Proceedings of the International Conference on
Information Technologies (InfoTech-2017)
20-21 September 2017, Bulgaria

DATA GOVERNANCE AS A BUSINESS TECHNOLOGY AND GENERAL DATA PROTEECTION REGULATION

Tzanko Tzolov

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

Abstract: General Data Protection Regulation (GDPR) has direct effect for all data controllers across the EU and all companies processing data of EU citizens. The lack of a communicated implementation methodology makes it difficult for the business to understand and it stay as more one administrative burden. Using Data Governance technology, each organization can prepare itself to implement the regulation and guarantee the rights of citizens to process their personal data. GDPR is a technological advantage and creates an environment of security and trust for partners and customers.

Key words: Data Governance, General Data Protection Regulation, Business Analysis

1. INTRODUCTION

In April 2016, after nearly four years of work, the European Parliament adopted the General Data Protection Regulation (GDPR)[1] (EU) 2016/679.

The right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society and must be balanced against other fundamental rights according to the principle of proportionality.

If we compare the purposes set out by the legislator in the old and new regulatory framework, we will arrive at two different starting points: The Directive seeks “to harmonise the protection...”, whereas the General Regulation seeks “to contribute to economic and social progress...” And while “protection” is always associated with limitations caused by restrictions imposed on something for something else’s sake, “progress” is related to the possibilities and ways of overcoming these restrictions.

It is on this basic underlying thesis that the author will try to outline a common model for putting Regulation 679 into practice.

The elaboration and emergence of the Regulation has been driven by several factors of social development:

- Exponential growth in cross-border personal data flows.
- Significant increase in personal data exchange and collection.
- Technologies have transformed both the economic and social life, while ensuring a high level of personal data protection.
- These changes call for a stronger and more coherent data protection framework at EU-level in order to create trust.
- Increased sensitivity of individuals to their own personal data.

And, of course, it is of paramount importance to define the subject-matter – in this case "personal data" – correctly. The data protection principles should be applied to any information relating to an identified or identifiable natural person.

Natural persons can be identified by reference to online identifiers provided by their devices, applications, tools, and protocols, such as Internet Protocol (IP) addresses, identifiers called 'cookies', or other identifiers, such as RFID tags [9].

The philosophy behind the changes made in GDPR has been driven by the development factors that have been mentioned above:

- More rights for citizens – a fundamental change in social relations. In the digital age, the business can earn the clients' trust and consequently grow in a secure environment.
- The principle of accountability has been introduced – as a way of demonstrating compliance with the requirements of the Regulation.
- Supporting the digital single market – earning the trust not only at EU-level but also on a global scale of anyone operating on the European market.
- New mechanisms for the transfer of personal data – along with traditional practices, an assessment of the level of protection can be achieved for the first time at partner level through compliance with the same practices and standards approved by the Committee.
- The Regulation provides answers and follows new technologies – the meaning and definition of "personal data" have expanded; the IP address and global location have already been considered to be such. Cloud computing has its legal rules and definitions. The technologies and principles that should be applied in the protection and establishment of information systems have been set out.
- Reducing administrative burdens – the registration required for data processing has been abolished and the presumption of reasonableness in determining charges and fines levied or imposed by regulatory authorities has been defined.
- The General Regulation has a wide scope of action.

2. BUSINESS AND ITS READINESS TO EMPLEMENT GDPR

The European Union is the second largest economy in the world and accounts for 22.8% of the nominal global GDP [2], making it a sought-after business partner in the global economy. GDPR clearly stipulates that the regulation applies to any company operating on the European market or processing personal data of European citizens. A survey carried out by the International Association of Privacy Professionals (IAPP) in December 2016 shows the readiness of businesses to implement the General Regulation [3]. (Fig. 1)

