



# GUIDE FOR A SUCCESSFUL DPO

*– creating support  
for your privacy  
program*

In collaboration with Privacy and  
Data Protection Consultant  
**-Vlatka Vuković**

## Contents

Introduction .....	2
DPO – a dream job? .....	3
1. INTRODUCE YOURSELF AND MEET THE COMPANY .....	4
2. FORM A PRIVACY TEAM.....	7
3. ESTABLISH A PRIVACY PROGRAM .....	9
4. MAKE YOUR JOB EASIER.....	12
5. TRAINING, CERTIFICATION AND PARTICIPATION IN PROFESSIONAL COMMUNITIES.....	13
Conclusion.....	16
About the author.....	17
About Data Privacy Manager .....	18

## Introduction

These guidelines are based on experiences of a privacy expert gathered throughout everyday practices and working with clients of **different sizes** from **different industries**.

*We have interviewed our partner, Vlatka Vuković, **Privacy and Data Protection Consultant & Co-Founder** at **Horvath Wolf**, whose extensive knowledge is supported by CIPP/E certificate and ISO 27001 Lead Auditor certificate.*

Vlatka shared **5 basic steps** for a successful privacy program that will help you **elevate your GDPR compliance** and enable you to evolve as a DPO and an expert.

## DPO – a dream job?

Designation conditions, position within the organization and tasks of the Data Protection Officer (DPO) are clearly defined in the GDPR. Reading those provisions, anyone would have wanted to be a DPO.

A DPO is an expert, reputable and respected, who answers directly to top management and is trusted by all organizational levels, independent and unbiased, resolving exciting legal-technology issues, with an entire team and all necessary resources at disposal.

DPO attends professional conferences, constantly improving knowledge and skills and cannot be dismissed or penalized for performing appointed tasks.

**Sounds like a dream job!** However, let's get back to reality.

Highly regulated and organized enterprises that have recognized the importance and benefits of having a DPO and the privacy team are **more an exception than a rule**. Most organizations still consider personal data protection and information security to be a burden and yet another regulatory obligation.

**DPOs fight daily for their place under the sun**, the same one granted by the law. It is to these fighters that these guidelines are intended.

# 1. INTRODUCE YOURSELF AND MEET THE COMPANY

So, you are hired or designated DPO. Congratulations! According to the appointment decision, your tasks are, among other things, the following:

- to **inform and advise** the controller or the processor and the employees who carry out processing of their obligations pursuant to the GDPR;
- to **monitor compliance** with the GDPR and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, **awareness-raising** and training of staff involved in processing operations, and the related audits;
- to **provide advice** where requested as regards the data protection impact assessment and monitor its performance;
- to **cooperate with the supervisory authority**;
- to act as the contact point for the supervisory authority on issues relating to processing, including the **DPIA** prior consultation, and to consult, where appropriate, with regard to any other matter.

**How are you supposed to work on these tasks if no one knows about you?**

Who are you, what is the purpose of your role, why is the DPO important, and how and why should you be contacted? Make sure the entire organization knows the answers to these questions.

Depending on the internal communication channels, ensure that the **news of your appointment and your contact information is made available** to everyone within the organization.

This can be achieved through an **internal newsletter, intranet article, circular memo, bulletin board**, or by sending an **official notice** to the business process owners. Do it in a way that is appropriate and commonly used to communicate important news or changes to the organization's business.

Participate in the drafting of the notice that will be easy to understand and tailored to the reader, whether he is a lawyer, pharmacist or sales representative. Along with the notice, you can also prepare a **leaflet** or a short **PowerPoint presentation**, stating your contact information, describing your tasks and explaining in which situations it is suitable to ask for your advice.

Since you've been appointed by the board, request that **you attend the next top management meeting**. There you will have an opportunity to get to know key managers and they will have the opportunity to get to know you.

Take this opportunity to make a **brief explanation of what is personal data protection**, why is it important, what are possible negative consequences of breaching the provisions of the GDPR, and how you can help the organization to operate successfully while still respecting all its legal obligations and right of individuals.

