STUDY OF EFFECTS OF INFORMATION SECURITY MANAGEMENT SYSTEM IN THE CONTEXT OF THE E.U. GENERAL DATA PROTECTION REGULATION APPLICATION

Razvan Cristian IONESCU
Ph.D. student, The Bucharest University of Economic Studies, Romania, razv77@gmail.com
Benjamin GRAB
Ph.D. student, The Bucharest University of Economic Studies, Romania, benny_grab@hotmail.com
Youssef HASSANI
Ph.D. student, The Bucharest University of Economic Studies, Romania, hassani.youssri@gmail.com

ABSTRACT

This article highlights an analysis of the information security management system and the General Data Protection European Regulation.

The main objectives of this paper were to study the common aspects between an information security management system and the General Data Protection European Regulation and to identify the advantages of the implementation of this management system in the context of the application of the European Regulation for data protection.

A study on twenty companies from various industries has been performed to assess to what extent an information security management system can be useful in the application of the General Data Protection European Regulation. These companies have been studied further to identify the common aspects between this management system and the European Regulation.

KEYWORDS

General Data Protection European Regulation, Information Security Management System, Compliance, ISO/IEC 27001, Integration, Management Systems

INTRODUCTION

The level of awareness of the European Union citizens regarding the protection measures for their personal data varies from country to country. There are individuals that are not always fully aware about the risks to their personal data, despite the publicity in all media on General Data Protection Regulation requirements. Studies performed on respondents revealed many individuals continue to be willing to give away their personal data to gain benefits from businesses (e.g.: discounts on goods and services or faster/better services). The same studies revealed that some consumers are also very concerned with privacy of their data (Presthus and Sorum, 2018).

The General Data Protection European Regulation requires the data controllers and processors to implement effective technical and organisational measures to protect the privacy of individuals. The lack of details from the Regulation regarding the precise technical protection measures and processes that must be applied to secure the personal data flows and their locations (except the very clearly specified ones: encryption, minimization, pseudonymization) generated a wave of assumptions of which should be the proper protection measures or the complete set adequate of security controls to ensure an effective protection of individuals' data.

On the other hand, it was difficult to include in a general applicable regulation, specific measures that should be implemented in any organization, regardless of its processes, resources, local regulatory requirements or industry.