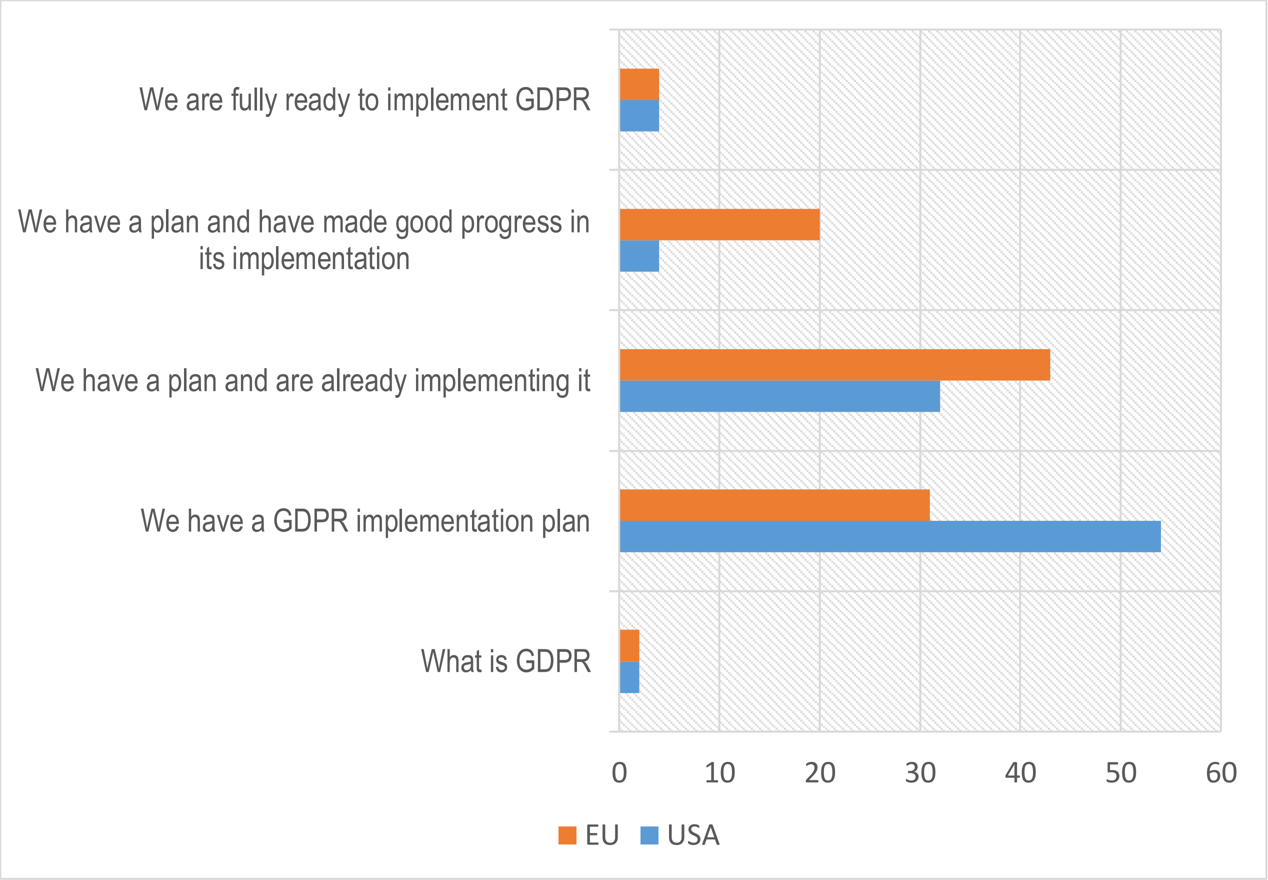

Fig. 1. Which of the following best describes your organization's preparation for the GDPR?

Companies have indicated the introduction of the regulation as a major problem, but the bad news is that nearly half of the respondents have not started implementing their GDPR implementation plans.