Keep this presentation **concise and informative**. Avoid complicated legal terms and **do not focus only on administrative fines**. Personal data protection is much more than that!

After meeting with the top management, **get to know other key roles** and key business processes. Simply send an email to colleagues with greater responsibilities (i.e. department and sector managers) and organize shorter, **30-to-45-minute meetings** with them.

This process will take some time, depending on the size of the organization and its business. Do not rush it, because this is **one of the most important steps** for a newly appointed DPO. It is one way to **get recognized as a partner and advisor**. It is an opportunity to provide your first advice and guidance.

**Do not act as a critic or an inspector**, the point of these meetings is to get to know the processes, but to get to know the people as well, and to look for “**allies**” for future tasks.

Certainly, an informative half-hour dialogue is not enough to get to know all processing of personal data nor to understand all business processes, but it is an **indispensable first step** and even a possible beginning of a wonderful friendship.

## 2. FORM A PRIVACY TEAM

If there is a possibility to set up a special department at the organizational level which will be in charge of privacy and personal data protection, such **department should be composed of experts** who are familiar with the business processes and who understand the fundamental requirements of the GDPR.

In the case of large, territorially dispersed systems, the hierarchy and responsibilities include the following roles<sup>1</sup>:

- *Chief privacy officer*
- *Privacy manager*
- *Privacy analyst*
- *Business line privacy leaders*
- *Incident response team*
- *Regional DPO*

However, it is not reasonable nor profitable for each organization to have a separate department that deals solely with privacy and personal data protection.

Depending on the size of the company and how business is organized, **the DPO must keep regular contacts and relationships with key departments**, i.e. HR and legal, IT, marketing, finance, sales, customer relations and customer support, and other key processes depending on the industry and types of relationships...

---



<sup>1</sup> *Privacy Program Management*, Russell R. Densmore



Employees with responsibilities within these departments should be made part of the **privacy network**, coordinators and contact points between “their” respective departments and the DPO.

### How to achieve this?

Let's recall what the GDPR says about the position and job role of a DPO:

 *The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.*   
(Article 38.1)

Therefore, if the board expects the DPO to be involved in all relevant matters in a timely manner and perform all the necessary tasks in all important issues, they must enable it. **Assignment of responsibility** is necessary for the implementation of privacy program at all levels.

So, **if you are not receiving all the necessary support**, kindly remind the management of the GDPR requirements and your position and tasks defined in the decision on your appointment.

Just in case, (once again) provide a rationale for why personal **data protection is not and cannot be a one-man show**.

### 3. ESTABLISH A PRIVACY PROGRAM

After you have introduced yourself, learned about the basic business processes and formed your team, it's time to **establish a privacy program**.

Privacy program is special, just like your organization is. **The program describes mission and vision**, and defines what you want to achieve in the area of personal data protection. It cannot be copied or plagiarized, and it depends on several factors.

First of all, it will depend on the **legal obligations** relating to the organization or arising from relevant **national legislation**. It will also depend on the **size of the organization** and its **territorial constitution, corporate culture, employee structure** and many other factors.

In short, privacy programs for a fast-growing startup employing 200 millennials and for a public authority providing utilities cannot be the same.

In addition to good wishes, the program must include serious **plans and tasks, deadlines and responsibilities**.

To make it easier for you, depending on all the aforementioned factors, check whether there are any GDPR provisions that are **not applicable** to your organization.

Given that there are only a few of such exceptions, and they rarely apply, the program will need to include the following necessary elements:

- **establishing the records of processing activities** and defining responsibilities for keeping it updated
- **personal data protection risks assessment** and defining responsibilities and the assessment methodology
- **defining adequate technical and organizational measures** for protection of personal data
- **incident management** – defining responsibilities and establishing a procedure for handling personal data breaches
- establishing a **procedure for handling data subject requests**
- defining the **methodology and responsibilities** for conducting legitimate interest assessments and data protection impact assessments
- defining new and maintaining current **policies and procedures**
- arranging **relationships with data processors**
- establishing **education and awareness-raising** programs
- establishing regular personal **data protection audits** (program, plan and methodology)

Only the basic requirements are listed, and you can specify them in more detail and divide them into several separate categories.

