Proceedings of the International Conference on
Information Technologies (InfoTech-2018)
20-21 September 2018, Bulgaria

A MODEL FOR IMPLEMENTATION GDPR BASED ON ISO STANDARDS

Tzanko Tzolov

Member of Personal Data Protection Commission
e-mails: tzolov@cpdp.bg
Bulgaria

Abstract: The implementation of GDPR within organizations should be considered in the context of achieving their business objectives. The emphasis should be on the benefits of its application and the added value to the business itself. The implementation models focus on risk-based thinking taking into account technological innovations, environmental factors, information management, supply chain management and globalization. In this article the author proposes the use of the ISO 9001:2015 standard, putting forward another idea of obtaining a methodology for GDPR implementation.
Key words: GDPR, Standards, ISO 9001:2015, implementation, model.

INTRODUCTION

The implementation General Data Protection Regulation (GDPR) to organizations should be seen in the context of achieving their business goals. Very clear have to emphasize the benefits for organizations and the values adding to business. It is absolutely wrong to understand GDPR like as another restriction to the operating environment. GDPR is a tool for generating a strategic advantage based on trust between the organization, its employees, clients and partners.

Building on business goals, deployment models should be focused on risk-based thinking, taking into account technology innovations, environmental factors, information management, supply management and globalization.

In this text, the author pointed ISO 9001: 2015 standard like a model for implementing GDPR and offering a further insight into how to achieve the methodology of the implementation process.

MODEL OF AN ORGANIZATION

The implementation of GDPR within a digital organisation pursuing its business objectives can be illustrated using the model shown in Figure 1.

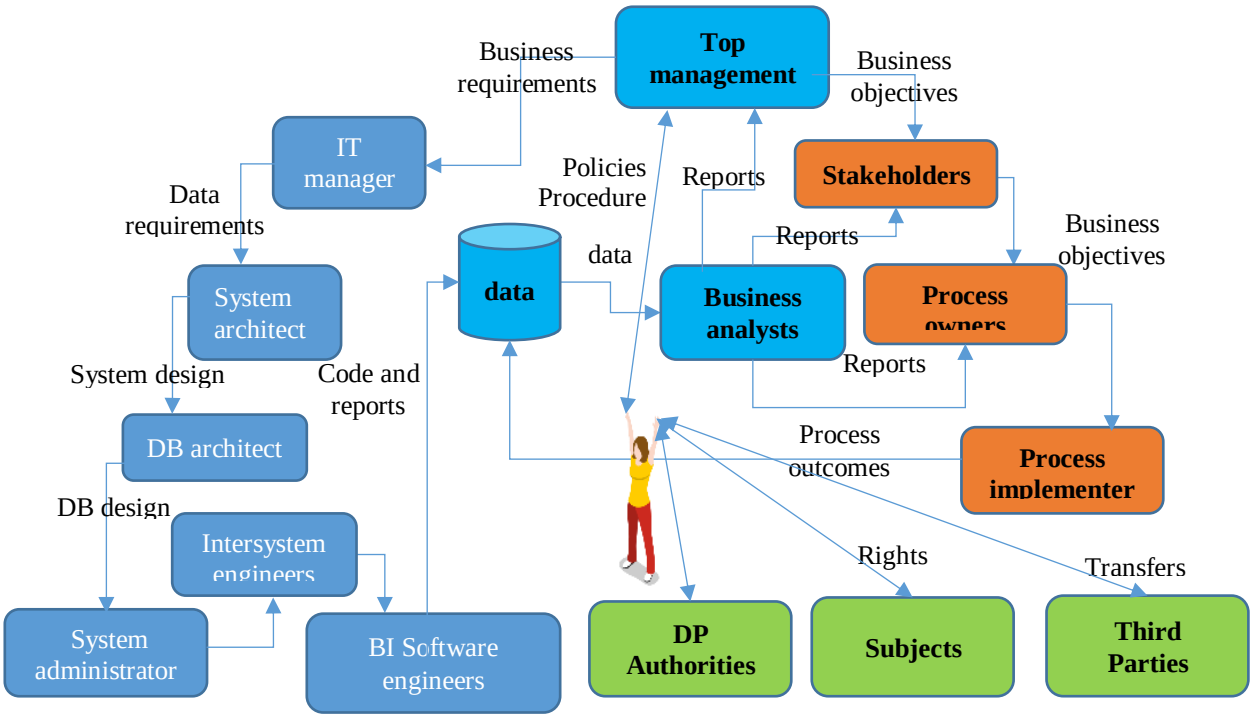

Fig.1. Model of an organisation in the digital age

The key requirements towards the model are to describe processes, set objectives and track key performance indicators, define roles and create consistent data models.

