Whitebridge White Paper

Data Protection Impact Assessment under the GDPR

March 2020

Table of contents

Introduction

Each founded over a decade ago, Whitebridge Advocatuur and Whitebridge Consulting have built up experience and received recognition for the quality of their work, in the field of complex technological projects. As a consequence, both Whitebridge Advocatuur and Whitebridge Consulting started helping clients soon after the text of the GDPR was approved.

Now that it has been almost two years since the GDPR came into force Whitebridge Advocatuur and Whitebridge Consulting have accrued an expertise in GDPR matters that is widely recognised in the marketplace and assisted a wide variety of clients in various sectors with GDPR related matters.

Data Protection Impact Assessments (DPIA) are an innovation in the GDPR, obliging companies such as yours to assess their processing of personal data under certain circumstances as explained below. This obligation is backed up by potential administrative fines up to 10 million euros, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year.

DPIAs are serious projects, especially when you as a controller find yourself time constrained.

From our experience we clearly see that many companies find themselves facing several challenges in conducting a DPIA:

- You need to determine (and document) whether a DPIA is required at all;
- You need to delineate the scope of your relevant processing, identifying the information being processed as well as the process streams where the data is used;
- You need to have the insight in your data, at rest and in motion, and your data management practices;
- You need to have insight in your security policies and operations;
- You need to get and document feedback from various internal departments involved;
- You need to identify all external parties involved in processing;
- You need to bring all this information together and evaluate it according to both the general criteria of the GDPR as well as various guidelines and national regulations.

And all this needs to be done as rapidly as possible to limit the impact on timelines and budgets.

This requires a wide array of competences and a pragmatic way of working. In these situations, it is good to know that Whitebridge is there to help you with your DPIA obligations.

This Whitepaper will provide you with an overview of the challenges and solutions in understanding:

- when and if a DPIA should be carried out;
- how a DPIA should be carried out;
- how to comply with your accountability obligations.

(When) Should a DPIA be carried out

The GDPR obliges controllers to carry out a data protection impact assessment (DPIA) whenever a processing is likely to result in a high risk to the rights and freedoms of individuals. This obligation applies both when a new processing is started as well as when a processing changes.

The GDPR is clear that a DPIA needs to be carried out before the start of a processing. But the question of whether a DPIA needs to be carried out is more challenging. The challenge for controllers is that they have to make the initial call whether a DPIA is needed. Making a wrong call either way has consequences. Making the wrong call and conducting a DPIA when it isn't necessary means a waste of resources and time. Making the wrong call and not conducting a DPIA when it is necessary could in the end result in fines from a supervisory authority.

The business decision for a DPIA has several angles:

- GDPR compliance is at all times required;
- Insight in the maturity of data management practices will potentially provide the improvement measures and improve the quality of data;
- The insights needed to apply risk management are an imperative.

The cost in time and resources to execute the DPIA and the threat of a potential fine are the cost side of the business case. This evaluation is difficult even for organisations with internal privacy expertise.

As Whitebridge Consulting's Paul van Wijngaarden says:

"The DPIA is not only often mandatory, but the real business value comes with its foundation for Data Analytics."

When a processing changes, often due to working with an external processor in connection with a process, an outsourced function, a cloud or SaaS solution, a DPIA should be carried out as soon as practical.

When part of the IT infrastructure is being sourced, it is important that the client should determine whether a DPIA is required before contract negotiations regarding such a sourcing begin. This is because it may be necessary for both client and vendor to work together on a DPIA before the contract is concluded, since the outcomes of a DPIA can impact both the design of a solution as well as its costs. For this reason, it is important for controllers to get the best possible advice on whether a DPIA should be carried out at the same time that a sourcing is being prepared. With the right advisors, it is possible to predict sooner whether a DPIA should be carried out as part of, or in connection with, an IT project.

A DPIA becomes a challenge when it needs to be carried out in the midst of ongoing negotiations. DPIAs need to be performed on time. With the right guidance of a data privacy specialist and an IT management consultant a DPIA can be executed in a matter of weeks.

Performing the DPIA

The performance of a DPIA requires more than just a focus on the requirements of the GDPR and the guidelines provided by supervisory authorities and the European Data Protection Board to smartly define what is the current status of practices, gather the evidence, assess the risks and document the results.

Performing a DPIA requires a comprehensive assessment approach together with the security framework to come to:

- a systematic description of the processing operations, the processing purposes and the legitimate interest pursued by the organization;
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of natural persons; and
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate GDPR compliance, taking into account the rights and legitimate interests of data subjects and other persons concerned.

