RESPONSUM

First 100 days of making impact as a DPO

responsum.eu info@responsum.eu +32 2 310 39 63

Index

Introduction 3

Key focus 1 | Getting started 4

Key focus 2 | Know your business! 7

Key focus 3 | Manage your relations 13

Key focus 4 | Get involved! 17

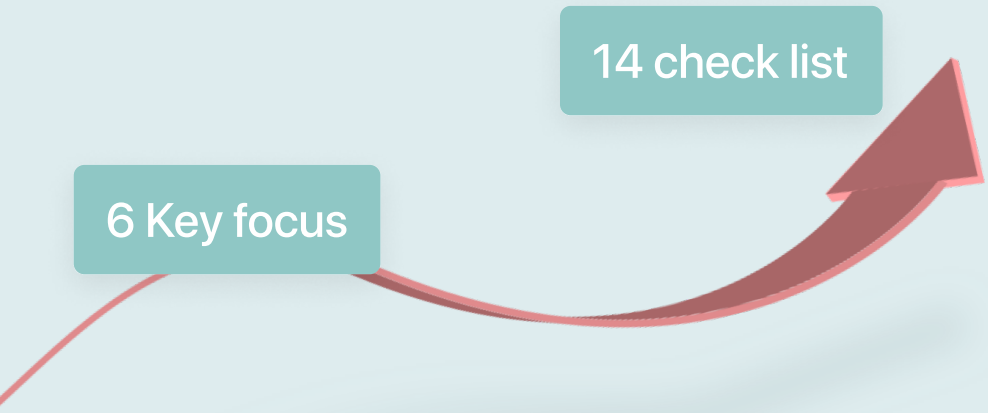
Key focus 5 | Always be prepared! 23

Key focus 6 | Keep working! 27

Final thoughts 31

Introduction

Are you starting out in your new role as a Data Protection Officer (DPO) or do you already have some experience in this matter? We have listed six focus areas to boost the kick-start of your new project, making sure that your impact will already lead to positive change in any new organization in the first 100 days of your employment.



Key focus 1

Getting started

Whether you are entering an organization that (miraculously) operated without a DPO or when you are replacing a colleague, you need to spread the word that that there is a new sheriff in town. Get yourself out there and create awareness about your new position.

Create awareness and assign responsibilities

When entering a new organization for the first time or when a new project gets approved by management and is ready for launch, you as DPO should take the lead to create awareness about the applicable privacy rules to mitigate potential risks when personal data is being processed, and more precisely to explain both your role & responsibility as well as the roles & responsibilities of everyone else involved.

Things to note!

According to article 39 (1) (b) GDPR, a DPO is assigned to monitor compliance with the GDPR and other data protection provisions. She/he should establish policies within and outside the organization, and thus shall be duty-bound for the assignment of responsibilities, awareness-raising and training of all staff involved in processing operations.

So, what is the best approach to take here? First, start off by making sure your name and role are known within the organization or with staff involved in the designated project and that you're both visible and approachable as a point-of-contact for everyone. This should help you delegate and take the lead when it comes to assigning responsibilities, both to yourself and others. A good DPO, must be a professional and assertive leader and someone who is not afraid to take the floor by implicating that privacy and data protection are key to the success of any organization or project.

Assigning responsibilities to staff should be done in an easy and accessible way, for example by having a meeting with the people involved in data processing activities to make them both aware and accountable for maintaining good practices. You can provide

support documents, guidelines and templates to help people understand the principles and pitfalls of good data protection practices, which, will empower the team and amplify the productivity of your work.

Creating awareness does not stop after you first come into office. Although the initial introduction to privacy rules is very important, keeping all the involved parties up to date will remain an essential aspect of your duties. Stay in touch with relevant stakeholders within your organization to see which departments might need extra guidance. If your organization has an internal communications department, try to get involved in the initiatives they take (e.g. newsletters or intranet).

"Get to know the organization and its people to learn which projects are active. What are the processes, where does data come in and go out,... try to get the full-picture as quickly as possible. Other than that, it helps tremendously if you're solution-minded and try to work constructively with the business. Gaining your colleagues' trust helps a lot in the long run."

Edward Huyghe, DPO at Teamleader

Key focus 2

Know your business!