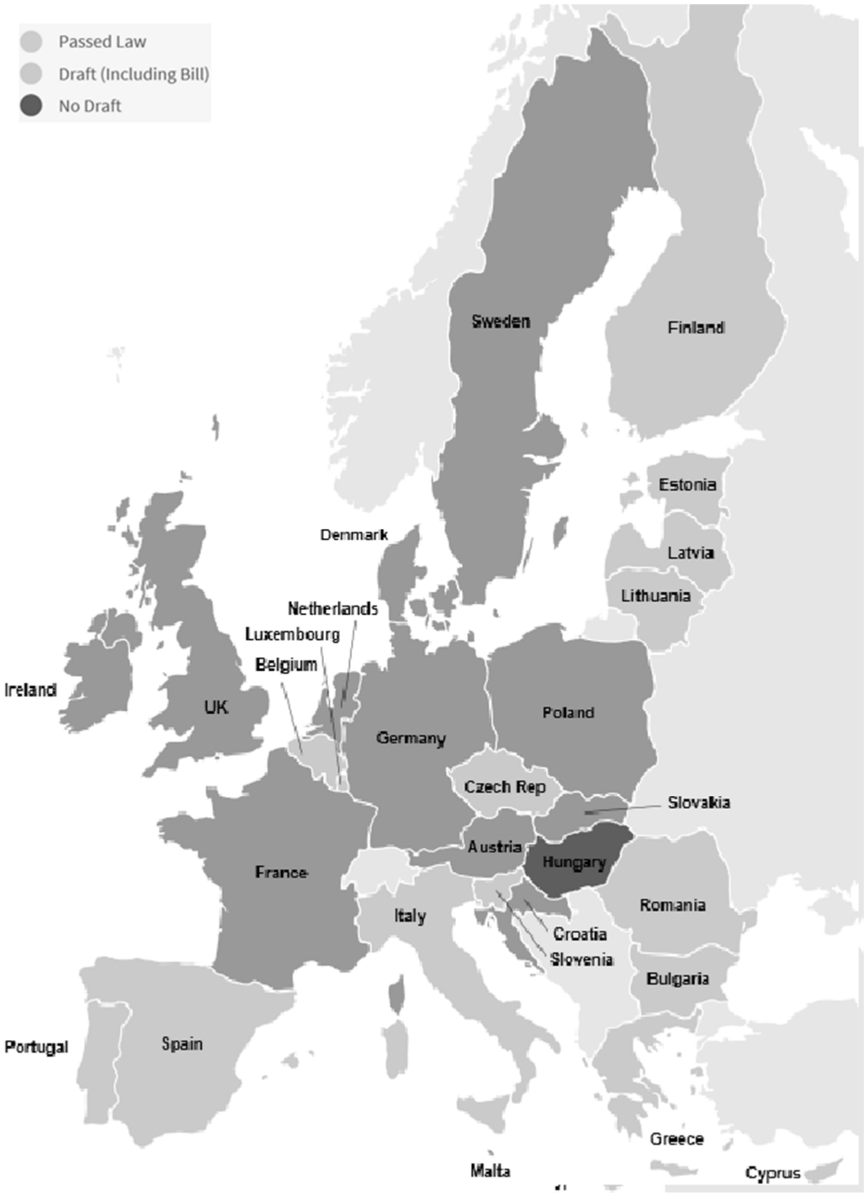
General concepts of security that are found in most industrial sectors can be applied in securing personal data according to General Data Protection Regulation as well. No matter the amount of security measures applied to protect personal data and mitigate the risks for rights and liberties of individuals, incidents might happen due to lack of awareness and good practice among personnel (Fatima and Colomo-Palacios, 2018) (Ionescu et al., 2018).

In general, the vulnerabilities are the weaknesses of an infrastructure, system, procedures or internal controls. Identification of vulnerabilities is performed by an assessment of examining the information systems to determine the adequacy of security measures, to identify the deficiencies and confirm the adequacy of such measures after their implementation (Dimitrakos, 2018).

Therefore, the authors of this paper consider an information security management system might be a solution in proposing clear and suitable technical and organizational measures to secure the personal data flows. This is possible because the technical measures used for protecting the sensitive information of the organization are similar with the personal data protection measures.

1. CURRENT STATUS OF INFORMATION SECURITY MANAGEMENT SYSTEMS AND GENERAL DATA PROTECTION REGULATION IMPLEMENTATIONS AROUND EUROPEAN UNION

There are different approaches in the General Data Protection Regulation implementation across the European Union. The level of implementations depends on the specific industry of the organizations, awareness process among employees and resources granted by the management for these implementations. Another difference is the right of each country to create local requirements as regards the implementation of the General Data Protection Regulation. The graph below shows the status of the issuance of these local laws and regulations, in each European Union country.



(Source: Latham & Watkins LLP, 2018)

Figure 1. Status of the issuance in European Union of local laws and regulations related to General Data Protection Regulation

The laws issued by various countries are a factor for individualization of General Data Protection Regulation implementation at local level.

