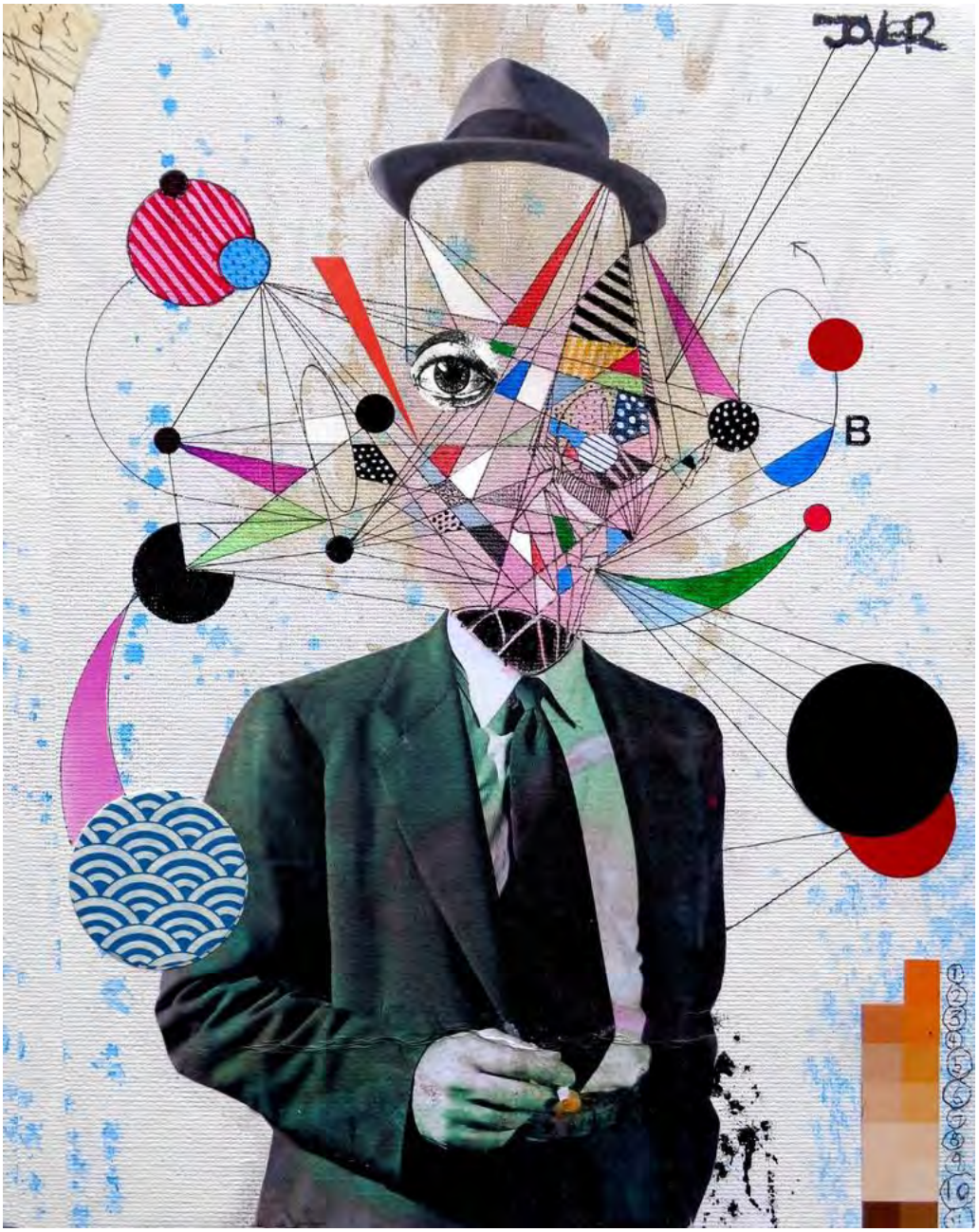
ARETI CHARIDEMOU

March 2022



Data Protection Impact Assessment ("DPIA")

A legal obligation and the benefits

Failing to carry out a DPIA or conducting a DPIA in an incorrect manner can lead to fines up to €10.000.000 or, if it's company to be penalized, the fine may be up to the 2% of the total worldwide annual turnover of the previous financial year. Therefore, complying with Article 35 of the Regulation is of vital importance for most business activities.

