RESPONSUM
privacy for everyone

eBook

Practical tips to execute quality DPIAs

responsum.eu info@responsum.eu +32 (0)2 445 50 10

Index

Introduction

This eBook shares insights on the practical challenges of a DPIA (not just the legal side), how to manage your organization's expectations, and advice on how to motivate and involve all the stakeholders in Data Protection Impact Assessments (DPIA).

Sometimes it can be difficult to make all the stakeholders identify the importance of privacy in general and of DPIAs specifically. Most people think that this is the responsibility of privacy professionals and teams, and businesses usually point the finger at them when they're looking for answers. In this eBook, we will discuss how you can show people that a DPIA is the responsibility of several members within an organization and not just the privacy team.

6 stumbling blocks and common mistakes

1. Who is responsible for the DPIA?

Most people are not aware of the fact that the DPIA is not exclusively a responsibility of a privacy professional. In fact, the person responsible for the DPIA is anyone who is responsible for the processing of personal data. For instance, this person could be a supervisor or a manager of the team. This makes a DPIA the responsibility of the business in general and not just the privacy crew.

2. GDPR still surprises

The GDPR isn't the first privacy regulation. Other laws preceded it, and surely many more will follow. Nonetheless, businesses are often not fully aware of all the GDPR requirements they must follow, turning GDPR into a constant surprise for them. This can hide many risks since people might think they are on the right track, but they might end up doing things the wrong way.

3. Lack of motivation

It's not strange that there's often a lack of internal motivation when it comes to privacy. As a privacy professional you should remind people that privacy is an obligation. Not just a legal one but also from a quality standpoint. Not complying with privacy regulation is a clear indicator that your organization is not yet on that level of professionality. Privacy should be a fundamental part of doing business in this day and age. To motivate them to strive for privacy compliance you should invest time in showing why privacy and specifically DPIAs are so important for your organization and how it will help the business grow in the long term.

4. FHA

How many times have you heard an excuse from your colleagues, so as not to perform a DPIA? *FHA* stands for Frequently Heard Arguments that people claim when they are asked to perform a DPIA. E.g., when the privacy team gives advice to other employees about DPIA tasks, chances are they will perceive it as telling them what they should do.

That's when the FHAs come in. Some of the most FHAs are lack of resources to perform a DPIA, lack of expertise or that this is exclusively a responsibility of the privacy team. The business can't be bothered with extra work. You might come across questions such as *"Do I need to reach a perfect score?"* or *"Can't I just outsource this?"*. That's when you need to have a prepared response to these arguments.

5. Response to the arguments

Clear up the roles

Define the roles from the beginning. Since you are the privacy professional, you are the one that has the knowledge, and you are expected to provide the organization you're working in with advice based on your knowledge. However, you have to make clear that it's not your responsibility to perform the DPIA or make decisions. Instead, you have to make certain that everyone is aware of these processes and knows their role in a DPIA. Roles will be discussed further on.

Lack of priority

Often, a DPIA is not considered a priority. However, in cases of crises, the business is available to provide the money, people and resources needed to overcome the crisis. This is proof that it's not a problem of lacking resources, it's a problem of not setting the right priorities.

Expertise

Frequently, the problem is not the lack of expertise, but the fear of the unknown. People tend to make things bigger than they are. When people outside of the privacy team are not sufficiently informed about DPIAs, it is rational to believe that it's impossible to perform one by themselves. However, many questions on a DPIA are not specialized, and no legal or academic knowledge is required since the topics could be answered by anyone. Examples of the questions could be why you are doing what you're doing,

what is your end goal, and why are you storing or asking for specific kinds of information. You don't need a PhD for these kinds of questions.

Aim high

Aim for a perfect score. This is something you need to add to your organization's culture as a privacy professional. For example, methods such as outsourcing are not sustainable long-term solutions. If you aim for a quality privacy solution, you must look for other more sustainable practices than just outsourcing. There will always be a new project or a change in standing procedures. Paying a consultant each and every time won't help you in the long run.

6. Common mistakes to avoid

Not having a clear scope

Don't just start a DPIA without a clear scope. You need to invest beforehand in the scope of your DPIA. Ask yourself questions like 'why or for whom am I performing this DPIA?'. Is it for example for HR? From the moment someone applies for a job until retirement. This is one example of a very broad focus. But if you focus only on

the recruitment part you can narrow the scope a lot. Not having a clear scope will frustrate you and your colleagues performing a DPIA.