Great, so you've created and maintained awareness on the roles and responsibilities of everyone involved in the processing of personal data and the existence of the GDPR! It doesn't end there though. Next, a DPO needs to know WHAT those processing activities are, and this can be monitored by maintaining up-to-date records of processing activities. After indexing all processing activities in your records of processing activities, take a closer look at them. Do all activities comply with the data processing principles? And is there a lawful basis for all processing activities?

Have up to date records of processing activities

According to CNIL, the French Data Protection Authority, the records of processing activities "allows you to make an inventory of the data processing and to have an overview of what you are doing with the concerned personal data". It is also a mandatory requirement stated in article 30 GDPR, so there's no way going around this.
In short, the record is a tool with inventory and analysis purposes, that, according to CNIL *"must reflect the reality of your personal data processing."*

The record allows a DPO to precisely identify, among others:

- The actors involved (controller, processors, representative, joint controller, etc.) in the data processing;
- The categories of data processed;
- The technical and organizational security measures implemented.
- The purpose of the processing (what you do with the collected personal data), who has access and who are the recipients of the personal data;
- For how long you are retaining the personal data;

Keeping this record up-to-date means getting involved in all the processes by asking questions in interviews with stakeholders, by reviewing the data quality, proper legal base and retention, and of course by making sure that every processing activity is lawful, fair and transparent, amongst all other principles laid out in article 5 GDPR. Properly maintaining the records of processing activities means you will be able to complete then next steps with relative ease.

Time-saver

Maintaining up-to-date Records of Processing Activities is perhaps one of the first steps, yet also one of the greater challenges for Privacy Professionals as it connects to a multitude of other GDPR requirements. Want to find out how RESPONSUM can do the work for you? Plan a free demo with one of our experts at

www.responsum.eu/request-a-demo

"Start drinking coffee with key stakeholders! Privacy is so much more than just rules and risks. You need to get people on your side. It is easier to get things done as a person people like than as the DPO who sends out an e-mail with everything that is wrong and noncompliant. Build those relationships within your organization and all your privacy advise will be way more effective. Privacy is a people business. Don't forget that. "

Kenneth Sleijpen, DPO at Municipality Sittard-Geleen in the Netherlands

Ensure compliance with processing principles

The seven processing principles of article 5 GDPR are the tenets that every person and organization that is involved in the processing of personal data should abide to, and the DPO must be guarding them vigilantly. To that end, DPOs should familiarize themselves

with the principles and understand both the intentions and implications the GDPR presents in the processing of personal data. In fact, these seven principles should already be known when you are employed as a DPO in a new organization or when you start on a new project, as this will serve as the baseline of your work. Moreover, this is the very core against which the level of Compliance with the GDPR will be calculated.

Let us revisit these principles briefly:

1. Thou shalt process personal data lawfully, fairly and in a transparent manner in relation to the data subject
2. Thou shalt collect personal data for specified, explicit and legitimate purposes and not further process in a manner that is incompatible with those purposes
3. Thou shalt make sure processed personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
4. Thou shalt ensure that processed personal data is accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
5. Thou shalt keep personal data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
6. Thou shalt process in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
7. Thou shalt be held responsible and accountable and be able to demonstrate compliance with the six6 other principles

Ensure you have a lawful basis for processing

Evidently, you have to be careful not to engage in illegal activities in the first 100 days in your role as DPO. By that, of course, we mean not only criminal offenses, but also violations and infringements with respect to article 6 GDPR when no valid legal basis can be demonstrated when you process or will be processing personal data.

The DPO is in the ideal position to review the purposes of the processing activities and to select the most appropriate lawful basis/bases for each activity. Make sure that you get it right the first time – changing a legal basis in the middle of the processing is something that is frowned upon and could get you into trouble with the authorities. Double-check if you have actually chosen the most suitable processing basis. You wouldn't be the first DPO to go with a legal basis that does not fit the actual processing activity. This decision should best be documented to demonstrate compliance.

Ok, you got the legal basis right this time, great! Now you have to make sure (by double-checking) that the processing activity itself is necessary for the intended purpose and there is no other less intrusive and reasonable way to achieve that purpose. This should

also be stated in the privacy notice to the data subjects involved.