What is a Data Protection Impact Assessment and How a DPIA is conducted?

Data Protection Impact Assessment (DPIA) is a self - monitoring process designed to identify potential risks relating to the rights and freedoms of natural persons/ individuals, which occur from processing their personal data and preparing a relevant report. Conducting a DPIA diminishes the Regulatory Authority's workload since all the information needed can be found within the relevant report. In this way, the Regulatory Authority obtains a wider overview of the data and simultaneously a DPIA/ the project eliminates unnecessary data collection and processing.
Furthermore, when it comes to specific categories of data, the processing is mandatory/ compulsory, especially when used automated decision-making processes or by extensive use of technological means. For example, it is mandatory when:

- There is use of CCTV system (security cameras),
- A hospital is processing health and genetic data
- There is a banking system for categorising customers

The compliance with a DPIA process is not only an organisation's obligation (Data Controller), but it is also a useful tool that benefits both the Regulatory Authority, and the company to carrying it out, ~~since~~ as it identifies loopholes and omissions. Additionally, it is extremely beneficial to the Data Controller/Processor, as it allows taking proper measures and avoiding sanctions by identifying the risks ~~identified~~, e.g. a possible leakage and omissions. Additionally, compliance with the DPIA is significant not only to avoid the pre – mentioned fines, but more importantly to retain and empower the organisation's reputation aiming to operate in a professional manner. In general, it is hard to identify omissions and loopholes. However, by conducting a DPIA these omissions and loopholes are not only easily spotted, but also it provides ways of dealing with such issues, especially if it is done under the supervision and guidance of a GDPR specialist.

What should be included in a DPIA report to be considered satisfactory and how can we ensure that those requirements are met?

These two key questions need to be clarified before conducting a DPIA. First and foremost, a duly prepared DPIA report clearly points out the reasons of conducting an impact assessment, as defined in Article 35 of the Regulation. Then, it should ~~be~~ describe~~d~~ in full detail which processing procedure has been followed, the types of data involved, the categories of individuals whose data have been processed and the extend of this processing. Also, a properly prepared DPIA report has to mention by whom it was carried out and what was the purpose of the processing.

It is important to clarify the purpose of the processing. ~~In~~ this way, the question of whether such processing is necessary for an organisation is automatically answered and it Is clarified whether the processing is necessary to achieve the Controller's purpose or whether there are other ways of achieving that purpose. In addition, the report should focus on the legitimate interest pursued by the controller and explain whether or not the processing constitutes a legal obligation. Also, it is necessary before conducting a DPIA to consider whether the processing is proportionate to the pursued purpose. In other words, the reports should point out whether this type of processing is necessary and appropriate or whether it could be avoided.

Moreover, a proper DPIA report analyses all the risks arising through/from the processing, specifically risks that may affect the rights and freedoms of the individuals. At this point it has to be highlighted that it should mention not only the existing risks but also the potential ones.

Lastly, before the final assessment, after having analysed the existing protection measures, it should propose additional measures to address the risks that has been identified. As already stressed out, the purpose of conducting a DPIA is to identify all risks in order to prevent them, either by proposing measures as safeguards or by concluding that treatment/ the processing is not feasible.

In conclusion, the legal obligation to carry out a DPIA promotes data security and enhances the control of business activities by reducing risks that could be fatal to the business.

ARETI
CHARIDEMOU

Areti Charidemou & Associates LLC

21 Vasili Michailidi Str.
3026, Limassol, Cyprus
P.O. Box 54708, CY-3727

T: +357 25508000
F: +357 25508032

E: www.aretilaw.com