If we look at GDPR as another regulation that imposes restrictions, then its introduction will boil down to minimising possible penalties for non-compliance. This is a defence strategy and is not the best way to invest. At the other extreme is the understanding that GDPR is a tool for business growth and an opportunity to demonstrate trust and integrity to clients and partners. In this case, the winning strategy is to demonstrate compliance with the Regulation. In the light of these thoughts, the requirements of the Regulation should be imposed on the company's technology model by seeking to improve business outcome indicators.

3. DATA COVERNANCE

Over the past three decades, business development has been marked and driven by the concepts of Big Data, Data Analysis and the Internet of Things. Information has become "the new oil" and a company's operating model is the model of available data.

The recently coined term "mature organisation" refers to the achieved level of information aggregation and the technologies used for its processing. Data integration and information technology allow us to talk about a business management model called "Data Governance" (DG).

Data governance involves a set of processes that ensure that the company's information assets are handled throughout the enterprise according to a set of rules. These processes include planning, specifying, activating, creating, acquiring, maintaining, using, archiving, retrieving, controlling and cleaning data. Data governance is an indicator of the maturity of the organisation and can be viewed in a wider context both as the technologies used and a new organizational culture. [5]

The Data Governance Institute uses the following definition: "Data Governance is a system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models which describe who can take what actions with what information, and when, under what circumstances, using what methods." Data governance is a quality control discipline for assessing, managing, using, improving, monitoring, maintaining, and protecting information. [4] Data governance is a business quality control technology (Fig.2).

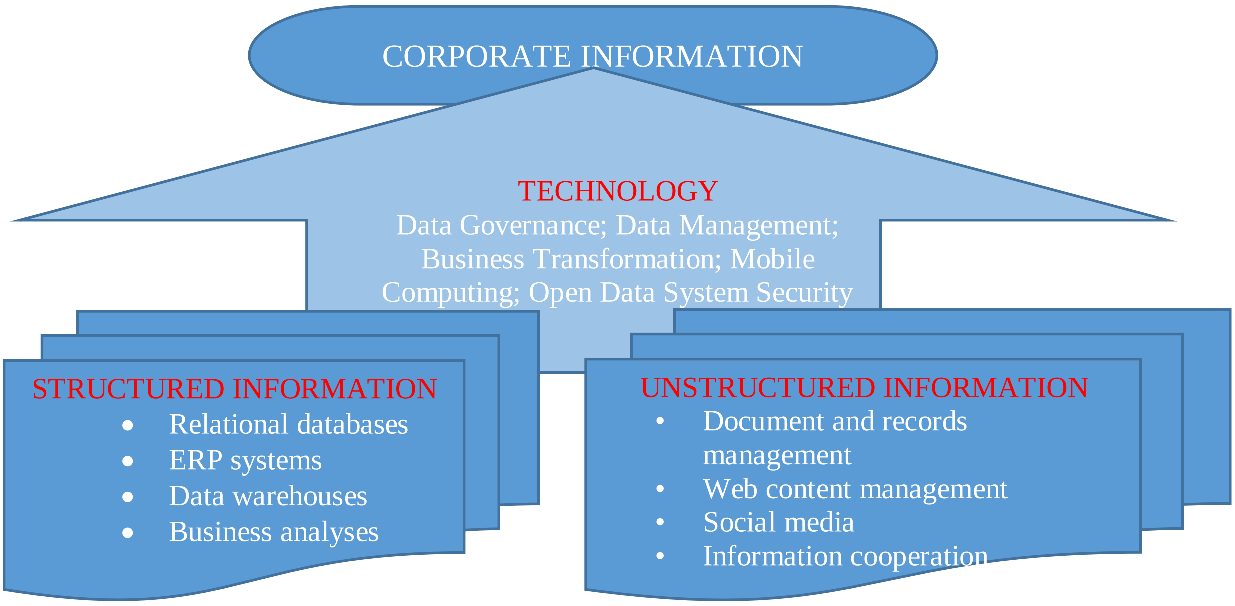

Fig. 2. Model of the corporate information in the Data Governance technology

DG can be used as the basis for building a system of rules for lawful processing and may include:

- Increasing confidence in decision making;
- Decreasing the risk of regulatory fines for non-compliance with statutory regulations;
- Improving data security for all processing operations;
- Accountability for data processing;
- A common understanding of processing among data controllers and supervisory authorities;
- Optimising employee performance;

On the other hand, the DG technology is based on change and risk management tools and programs. Some classical examples of the application of this technology are regulations such as the Sarbanes-Oxley act1, Basel I and II2, HIPAA3. Analysing the nature of the General Data Protection Regulation, we can safely put it among the items in the list above as potentially applicable to the DG technology [6].

The cross-cutting theme in each of these regulations is risk management as a departure from any particular regulation. The technology is aimed at improving data quality in terms of accuracy, accessibility, consistency and completeness. DG is usually based on a certain form of methodology for tracking and improving corporate data such as Six Sigma4 and data mapping, profiling, cleaning and monitoring tools. A fundamental requirement for data optimisation at departmental level is the elimination of inconsistent and redundant processes.

Data governance can also be seen as a balance between technology, use of data in a different way, protection, constant change, accountability and privacy. It is of paramount importance to any organisation, regardless of whether it is known as Data Governance, Information Resource Management, or Enterprise Information Management, and companies are becoming increasingly aware of the fact that the data they have available is a valuable asset that needs to be managed properly in order to achieve success.

In order to use DG, the organization must have capabilities in the following areas (Information Technology capabilities) [5] (Fig. 3)

[1] Sarbanes Oxley Act, section 404 – an act passed by the US Congress in 2002 in response to major accounting malpractice scandals with publicly traded companies - Enron, Worldcomi, etc.

[2] Recommendations to the banking legislation to implement banking systems based on risk assessment.

[3] The Health Insurance Portability and Accountability Act of 1996

[4] Six Sigma - a measure of quality that strives for near perfection. Six Sigma is a disciplined, data-driven approach and methodology for eliminating defects (driving toward six standard deviations between the mean and the nearest specification limit) in any process – from manufacturing to transactional and from product to service.

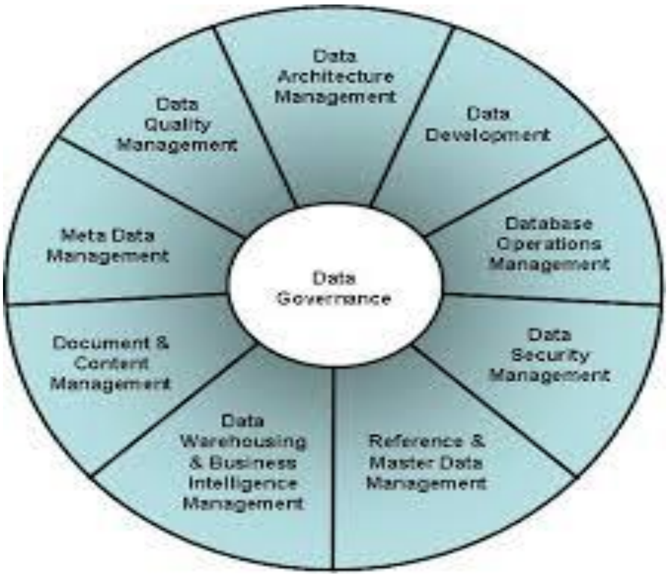
Data Architecture Management
Data Development
Database Operations Management
Data Security Management
Reference & Master Data Management
Data Warehousing & Business Intelligence Management
Document & Content Management
Meta Data Management
Data Quality Management
Data Governance

Fig. 3. Information Technology capability in Data Governance technology

Data Architecture Management: The development and maintenance of enterprise data architecture5 within the context of all enterprise architecture, and its connection with the application system solutions and projects that implement enterprise architecture.

Data Development: The data-focused activities, including data modelling and data requirements analysis, design, implementation and maintenance of databases.

