VOICU FILIPESCU
Attorneys at Law
News in Laws – Legal Monthly Newsletter
February 2018

cover article

Data Protection Impact Assessment (DPIA) according to GDPR - a practical approach

After having dealt with a problem of practical interest for companies in the December 2017 issue of our newsletter in terms of GDPR requirements, we intent to cover in this article another topic of major interest for companies: when must they assess the impact of their processing of personal data activities and, if so, how do they make this assessment?

What is DPIA, when is it necessary, and why?

The Data Protection Impact Assessment, also known under the **DPIA** acronym, is a mandatory requirement under GDPR under Article 35 and will apply only to processing operations to be initiated after May 25, 2018.

Specifically, DPIA allows organizations to explore how a particular project or a particular system involving personal data processing activities will affect the right of data subjects to protect their data. In particular, a type of processing involving the use of new IT technologies (e.g. in the case of a new IT system for storing and accessing personal data, or using existing data for a new and more intrusive purpose) but also the nature, purpose and the context of a processing activity may result in a high risk for the rights and freedoms of individuals. A single assessment may address a set of similar processing operations that present similar high risks.

Performing an impact study such as DPIA should not be a lengthy or complex process, the following containing a set of practical guidelines to perform such a process.

What are the minimum aspects which a DPIA must include?

DPIA must include at least:

- a description of the envisaged processing operations and the purposes of the processing;
- an assessment of the necessity and proportionality of the processing;
- an assessment of the risks to the rights and freedoms of data subjects.

The measures envisaged to:

- address the risks;
- demonstrate compliance with this Regulation.

DPIA-related responsibilities

The obligation to make the DPIA is provided by the GDPR under the responsibility of the controller, and the latter must involve its Data Protection Officer (DPO) and Chief Information Security Officer (CISO), but it is advisable for the controller to obtain the opinion of independent experts in various fields (IT, security, law, sociology, ethics, etc.).

Generally, responsibility for the data protection impact assessment belongs to the Controller's Information Owners, notably human resources, marketing, information security, but is not limited to them.

In practice, it will be useful for organizations to prepare methodologies for the DPIA, to be disseminated by the Information Owners.

Is a DPIA necessary for every project?

There are no provisions in the GDPR that expressly and limitingly determine where the DPIA is required. As a matter of principle, a DPIA will be needed where the processing project has a very broad purpose or uses information that is likely to create a **high risk** for the rights and freedoms of individuals or where new and intrusive technologies are used, or when private or sensitive information is used in a new and unexpected manner.

In assessing the risk, it is considered that where the benefit or need for processing is greater, the risk associated with the processing will be higher.

Article 35 of GDPR highlights only some situations where DPIA is mandatory. For example, when processing a wide range of special categories of data, or any personal data related to criminal or minor offenses. Furthermore, if processing is based on an automatic decision-making mechanism, including profiling, the DPIA will be required. The last case under Article 35 is the systematic monitoring of a large scale accessible area (entry into a company with very many employees).

However, if the processing of the data does not endanger the rights and freedoms of individuals or if it has already been authorized for similar operations then DPIA will not be necessary. The same is true if there is a legal basis in EU or Member State law.

The first steps to identify whether a DPIA is necessary

Organizations asking whether or not a particular personal data processing project will require DPIA will have to answer the following set of questions:

- what kind of data do we have?
- do we really need all this data?
- how do we use the data we have?
- which risks arise from processing this data?
- how we can minimize these risks?

A preliminary analysis of the need for DPIA can be made on the basis of the processing registry you have already prepared on the basis of GDPR.

Why should one perform a DPIA?

- to identify the risks that might arise on the protection of citizens' private data;
- to identify the degree of compliance with data protection obligations;
- to protect the reputation of the organization;
- to inspire public trust in one's product/project;
- to avoid expensive claims for damages later on.

When should one start a DPIA?

DPIA is an effective way to protect against risks when made at the early stages of the project, namely when:

- the project is in the creation stage;
- you know what you want to do;
- you know who will be involved in the project.

But the DPIA must be finalized before:

- the decisions on the processing of personal data are final;
- the computer systems are purchased;
- the contractual agreements are finalized by signing a legal commitment;
- you lose the possibility to change your mind.

If you have made the DPIA and is showed that the risk is low, processing can begin and it will periodically be reassessed if changes occur.

If the processing risk has been identified as high or if it is not clear that a DPIA is required, you have two options:

- don't start the processing;

- consult the supervisory authority before proceeding with any processing activities. Together with the authority, you will be able to find the risk minimization solution (technical and organizational measures) and implement it. Processing can start and can be periodically reviewed if changes occur. If you do not find remedies with the authority - you will not start processing or significantly alter your processing.

It is to be expected that the nation supervisory authorities draft and publish a list of the types of processing activities subject to the DPIA requirement, and a list of processing activities for which DPIA is not necessary.