The Impact of GDPR on IT/IS

Vlasta Svatá

Department of Systems Analysis, University of Economics, Prague, W. Churchill sq. 3, 130 00 Prague 3, email:svata@vse.cz

Abstract: **The article focuses on GDPR and emphasizes the implications of ensuring compliance in IS/IT. It stresses the importance of information security management and data governance. The main output is the table outlining the main responsibilities of data controllers and processors and their impact on IS / IT management.**

Keywords: **GDPR, information security, data governance, IT/IS perspectives of GDPR.**

I. Introduction

IT professionals can act as strategic partners to businesses currently working toward compliance with the European Union General Data Protection Regulation (GDPR), scheduled to come into enforcement on 25 May 2018. Even to the fact, that GDPR compliance is not solely a technology issue (it requires attention and remediation expertise from various functions within the business, e.g. human resources, legal, compliance, marketing, communications) technology acts as a common denominator across business processes and plays a significant role in the collection, processing, storage and transfer of personal data [3]. The main aim of the article is to clarify the status of personal data protection in information security management, and thereby partially reduce concerns about the introduction of regulation into practice. At the same time, some new aspects that the new regulation brings to IT management should be highlighted.

II. Protection of Personal Data Privacy, Information Security and Data Governance

Confidentiality / privacy is a fundamental right, necessary for autonomy and protection of human dignity, serving as the basis on which other human rights are built. On the other hand IT fundamentally restricts the right to privacy being integrated, globalized and mobile. This fact is counterbalanced by the constant improvement of frameworks for the introduction of controls into the IS / IT environment. All of them should artificially balance the loss of privacy. The development of such countermeasures range from securing the primitive need to "be alone - give me a peace" up to complex concepts (legal, socio-psychological, economic or political). Some of the concepts are more reactive (GDPR is an example) some are more proactive, eg. European Data Protection: Coming of Age). This document takes in a count seven categories of privacy:

- Privacy of the person: protection against unauthorized body failure (genetic tests, blood tests, implants, ...).
- Privacy of behavior and actions: protection of ideas, emotions, orientation - sensitive information (camera systems, police body cameras).
- Privacy of communication: protection of all communication channels (printed, voice, video, digital) (hidden microphones, mail, postal services).
- Privacy of association: the right to associate with other persons without unauthorized monitoring and marginalization (DNA tests for ethical proof, employee release based on DNA tests, ...).
- Privacy of data and image (information): protection of personal information in all forms (leakage of financial, health information, dissemination of images without the knowledge of persons).
- Privacy of thoughts and feelings: protection against their spread or use against persons (requesting password for access to the social network when recruiting, requesting information on religion and political orientation).
- Privacy of location and space (territorial): protection against technology that can monitor the location, space, and general environment of an individual (video, drones, work and home monitoring).

	Social media	Cloud computing	Apps	Big Data Analytics	Internet of Things	BYOD	Tracking and surveillance
Privacy of the person			X	X	X		X
Privacy of behaviour and action	X		X	X	X	X	X
Privacy of communication	X	X	X	X	X	X	
Privacy of data and image	X	X	X	X	X	X	X
Privacy of thought and feelings	X	X	X	X	X	X	X
Privacy of location and space	X	X	X	X	X	X	X
Privacy of association	X	X	X	X	X		X

Fig. 1. Privacy categories and technologies [2].

Fig. 1 shows how separated IT influence the privacy categories.

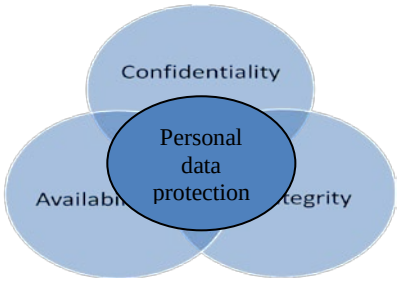

Fig. 2. Information security CIA Triad.

Great majority of international reactive frameworks for information security are designed to protect the confidentiality, integrity and availability of computer system data from those with malicious intentions. Confidentiality, integrity and availability are sometimes referred to as the CIA Triad of information security. Based on this definition we can conclude, that protection of personal data is preservation of confidentiality, integrity and availability of data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information. Protection of personal data thus can be viewed as application of information security controls over the specific types of data – personal data. The base for GDPR is thus the compliance with information security frameworks, but it is only a necessary but not a sufficient condition. GDPR goes beyond the information security frameworks, as its main aim is to improve data governance.