*The DPO and the privacy team define the privacy program, but they cannot be held solely responsible for its implementation!*

The **DPO advises and provides expert assistance**, while the privacy program is implemented operationally by competent employees.

**The board must provide the resources**, primarily human and financial, to implement the program. Let's remind ourselves of what the GDPR says about that matter:



*The controller and processor shall support the data protection officer in performing the tasks by **providing resources necessary to carry out those tasks** and access to personal data and processing operations, and to maintain his or her expert knowledge. **(Article 38.2)***



## 4. MAKE YOUR JOB EASIER

One of the tasks of a DPO is to **advise on the selection of methodology** and other [technical solutions for privacy program implementation](#), such as records of processing activities platform, risk assessment tools, DPIA tools, software for legitimate interest assessments or for managing data subject requests.

Instead of defining new methods and frameworks, use those that have been **tested and recommended** by supervisory authorities and other professional organizations.

If your organization's needs require the use of sophisticated tools, and publicly available templates are not good enough to meet your needs, **opt for one of the advanced technical solutions**.

When choosing such a solution, consider the **needs of the organization** and the **complexity** of the operational function in implementing the privacy program. Of course, make sure to check other users' experiences and reviews of the chosen tool.

## 5. TRAINING, CERTIFICATION AND PARTICIPATION IN PROFESSIONAL COMMUNITIES

Let's make it clear right away – **there is no DPO certificate**, nor is such certification mandatory under the GDPR. However, it's always helpful to **attain new knowledge through various training, courses or webinars**.

Among the many courses that are out there on the market, find those that best suit your needs and the needs of your team.

When doing so, **consider the prerequisite knowledge** for taking the course, learning outcomes, teaching style, content quality, and the expertise and professional reputation of the lecturers themselves.

In addition to publicly available courses, get informed about **tailor-made, in-house workshops** provided by highly specialized experts. This way you will receive a **custom-made training**, tailored to your organization's core business and the needs of your privacy team and other responsible employees.

**Do you need a certificate?** Certificates are not mandatory. However, like all other certificates, they serve the purpose of demonstrating competences.

If you decide to get certified, choose **internationally recognized and valued certifications**, some of which are sought after as an advantage, and sometimes also as a requirement for privacy roles in the EU.

Apart from training courses, you can also learn a lot from your peers. **Find out if there is a professional community** of privacy professionals operating in your vicinity. Get in touch with them and request membership.

By working with such a community, you will meet many interesting and experienced professionals, **share experiences** with them and tackle some seemingly insoluble situations together. Sometimes you will disagree and have different opinions, but you will certainly enjoy the discussion.

**Attend conferences** and similar public events, especially those organized by a competent supervisory authority.

Conferences are great opportunities to **meet experts**, both from the academic circle and the industry, as well as representatives of the **supervisory authority**. The connections and acquaintances you make and continue to build will certainly be useful for your future work and career development.

**Be active on social media platforms for professionals.** Expand your professional network, follow proactive individuals, read expert articles, share interesting and useful content.

Follow specialized **privacy portals** and sign up for privacy and data protection newsletters to find out the most important news and events on a weekly or monthly basis.

In addition to the mandatory and professional literature (laws, judgments, guidelines, etc.), try to find time for other activities as well. Choose interesting **documentaries, podcasts, panel discussions, books...**

*Once you start, you won't be able to stop.*



## Conclusion

Compliance is an ongoing process and can never be completed. Therefore your tasks will also never end.

Don't be strict with yourself because you have a feeling that you still have a lot to do and learn. This feeling is real and justified, as privacy and personal data protection is a comprehensive regulation that is constantly evolving and adapting to new social circumstances and the advancement of technology.

Therefore, be proactive and constantly raise awareness of the importance of personal data protection. Do what you can and promote the DPO role. And following these guidelines will help others help you.