Database Operations Management: Planning, control and support for structured data assets across the data lifecycle, from creation and acquisition through archival and purge.

Data Security Management: Planning, implementation and control activities to ensure privacy and confidentiality and to prevent unauthorized and inappropriate data access, creation or change. Building a monitoring system based on automatic logs and log records.

Reference & Master Data Management: Planning, implementation and control activities to ensure consistency of contextual data values with a “golden version” of these data values.

Data Warehousing & Business Intelligence Management: Planning, implementation and control processes to provide decision support data and support knowledge workers engaged in reporting, query and analysis.

Document & Content Management: Planning, implementation and control activities to store, protect and access data found within electronic files and physical records (including text, graphics, image, audio and video).

[5] Data that is shared by multiple enterprise systems regardless of the location of the system of initial entry. According to this concept, systems are not data owners, but merely define requirements for their quality. A new way of describing corporate data is also required – the concept of metadata is introduced.

Meta Data Management: Planning, implementation and control activities to enable easy access to high quality, integrated metadata.

Data Quality Management: Planning, implementation and control activities that apply quality management techniques to measure, assess, improve and ensure the fitness of data for use.

4. A TRADITIONAL INFORMATION ARCHITECTURE

Each area (information technology) can be described using the following elements: objectives and principles; organisational culture; roles and responsibilities; activities; techniques and practices; providers and users; tools. To sum them up even further, these descriptors can be narrowed down to only 3 – people, processes and technologies. [7]

A DG-based business organizational model is based on the following basic assumptions:

- a corporate data level has been reached;
- employees have standard roles with clearly defined rights and obligations;
- the data is accessed through applications commissioned by process owners and stakeholders;
- there is a system of policies and rules;
- all business processes are described as data streams;
- system adjustments are made on the basis of risk assessment and impact analysis;

Corporate data are structured in records that are consistent, free of redundancies, with a single source of authenticity, up-to-date, reliable and available.

We can divide the model into several steps:

- Data governance concept – the processes in the organisation are described on the basis of a business analysis. Objectives are defined for each process and the information flows are described. The processes are subdivided into sub-processes and data and then a process map is drawn up;
- Organisational structure of data governance – the relationship between processes and roles are described;
- Specifying Process Owners – rights and obligations in data exchange between processes.
- Detailing the processes – information necessary for the business. Definitions and metadata classification. Data quality requirements and data protection. People and activities supporting the process.
- Setting up data governance programs – procedures that provide businesses with the necessary information.

Using the steps mentioned above, each organisation can be described through: processes, roles, performance indicators, and development models. [9]

The processes are described in terms of input data (documents and plans), outputs (documents and products), business attributes (objectives, norms and standards), tools and techniques.

The roles are defined according to specific activities and include responsibility, preparation/accountability, consulting and information provision.

Objectives are set according to the SMART criteria (specific, measurable, achievable, realistic and timely) and the indicators. Regulations and industry standards are used as process input elements.

The formal description of a business process includes:

- Definition: Process description (knowledge).
- Objectives: Intended results.
- Process: A list of discrete activities and sub-activities to be performed with **indicators** for each group of activities.
- Input elements: What documents or raw materials are directly related and necessary to the commencement and continuation of the process?
- Roles
  - providers: roles and/or teams that provide process input data.
  - implementers: roles and/or teams that implement the process.
  - stakeholders: roles and/or teams that are informed about or consulted on the implementation of the process.
- Tools: The types of technology used by the process.
- Products: What is the direct process output?
- Users: Roles and/or teams that expect and receive the output.
- Measurement: quantifying process performances based on the objectives achieved.

