Data Protection Impact Assessment - an integral component of a successful research project from the GDPR point of view

Gizem Gültekin Várkonyi  
 University of Szeged  
 Szeged, Hungary  
 gizemgv@juris.u-szeged.hu

Anton Gradišek  
 Jožef Stefan Institute  
 Ljubljana, Slovenia  
 [anton.gradisek@ijs.si](mailto:email@email.com)

ABSTRACT

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

*Information Society 2020, 5–9 October 2020, Ljubljana, Slovenia*

© 2020 Copyright held by the owner/author(s).

Past years have seen rapid advances in the field of harnessing the ICT to tackle several medical problems. The field of research was busy, with research projects sprouting up combining artificial intelligence and algorithmic decision making systems, smart sensors, and data mining approaches to generate new knowledge about diseases. These systems are being developed for better management of chronic diseases, and to assist the elderly with independent living. While the algorithms themselves can be developed using anonymized or synthetic data, conducting a pilot study is often one of the key components of a research project, and such studies unavoidably involve actual users with their personal data. In the EU where the AI researchers, including the computer scientists and engineers, are obliged by the General Data Protection Regulation rules, may not always be fully familiar with the details of the GDPR, a close collaboration with a lawyer specialized in the European data protection legislation is highly beneficial for the success of a project. In this paper, we outline some concepts that the researchers should be aware of through a study pointing to a practical guideline to conduct a self- Data Protection Impact Assessment.

KEYWORDS

data protection, impact assessment, GDPR, Artificial Intelligence, medical data

1. Introduction

We can look at artificial intelligence (AI) dealing with personal data from two different perspectives. On one hand, it offers great benefits for the users, developers, and researchers, if used correctly. For example, AI-enabled health care technologies could predict the treatment of diseases 75% better and could reduce the clinical errors 2/3 at the clinics using AI compared to the clinics that do not [1]. On the other hand, the improper handling of personal data can quickly lead to abuse, sharing sensitive information, or other problems (unwanted data disclosure, complex and costly legal procedures, high number of fines, etc.), therefore it has to be handled with the utmost care. In this paper, we will focus on legality of medical applications containing personal sensitive data, such as the analysis of sensor data to help patients with chronic diseases manage their condition and improve the quality of life, or to help the elderly with independent living by providing safety features and improved communication channels.

Developing a product for a target population, for example people with diabetes, chronic heart failure, obesity, dementia, skin cancer, etc., typically starts with a research project, either in a company or within a consortium of research institutions and hospitals. One of the key components of such a project is collecting substantial amounts of data in a pilot study, with participants that resemble the target audience for the final product. When planning the pilot study, researchers enter a slippery terrain of dealing with personal data, as the participants are providing their own data for the purpose of the study. For an illustration, we can imagine a project where we collect medical data of three types; general medical data provided by the medical doctor responsible for the participant, lifestyle data collected by either wearable or stationary sensors, and self-reported data that is obtained via questionnaires that the participants fill.

Right to data protection is one of the fundamental rights recognized in most of the European legislation, mainly in the Charter of Fundamental Rights and the General Data Protection Regulation (GDPR). The GDPR entered into force on the 25th of May 2018 replacing the Directive 95/46/EC with two aims: ensuring uniform data protection rights and rules EU-wide and towards data controllers and keeping up with the technological developments challenging efficient protection of personal data [2]. The effect of technology pointed out the need for more proactive ways to safeguard right to data protection and the GDPR mirrored this need by introducing a risk-based approach entrusted in the Article 35 of the GDPR introducing the Data Protection Impact Assessment (DPIA). As such, DPIA ensures data controllers comply with the GDPR requirements especially at an early stage of a new project. Those requirements could be specific to the right to data protection introduced in the GDPR such as the Article 25-Data Protection by Design, or to general principles that have already existed in European data protection legislation such as the principle of accountability. In fact, DPIAs are one of those ways for materializing and ensuring the accountability principle which has always been a legal compliance element and is now being utmost challenged by the risks deriving from the new technologies, such as AI [3].

