Journal scientific and applied research, vol. 18, 2020
International Journal

Original Contribution

ISSN 1314-6289

A PROPOSED METHODOLOGY FOR CONDUCTING DATA PROTECTION IMPACT ASSESSMENT AND RISK ASSESSMENT IN AN ORGANIZATION

Goran Prodanov

DEPARTMENT OF MANAGEMENT OF SECURITY SYSTEMS, FACULTY OF TECHNICAL SCIENCES, KONSTANTIN PRESLAVSKY UNIVERSITY OF SHUMEN, SHUMEN 9712,115, UNIVERSITETSKA STR.

E-MAIL: goranp@abv.bg

ABSTRACT: *Two years after the enforcement of the General Data Protection Regulation (GDPR) many organizations in Bulgaria are still experiencing problems with its implementation. Part of the reason is that there is a lack of methodological guidelines provided by the Bulgarian data protection authority (CPDP) on how to assess and manage the risk associated with the processing of personal data. Here is a basic structure of such methodology which can be used by organizations in the public and private sector alike. It is heavily influenced by the principles adopted by the French data protection authority (CNIL) which was the first to introduce such guidelines. The methodology can be implemented as is, or expanded according to the specific organizational needs.*

KEY WORDS: *Personal Data, GDPR, Risk Management, Risk Assessment, Data Protection Impact Assessment.*

1. Introduction

This paper aims to provide a unified approach to data protection risk management, including the identification, assessment and control of risks (potential events or situations) that could threaten the rights and freedoms of individuals in regards to their personal data. Data protection risk management is a structured, consistent and continuous process that should be an integral part of the senior management of every organization, regardless of its sphere of activity. Applying such an approach enables the organizations to manage the risk by identifying, assessing and controlling potential events or situations that may adversely affect data subjects and limiting the likelihood of such events / situations occurring. It is a “continuous improvement process” and as such “it sometimes requires several iterations to achieve an acceptable privacy protection system” [1].

The main objectives of the risk management process are the timely detection and counteraction of significant risks for the organization, the extraction of preliminary information on possible methods to reduce the negative impact and the likelihood of risks and the implementation of technical and organizational measures tailored to the degree and significance of the various risks.

The requirements and provisions of Regulation (EU) 2016/679, also known as the General Data Protection Regulation (GDPR) and the Personal Data Protection Act of the Republic of Bulgaria have been taken into account when developing this methodology, which consists of five stages shown below.

2. Defining the personal data processing operation and its context

This stage is the starting point in the risk assessment and is fundamental for the data controller in defining the scope of the personal data processing operation, subject of the assessment. In order to standardize the process of defining the personal data processing operations, the following set of questions has been developed:

- *What types of personal data are processed?*
- *What is the purpose of the processing?*
- *What are the means of the processing?*
- *Where does the processing of personal data take place?*
- *What are the categories of data subjects?*
- *Who are the recipients of personal data?*

While answering these questions, organizations should also take into account the different stages of the processing of personal data – collection, processing, transfer, storage and destruction. Some experts in the field give an even broader meaning of the term “processing” and consider it as “any operation or set of operations carried out with personal data by automatic or other means such as collecting, recording, organizing, structuring, storing, adapting or modifying, retrieving, consulting, using, disclosing by transmission, dissemination or otherwise making the data available” [2].

3. Data protection impact assessment

Based on the analysis performed in the previous stage, the data controller should assess the impact on the rights and freedoms of data subjects in the event of a breach of personal data security. Four impact levels (Low, Medium, High and Very High) have been proposed, as shown in the following figure:

Impact Level	Description
Low	It is possible that data subjects will encounter some minor inconveniences that they would overcome without a problem (time lost, irritation, etc.).
Medium	Data subjects may face significant inconveniences that they will be able to overcome despite some difficulties (additional costs, difficulty to access services, fear, misunderstanding, stress, minor physical ailments, etc.).
High	Data subjects may face significant consequences that they should be able to overcome, albeit with serious difficulties (misappropriation of funds, property damage, job loss, deterioration of health, etc.).
Very High	Data subjects may experience significant or even irreversible consequences that they may not be able to overcome (inability to work, long-term psychological or physical ailments, death, etc.).

Fig. 1. Impact Levels

The impact assessment is a qualitative process and the data controller should take into account a number of factors such as: the types of personal data processed; the need to perform the processing activity; the volume of personal data; special characteristics related to the activity of the data controller, as well as special categories of data subjects.

In Article 32 of the GDPR three objectives are mentioned that must be achieved and taken into account when processing personal data. They are *confidentiality, integrity* and *availability* [3]. Figure 2 could be used to assess the impact if any of the above objectives are violated.

№	Objectives	Result
1	Please assess the impact on data subjects of the improper disclosure (**confidentiality breach**) of personal data in the context of your activities.	○ Low ○ Medium ○ High ○ Very High
2	Please assess the impact on data subjects in the event of an unlawful change (**integrity breach**) of personal data in the context of your activity.	○ Low ○ Medium ○ High ○ Very High
3	Please assess the impact on data subjects in the event of unlawful destruction or loss (**availability breach**) of personal data in the context of your activity.	○ Low ○ Medium ○ High ○ Very High

Fig. 2. Impact assessment

Following this assessment, the different impact levels (in case of breach of confidentiality, integrity and availability) will be derived. The highest of these levels will be considered as the final result of the impact assessment for the respective personal data processing operation.

4. Defining possible threats and assessing their likelihood

At this stage, the task of the data controller is to identify the threats (external and internal) related to the general environment for personal data processing and to assess the likelihood of their occurrence.