Roles

Your role in a DPIA as a privacy professional is an advisor. However, you need other members on the team that will help you make the dream work. Some roles you might consider including in the DPIA are:

1. Someone that will know all the process steps within their job (per target of the DPIA) from A to Z;

2. Someone that has more technical knowledge about security;

3. Someone that has knowledge about the applications they are using in their business;

4. Someone that is aware of legal issues, for example legislation such as GDPR, but also international law.

If you want to get truthful answers you shouldn't just send questionnaires to your colleagues and expect them to know what these questionnaires mean. They will probably only give you the answers you want to hear. Explain to them what this is, what it means, and what their role is. The goal is to understand the full data process as it is so the organization can qualify all the risks. If you don't have the full picture why bother with a DPIA?

In RESPONSUM's "Projects" Module you can centralize all the information early in the process. There, you can also explain who has which role in a DPIA, the purpose of the project, and all the information you need in the design phase.

Know your audience

Understand the level of privacy knowledge your audience has. Make sure you know to whom you're talking before starting a DPIA. A DPIA is a tool to know how things are happening in your organization, not another goal you should reach and then forget about. If a DPIA is just a checklist, you are doing it wrong.

Too much sense of responsibility

As a privacy professional, you probably have that sense of responsibility to help people out. Sometimes that sense of responsibility can take over a DPIA just to help people get it done. But you should remember that it's not your job to do it, just support it. Taking over is something else than helping out. Why sell the fish if you can teach the organization to catch the fish themselves. This will help everyone out in the long term.

Manage expectations

"By failing to prepare, you are already prepared for failing"
- Benjamin Franklin

Oftentimes, people just start off a DPIA and do not invest time in the preparation of the process. Instead of investing time only in actually doing the DPIA, make sure that everyone that has a role in it is aware of the reasons to do it in the first place, besides the fact that it's required by law.

Focus on the added value

Process improvement

DPIAs add value to business processes. By communicating the added value and importance of a DPIA to the people in your organization, they will be more inclined to help you. For example, in practice, a process might consist of 20 steps. Through a DPIA you have to check every step and then you might realize that 5 of those steps are not necessary. If you take into consideration the risks that might be hidden in this, you can make the processes more efficient, while you could lower costs.

Awareness

A DPIA can be hard, scary, new, frustrating, and take a lot of time. But in the end, it will also help you raise awareness within your organization. When people are more aware of privacy, they are more inclined to ask for advice beforehand.

Mitigating risks

With a DPIA you minimize or diminish unknown or unnecessary risks. For instance, managers are responsible for processes, and people who are responsible need to take risks. With a DPIA they can make sure they are aware of what the risks are and if they should accept them or mitigate them.

Confidence

It's not strange that sometimes people that are responsible (e.g.: managers, department leaders, or supervisors) are insecure about DPIAs. Things that might cause them insecurities are the fear that their work can't continue, or they might do something wrong, or they don't have all the answers. However, after they execute the DPIA, they know the process better than they did before, and unnecessary risks are taken away. That way, they get more confidence in their own process, resulting in them being more inclined to help you with future DPIAs or other privacy related topics.

Hard skills

DPIAs are here to stay and after a few years, you need to revisit them. If there is a big change in an assessed processing activity, you need to reopen the DPIA again. It's something that will stick

with the organizations so make sure it's as fun or as efficient as it could be and that this is a part of your business.

Time investment

A DPIA will typically take 40-60 hours for an average organization. It can be less or way more than that. Before starting a DPIA, you should set the right expectations. If you're doing a DPIA and it's taking longer than the business thought it would take, people will get frustrated and will come back with the FHA (Frequently Heard Arguments), with reasons not to perform a DPIA.

Deadlines

Work with deadlines. Make sure everybody stays on track to ensure everyone finishes a DPIA in a timely fashion. If a DPIA is not finished or is not completed in a right way it should still go to the DPO. Waiting on the business can take forever. It's better to give the DPO a unfinished product so the DPO can give advice than keep a DPIA dragging for years without any improvement.

Tailor to your organization

Privacy Maturity Levels

As a privacy professional, you need to determine the kind of organization you're working with. Ask yourself questions such as, "What are the privacy maturity levels at this point" or "Where are you at right now"? Are you in an organization that it's still new to receiving a request from a data subject? Or are you an organization where when there's a need for a DPIA everyone knows what needs to be done? You shouldn't expect that the business will do everything straight away or the board will take this seriously enough. As a result, you've got to make sure to identify the level you're at and what the ambitions of the organization are.

"If you're at a level of 6/10, and your ambition as a privacy professional is to stay there or even go to a 7, it will not help if you aim for a 10: the only thing you'll do is frustrate the business and yourself. For some organizations – for instance in healthcare, banking or government – a 6 might not be enough, because the standards for these field are higher than for some commercial companies. If a 6 is not enough for your field, you have to make sure that the organization you're working with is in line with your approach."

The privacy policy as a foundation

The privacy policy is one of the main things you need to get in order because, in the privacy policy, you can arrange many issues, such as your role, other people's roles, what makes a DPIA necessary, how the business is responsible or why you need to make it a part of your business's culture. Through a privacy policy, you can (hopefully) have fewer discussions about why you need to do this in the first place.