Finally, a DPO should be aware of any special categories of personal data that are processed, which requires the identification (and documentation!) of a specific condition that makes such processing lawfully. Be sure to go through these conditions listed in article 9 (2) GDPR. The same should be checked and documented when processing criminal offence data according to article 10 GDPR when under control of an official authority or otherwise authorized by law.

"Planning and proper prioritization are key to a DPOs success. Find out the strategy, short and long term plans of the organization to ensure you have a comprehensive view of your tasks. Creating a good internal network within the organization will make your life a lot easier."

Bavo Van den Heuvel, Chief Knowledge Officer at CRANIUM & RESPONSUM

Key focus 3

Manage your relations

Your business does not operate on an island. You are always connected to other businesses, customers and other stakeholders. As a DPO you are responsible for managing the relationships you have with all these parties. Enjoy!

Ensure you can manage the data subject requests

Apart from being in (and taking) a leadership position as a DPO – hey, the "O" stands for Officer after all – any DPO starting out should also be a people and process manager, meaning that they have the know-how and capabilities to manage requests coming their way, and often those requests are coming from the data subjects.

A quick recap

GDPR not only imposes minimum norms and obligations regarding the processing of personal data that organizations must abide to, they also provide a set of rights that the persons whose data is effectively being processed one way or another, can exercise towards the organization – meaning towards you (because you're responsible after all).

How do you manage this, we hear you say? First of all, it is useful to have a dedicated mailbox to receive data subject rights and complaints. This provides for an easy workflow and helps you to maintain a useful overview of monthly/yearly requests. That data can further be used for reporting to the business and/or the supervisory authority.

Make sure that data subject requests are answered within the given timeframe to meet the transparency requirement under article 12 GDPR. Any data subject rights request should be answered without undue delay and in any event within one month of receipt of the request. The information that you as DPO provide towards the data subject should always be concise, transparent, intelligible and in an easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.

Oh yeah, you can't charge the data subjects for providing them the information they

seek, unless those requests are manifestly unfounded or excessive, in particular because of their repetitive character. Then, and only, then, a reasonable fee for the administrative costs can be charged. The other option is to simply decline such requests.

Update agreements with controllers, processors and sub-processors

Although the role of a DPO is often misconceived as purely a legal expert (it actually requires comprehensive technical know-how and IT-skills as well), reviewing and updating the so-called data processing agreements between controllers, processors and sub-processors can take a large part of your time available for the organisation or within a given project.

Article 28 (3) GDPR acts as a checklist of minimum requirements that a controller-processor relationship should stipulate. When reviewing data processing agreements, this checklist can help you determine whether the wording of certain clauses of the contract needs updating, or other amendments should be made. Furthermore, the agreement dictates the roles and responsibilities between the parties, so that in case of disagreement both parties can refer to these clauses. In the light of article 26 GDPR, a different agreement should govern the relationship between two joint controllers, clearly defining their respective roles and responsibilities towards the data subjects.

Besides, you absolutely must check if the processor (and sub-processors) are providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of GDPR, as this ensures the protection of the rights of the data subject – and you hopefully won't receive large amounts of requests and complaints of data subjects.

Finally, if you notice that personal data is transferred outside of the European Economic Area (EEA), the agreements between controllers, processors and sub-processors must include a mechanism of transfer, such as Standard Contractual Clauses or other appropriate safeguards.

Check if Transfer Impact Assessments are necessary

A Data Transfer can happen when personal data becomes subject to third country legislation. It doesn't necessarily mean that your data is leaving the EU. It just means that the data falls under another law outside the EU. Examples are remote support, certain obligations by third countries to hand over personal data or data duplication for availability reasons. This can have big consequences, as not every law is as strict or comprehensive as the European GDPR. To protect data subjects' personal data, you might be obligated to **verify if your processors their processing activities can result in a transfer. If that is the case you will have to make a Transfer Impact Assessment (TIA).** Through this TIA, you'll be able to review if the laws of the third country offer sufficient data protection and allow you to estimate the potential impact of your data transfers on your data subjects' rights and look for extra technical and organisational measures to lower the impact of a possible transfer.

Key focus 4

Get involved!

Contrary to what some privacy-newbies might believe, DPO's do not work against the business. They work WITH the business to ensure all products and services are delivered in a way that does not violate the rights of data subjects. To achieve this, the DPO should be involved in all aspects of the business right from the start!

