International Journal of IT/Business Alignment and Governance
Volume 10 • Issue 1 • January-June 2019

A Data Privacy Governance Model

The Integration of the General Data Protection Regulation Into Standard Based Management Systems

Margareth Stoll, Independent Researcher, Italy

ABSTRACT

The importance of data privacy, information availability and integrity are increasingly recognized. The new EU general data protection regulation 679/2016 obligates stringent legal requirements with high sanctions for noncompliance. Most organizations worldwide are affected directly or indirectly. It requires overall a risk and evidence-based data privacy management as part of corporate governance. More than 1.6 million organizations worldwide are implementing a standard-based management system, such as ISO 9001 or others. To implement the new data protection regulation in an effective, efficient and sustainable way, the author provides design-oriented guidelines on how to integrate the legal requirements into standard based management systems. The holistic data privacy governance model integrates different information security governance frameworks with standard based management systems in order to comply the regulation. In that way data privacy is part of all strategic, tactical and operational business processes, promotes corporate governance, legal compliance and living data protection.

KEYWORDS

Business Process, General Data Protection Regulation, Information Security, Information Security Governance, Management System, Policy, Privacy, Privacy Impact Assessment, Quality Management System, Risk Assessment

INTRODUCTION

Data privacy is a principal statutory right of the European Union and most countries all over the world. Due to increasing digitalization, interconnected, mobile and virtualized business, artificial intelligence, big data and customer tracking larger volumes of data are produced, analyzed and exposed to threats and misuse. Data and information systems are faced with increasing privacy threats from a wide range of sources, such as human curiosity, employees' actions, computer-assisted fraud, cyberattacks, phishing, sabotage, theft, fire or infrastructure incidents. Ponemon surveyed an increasing likelihood of data breaches and estimates that an organization will have with 27.7% probability a data breach in the

DOI: 10.4018/IJITBAG.2019010105

Copyright © 2019, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

next two years (Ponemon, 2017). A data breach may result in physical, material and/or non-material damage, such as damage to reputation, loss of customer (Martin, Borah & Palmatier, 2017), cost of mitigating and recovery, reduction of share price, discrimination for the person concerned and other significant economic or social disadvantages. Thus investors, boards and customers, as well as laws and authorities demand ongoing a higher level of data privacy. The clients of 90% of participants in a worldwide survey are concerned about the privacy of their data (Harvard Business Review Analytic Services, 2017). Most modern corporate governance guidelines make the board and specifically the CEO responsible for the well-being of the organization.

The new EU General Data Protection Regulation (GDPR) 679/216, (EU, 2016) obligates stringent legal requirements with administrative sanctions for noncompliance up to the greater of 4% of the total worldwide annual turnover or €20 million. It offers also great opportunities for enterprises by harmonizing a major part of the data privacy laws in the different EU countries, by driving new needs for services, IT systems and digitized products in order to fulfill the enhanced data privacy requirement, and others. The EU estimates €2.3 billion economic benefits of having one harmonized law (http://ec.europa.eu/justice/smedataprotect/index_en.htm). It affects after May 25, 2018 any enterprise doing business in Europe with their suppliers over all levels and all organizations worldwide which process data that can be used to identify directly or indirectly natural persons in Europe. 85% of responding organizations in a worldwide survey expect to be affected and 42% expect significant impacts (Harvard Business Review Analytic Services, 2017). Thus, data privacy and security for 81% of surveyed organizations has become a high priority (Harvard Business Review Analytic Services, 2017). Data privacy, the availability of all essential assets, confidentiality, data integrity and legal and regulatory compliance are central for organizations' success (Bélanger & Crossler, 2011; Da Veiga & Eloff, 2007; Sowa, Tsinas & Gabriel, 2009; von Solms & Solms, 2009;). This poses great challenges for small and medium sized organizations. They need a very efficient and functional approach, which can be smoothly integrated in their daily business.

More than 1.6 million organizations worldwide are implementing a standard based management system based on international standards (e.g. quality ISO 9001, or environment ISO 14001, information security ISO 27001, IT service management ISO 22000 and others) (ISO, 2017a). In order to promote an efficient integration of different standards, the International Standard Organization [ISO] released a common structure for all management systems' standards, the Annex SL of the ISO/IEC Directives (ISO, 2013c).

Several international best practices for information security management have been developed to provide guidance and ensure comprehensiveness. Some of the most commonly used include Control Objectives for Information and related Technology (COBIT), Information Technology Infrastructure Library (ITIL) and national guidelines, such as NIST SP 800 series in the US or IT Security Guidelines from the Federal Office for Information Security in Germany.

Despite the huge amount of research on privacy and information security (see Bélanger &Crossler, 2011; Cram, Proudfoot & D'Arcy, 2017; Moody, Siponen & Pahnila, 2018; Pavlou, 2011; Smith, Dinev & Xu, 2011; Willison & Warkentin, 2013), the calls for more interdisciplinary information security research (Angst, Block, D'Arcy & Kelley, 2017; Dhillon & Backhouse, 2000; Dinev 2014; Pavlou, 2011; Warkentin &Willison 2009) and for studies at the group and organizational level (Bélanger &Crossler; 2011; Pavlou, 2011), the current understanding of information security and data privacy (Dinev, Xu, Smith, & Hart; 2013) is largely fragmented. We found no integrated management system and data privacy framework.

To close this gap and comply optimally with GDPR, we have developed an efficient, effective and sustainable data privacy governance model. This model integrates the GDPR requirements, different information security governance frameworks, best-practice methods (COBIT, ITIL) (IT Governance Institute, 2007; Office of Government Commerce, 2007), ISO standards and the general requirements of standard based management systems. The holistic approach integrates data privacy

18 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/a-data-privacy-governance-model/233157

Related Content

Competing Methodologies: Possibilities from a Point of View
Stephen Rainey (2013). *Ethical Governance of Emerging Technologies Development (pp. 296-311).*
www.irma-international.org/chapter/competing-methodologies-possibilities-point-view/77195

The Impact of IT Resources on the IT Business Value: Evidence From a Systematic Literature Review
Janusch Patas, Jens Bartenschlagerand Matthias Goeken (2011). *International Journal of IT/Business Alignment and Governance (pp. 48-62).*
www.irma-international.org/article/impact-resources-business-value/62096

Governance Structures for IT in the Health Care Industry
Reima Suomiand Jarmo Tahkapaa (2004). *Strategies for Information Technology Governance (pp. 357-381).*
www.irma-international.org/chapter/governance-structures-health-care-industry/29910

Macroeconomic Implications of Virtual Shopping: A Theoretical Approach
I. Hakan Yetkinerand Csilla Horvath (2001). *Managing Internet and Intranet Technologies in Organizations: Challenges and Opportunities (pp. 104-126).*
www.irma-international.org/chapter/macroeconomic-implications-virtual-shopping/25890

Socio-Technical Punctuated Equilibrium Model Enhanced with Social Network Theory: As the Descriptor of Changes in the Equilibria of CIO Work
Tomi Dahlberg, Päivi Hokkanenand Mike Newman (2017). *International Journal of IT/Business Alignment and Governance (pp. 1-16).*
www.irma-international.org/article/socio-technical-punctuated-equilibrium-model-enhanced-with-social-network-theory/180691