After the business analysis has been made, the organisation can be presented using a DG model. (Fig. 4)

5. NEW INFORMATION ARCHITECTURE AFTER GDPR

The introduction of a new regulation such as GDPR will change the organisation because it changes the operating conditions. We can classify the changes according to type as follows:

- Changes to existing processes – in this case the regulation is introduced as an amendment to the input requirements for each process;
- Introduction of new processes – a review of the General Regulation has shown the need of programming new processes – notifications of system breaches, withdrawal of consent, etc.;

- Changes to the organisational structure – introducing new “players” both internal (data protection officer) and external (personal data owners and even entities that are not related to the organisation) to the organisation.

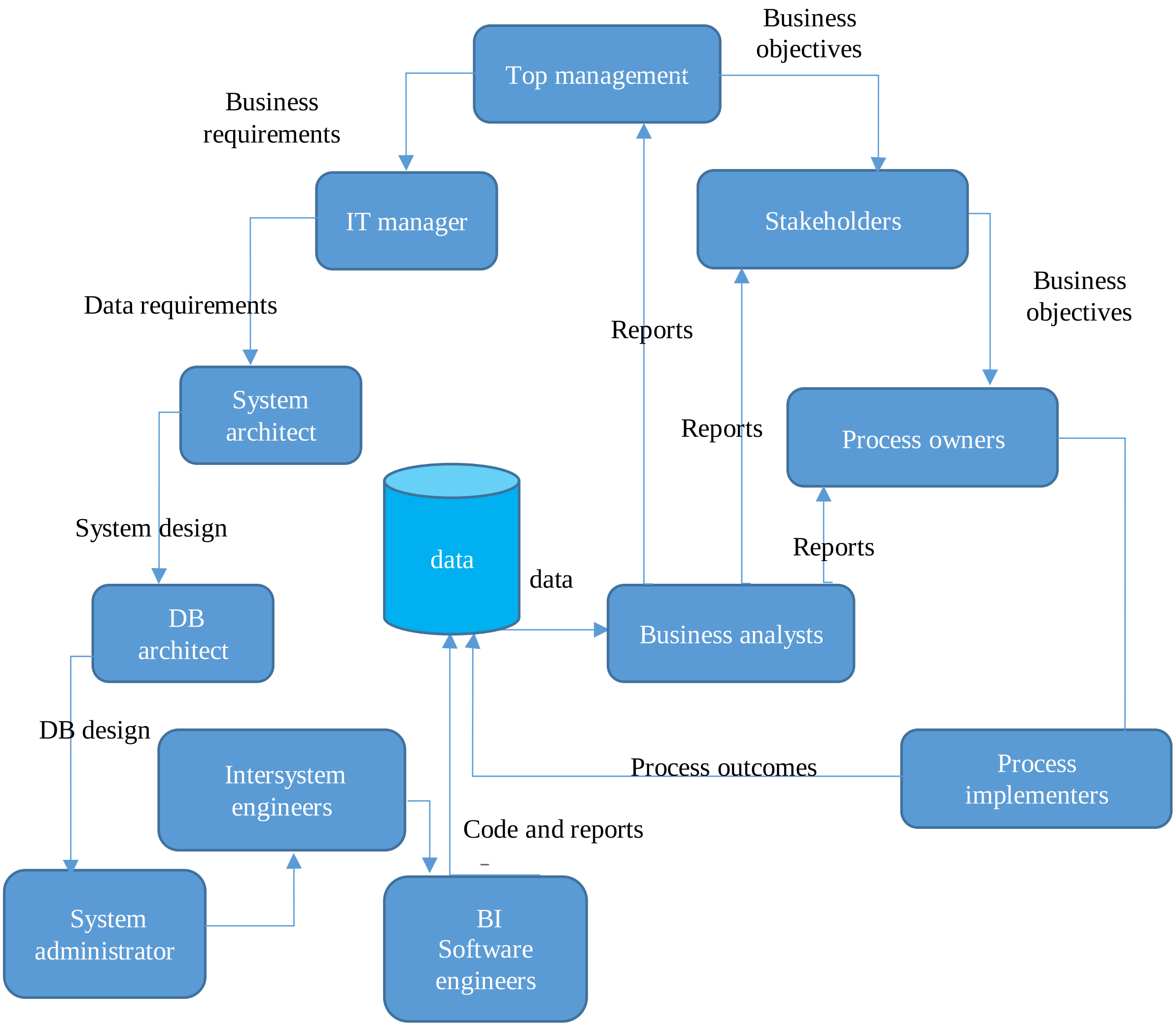

Fig. 4. Traditional Data Governance Model

The DG technology is a management technology that also allows change management. Hence, we have to follow the path known as “change implementation”:

- Business Analysis – reveals all business processes affected by the implementation of the regulation. Complete data inventory – special attention is given to storage locations, their type and their secondary use (for purposes other than that for which the data was collected). The regulation is drawn up as an amendment to the input requirements. The users’ rights for handling data and their roles in the organisational model are defined.
- Gap Analysis – new processes are revealed and designed. New players are introduced and the manner and format of interaction with

them are defined.

- Risk Analysis and Impact Assessment – the system operation rules are changed – new operating policies and procedures are introduced in the organisation. The final system state is described and the key performance indicators (KPIs) are set out.
- The organisation reaches a new sustainable position – a new, more mature operating model is introduced – the change is implemented.

The Data Protection Officer (DPO) has to be institutionalized based on the following assumptions [8] (Fig.5):

- DPO is independent, is delegated tasks and reports only to senior managers;
- DPO has access to the entire enterprise structure when performing his/her duties;
- DPO can be viewed as the owner of any process within the organisation and hence he/she can initiate a process change.

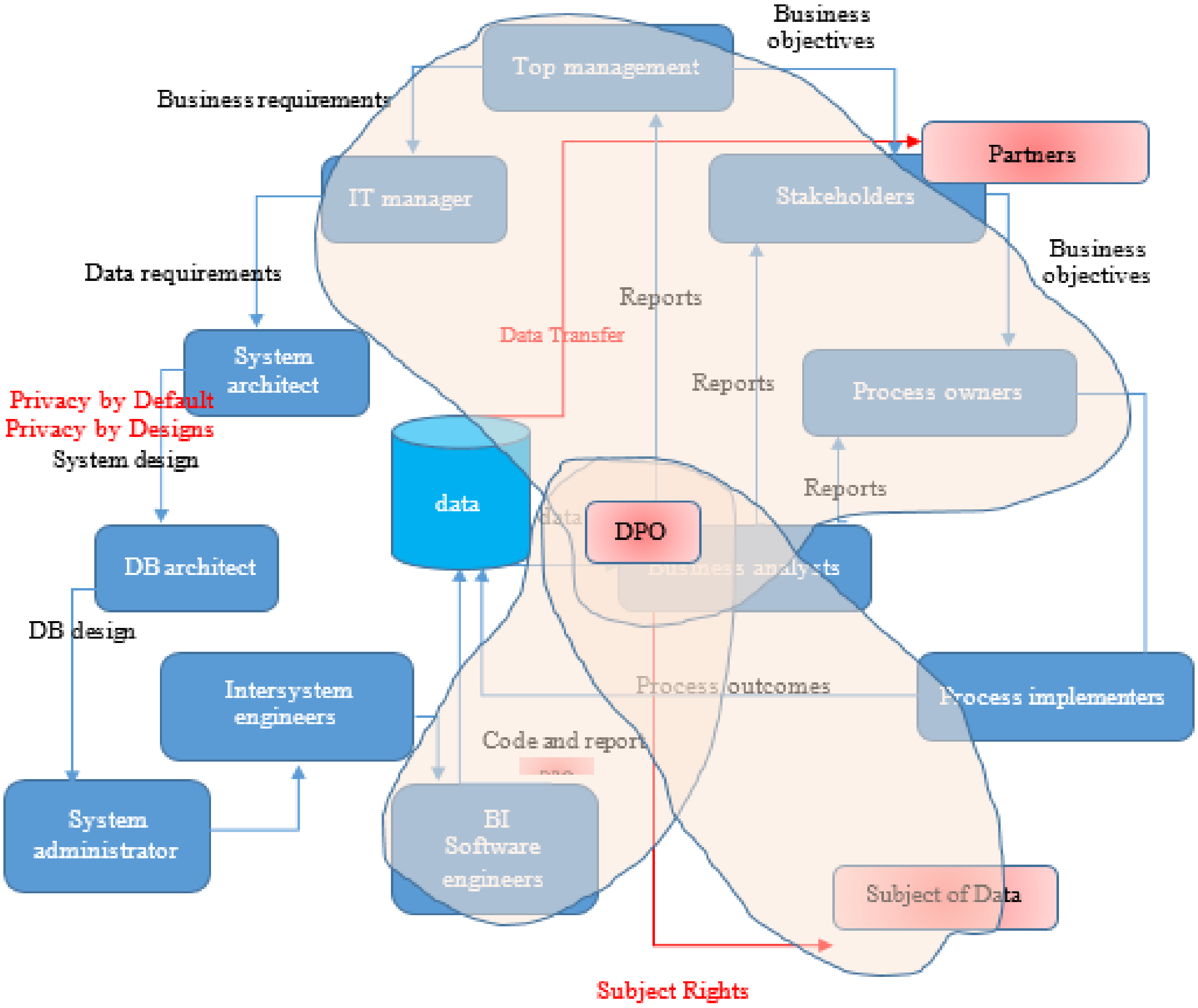

Fig. 5. New Data Governance Model with GDPR

6. CONCLUSION

The model improved in accordance with GDPR would have the following advantages:

- Data protection is institutionalized as a function of the senior management and the Data Governance Council, comprising senior management representatives overseeing DG programs;
- The Council appoints DPO to be the leading data protection business analyst and formalises his/her role and responsibilities in DG Technology. This ensures the introduction of new processes related to personal data protection;
- DPO works closely with the other business process owners and sales teams in order to ensure the legitimate secondary processing and visualisation of data;