Ensure the security of personal data processing

During your work as DPO, it is helpful to understand that the security of personal data will be governed by two frameworks: **Data Protection by Default** and **Data Protection by Design**. These frameworks are key to safeguarding security, as they shall act as control measures for ensuring ongoing confidentiality, integrity and availability – often referred to as the "CIA" of processing, and no, we don't mean the US Central Intelligence Agency here, no pun intended –of the personal data that is being processed.

- **Data Protection by Default** means that controllers of personal data shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.

- **Data Protection by Design** refers to the fact that the controller, both at the time of the determination of the means for processing and at the time of the processing itself, implements appropriate technical and organizational measures, which are designed to implement data-protection principles in an effective manner and to integrate the necessary safeguards into the processing.

Any good functioning DPO should know these frameworks by heart. This way, you can easily define and check on certain controls that safeguard security (and, when necessary, implement them in a Data Protection Impact Assessment, or DPIA).

Here are some examples of controls you can do – and should do – as a newly appointed DPO:

- Perform a risk assessment of the security measures and analyze whether the level security is appropriate
- Take into account the state of the art of new technologies and the costs of their implementation
- Check, update and timely review existing and/or lacking (security) policies
- Use techniques such as encryption and/or pseudonymization on personal data when needed
- Have back-up and restore measures readily available (see below)
- Provide stress and pen-testing to determine whether the existing security measures are still adequate
- Ensure proper access control
- Assess any other technical and organizational measures that can prove added value to your organization and to the protection of personal data in particular

"Networking with other DPOs is vitally important, as those connections can serve as great sounding boards. Sharing experience and expertise is very valuable, especially in a sector that is relatively young and dynamic like GDPR."

Hanne Elsen, DPO at UGent

Define core-business processes and inject Data Protection by Design

Data Protection by Design is about being Privacy-minded and GDPR-compliant from the start when defining a new processing activity and choosing the data processing systems that you want to put in place or already have in place for processing personal data. It is considered a more holistic approach that combines the legal, compliance and IT aspect for ensuring effective implementation of privacy and Data protection principles any system processing personal data.

When selecting or developing data processing systems that process personal data of EU residents, you need to take into account the Privacy and Security principles as stated by GDPR (Chapter 2 – Article 5-11 & Article 32) and possibly other principles enforced by local law or specific to the sector you are active in.

A few options are available as to how to make sure the newly chosen or to be developed data processing system adheres to these principles, you can either:

A

Change the requirements so that it is less intrusive on the Data Subjects' Privacy and embed Data Protection by Default (start with the least intrusive settings and request consent or base yourself on another legal basis to collect more information later)

B

Implement Technical and Organizational Measures *(Also referred to as TOM's)* in order to assure the Privacy and Data protection risk is lowered significantly for the Data Subject.

But how can you as a DPO take control in this process? When you start as a DPO, the organization you work for will already have a lot of ongoing activities processing personal data. The first step should be to get a thorough understanding of these activities and the way in which the personal data is being processed.

An organization never stops to evolve though, and so does the way personal data will be processed. Don't forget to keep in touch regularly with the stakeholders of these processing activities (by conducting regular Privacy workshops and/or attending strategic business meetings where new ideas are discussed). Being more involved in the organization as a DPO will allow you to help coordinate from the start any future plans involving the processing of personal data.

Do a pre-DPIA to see if a DPIA is needed

Look back at your Data Protection by Design plan and focus on the core -activities of your company. If your company processes certain data of data subjects that might imply a big risk for their privacy rights, a DPIA might be obligatory or advisable. Because preparation is key and time is limited, you can start by carrying out a pre-DPIA for every processing activity or set of processing activities that you deem more "sensitive". The outcome of this DPIA will help you decide if you need to carry out a complete DPIA or not.

The pre-DPIA checklist includes these questions:

- Perform a risk assessment of the security measures and analyze whether the level security is appropriate
- Does the project include automated decision-making?
- Does the project include systematic monitoring?
- Are “sensitive personal data” being processed?
- Does the project include large-scale data processing?
- Does the project include matching or combining data sets?
- Does the project include processing of data related to vulnerable data subjects?
- Does the project include matching or combining data sets?