*Good luck and enjoy your DPO journey!*

## About the author







**Vlatka Vuković** (CIPP/E, ISO 27001 LA, ISO 9001 LA) is a lawyer, cofounder and the Lead Consultant at [Horvath Wolf](#). She is a **passionate privacy and data protection specialist**. With her risk-based and pragmatic approach she helps clients from highly regulated industries, including financial services, insurance, marketing, pharma, telecommunications, transport and tourism, gambling etc. **She holds lectures and courses** in the field of personal data protection, and is a regular speaker at privacy conferences.







## About Data Privacy Manager

Data Privacy Manager is a **mature platform** used in many different vertical markets, helping its users, both data controllers and data processors, to regain control over personal data they have been entrusted with.

Data Privacy Manager is comprised of **10 modules** that can help you with your GDPR challenges:

 <p>Records of Processing Activities</p>	<p>Records of Processing Activities is a must-have module for any DPO that wishes to <b>minimize the risk</b>, cooperate with different organizational units and <b>divide responsibilities</b> between Legal, HR, IT, and Marketing. This module gives you access to all processing activities and their changes, while other roles can <b>create, edit, and (de)activate processing activities</b>. Each processing activity has its owner, which indicates who is responsible for updating information related to processing.</p>
 <p>Consent and Preference Management</p>	<p>Consent and Preference Management module gives you <b>real-time insight</b> into the complete personal data lifecycle from the moment of opt-in to the data removal. <b>Consolidate your data</b>, centrally <b>manage notices</b> while Consent and Preference Management module propagates them to all consent collection channels, automatically updating them across multiple marketing layers.</p>
 <p>Third-Party Management</p>	<p>Third-Party Management is the most sought-after GDPR <b>risk assessment</b> module that allows you to manage your <b>Data Protection Agreements while</b> guiding you through the vendor management process workflow. Management of the Agreements is possible with <b>smart notifications</b> that will inform you about all important events making sure you are on top of your compliance program at all times.</p>
 <p>Privacy Portal</p>	<p>Privacy Portal is a <b>self-service interface</b> for managing data subjects' privacy preferences that allow them a simple but <b>highly secured access</b> to their personal preferences and provides them prescribed by law information like your privacy policy and DPO information. Give your customers unmistakable insight into given consents with easy OPT-IN or OPT-OUT status change.</p>
 <p>Privacy 360</p>	<p>Privacy 360 is a reporting module and a perfect solution for the Data Protection Officer's challenges. It gives a DPO an <b>overview of all data</b> and locations where personal information is stored about the specific data subject. Privacy 360 answers the questions: <b>what data is collected, how the data is processed and where is data stored?</b></p>
	<p>Data Subjects Request module tackles with the most customer exposed and time-consuming GDPR challenge, turning requests into automated workflows with a clear insight into data every step of the way. When the entire process is automated, the IT systems, on which the data is stored, can execute user</p>

Data Subjects Request	requests timely and accurately. <b>Improve your response time, fulfill the request and always have reliable data to back you up.</b>
 Data Inventory	Data Inventory helps you <b>discover personal data across multiple systems</b> in the cloud or on-premise. The Data Inventory module connects to all relational databases of the company, making search inquiries, <b>eliminating false positives</b> and identifying all personal information across multiple systems.
 Data Removal	Data Removal is the <b>only GDPR compliant Data Removal solution</b> currently available. The module automatically gives instructions to a different system when data deletion needs to be executed and enables you to <b>define data retention and data removal operationalization</b> on different data categories.
 Data Flow	Data Flow module gives you total control and an overview of all personal data processes within an organization. <b>Streamline your processes</b> and cover all data processing bases following personal data from the collection point through archiving and data destruction.
 Risk Management	Risk Management module empowers your DPO with a <b>high-level overview of risks</b> associated with each processing activity; and to allow for a more detailed insight into residual risks behind a particular processing activity by means of linking it to a relevant <b>data protection impact assessment</b> .

If you would like to find out more about our solution Data Privacy Manager feel free to contact us at [info@dataprivacymanager.net](mailto:info@dataprivacymanager.net) or ask for your [14-days free trial](#).