GDPR requirements have been defined as policies and procedures to be embedded into business processes and the roles of the players within the system.

The similar perception of the context of the organisation gives us reasons to look for an opportunity to apply the ISO 9000 family of standards as a methodology for the implementation of the general data protection regulation.

ISO 9001:2015 is based on the process approach and risk management, which also underpin GDPR.

ISO 9001 AS A SYSTEM

A major highlight of the revised ISO 9001:2015 was the transition to the Annex SL structure of the ISO Directive. This provides a framework for the development of integrated management systems based on several structurally homogeneous regulations.

The process approach introduced in the 2015 revision of the standard requires organisations to manage their processes in order to achieve planned results in accordance with the strategic goals of the organisation. The Deming Cycle: Plan – Do – Check – Act (PDCA) is the tool used to analyse and measure each process.

ISO 9001:2015 now requires organisations to identify, record, apply, maintain and continually improve processes and their interactions.

A new clearly defined methodological requirement is risk-based thinking. Risk is viewed as the impact of uncertainty and organisations should assess and manage it by planning and implementing appropriate measures.

The structure of ISO 9001:2015 is shown in Figure 2

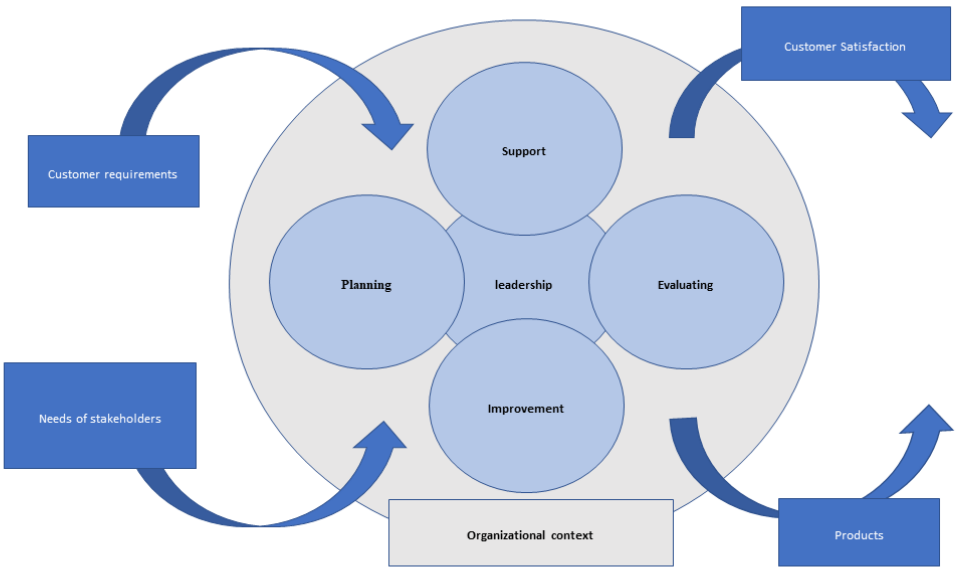

Fig.2. Structure of ISO 9001:2015

The Annex SL of the ISO Directive has the following structure: (1) Scope; (2) Normative references; (3) Terms and definitions; (4) Context of the organisation; (5) Leadership; (6) Planning; (7) Support; (8) Operation; (9) Performance evaluation; (10) Improvement.

GDPR REGULATION OR STANDARD

The main aim of the Regulation is to sustain the development of the digital economy and to overcome the legal limitations affecting data transfers. Taking globalisation and new technologies into account, the territorial scope fully matches the definition of standard, i.e. it has a global reach applying to every organisation around the world that processes the data of European citizens and to every individual whose data are being processed by a European company.