The goal of these questions is to evaluate whether the impact of the processing is directly proportional to the business purpose, as the risk level needs to be adequate to the actual activity. If you reach a score of 2/9 on the pre-evaluation, you’ll have to create a DPIA. Even if you’re analyzing an existing processes, it’s never too late to carry out a DPIA. More information on the pre-DPIA can be found here:

https://ec.europa.eu/newsroom/article29/items/611236

Key focus 5

Always be prepared!

GDPR gave us not only a framework for what to do to ensure privacy, it also created one for audits by Supervisory Authorities. As a DPO it is your job to guide your company through these audits as smoothly as possible. You can do this by taking the following steps.

Maintain and sustain your acquired level of compliance

Unfortunately, the road to compliance has no end – it goes on indefinitely. This means you should understand GDPR compliance as an iterative process that can only be achieved by setting milestones and KPI's to determine an organization's "level of compliance". As DPO, your reply towards the organization when someone asks whether they are compliant should always be something in the line of *"we're on the right track, but there's no finish line that we can cross to determine that we've won the race. It is an achievement that must be maintained and sustained by continuous effort and good practices"*.

Non-compliance with the GDPR will be subject to administrative fines up to 20,000,000 EUR, or up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher. Those are some big bucks to be paid – not to mention the damages incompliance can mean to the organization's brand and customer trust.

As DPO, here are three things you can do to maintain and sustain the acquired level of compliance in any organization:

- Keep a clear overview of all dataflows within and in-and-out of the organization. The records of processing activities can help you to keep track, complimented with additional periodic audits and findings.
- Keep your policies, procedures and work instructions up to date with the latest privacy rules and recommendations. Make sure to always test these against the technologies and other applications you're using.
- We've mentioned it several times now, but awareness about data protection remains central in any good compliancy framework. When people understand the risks related to the processing of personal data, they are keener to implement these concerns into properly defined strategies and workflows.

Keep everything documented, as if your SA would audit you next week

Are you the kind of DPO that literally documents everything as if your life depends on it, up until the point that your colleagues are annoyed because you're acting more like a bookkeeper than an advisor? Perfect, you're doing a awesome job! We're not saying that it is essential in your role to be disgruntled by your organization for being overly accurate and hyper-labelled but being methodical by keeping track of everything that you do helps you tremendously when the Supervisory Authority comes knocking at your door.

Just as in a courtroom proceedings, coming up with evidence and proof that you are not guilty of suspected ill-behaviour, malpractices, or possible infringements of the GDPR can help you SHOW compliance towards the authorities and any other stakeholders – especially the data subjects – as well.

We're not only talking about the records of processing activities (but this is an important one) but also any policy or decision-making process, work instruction or even meeting minutes following up on certain privacy-related events or incidents.

Have a list of incidents and breaches

Preferably, you'll never have to face (the backlash of) data breaches and other incidents. But in the situation that it DOES happen, it will be useful to come back to a list where such adverse events are registered to determine whether a personal data breach is suspected and if it should be reported to the supervisory authorities, and in certain circumstances, also to the data subjects. Then again, article 33 (5) GDPR obliges you to record these anyway. It also speeds up the notification process – which is another good thing, of course.

Be aware that the notification period of any personal data breach towards the supervisory authorities shall occur without undue delay and, where feasible, not later than 72 hours after having become aware of it. The list of incidents and breaches can also help you determine the additional details and information needed to properly report a breach and to take the necessary precautions and mitigating measures to de-escalate the events and avoid further risks towards the data subject and respectively your organization.

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the GDPR states that the controller shall communicate the personal data breach to the data subject without undue delay. If you're the DPO of an organization that acts as a controller when processing personal data, a clear and structured list of incidents and breaches can help you manage and hopefully avoid the possibility and the probability of risks occurring.

Key focus 6

Keep working!

When the initial privacy implementation is finished, it is not time to relax and watch the business run as usual. Keep checking in on all departments to see whether or not all procedures are followed. Make sure new processes keep getting run by you and make adjustments when necessary. Let new employees know about the privacy policy of your company and guide them through the wonderful world of GDPR!