- IT teams (system engineers, DB architects, and software developers) work under DPO's supervision. This involves introducing Master Data Management, Data Quality, Data Archiving, Privacy by Design and Privacy by Default principles as part of the technology used.
- The DG framework is amended in accordance with GDPR, but complies with leading business requirements;
- Data Stewards work with business and IT representatives, while adhering to the instructions of the Data Governance Council and DPO's guidelines;
- DPO works closely with the IT department in order to improve the Security Development platform and technology (processes for better quality, data accessibility and security)
- DPO works closely with all stakeholders in order to formalise business processes and change development trends in the form of recommendations to DG programmes.
- DPO informs the Data Governance Council on a regular basis of the status of the DG programmes.

The Council monitors the development of the DG programmes by proposing changes to the policies and procedures.

REFERENCES

[1] European Parliament, 2016, *Regulation (EU) 2016/679 of the European parliament and of the council of 27 April 2016on 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)* Official Journal of the EU, L119/1

[2] International Monetary Fund, Retrieved 12 October 2016", *Report for Selected Country Groups and Subjects"* , (available at www.imf.org.)

[3] IAPP-TRUST 2016 study on privacy practice, *Preparing for the GDPR: DPOs, PIAs and Data Mapping,* (available at www.iapp.org)

[4] Gwen Thomas The Data Governance Institute 2015 *the DGI Data Governance Framework*

[5] The Data Management Association 2014 *DAMA-DMBOK2 Framework*

[6] Microsoft, Trustworthy Computing, 2010 A Guide to Data Governance for Privacy Confidentiality and Compliance

[7] Santanu Guha, 2017 *Data Governance using Machine Learning*

[8] CRC Press, Paul Lambert, 2016 *The Data Protection Officer Profession, Rules and Role*

[9] Springer, Ammar Rayes Samer, Salam 2017 Internet of Things From Hype to Reality.