Start with high-level risks (DPIA check)

Before starting to perform a DPIA, ask yourself one main question: Is this necessary? If you have 10 DPIAs that need to be done, make sure you prioritize the one that will prevent your organization to be on the cover of a newspaper next week. Of course, there is always room for improvement. You can even have 50 DPIAs that need to be done and you would like to complete them in the next couple of weeks. Nevertheless, this depends on the maturity levels and ambitions of your organization. If you don't have the budget to go for ten DPIAs in a year, it's better to agree with the business and the DPO to focus on the ones with the high-level risks. This is also something the privacy professional can bring added value to. When everything is important, what risks do you take on first? Educate the organization so they can have an educated discussion on what risks to tackle first. Define the ones that need to be done this year, and the ones that are for the next year, or even the year after that. It's also a risky approach but the GDPR is based on that, it's risk-based legislation.

Within the RESPONSUM tool you can **perform pre-DPIAs** to check if there's a need to perform a DPIA in the first place. Want to learn more? Visit responsum.eu/privacy/dpia-data-protection-impact-assessment/

Privacy Champions

Find or create within the company people or teams that will have more knowledge on the GDPR, and privacy in general and make sure they help spread awareness within the business. You can't do it on a central level with a privacy team alone, you need to do it in the core of your business, before a process is implemented, in the design phase. Something that can definitely work really well is including privacy champions!

"What are privacy champions? Give a privacy award each month to employees that perform remarkably well in privacy issues to acknowledge that. The benefits of this are that it creates awareness each and every month in the organization, but it also helps to motivate the business to go a step further to be part of improvement, where privacy is seen as quality. This can be a kind of inspiration."

RESPONSUM offers two types of licenses: power users and normal users. Power users are people from the privacy team, and normal users' licenses are free of charge and can be given to employees, such as to all your privacy champions. Through our tool, you really get the possibility to connect with all the privacy champions within the RESPONSUM platform.

9 keys for success

We summed up the key takeaways that will help you refine DPIAs in your organization.

1. Communication

Communication is key on a DPIA throughout the process, from preparation to execution. To build a strong foundation for communication you can start with writing a clear privacy policy. Within the privacy policy you can cover several topics, from what a DPIA is to when you should do it or who is responsible for what. After you complete the privacy policy make sure to communicate it throughout your organization. For example, give presentations to the employees or send out the right information on the DPIA.

2. Get off on the right foot

Prepare. Make sure you prepare for everything that can indicate usefulness and necessity, so people do not question that. Focus on the added value. Keep in mind the audience you are talking to, their background, the challenges they face, what is their expertise, and what knowledge they lack.

3. Scope

Make sure you set the right scope. Understand the needs of your business and why you need to perform a DPIA. Ensure the scope is not too broad and you do not miss any kind of important information.

4. Roles

Make sure you have the people you need with specific roles defined. Have a legal person, a security person, and a person that knows everything about the specific business processes. This way, you can collect all the information you need to perform the DPIA from day 1, and you will lessen the risks of missing important information.

5. Expectation management & time investment

Expectation management and time investment (in terms of how much time it would cost you) are very important so nobody is unpleasantly surprised. Make a timeline of the process and the different stages and estimate how much time is expected to complete the DPIA. Also evaluate during the DPIA process. Better to be open and honest when things will take longer. Lack communication often leads to frustration.

6. Responsibility in the right places

Make sure that the roles that are responsible for specific actions are included in your privacy policy. In the privacy policies, you can describe what a DPIA is and what roles are in the DPIA to make sure that the foundation is set right. That way you stay far away of the discussion who is responsible for the DPIA. This is always the process owner.

7. Stay involved (but not too much)

Don't just throw the questionnaire and see how it goes. It's still your responsibility to deal with it and you got to stay involved. But be careful not to get involved too much. If you always take over a DPIA, you don't help yourself, or the business in the long run.

8. Follow up

The follow-up is not a topic that is much talked about. When a DPIA is finished there's a piece of advice from the DPO with some measurements that need to be taken. You as a privacy professional must make sure that you at least check up with the business if they're actually acting on it, and if they need some kind of help with it.

With RESPONSUM you have the opportunity to upload DPIAs that you have already documented before, centralize all the information in one place, and share them with your organization.

9. Make it a part of the business

A DPIA should be a business matter, not just a privacy thing. Privacy is a quality requirement of the business. If you want your business to run well, you must make sure that privacy management is at the right level.

How does a DPIA work in RESPONSUM? A guided approach

In the "DPIA" Module, we provide you with a guided approach to documenting a DPIA through several steps.