GDPR also promotes the use of standards as proof of compliance (information security 27000, cloud processing 27018), and as methodology for meeting different requirements (risk management 31000). The philosophy of certification or self-regulation is also based on the use of commonly accepted standards.

Even the terms and definitions used in GDPR correspond to the SL scheme which is yet another sign of homogeneity and compatibility.

The analysis of the environment starts with defining the players – data subjects, data controllers, data processors, data recipients and supervisory authority. Their functions and tasks are defined by their involvement as stakeholders, and their rights and obligations determine the scope of the personal data protection system. The processes are presented as data flows and divided into a core process and supporting processes. This analysis reveals the data (presented as RG), all internal and external users and identifies the key performance indicators of the organisation.

The regulation clearly lays down that the managing director of the organisation shall be the personal data controller who shall not delegate these rights to another person even if he or she uses the services of a data security officer. All policies and procedures shall be put in place after his or her approval. The roles of the employees within the organisation shall be aligned with business processes and their obligations concerning the processing of personal data shall be determined by the data controller.

Under GDPR planning is a process aimed at reducing the risk of data processing activities and is defined as an impact assessment aimed at identifying high risk data processing activities. The risks to the rights of individuals are of paramount importance. What's analysed are the data and their storage and transfer formats (protocols), the information technology (IT) used and its interfaces as well as all processes and procedures. Finally, specific measures for mitigating the risks are defined and put together into an implementation plan.

The implementation of the plan involves financial, human, technological and infrastructural resources. This stage also involves defining the necessary competences by focusing on staff training, infrastructure development and introduction of new technologies. Documentation is an obligatory process for meeting the organisation's reporting requirements.

The auditing of the data protection system involves constant monitoring (by a data security officer, internally or externally appointed), complete certification (of systems, people, services and products) by accredited organisations, self-assessment by means of stamps and markings or self-regulation within industries or associations.

The national supervisory authority performs full supervision of the data protection system.

The organisation is responsible for improving the system using impact assessments, industry self-regulation and formal warnings given by the national supervisory authority.

The General Data Protection Regulation (GDPR) possesses within itself all the sections of the requirements of the SL Scheme, but it is still a Regulation. It is an EU-wide regulation and is complemented by other rules concerning the supervisory authorities, the interaction between them and the powers conferred on them by this Regulation.

JOINT USE GDPR AND ISO 9001:2015

The compatibility between the Regulation and the Standard within the scope of Annex SL allows us to look for a way to implement GDPR within organisations using ISO 9001:2015 as a methodology.

The stages of implementation can be described using the model shown in Fig.3.