The level of information security management systems certifications across the same countries mentioned in the graph above, is mentioned in the following statistics:

Table 1. Level of information security management systems certifications across European Union countries

Country	**Number of information security management systems certifications in 2017**
Austria	146
Belgium	127
Bulgaria	250
Croatia	123
Cyprus	32
Czech Republic	463
Denmark	57
Estonia	9

Country	Number of information security management systems certifications in 2017
Finland	72
France	342
Germany	1339
Greece	727
Hungary	472
Ireland	209
Italy	958
Latvia	42
Lithuania	85
Luxembourg	25
Malta	18
Netherlands	913
Norway	87
Poland	705
Portugal	112
Romania	440
Slovakia	173
Slovenia	70
Spain	803
Sweden	148
Switzerland	171
United Kingdom	4503

(Source: The International Organization for Standardization, 2018)

Information Security Management System can be improved if Six Sigma techniques are applied. There are implementations improved by some Six Sigma techniques (Ionescu, 2018) that could be used for General Data Protection Regulation issues as well.

2. RESEARCH METHODOLOGY

A sample of twenty Romanian companies, from various industries, has been assessed by the authors of this paper, between March 2018 and January 2019 to assess if their already implemented information security management system was used in the adoption of the security requirements of the General Data Protection Regulation. A comparative analysis has been performed during these assessments, between the general security controls found as implemented for their critical information assets and the specific personal data security requirements from the General Data Protection Regulation.

The authors identified and classified the most common difficulties these organizations faced during the adoption of the General Data Protection Regulation security requirements despite their existing information security management system for all their sensitive information assets.

3. RESEARCH RESULTS

3.1 The research results about the difficulties encountered by the assessed companies during the adoption of the security controls required by the General Data Protection Regulation

Even the controllers and processors are not forced by the General Data Protection Regulation to have an information security management system implemented as evidence of their compliance. They can use the possible existence of such management system as an opportunity to comply faster and better with this European law.

All the assessed companies have implemented an information security management system before the adoption of the General Data Protection Regulation. This assisted their staff in better understanding the specific personal data protection principles of the General Data Protection Regulation. The main difficulty was how to map the personal data security requirements into the existing general information security management system applicable for the whole organizational assets not only to the personal data.

The following statistics was concluded following the assessments performed by the authors in the sampled companies. It shows the implementation difficulties and doubts the staff of these companies experienced during the General Data Protection Regulation implementation process:

Table 2. Implementation difficulties and doubts encountered by the employees of the assessed companies

Doubt or problem encountered by the General Data Protection Regulation implementation team	Percentage of companies from the assessed sample
Doubts if appointing a Data Protection Officer is mandatory in the specific case	20%
Doubts about the relation between the Data Protection Officer and the Information Security Officer	30%
Problems in changing of the existing software whose internal data processing were found as not compliant with the General Data Protection Regulation	95%
Lack of understanding of the application of the risk assessment process in the General Data Protection Regulation	60%
Identification of a data processing inside a business process	60%
Problems in understanding and application of pseudonymization	85%
Problems in application of encryption on all levels	40%
Problem in understanding the entire data flow for the whole business	40%

(Source: Authors, 2019)

Most companies found a solution for the difficulties mentioned above by the date this article was issued.

3.2 The research results about a comparative analysis between the information security management system and the requirements for the data protection mentioned in the General Data Protection Regulation

The companies involved in the study inspired themselves from their existing information security management system to identify the opportunities they have, to comply with General Data Protection Regulation as well.

The complete list of security controls to be implemented to assure the General Data Protection Regulation compliance is difficult to be specified in one single document, especially because controllers and processors are very different, in terms of: volumes and categories of processed data, size, budget, technical and legal competencies, level of regulatory requirements, industry field where they activate, geographical area where they operate. Therefore, both the information security management system and General Data Protection Regulation are asking controllers to perform a risk analysis before considering the appropriate protection measures for the data. The controller must take adequate protection measures in dependence of the results of this analysis.

The risk management process is required both by General Data Protection Regulation and the information security management system. Here is a difference between the two studied approaches: whilst an information security management system requires an organization to identify the information security related risks, General Data Protection Regulation requires the risks upon rights and freedoms of natural persons, posed by processing, to be identified. So, the risk analysis required by an information security management system is not sufficient to claim compliance with General Data Protection Regulation risk analysis, although 10% of the assessed companies claimed their information security management system cover all the General Data Protection Regulation security requirements. Therefore, these 10% of the companies did not extend or update their existing risk analysis from the beginning of the implementation. This turned out to be a wrong and risky approach, as the specific risks upon the rights and freedom of individuals haven't been taken into consideration in these cases.