Data governance is a term used to describe the overall, comprehensive process for controlling not only the data security (CIA Triad) but the efficiency, effectiveness, relevance and compliance as well. Data governance consists of the processes, methods, tools, and techniques to ensure that data is of high quality, reliable, and unique (not duplicated), so that downstream uses in reports and databases are more trusted and accurate. A data governance program should be a part of an IT governance program. While data/information security is mainly in responsibility of IT professionals (processors or third parties), data governance is in responsibility of business managers – controllers that determine the purposes and means of the processing of personal data. GDPR compliance is thus the corporate responsibility of the data controller, not of the DPO, internal auditor or CIO.

III. Personal Data and Personal Data Processing

Before we will discuss the impact of GDPR on IT management it is necessary to specify who does the GDPR apply to and what data does the GDPR apply to.

The GDPR applies to processing carried out by organizations operating within the EU. It also applies to organizations outside the EU that offer goods or services to individuals in the EU. Transfers of personal data outside the EEA (European Economic Area) are not allowed unless the country has an adequate level of protection for the processing of personal data. For instance in 2016 the European Commission approved the Privacy Shield, enabling easy transfer of personal data from the EU to selected companies without the need to obtain permission from the national data protection authority or the conclusion of a standard contractual clause with the US data processor. The GDPR applies to both the 'controllers' and 'processors'. The controllers determine the purposes and means of processing personal data and ensure that the contracts with processors comply with the GDPR. They are not relieved of their obligations where a processor is involved and they shall be responsible for, and be able to demonstrate, compliance with the GDPR principles. The processors are responsible for processing personal data on behalf of a controller. They are required to maintain records of personal data and processing activities and they will have legal liability if they are responsible for a breach. The GDPR does not apply to certain activities including:

- covered by the Law Enforcement Directive
- processing for national security purposes
- processing carried out by individuals purely for personal/household activities.

The GDPR applies to 'personal data' (both automated and manual filing systems) meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. In case of manual data it must be accessible according to specific criteria. This could include e.g. chronologically ordered sets of manual records containing personal data. Special categories of personal data are sensitive data, pseudonymised data and children's data. Sensitive data include genetic data, and biometric data where processed to uniquely identify an individual. Pseudonymised data (coded data) can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual. Examples are all types of electronic traces, e.g. Internet proxy addresses and cookie identifiers. Children's data processing needs the consent of the holder of parental responsibility and the data need specific protection as children may be less aware of the risks. Personal data that are excluded from compliance are:

- data relating to criminal convictions and offences
- organizational data
- data of deceased persons
- data to help prevent crime (investigation, detection, prosecution)
- data not arranged according to the specified points of view
- anonymous data (statistics, research).

Personal data processing is any act or set of acts that the controller or processor systematically performs with personal data by automated or other means. Examples are collecting, recording, arranging, structuring, storing information, accessing, editing or editing. This definition of data processing is no surprise, but the Article 5 of the GDPR requires that personal data shall be

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

The requirement to have a lawful basis in order to process personal data is not new. It replaces and mirrors the previous requirement to satisfy one of the 'conditions for processing' under the Data Protection Act 1998. However, the GDPR places more emphasis on being accountable for and transparent about the lawful basis for processing [1] . The identification of the lawful basis is important not only because the organizations should provide people with information about their lawful basis for processing (this information must be covered in the privacy notice) but it has a big consequences on to IT/IS area. The reason is, that the lawful basis for processing can also affect the rights that are to be available to individuals.

There exist the six lawful bases:

- Consent- should be given by a clear affirmative act of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement.
- Contract - processing should be lawful where it is necessary in the context of a contract or the intention to enter into a contract.
- Legal obligation - legitimate basis, laid down by law including the necessity for the performance of a contract to which the data subject is party.
- Vital interest - it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person (e.g. humanitarian purposes).
- Public task - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority; the processing should have a basis in Union or Member State law.
- Legitimate interest – e.g. where there is a relevant relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller, when it is necessary for the purposes of preventing fraud and for direct marketing purposes.

The GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

Fig. 3 shows the relevance between the six lawful bases and voluntary rights for individuals (the others are obligatory in each case).

IV. Important Issues from IT/IS Perspective

Despite the fact, that GDPR being data governance regulation, not the data security regulation, is in accountability of board and business executives, IT professional both from the controller´s and processor´s organizations are to be expected to address a range of tasks that goes beyond their existing responsibilities. The extent of these tasks is influenced by the following three aspects that are specific for each organization:

- Decision about the lawful base for personnel data processing – has an impact on the scope of GDPR application (see Chapter III)
- Codes of conduct – guidance on the implementation of appropriate measures and on the demonstration of compliance by the controller or the processor. They should include identification of the risk related to the processing, their assessment in terms of origin, nature, likelihood and severity, and the identification of best practices to mitigate the risk.
- Designation of the data protection officer – represents the new role within the organization and thus needs new redefinition of the RACI chart and redesign of the IT and business processes.