The legal body of GDPR knowledge forms the backbone to concise and effective projects. The project then needs to produce the required proof of data, processes, controls, governance etc. to assess the risks. Next, the risks of the observed state are defined and the measures to be applied to organisation, processes and technology, including security are determined.

The assessment not only comprises the collection of data, but also needs to involve the stakeholders in the organization.

They are the owners of the data and have the insights of the processing.

Next, the Chief Information Security Officer, the Data Privacy Officer and the IT architects will be consulted.

You, as a controller will be the owner of the DPIA, as this will provide a valuable action plan.

Whitebridge has the assessment templates and project plans that assure efficient execution by providing both legal input and IT management models.

As Whitebridge Advocatuur's Pavle Bojkovski says:

"A successful DPIA requires a team effort. Even though we consider ourselves the experts on legal matters, we keep in mind that this is just part of the input that a team needs to deliver a client success."

Whitebridge

Accountability

A completed DPIA can be used to establish that the customer has complied with its accountability requirements under article 24 GDPR. Controllers also need to be able to demonstrate their compliance with the principles relating to the processing of personal data. This requires organisations to be aware not just of the personal data that they process but also of the wide variety of internal procedures that go into the processing of personal data.

With the right assistance companies can construct the overview of their personal data processing operations and create registers of personal data processing.

Whitebridge Advocatuur regularly and consistently helps its clients in ensuring that they comply with the requirements of the GDPR in such a way that clients can easily demonstrate their compliance, pre-empting any questions a regulator could pose.

A proven collaboration

In particular, the proven collaboration between Whitebridge Advocatuur and Whitebridge Consulting will provide you both with business consulting and legal expertise from a well-adjusted team.

Whitebridge Advocatuur's dedication to excellence in the field of privacy law has been awarded with multiple prizes and a consistent, high rating in various rankings. Despite being two separate and independent companies, Whitebridge Advocatuur and Whitebridge Consulting are regularly called in by clients to assist in a variety of business cases so that their experience and dedication can mitigate the challenge of performing a DPIA.

Whitebridge Advocatuur has extensive experience in assisting controllers both in ensuring that they can demonstrate that their processing is in accordance with the GDPR as well as in assisting controllers in evaluating whether a DPIA needs to be carried out.

As Anja Dekhuijzen, Founder of Whitebridge Advocatuur says:

"We can provide both the legal framework for making and documenting such a determination as well as provide legal input and evaluation on the controller's decision whether a DPIA needs to be carried out." Whitebridge Advocatuur has the extensive experience to help controllers navigate the lists of processings that are subject to a compulsory DPIA as well as the rules of various national data protection authorities."

Whitebridge Consulting has a long-established capacity in assisting clients with their IT and sourcing strategy. Both in traditional environments as well as in digital transformation solutions. Next, the consultants are proficient in identifying all relevant data from the operations in existing architectures and documenting data flows and processing and the impact of such data flows and processing. Whitebridge Consulting carries such reviews out as part of health checks on existing relationships between controllers and their suppliers, which health checks can result in updates in the operations or a redefinition of the service constructs. This in turn can also impact the determination of whether a DPIA needs to be carried out.

Whitebridge Consulting's Managing Partner Gerwin Pol agrees, saying:

Especially in the use of processors by cloud and SaaS services that make Digital Transformation work, a DPIA is mandatory.

With the experience working for a wide range of clients, ranging from leading multinational corporations to municipalities, Whitebridge can rapidly deliver usable and applicable knowledge to clients. This way Whitebridge promptly creates and delivers unbeatable client value.

Conclusion

Whatever your IT project entails, you need to make sure that you make a timely and documented assessment on whether you are required to carry out a DPIA. Likewise, should you realise that a DPIA is required, you should make sure that you perform that DPIA before the start of your new IT project. A failure to either make the DPIA determination or to perform a DPIA on time can result in significant missed opportunities and direct costs through project delays and cancellations. You can rely Whitebridge Advocatuur and Whitebridge Consulting for a to-the-point implementation backed up by in-depth expertise and a unique experience profile to help your company cross any data protection challenges.

Contact us

Whitebridge Advocatuur and Whitebridge Consulting are there to assist you with any DPIA question or matter that you may encounter.

Whitebridge Advocatuur

mr. drs. Anja E. Dekhuijzen MCJ
Lawyer
+31 6 2951 3067
dekhuijzen@whitebridge.nl

mr. Pavle Bojkovski
Senior Advisor
+31 6 3206 9141
bojkovski@whitebridge.nl

Whitebridge Consulting

Gerwin Pol
Managing partner
+31 6 5732 4652
gerwin.pol@whitebridge.eu

Paul van Wijngaarden
Partner
+31 6 1292 3750
Paul.vanwijngaarden@whitebridge.eu