The assessment of the impact and risks is a common requirement of General Data Protection Regulation and of the information security management system, although the last one emphasizes more on risk assessment than impact assessment. Both approaches impose that the impact upon protection of personal data (General Data Protection Regulation) and upon critical information assets (information security management system) has to be considered. One major difference is that the General Data Protection Regulation is very specific on Data Privacy Impact Assessment process, whilst information security management systems do not clearly specify how to conduct an impact assessment.

Most of the assessed organizations integrated the risk assessment requirements from the Regulation and management system, by applying some minor changes to their existing risk management methodology and adapting it to General Data Protection Regulation.

The security in the development process from information security management system is very similar to the concept of "privacy by design" from General Data Protection Regulation. Thus, almost 100% of the assessed organizations that have implemented an information security management system, extended their rules for development of software, systems and/or projects to fit the General Data Protection Regulation requirements as well.

The "security by default" concept has existed already in the information security management system of these organizations, so they only had to check if their current security rules for protecting their sensitive information are effective for the processing of personal data as well.

The General Data Protection Regulation data minimization principle implementation determined both controllers and processors to renounce at about 10-15% of their collected data, because it was not identified any reasonable justification for data processing (e.g.: collection, storage). This principle was adopted in conjunction with the well-known security concept "need to know", so that restrictions to the processing stages have been applied to control the access to personal data.

The main attributes of information security are the confidentiality, integrity and availability of critical information. This approach is similar with data protection concepts from General Data Protection Regulation. The Regulation adds a fourth security attribute, which is the resilience of processing systems and services as a mandatory requirement for personal data protection. However, the resilience concept is implied in the information security management system as well, even it is not mentioned explicitly in the information security definition.

The incident management and business continuity processes are mandatory processes in the General Data Protection Regulation and in the information security management system. These processes are more detailed in the information security management system in comparison with General Data Protection Regulation where the only requirement is that the personal data to be restored in a timely manner in case of an incident. The testing of the business continuity plan is met in General Data Protection Regulation also, which requires a process for regularly testing the measures for the security of processing.

The monitorization and testing of the effectiveness of the security controls is a process mentioned in the Regulation and the information security management system. This monitorization process must be regularly to identify in advance the possible vulnerabilities and nonconformities.

The most important similarities between some General Data Protection Regulation security requirements and information security management system, identified by the authors during this study, have been summarized in the table below:

Table 3. Similarities between General Data Protection Regulation security requirements and information security management system

Topic	**General Data Protection Regulation requirement**	**Information security management system requirement**
Defining context	"Taking into account … the nature, scope, context and purposes of processing"	The organization and its context must be understood
Risk necessity	"Taking into account the …. as well as the risks"	Actions to address risks and opportunities must be taken
Requirement to protect personal data	"This Regulation protects … and in particular their right to the protection of personal data."	Privacy and protection of personally identifiable information controls must be in place
Mandatory protection measures	"…the controller shall … implement appropriate technical and organizational measures"	The organization shall define and apply an information security risk treatment process to determine all controls that are necessary
Types of security measures (e.g.: encryption)	"...the controller and the processor shall implement… pseudonymization and encryption of personal data"	Encryption is recommended in many controls
Privacy by design	"Data protection by design and by default"	Security in development and support processes must be in place
Incident management	"Security of processing"	Information security incident management must be in place
Business continuity	"Security of processing"	Information security aspects of business continuity management must be in place
Restrictions to information	"Security of processing"	Access control measures must be in place
Security reviews, monitorization of compliance	"Security of processing"	Information systems audit and security reviews must be in place
Attributes of security	"…the controller and the processor shall implement appropriate technical and organizational measures to ensure …: … confidentiality, integrity, availability and resilience"	The information security management system must preserve at least the confidentiality, integrity and availability of information
Segregations of duties	"Position of the data protection officer" "The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests."	Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
Defining a responsible for the process of security	Designation of the Data Protection Officer	Information security roles and responsibilities must be defined. Organizational roles, responsibilities and authorities must be defined