Make a remediation plan and maintain it regularly

An important part of your role as DPO is to make sure that the personal data that is being processed under your watch remains secure throughout its lifecycle. To that end, it is important to have procedures and policies in place to correct any error or mistake and to eliminate any other data quality issues.

This can be achieved by creating and maintaining a remediation plan for proper data management. Such plan will aid you in determining whether stored data remains relevant for the organization or to the scope of the project.

To prepare yourself in an adequate way you should first distribute roles and responsibilities in your team so that everyone can play his/her part within the purposes of the remediation plan. Here, you can focus on certain areas/aspects of data remediation (this can also be governed through internal policies) and allocate proper resources towards this issue.

The final step includes reporting back towards the organization and to review/update the remediation plan in a timely manner. Apart from a legal and IT-security profile, a good DPO is also a great strategist who understands the value of implementing a step-by-step approach to achieve goals.

Work on proven awareness towards co-workers that process personal data

If you really want to make a significant impact within your first 100 days as a DPO,

focusing on proven awareness within an organization will definitely reward you with a notable return of investment.

We already stated the need and the added value of focusing on awareness towards co-workers and staff hereinabove, and an excellent DPO is one who influences and guides an organization or staff working on a project related to data processing towards compliance with the GDPR. To that end, article 39 (1) (b) GDPR gives a great hint on how to elevate the awareness level within an organization or team: awareness sessions and trainings, of course!

Ok, so you've decided to present your (first) awareness training course on privacy and data protection. Great! To make sure that you'll flourish in your role as trainer/coach, you should focus on the following:

1. Presentation skills are the key to success: be calm, confident, well-spoken and determined
2. Come prepared, knowing your stuff makes you all the more believable, and people will pick things up easier
3. Focus on your audience: don't make it too high-level and complex (unless required)
4. Do not focus on the rules, but the people: make sure to implicate the roles and responsibilities of the staff involved in personal data processing
5. Put the data subjects first: determining risks for the organization is one thing, but it's really about the people whose data are being processed
6. Provide the participants with additional information sources, but keep it conveniently
7. Make plenty of room for questions and remarks – it is likely that not everyone is on the same line immediately
8. Provide a clear follow-up process with recurring trainings/awareness events
9. Put the theory to practice: evaluate the knowledge and responsiveness of staff by organizing assessments and/or tests
10. Automate where possible

Phish your own organization!

As RESPONSUM is focused on making the life of a DPO easier, elearnings and phishing simulations are part of our offering. Want to know how it works? Check out **www.responsum.eu/awareness.**

There, with just a couple of tips & tricks you should be on your way!

Design, maintain and update existing policies

Start by asking for all the existing policies, ranging from car policies to privacy policies. Get them from under the dust and review them thoroughly for any inconsistencies (in the policy or with regard to other policies), flaws, or faults. Check if they're still up to date, safe and check if they maybe need a touch-up here and there. Don't forget to check if there's a system in place for follow-up. It's not good practice to create a policy to never be looked at and reviewed ever again. Regulations and your internal directives evolve through time and it's important that your policies adapt accordingly in order to guarantee safety and compliance.

If the organization has too many policies in place to review all at once, **create a step-by-step plan on how to tackle this job**. Your life will become a lot easier if you create a feasible schedule in which you prioritize the most urgent and pressing policies that need to be checked and updated. If you have a schedule and you manage to keep to it, you'll be well-prepared once there's an audit. From our experience it seems best to review each policy at least every three years.

Final thoughts

We have determined 6 chapters that any DPO starting out for the first time in the field of privacy, security and data management can use to boost his or her own productivity and amplify the quality of their output and deliverables. These suggestions were directly extracted from the GDPR itself, ensuring ongoing compliance towards the most elaborate privacy regulation that exists in the world today.

The job of Data Protection Officer –a challenging role that deserves to be spelled out in full from time to time – engages you to put theory into practice and action. Often seen as a limiting factor in organizations that want to discover, expand and engage with society without boundaries, DPOs find themselves to be in a suitable and strategic position to have everlasting influence in this process, by creating a road towards innovation and compliance.

In fact, DPOs aren't the limiting factor, they define growth by making an impact, even within the first 100 days.

responsum.eu/request-a-demo/

Book a Free Demo

responsum.eu info@responsum.eu +32 2 310 39 63