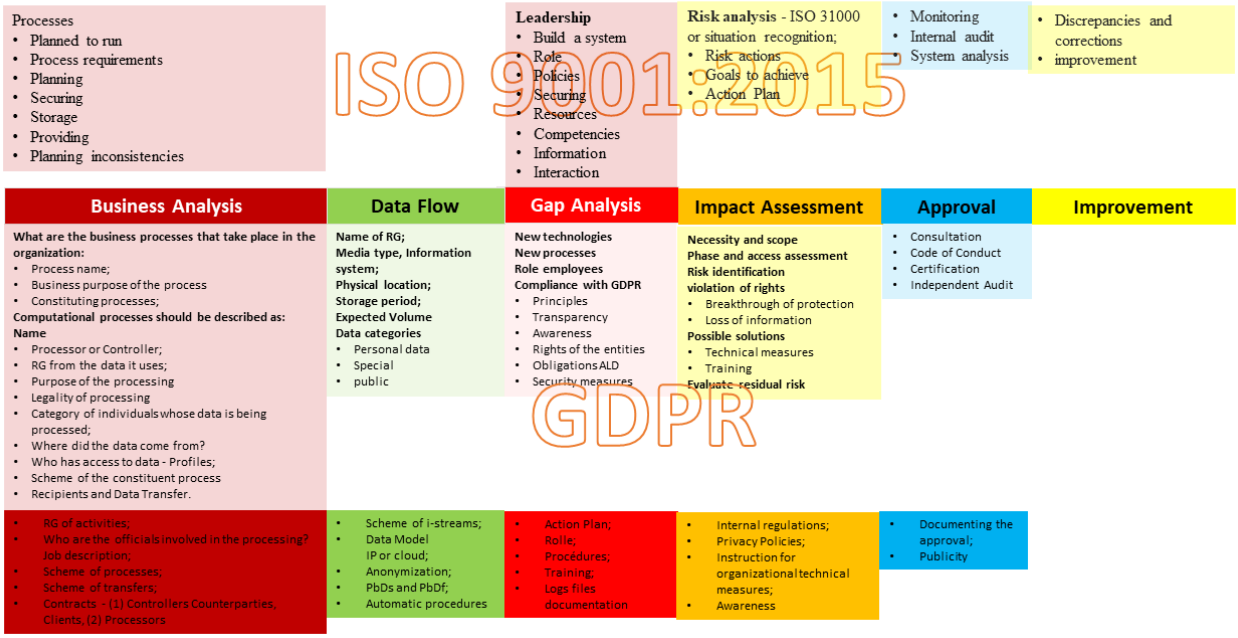

Fig. 3. A model for the joint implementation of Regulation 679 and ISO 9001:2015

Business analysis – in accordance with the ISO 9001 standard, this first stage describes the processes within the organization following the business model. The records to be processed and the officials involved in the processing activities are identified. The process scheme and the data exchange scheme with recipients and transfers to third countries are outlined. The legal basis that is to be updated or created for controllers and processors is set out.

Data flows – at this stage the business flows are converted into data flows. The purpose of this stage is to disclose processing activities, information systems and communication channels for data exchange. The categories of data being processed, the data scheme and the physical location where data will be stored are also described at this stage.

A data model, an information flow diagram, the processing technologies used and a system infrastructure diagram are prepared.

Analysis for GDPR compliance – the leadership and assurance assessment is used to verify the compliance with the GDPR principles, the transparency of processing operations, the awareness and rights of data subjects, the obligations of controllers and the organisational and technical data protection measures used.

A GDPR implementation plan is prepared, the roles within the organisation are defined, the necessary data protection technologies and infrastructure are identified,

procedures and training needs are set out, rules for the log files maintained and a structured log keeping scheme are created.

Impact assessment – the purpose of the impact assessment is to reduce the risk using the risk management methodology and to demonstrate that the data processing is done in accordance with GDPR requirements.

The risk assessment should identify the risks for the rights and freedoms of data subjects, the risks of security breaches or data loss. The risk level can be determined by using ISO 31000 or by recognising situations already assessed as risky and then following ISO 9001 in order to identify the actions that should be taken, the objectives that should be achieved and to prepare an action plan.

The risk analysis should identify the processing activities and stages that pose the highest risk so as to target the impact assessment precisely at them.

The impact assessment should result in a proposal for organisational and technical data protection measures, training and a residual risk assessment. The process documentation involves drawing up operational rules and procedures for the employees, instructions for the organisational and technical data protection measures, and the necessary materials for transparency and for raising data subjects' awareness.

Verification of compliance – apart from the monitoring, auditing and system analysis recommended under ISO 9001, GDPR also provides for additional mechanisms for compliance verification.

GDPR allows data controllers to consult the supervisory authority when the residual risk of an impact assessment they have conducted is high. Another possibility for guidance on the GDPR's requirements is the use of appropriate certifications and codes of conduct approved by the supervisory authority.

CONCLUSION

The joint use of GDPR and the ISO family of standards is a powerful mechanism for implementing the Regulation within the organisation. The standards can be used at the implementation stage as a methodology (ISO 9001: 2015), as a mechanism for completing different stages (ISO 31000), or as proof of compliance with the Regulation (ISO 27000 (27001, 27017, 27018)).

REFERENCES

[1] Regulation (EU) 2016/679 of the European Parliament and of the Councilof 27 April 2016 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 *(General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).*

[2] ISO 9001, Quality management systems — Requirements

[3] ISO/TS 9002, Quality management systems — Guidelines for the application of ISO 9001:2015.

[4] ISO 31000, Risk management — Guidelines