Technology, an MSc in political science from University of Vienna, an MSc in business informatics from Vienna University of Technology, and a PhD in computer science from Vienna University of Technology. He is a member of the IFIP WG 11.1 – Information Security Management, the IEEE Systems, Man, and Cybernetics Society and ISC².

Johannes Göllner, MSc MSc Is Head of the Section Knowledge Management of the Department of Central Documentation and Information Service at the National Defence Academy of the Austrian Federal Ministry of Defence and Sport, Vienna, since 2011; his research areas and consulting foci include Knowledge Management & -Development, Trend- & Risk Analysis and Scenario Planning & Development, since 2009; former positions include Chairmanship of the Steering Committee of ON Committee 246 “Risk-, Security & Crisis Management” at the Austrian Standards Institute (2003-2008) and national delegate at ISO and CEN, Researcher and Lecturer assignments Risk-, Crisis-, Security Management, Critical Infrastructure and Head of the Section Risk Management and Course Director of the Master of Business Administration (MBA)-Programm “Environmental Threats and Disaster Management” and staff officer at the NBC-Defence School of the AAF and Lecturer assignments at the University of Natural Resources and Life Sciences Vienna and University of Vienna, since 1999; has been further Senior Researcher & Deputy Leader-experience in kind of Inhouse Consultant of the EU-Research-Project “FOCUS-Foresight Security Scenarios: Mapping Research to a Comprehensive Approach to Exogenuos EU Roles”, 2009-2012.

Univ. Prof. DDr. Gerald Quirchmayr holds doctors degrees in computer science and law from Johannes Kepler University in Linz (Austria) and currently is Professor at the Department of Distributed and Multimedia Systems at the University of Vienna. In 2001/2002 he held a Chair in Computer and Information Systems at the University of South Australia. He first joined the University of Vienna in 1993 from the Institute of Computer Science at Johannes Kepler University in Linz (Austria) where he had previously been teaching. In 1989/1990 he taught at the University of Hamburg (Germany). His wide international experience ranges from the participation in international teaching and research projects, very often UN- and EU-based, several research stays at universities and research centres in the US, Asia and EU Member States to extensive teaching in EU staff exchange programs in the United Kingdom, Sweden, Finland, Germany, Spain, and Greece, as well as teaching stays in the Czech Republic and Poland. International teaching and specialist missions include UN-coordinated activities in Egypt, Russia and the Republic of Korea. He has served as a member of program committees of many international conferences, chaired several of them, has contributed as reviewer to scientific journals and

has also served on editorial boards. He is a member of the Austrian and German computer societies and a member of IFIP working groups. For his contributions to the international IT community he was received the IFIP Silver Core Award in 1995. His major research focus is on information systems in business and government with a special interest in security, applications, formal representations of decision making and legal issues. His publication record comprises approximately 150 peer reviewed papers plus several edited books and conference proceedings as well as nationally and internationally published project reports. In July 2002 he was appointed as Adjunct Professor at the School of Computer and Information Science of the University of South Australia. From January 2005 until January December 2010 he headed the Department of Distributed and Multimedia Systems, Faculty of Computer Science, at the University of Vienna and served as Vice Dean of the Faculty of Computer Science from October 2008 until October 2010. Since January 2011 he serves as deputy head of the MIS group.