(Source: Authors, 2019)

As regards the most encountered differences between General Data Protection Regulation requirements and the ones from the information security management system, in terms of security, they have been summarized below:

Table 4. Differences between General Data Protection Regulation security requirements and information security management system

Topic	General Data Protection Regulation requirement	Information security management system requirement
Types of risks to be identified	Risks for rights and freedoms of natural persons posed by the processing	Risks associated with the loss of security of critical information
Types of security measures (*pseudonymization*)	Recommended	Not required explicitly
Types of security measures (*encryption*)	Highly recommended, in some cases mandatory	Recommended
Attributes of security	Mandatory resilience	Resilience is not mandatory but recommended
Breach notifications	Mandatory reporting to Data Protection Authority/Individuals (upon case)	Not mandatory to report outside the organization
Rights of individuals	Mandatory to consider	Not required

(Source: Authors, 2019)

3.3 The research results about the wrong approaches found in the sampled organizations as regards the implementation and integration of the information security management system and the General Data Protection Regulation requirements

The interviews held by the authors of this study with the staff of the audited organizations during the information security management system and General Data Protection Regulation assessments, revealed some wrong approaches in the implementation process. These approaches have been summarized in the below table:

Table 5. Wrong approaches in the General Data Protection Regulation implementation process

Type of wrong approaches found in the sampled organizations	Percentage of organizations from the assessed sample	Effects upon the compliance level of the organizations
The risk analysis performed for the information security management system hasn't been changed when the General Data Protection Regulation has been implemented. There are no identified risks upon the rights and freedoms of the individuals whose personal data are processed by the organization.	70%	There is no traceability between the risk analysis required by the Regulation and the specific mitigating measures.
The Data Protection Officer is the same with the IT administrator.	10%	Conflict of interest between the two roles.
The management of the company nominated the Data Protection Officer to implement the General Data Protection Regulation requirements because this person has the required knowledge to do the implementation.	80%	Conflict of interest between the monitorization and the implementation duties.
The management of the company is not be involved in General Data Protection Regulation implementation and its compliance monitorization since there is a Data Protection Officer appointed for this task.	40%	Lack of fulfilment of the Regulation requirements.
Data Protection Officer will be accountable for any fine or penalty regarding General Data Protection Regulation noncompliance.	70%	The Regulation protects this function against these sorts of actions from the management, if the Data Protection Officer has fulfilled his/her tasks properly

(Source: Authors, 2019)

CONCLUSION

The study revealed a strong relation between the information security management system and the General Data Protection Regulation security requirements. There are many similar principles and approaches between this management system and the Regulation.

Despite the Regulation does not specify very clearly all the possible security measures for the personal data protection, the previous implementation of the information security management system can help organizations to understand and better fulfil the legal requirements for the personal data protection.

In most of the cases, the technical controls in place for protecting critical information assets were the same with the measures for protecting the personal data processed by the organization.

The continuous improvement cycle concept used for the information security management system can be used also for the General Data Protection Regulation implementation and monitorization strategy.

Furthermore, the information security management system and General Data Protection Regulation requirements can be integrated for a more successful implementation as their security objectives are almost common. If this management system is used to extend the General Data Protection Regulation scope, all the critical information assets will benefit of security protection measures, not only the personal data.

Even the information security management system is implemented voluntary by organizations, General Data Protection Regulation requirements are mandatory so more attention must be applied upon this Regulation than on a voluntary management system, as the risks for the organizations are much higher when a non-compliance or an incident occurs.