Regulation of AI indeed has been fulfilling the EU institutions’ agenda during the last couple of years. For example, the European Commission generated several policy papers pointing to the regulation of AI based systems [4] [5] which focused on the importance of system design that should be human-centric and trust-gaining. The policy papers summarize the data protection and privacy concerns as a problem and suggest that legal compliance together with ethical system design is at the utmost importance to gain trust of AI users which then could boost the AI developments in the EU. The DPIA requirement embedded in the GDPR is such a tool that could be used as a proof before the users to gain their trust towards the AI system. For this reason, we think that the DPIA is an essential requirement to be fulfilled for any AI project, if the project stakeholders aim at fulfilling both legal compliance and gaining user trust. However, there is no standard set for conducting a DPIA by the law-maker, as well as there is a lack of experience in practice since the GDPR is quite a young legislation. Specific to the AI driven research project, there are few examples existed in the literature illustrating a DPIA implementation, if none. In this paper, we discuss some of the aspects of DPIA that the researchers should have in mind while working on a research project.

1. Data Protection Impact Assessment in the GDPR

Article 35 of the GDPR does not provide an explicit description for the DPIA, however, Article 29 WP’s guideline on the DPIA provides the following definition:

*“A DPIA is a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data.”*

According to this definition, and in a narrower sense, the DPIA is a process consisting of several other sub-processes to describe the risks and assess the legality of the system in terms of data protection. These risks could be related to system security, system design, implementation, administration and development on a further run. The aim of the DPIA is to take appropriate safeguards to minimize the risks, if impossible to eliminate all. DPIA is not a simple one-time reporting activity, it is an ongoing process that should be continuously carried out during the lifetime of a project, therefore DPIA should always be monitored and updated [6].

It is the data controllers’ responsibility to convey a DPIA, but in fact, the GDPR does not assign them an obligation to carry out a DPIA for every data processing activity. DPIA should be carried out when the data processing activity is likely to constitute a “high risk” to the rights and freedoms of natural persons (e.g. users of an AI service who both benefit from the service and contribute to it with their data), as the Article 35 (1) refers. How to decide whether a certain data processing activity would be resulting in a high risk is not an easy task, but there are several guidelines and list of processing requiring DPIA published by the National Supervisory Authorities [7]. These lists could be the first sources for the data controllers to decide about the necessity of the DPIA for a certain project [8].

After determining the necessity to conduct a DPIA, the next step should be assessing the severity and likelihood of the risks which would come forward based on the data controller’s own assessment. Although there is no standard specified for how to convey a DPIA, failure to conduct a right assessment raises a risk for the data controllers; they may face several sanctions, especially financial penalties. Apart from that, conducting a right DPIA would be beneficial for the data controllers not only from the legal and the financial point of view. Wright [8] lists these benefits and refers that a DPIA could help data controllers to avoid implementing irrelevant solutions from the beginning of the project which may refer to assessing the technical feasibility of the system in parallel with the legal compliance. Therefore, the DPIA could help data controllers to save time and money. It also prevents the companies from losing their reputation (or from the scandals, as such occurred with the Cambridge Analytica (or, Equifax, Facebook, etc.). Finally, a DPIA document can be a trustworthy source which could be used as evidence before the public, as well as the related authorities, to prove the data controller's respect to privacy and right to personal data protection.

When planning a research project, the DPIA shall not be conducted neither after launching nor during the implementation in order to ensure proactive measures. Specific to the medical applications referred to in the present article, the DPIA should be conducted based on two legal obligations as provided for by the GDPR. Firstly, the Article 35 (3) point (a) of the GDPR clearly indicates that those data controllers that are using automated tools to evaluate personal aspects of natural persons, including profiling, are required to conduct a DPIA. Secondly, as the (b) point of the said article indicates, processing special categories of data also requires data controllers to conduct a DPIA. Medical data that will be evaluated in the project is classified under the GDPR as special data categories. Furthermore, a medical project focuses on developing an AI-based system includes an automated decision making system (the AI software itself together with the algorithms to be developed) with profiling tools (surveys and hardware equipment). Based on these statements, it is clear that a DPIA must be conveyed by the data controller to see the risks and safeguard these risks in line with necessary tools. These tools might be either organizational or technical tools that could help mitigating the risks.

1. Preparing the DPIA

The algorithm planned within the AI based medical software project is going to enable collecting data subjects’ sensitive data based on profiling and processing that data. In addition, a large amount of data will be collected for feeding the algorithm conveying a risk for data subjects, basically, the data subjects may lose significant control of their own data stored and processed by the AI system. Based on these inputs, the project may reveal risks for rights and freedoms of the data subjects involved, if these risks are not mitigated.  Therefore, it is a clear obligation for the data controller to conduct a DPIA and identify the risk categories with the planned mitigations when necessary. The following part shall present an assessment part of the actual DPIA since we skip the preparation phase of a regular process which includes planning, document collection, consultations with the stakeholders, etc. [6], which is not of particular interest for this paper. We identify three specific assessment procedures to be taken into account during the preparation of a DPIA.