1. In the first step you **Set Up** your project and you can provide the DPIA with a name or a description.

2. In the second step, you **Select the project** you defined before, to have all the information centralized.

3. In the third step, you have the **Pre DPIA**. There, you get a lot of insights on whether you should perform a DPIA, while RESPONSUM will provide you with recommendations on that. You can document the DPIA with a risk-based approach in the following steps.

4. In fact, in the fourth step, you can find **Risk Identification**, where you get a risk library and you can just select the name, statement, type, and provide a description.

5. In the fifth step, you can find the **Risk Assessment**, meaning the impact of the identified risk on the data subjects. You can just check and add in the DPIA through the available list whether it is about material, physical or moral risk. You can also choose the probability that the risk could occur, with risk levels defined by you. Then you have a calculated overview of the risk level, while you can - if necessary - make manual alterations later.

6. In the sixth and last step, you start documenting the **Risk Handling/ Action Plan,** meaning how you will handle these risks. You have different threats available, and you can for example accept them or already start mitigating them. Then you can link a certain measure or procedure that defines how you start mitigating the risk. Our task management module allows you to send specific tasks to for example the privacy champion to get all the necessary information. Here you have the ability to select the users and provide priorities or set a deadline. Then on a task itself, it's possible to comment and communicate all the necessary information.

3 essential tips for immediate success

Use these 3 essential tips and see improvements this year.

1. Make DPIAs part of the business via policies

Why do you need to do it? Who is responsible for it? Make sure there are a lot of policies for the business side of things so that people know whom to call, and whom to ask. Make sure it's written down, so you don't have to have the same discussion every time.

2. Prepare for successful launch

Make sure you invest in the preparation. Give presentations to the board or to the managers so everybody knows what a DPIA is and does and why they should want to do it. Every person on the team must understand that they shouldn't do it just because it's the law, but to make sure they know about the added value.

3. Right sense of responsibility

Help people out, even sometimes help them out a bit more because it's the first time in the business, but never take over. There are chances they will think that the DPO or the privacy officer is there to take over all the privacy issues. That's something you should get out of people's heads. Privacy is the responsibility of the whole business, and you want to make sure that the team works together to actually make the dream work.

Final thoughts

DPIAs can add value to your organization and help your business grow. However, it's not exclusively your responsibility as a privacy professional to perform a DPIA. Your responsibility is to create awareness within your organization and advise or help the employees when needed, without constantly taking over. If you train and show the other employees the benefits of a DPIA you will help yourself, the employees, and the business flourish.

Do you have any questions on how RESPONSUM can help you perform DPIAs? Book a free demo via our website responsum.eu/book-a-demo/.

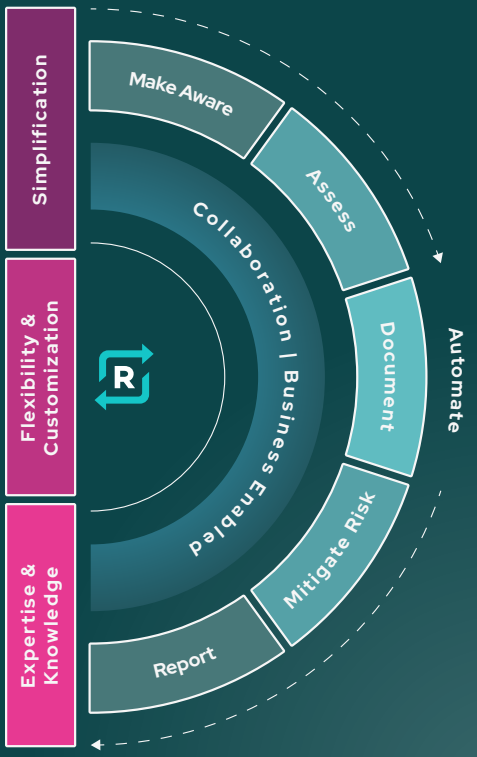
Thanks to our contributors

Kenneth Sleijpen (CIPP/E, CIPP/US & CIPM) is a Lawyer experienced in companies within the profit and non-profit sector with specialization in (local) Government in different privacy roles.

He is Chapter Chair NL for the International Association of Privacy Professionals (IAPP) and a member of the Expert Advisory Board of RESPONSUM.

Herlinde Aerts is RESPONSUM's Product Manager that spearheads the product vision and is a part of the leadership team. She has a strong background in business administration and project management, and she is dedicated to helping customers across the globe* achieve success.

*RESPONSUM is available in eight languages: English, French, Spanish, Dutch, Italian, German, Portuguese, and Thai.



RESPONSUM

Privacy for everyone

Simplify and automate your GDPR compliance challenges. Implement a lasting privacy culture throughout your organization. Manage your Personal Data Lifecycle.

Book a meeting to check it out for yourself

Book a meeting

responsum.eu
info@responsum.eu
+32 (0)2 445 50 10