The results of the study revealed doubts, problems and misunderstandings from the employees of the audited organizations as regards some security requirements from General Data Protection Regulation. The study and implementation of an information security management system could clear these issues as this management system is more specific regarding the security controls that must be in place for an adequate level of protection.

General Data Protection Regulation implementations should benefit upon the information security management system experiences, in order to understand better and faster what must be done. The success of the General Data Protection Regulation implementation, regarding the security requirements, can be assured if the information security management system is implemented properly and combined with the legal requirements. Integration of an information security management system with General Data Protection Regulation is a key factor in acting successfully in case of a data breach or a security incident. Integration is necessary also to reduce the bureaucracy and response time in case of a complaint, investigation or an incident. Even the information security management system does not impose a certain response time in case of a complaint or incident, General Data Protection Regulation is very specific in this regard.

General Data Protection Regulation also demands some processes to exist and be effective but does not describe in detail these processes (e.g.: incident management, business continuity, monitorizations of the effectiveness of the security controls). Information security management system can be used to provide a clear picture of how these processes can de designed to be effective. For example, the incident management process is described in information security management system as a flow starting from the detection and reporting to the learning from information security incidents. Therefore, information security management system requirements can be a real help in the implementation of the security requirements from General Data Protection Regulation.

Improvements of the General Data Protection Regulation implementations can be obtained also if other techniques are applied, such as the ones for problem solving from Six Sigma methodology. The authors consider the integration of Six Sigma and General Data Protection Regulation might reduce significantly the security incident rates, so opportunities for further studies in this direction are still provided.

REFERENCES

1. Dimitrakos T. (2018). How to Develop a Security Controls Oriented Reference Architecture for Cloud, IoT and SDN/NFV Platforms. *IFIP International Federation for Information Processing, Springer International Publishing AG 2018, https://doi.org/10.1007/978-3-319-95276-5_1*
2. Fatima A., & Colomo-Palacios. R. (2018). Security aspects in healthcare information systems: A systematic mapping. *CENTERIS – International Conference on ENTERprise Information System/ ProjMAN – International Conference on Prokect MANagement/HCist – International Conference on health and Social Care Information Systems and Tehnologies, CENTERIS/ProjMAN/HCist 2018, Procedia Computer Science 138 (2018) 12-19.*
3. Ionescu R., & Ceausu I., & Ilie C. (2018). Considerations on the Implementation Steps for an Information Security Management System, *Proceedings of the 12th International Conference on Business Excellence – ICBE 2018, pp. 476-485, https://doi.org/10.2478/picbe-2018-0043*
4. General Data Protection Regulation (2018). https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&qid=1543667361282&from=EN
5. ISO (2013). ISO/IEC 27001:2013 - Information technology -- Security techniques -- Information security management systems – Requirements. *ISO.*
6. ISO (2013). ISO/IEC 27002:2013 - Information technology -- Security techniques -- Code of practice for information security controls. *ISO.*
7. Latham & Watkins LLP (2018). *https://gdpr.lw.com/Home/Implementation*
8. Presthus W., & Sorum H. (2018). Are Consumers Concerned About Privacy? An Online Survey Emphasizing the General Data Protection Regulation. *Centeris – International Conference on ENTERprise Information Systems, ScienceDirect, Procedia Computer Science 138 (2018) 603–611*
9. ISO (2018), https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1
10. Olaru M., & Ionescu R., & Maftei M., & Ilie C. (2017), Application of Six Sigma Tools for Improvement of Information Security Management System, *30th IBIMA Conference, Proceedings of the 30th International Business Information Management Association Conference (IBIMA), pg. 5779-5784, ISBN 978-0-9860419-9-0, http://apps.webofknowledge.com.am.e-nformation.ro/full_record.do?product=WOS&search_mode=GeneralSearch&qid=11&SID=C1KpTz2WpurzX6a3P7Z&page=1&doc=2*