In order to standardize this process, a number of questions have been proposed that aim to characterize the data processing environment that is directly related to the threats. They relate to four main dimensions (assessment areas) of the environment, namely:

- Network and technical resources (hardware and software);

- *Is any part of the processing of personal data carried out via the Internet?*
- *Is it possible to provide access to an internal system for processing personal data via the Internet?*
- *Is the personal data processing system connected to another external or internal IT system or service?*
- *Can unauthorized persons easily access the personal data processing environment?*

- Processes / procedures related to the personal data processing operation;

- Are the roles and responsibilities regarding the processing of personal data clearly defined?

- Are the rules for the use of the network, the systems and the physical resources of the organization clearly defined?

- Are employees allowed to carry and use their own devices to connect to the personal data processing system?

- Are employees allowed to transfer, store or otherwise process personal data outside the premises of the organization?

- Third parties involved in the personal data processing operation;

- Is the processing of personal data carried out by an indefinite number of employees?

- Is any part of the personal data processing operations carried out by a third party (Data Processor)?

- Are the obligations of the parties / persons involved in the processing of personal data clearly defined?

- Are the employees involved in the processing of personal data aware of the issues related to information security?

- Do the parties / persons involved in the processing of personal data follow the best practices in the storage and / or destruction of personal data?

- Sphere of activity and scale of processing.

- Is the sphere of activity prone to cyberattacks?

- Has the organization suffered a cyberattack or other type of security breach recently?

- Does the processing operation involve a large number of persons and / or personal data?

- Are there industry-specific security best practices that are not adequately followed?

Following this approach, the likelihood of threat occurrence can be defined for each assessment area as follows:

- Low - the threat does not seem likely to materialize;
- Medium - it seems difficult for the threat to materialize;
- High - there is a certain probability that the threat will materialize;
- Very High - there is a high probability that the threat will materialize;

Figures 4 and 5 below can be used to document the likelihood of threat occurrence for each assessment area and thus to derive its final value.

Assessment Area	**Likelihood**	
	Level	**Result**
Network and technical resources (hardware and software)	○ Low	1
	○ Medium	2
	○ High	3
	○ Very High	4
Processes / procedures related to the personal data processing operation	○ Low	1
	○ Medium	2
	○ High	3
	○ Very High	4
Third parties involved in the personal data processing operation	○ Low	1
	○ Medium	2
	○ High	3
	○ Very High	4
Sphere of activity and scale of processing	○ Low	1
	○ Medium	2
	○ High	3
	○ Very High	4

Fig. 4. Assessment of the likelihood of threat occurrence by areas

Overall result from Figure 4	**Likelihood level**
4 – 5	Low
6 – 10	Medium
11 - 14	High
15 - 16	Very High

Fig. 5. Likelihood of threat occurrence level

The likelihood of threat occurrence is derived after summing the four results obtained from Figure 4 which are then associated with the indicative values in Figure 5.

5. Risk assessment

After assessing the impact level of the personal data processing operation and the respective likelihood of threat occurrence, the final risk assessment can be started. As shown in Figure 6 the risk level is categorized as low, medium, high and very high.

Risk Level	Risk Factor
Very High	16
High	8 – 15
Medium	4 – 7
Low	1 – 3

Fig. 6. Risk categorization

The risk level can be defined as a result of the combination of the impact level and the likelihood of threat occurrence and reflects its overall importance in terms of the rights and freedoms of data subjects. It can be represented through the use of the so-called risk matrix shown in the figure below [4]:

		Likelihood of threat occurrence (P)			
Impact Level (S)	4 Very High	4	8	12	16
	3 High	3	6	9	12
	2 Medium	2	4	6	8
	1 Low	1	2	3	4
		1 Low	2 Medium	3 High	4 Very High

Fig. 7. Risk matrix

The assessment of the identified risks in terms of likelihood and impact level is made on a four-point scale from 1 to 4, with 1 being the lowest value and 4 being the highest value.

The risk factor is calculated by the following formula:

P x S = V, where:

P - Likelihood of threat occurrence (1-4);

S – Impact level (1-4);

V - Risk factor (P x S).

6. Risk response

Once the risks have been identified and their likelihood and severity have been assessed, an appropriate response should be considered. Taking measures and actions to respond to the identified and assessed risks is a very important stage of the risk management in general.

The following response options are possible:

- *Risk mitigation* – this is the most common reaction that the data controller should apply. The reason for this is that the risk can rarely be completely avoided. Therefore, technical and organizational measures should be taken to provide reasonable assurance that the risk is limited to acceptable parameters. The risks subject to this response should be monitored periodically;
- *Risk tolerance* – such a response is possible if certain risks have a limited impact on the rights and freedoms of data subjects or if the costs of taking action are disproportionate to the potential benefits. In these cases, the reaction may be to tolerate the risks. However, such risks must be constantly monitored. It is possible that various external or internal factors affect the likelihood and severity and shift the risk to another higher category;
- *Risk termination* – some risks can be limited or reduced to an acceptable level only by terminating the processing operation. However, this is the least common reaction, because in the public sector, the possibilities for terminating an operation are very limited. A significant part of the activities carried out are determined by government policies, laws and regulations.

The risk assessment plays a key role in selecting the appropriate risk response. Given the fact that the characteristics of the risk may change in time, a subsequent review of the risk may be conducted and therefore the determined response may be changed.

References:

[1].https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf (Accessed: 15 June 2020)

[2]. Krasteva, D., Andrey, A., Zashtita na lichnite danni – misiya vazmozhna, Rezon – Bulgaria, Sofia, 2018

[3].European Parliament and Council of European Union (2016) *Regulation (EU) 2016/679. Available at:* https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN (Accessed: 15 June 2020)

[4].https://www.microtool.de/en/knowledge-base/what-is-a-risk-matrix/ (Accessed: 15 June 2020)