1. The first part of the DPIA is the Data Specific Assessment (DSA). The DSA is the procedure where the data to be used in the AI project should be introduced very specifically in order to comply with the basic rules of the GDPR, mainly, the purpose limitation, transparency, accuracy, data minimization, and consent. It should be kept in mind that one of the requirements to be ensuring a valid consent is identifying the concrete data list, together with the planned processing activities of that data in the frame of a research project. Information serving to identify the data controllers or processors are the natural elements of the DSA.
2. Next, the Data Subject Specific Assessment should explain all the details of how the data controller ensures the rights of the data subjects and protects their informational self-determination right. The key point in this assessment is to gain trust of data subjects as required by law and ethics. One of the key aspects here is to make sure that the data subjects are familiar with the ways their data will be used, that they can request the removal of their data if so desired, and that they have a certain access to the decisions made by the algorithm about them. The latter point is to some degree complex. Classification models based on decision trees are easily comprehensible to humans. On the other hand, models that are based on complex multilayer neural networks are essentially black boxes where it is not possible to determine why a particular decision was reached based on easily interpretable rules. The social implications of such decision-making are an interesting field of research on its own. Finally, the system should offer tools for the data subjects to keep the data accurate and to block third party access, as the two rights provided by law.
3. The Project Specific Assessment is the last part of the DPIA, presenting and explaining the legal basis for data processing, the project partners including the data controller, and the security measures that will be implemented to safeguard the data processed during the project. As the project likely deals with sensitive medical data, security protocols have to be elaborated, which include proper hierarchy regarding the data access, encryption algorithms, regular security updates, and physical access to the hardware where the data is stored.

The final but an ongoing phase of the DPIA is the monitoring phase. Whenever there is a new element embedded in the project, and this element seems to change the balance of the risks earlier assessed, the DPIA should be reviewed. This element could be involving a new data type in the algorithm or planning a commercial use of the algorithm. Bearing in mind the fact that ML and algorithms are referred to as entirely new technologies [3] and the growing amount of data together with a variety of hardware would raise the privacy risks [9], we suggest the project team to review the DPIA periodically.

1. Conclusion

Data Protection Impact Assessment is an integral part of any research project focusing on development of an AI algorithm with personal data. It should be conducted in the planning stage of the project and occasionally reviewed once the project is ongoing. This way, the project team, otherwise called data controllers, are able to identify the potential risks and find mitigation strategies for certain weak points. Last but not least, by conducting the DPIA, the project team fulfills the legal requirements, ensures higher trust of people involved, and avoids unforeseeable problems that might later occur.

ACKNOWLEDGMENTS

This work was supported by the ERA PerMed project BATMAN, which was financed on Slovenian side by the Ministry of education, science, and sport. An extended version of this paper was submitted to journal Informatica.

REFERENCES

1. “The AI effect: How artificial intelligence is making health care more human”, [Online], study conducted by MIT Technology Review Insights and GE Healthcare, 2019. Accessed from: <https://www.technologyreview.com/hub/ai-effect/> Last accessed: 20 April 2020.
2. EDPS (2012). “Opinion of the European Data Protection Supervisor on the data protection reform package”, (7 March 2012).
3. ICO (2018). Accountability and governance: Data Protection Impact Assessments (DPIAs).
4. European Commission (2018). Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Artificial Intelligence for Europe. COM (2018) 237 final.
5. European Commission (2018) Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Coordinated Plan on Artificial Intelligence. COM (2018) 795 final.
6. Wright, David. (2012). The state of the art in privacy impact assessment. Computer Law & Security Review, 28(1), 54–61. [https://doi.org/https://doi.org/10.1016/j.clsr.2011.11.007](https://doi.org/https:/doi.org/10.1016/j.clsr.2011.11.007)
7. Hungarian National Authority for Data Protection and Freedom of Information (NAIH), List of Processing Operations Subject to DPIA 35(4) GDPR <https://naih.hu/list-of-processing-operations-subject-to-dpia-35-4--gdpr.html>
8. Wright, David. (2011). Should Privacy Impact Assessments Be Mandatory? Commun. ACM, 54(8), 121–131. https://doi.org/10.1145/1978542.1978568
9. Chandra, Sudipta., Ray, Soumya., Goswami, R.T. (2017).  Big Data Security: Survey on Frameworks and Algorithms, in 2017 IEEE 7th International Advance Computing Conference (IACC), Hyderabad, pp. 48-54. doi: 10.1109/IACC.2017.0025