Next table provides the summarization of the controller´s responsibilities and their impact on IT/IS.

	Right to erasure	Right to portability	Right to object
Consent			x
Contract			x
Legal obligation	x	x	x
Vital interest		x	x
Public task	x	x	
Legitimate interest		x	

Fig. 3. Relationships between the lawful bases and rights [1].

TABLE 1. Overview of controllers and processors GDPR responsibilities and their impact on IS / IT management

Responsibilities of the controller and processor	**Impact on IT/IS**
Data protection principles: • lawful, fair and transparent processing • collected for specified, explicit and legitimate purposes • minimization • accurate data • kept no longer than is necessary • secure data	Provide consultancy what, where and how long are personal data collected, processed and stored
Implementation of the appropriate technical and organizational measures	Implement methods for the pseudonymisation and encryption of personal data Ensure information security (confidentiality, integrity, availability) by choosing and implementation of the appropriate framework (ISO 27000, Cobit 5, Cobit Security Baseline, ..); impact on: • business continuity (back up and disaster recovery plans) • risk assessment • access controls • physical security Do not engage another processor without prior specific or general written authorization of the controller Check all contracts that are binding on the processor whether they sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the

	obligations and rights of the controller. Continuous testing, assessing and evaluating the effectiveness of technical and organizational measures
Approvement of certification mechanism (is voluntary)	Adherence to the approved certification mechanism and cooperation with the certified bodies
Notification of a personal data breach to the supervisory authority	Immediate notification the controller of a personal data breach in a formal way (breach nature, consequences, taken measures, etc.)
Data protection impact assessment	Assessment of the impact of new IT on the personal data protection (cloud computing, big data, IoT, BYOD, …)
Designation of the data protection officer (DPO)	Support the DPO in performing the tasks (access to personal data and processing operations) Ensure that DPO tasks and duties do not result in a conflict of interests Provide IT/IS consultancy
Codes of conduct	Adherence to the codes of conduct; impact on: • declaration, that personal data processing is fair and transparent • the pseudonymisation of personal data (e.g. whether System design permits the attribution of pseudonymized data to natural persons, domain segregation is applied to separate attribution data from pseudonymized data; and access to meta-data is appropriately restricted) • the information provided to the public and to data subjects • the notification of personal data breaches • the transfer of personal data to third countries • the information security measures and procedures Cooperation with the accredited body while monitoring compliance
Transfers of personal data to third countries or international organizations	Provide consultancy as regard the appropriate safeguards, and condition that enforceable data subject rights and effective legal remedies for data subjects are available Provide contractual clauses about safeguards
Lawfulness of processing	Consent processing • the need to record the consents, purpose and validity and to check them in personal data processing • to be able to withdraw the consent at any time
Rights of the data subject	To check possibilities how to automate the realization of the separate rights; impact on • authentication of the data subject enforcing its law • personal data encryption
	• changes in process, data, application models (additional controls, identifiers, functions) • changes in application interfaces (menus) supporting the communication with data subject • process analysis for separate rights enforcement
Records of processing activities	Provide consultancy about the items needed, mainly: • the purposes of the processing • the categories of data subjects and of the categories of personal data • the categories of recipients • transfers of personal data to a third country • time limits for erasure • general description of the technical and organizational security measures • the name and contact details of the processor(s)

V. Conclusion

IT plays a dual role in the protection of personal data: in one it poses a threat, the other is an effective protection tool. Balancing these two roles is an endless and costly task for all organizations. As a consequence GDPR cannot be viewed as a sprint to finish line. It represents one of the great opportunities that provides the basis for deepening collaboration between business executives and IT professionals. In many cases, IT professionals can assure managers that the required controls are already implemented or can be done automatically, in other situations they can point out the IT risks that they pose to the protection of personal data. In any case, without deeper ongoing cooperation and communication between these parties, ensuring compliance with the GDPR will be the only investment without any value for business.

References

[1] Information Comissionair´s Office, Guide to the General Data Protection Regulation, 22 March 2018

[2] ISACA Privacy principles and program management Guide, http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/ISACA-Privacy-Principles-and-Program-Management-Guide.aspx

[3] O.Osagiede Beyond GDPR Compliance – How IT Audit Can Move from Watchdog to Strategic Partner, isaca.org

[4] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR)