DPOrganizer

How to involve your colleagues in privacy management work

Your guide to beating organisational resistance and driving collaboration on privacy.

PUBLISHED: 27.3.2019

This information is meant for educational purposes only and should not be used as or considered a substitute for legal advice. Make sure to seek appropriate counsel for any specific situation.

Key takeaways from this guide

- ✓ **How the work of the privacy privacy professional is structured.**
- ✓ **Key barriers to collaboration confronting privacy teams.**
- ✓ **Ways to push for effective collaboration and better internal structures governing privacy management.**

INTRODUCTION

For privacy professionals, it's the million-euro question: how can I involve the wider organisation in privacy management, to what extent should I, and with what objective in mind?

Such questions challenge privacy professionals everyday, often sparking subsequent ones such as: how do organisations with best practice privacy-programmes manage collaboration on privacy matters? Or more generally – what could I be doing better here?

Answers to these questions exert a lasting influence on the efficiency of your privacy program, and your ability to drive impact at your company.

In this guide, we give you a practical overview of the job of the privacy professional today, including an analysis on where the function sits in many organisations, who occupies it, and to whom the role reports. Then, we offer advice on understanding the scope of the privacy professional's role. We look at how it should evolve within your organisation, how this role can work to overcome barriers to collaboration on privacy, and how you, the privacy professional, can build processes to ensure effective collaboration on privacy long-term.

The job of privacy today

IAPP's joint report with EY presents some of the most insightful research to date on the development of the privacy professional's role since the enforcement of GDPR.

It further details the location of the role, its relation to other roles, and how this varies throughout different organisations.

THE PRIVACY FUNCTION IS EXPANDING AND CHANGING

It goes without saying that the number of privacy professionals in companies continues to rise. Since 2017, the global average number of employees working full time in privacy has grown from 6.8 to 10, where larger companies with 5000+ employees saw much of that increase[1].

The role has also increasingly evolved away from its location in legal, even though this still remains where approximately 43% of companies place their privacy function. Since 2015 for example, the percentage of companies placing the privacy function in Information Security has increased from 9 to 19%, while the percentage of companies placing the function in compliance has dropped from 33% to 19%. This can also vary by industry. 50% of health industry companies place privacy functions inside compliance, whereas 33% of tech companies place privacy within information security[2].

This trend shouldn't be surprising. Privacy and the processes governing personal data usage have more far-reaching effects in companies than do other regulatory requirements. Their placement outside legal silos reflects this.

[1] IAPP-EY, Annual Privacy Governance Report, 2018.
[2] Ibid.

STRUCTURING PRIVACY WORK

Leadership on privacy appears consistent. For 56% of companies, the privacy leader is also the DPO. This differs however between the EU and the US. In the US, the privacy leader is more senior than the DPO, where as in the EU, 67% of companies report that the privacy leader is the DPO.

Even despite the rising relevancy of privacy in many companies and the appointments of DPOs however, the percentage of privacy leaders who have non-privacy responsibilities still hangs at 61%. Thus, even though 8 in 10 privacy leaders say privacy matters are reported directly to the board, the percentage of privacy leaders having responsibilities outside privacy shows privacy efforts are still in their infancy. Companies appear reluctant to dedicate leadership full-time to privacy.

Even though investment in privacy is rising, privacy teams remain small. In fact, only 27% of DPOs have full-time staff. Here, privacy team numbers across a number of company sizes reflect disproportionate distributions. For example, companies with less than 5,000 employees have a median of 1 full time privacy employee in a privacy program, whereas firms of 25,000 to 75,000 employees may only have 5 full time staff in privacy programs.

Additionally, even though privacy staff remain in high demand, only about 40% of companies plan on increasing full-time staff in a privacy program[1].

THE BIGGER PICTURE

Regardless of increased spending on privacy projected for the coming years, the privacy staffing stats above still demonstrate how a number of privacy professionals must work alone or in small teams to drive privacy compliance at massive organisations with extensive personal data processing.

It can leave privacy professionals wondering, as we've mentioned above, *how can I increase collaboration on privacy to manage GDPR compliance in an organisation as extensive as mine?*

[1] Ibid.

Drive interdepartmental collaboration

Privacy Programs Differ - but collaboration is a challenge for everyone . As you can see from our recap of how companies currently structure their work on privacy, internal processes can vary, along with spend and team size.

From our conversations with privacy professionals however, we've seen that the general experience of working in the area of privacy management, especially with relation to the GDPR compliance, does not vary.

Experiences in this area are marked for many by more barriers to collaboration on privacy than enabling mechanisms. Combine this fact with fresh, complex legislation and a lack of resources to pursue full compliance, and one can immediately see why firms still find privacy management so fundamentally challenging - *and why privacy professionals like you may still be looking for ways to perfect their internal processes.*

COMMON BARRIERS TO COLLABORATION, AND PRIVACY SUCCESS

In any organisation where multiple business functions process personal data (ie. almost every business on the planet), a privacy agenda will be continuously confronted with a variety of challenges. However, chief among these challenges is collaboration.

This core collaboration issue essentially stems from how the work on privacy is structured. In medium to enterprise sized organisations, work on privacy and compliance with the GDPR requires input from stakeholders on a number of levels and typically, from leaders in every department. To drive initial momentum here, companies require board-level buy-in, a privacy leader or a team of privacy leaders, extensive legal expertise, and technical support.

You see where this is going. A program which transcends departments, involves multiple business functions, and multiple new (legal) ambiguities can spell disaster for those responsible for its success (for you).

The sheer image of it seems to challenge the possibility of effective collaboration on privacy. But in order to improve and diagnose this chaotic image, we need to understand exactly what the challenges to collaboration are for the individuals running privacy.

It's time for barrier number one.

1 Lack of buy-in

"There's information on our personal data processing everywhere, but it's just out of my grasp." We see this everywhere.

Recall that each business function often works with different categories of personal data, on different legal grounds, in vastly different IT systems. You, the privacy professional, are charged with gathering all this information effectively, efficiently, and on a regular basis from now on.

Many a DPO will confront resistance here because departments aren't incentivised from leadership to provide the kind of information necessary to complete records of processing. Or, even if the information is provided on processing activities, there can be little to no momentum as regards to taking action on any gaps or risks found by the privacy professionals.

In essence, the first barrier to collaboration revolves around lack of incentive to assist in the labour required to document specific data processing activities.

This brings us to barrier number two.

2 My departemental contacts can't spare the time

Another extremely common barrier. More often than not, privacy responsibilities – including records of processing creation – get passed either to department heads or to the individuals with direct control over the systems processing personal data in each department. We've seen this in a variety of organisations.

Unfortunately, these individuals will always have more pressing work to complete.

In the absence of coordinated guidance on completing privacy tasks, they may consider privacy work an added, perhaps even irritating task.

This brings us to our third, and most important barrier to cooperation on privacy.

3 Unstructured Privacy Agendas

A mental image of the way work on privacy is commonly structured might be taking shape in your mind by now.

Envision a long list of privacy related tasks, related to virtually every department, but disconnected from each department's core priorities. At the very top, this privacy agenda may be driven by stakeholders at the board-level, but its actual implementation is often left to privacy professionals like yourself.

One may find it hard to imagine a less-ideal scenario then the one above. Privacy professionals are tapped from existing legal or technical functions to drive complex responses to difficult questions on company-wide processing of personal data.

The above can result in scenarios where you are forced to play the role of task-master or advisor with those individuals in each department who have been given extra privacy responsibilities that they may dislike and/or misunderstand.

Can you understand the structural problem? Instead of tying success on privacy and GDPR compliance to the core priorities of each department, boards often haphazardly place privacy responsibilities on top of each department's daily workflow. Privacy is added externally rather than being built in to core business processes at each organisational level.

The result? Privacy professionals like you are appointed to corral countless stakeholders into providing information and taking action on privacy without being given the tools to make this easy or relevant. When it comes time to report on compliance progress or known risks, the identified gaps become meaningless because no efficient structure with which organisations can close these gaps exists.

MEET COLLABORATION CHALLENGES HEAD-ON

Luckily for privacy professionals (or privacy heroes as we like to put it) like yourself, these barriers to collaboration and success can be beaten.

Now that you know what specific challenges you face, you can go right to the heart of each issue.

INTERNAL SELLING SPIKES BUY-IN ANY DAY

Let's start with problem one, lack of buy-in. If you work in an organisation where privacy responsibilities have been delegated to disinterested department heads or system administrators, you need to put in the extra leg work to find other individuals in each department who are motivated by privacy concerns.

This will prove less difficult than it seems. Personal data protection presents a core concern for many consumers in today's data driven society, consumers who work in each department at your organisation. Come to those facing extra privacy responsibilities in each department with an openness to delegate core privacy tasks to individuals looking to step up to the plate.

In this way, you can guide departments with your legal, technical and privacy expertise to integrate privacy practices into their work internally. You will then have recruited other privacy champions who are motivated to see the work done in their departments.

Be prepared to internally sell privacy compliance as another method to drive stakeholder buy-in. Increasingly, investments in doing the work on privacy and GDPR compliance have been linked to shorter sales cycles, less data breaches, and better data governance.

You can use these points to your advantage when working with each department, showing them that if they put in the work now, their customers will reward them later.

NO TIME? NO PROBLEM

Let's move to collaboration barrier number two, lack of time. When individuals you rely on to drive privacy compliance in each department tell you they have no time, it's important to realise this stems from a lack of privacy understanding, and the perception that documenting personal data will be daunting. You need to provide them with a precise format for completing privacy tasks that is easy to work with.

THROW OUT YOUR SPREADSHEETS

If you are trying to push individuals at your company to document their respective personal data processes and complete the work to close any gaps in oversight, than trying to get them to execute this in an excel sheet with seven thousand rows just won't work out. Internal stakeholders will understandably protest that they don't have the time.

Luckily for you, cost-effective, scalable privacy management solutions already exist on the market. With a flexible and easy-to-use privacy management solution, empowering internal stakeholders to complete their privacy work, and follow up on requested changes, becomes much faster and more intuitive.

You need to look for a tool that already provides a custom-structure for documenting information assets and data processing flows in a way necessary to prove compliance, and sustain it over time.

As opposed to spreadsheets, with a tool like DPOrganizer for example, you can move beyond building out one time, stand-alone records of processing activities. Instead, from the moment you (or your team of privacy heroes) start tracing data processing with intuitive wizards, you'll discover myriad possibilities to monitor, track, review, and assess the data processing activities you record.

You'll not only structure your processing of personal data effectively in a compliance sense, but you'll also be loading your processing details into a sustainable digital structure that builds, audits, and protects your privacy program long-term.

Providing stakeholders access to such a tool presents a viable option for easing time complaints.

In a tool built for easy privacy compliance, individuals with access to privacy information, but who have no legal, compliance, or technical expertise, are guided to enter in the information they work with on a daily basis, in a flexible format.

With the ability to assign data processing reviews, kind reminders, and track risks, it becomes easier for you to tackle collaboration directly.

This brings us to our last barrier to collaboration.

BUILD INTERNAL PRIVACY AGENDAS ORGANICALLY

With privacy regulations fresh, complex, expensive, and worrisome for many a board-member, it will take time before businesses manage to build top-down structures that integrate privacy directly into each business function without clunkily attaching them to each manager's duties.

In the meantime, implementing a lightweight, effective privacy management solution such as DPOrganizer helps compensate for a lack of efficient workflows surrounding privacy and GDPR compliance.

This is because a tool like DPOrganizer is custom-built to help companies build upon their initial work on privacy. Using flexible data mapping features that guide you to structure company-wide documentation of data-processing activities, flows, storage locations, access-points, subject categories, and more, you'll be able to empower every individual at your organisation to contribute to filling in the gaps on how personal data is processed.

When it comes to driving a privacy agenda, this is already half the battle.

In order for companies to move forward on their GDPR compliance, they need an efficient, interactive way to coordinate knowledge sharing on privacy. Instead of sending privacy professionals like you into every business department to corral effort on privacy, collect results, and come back with requisite action points, a company needs a CRM-like software to guide these efforts.

With a software that asks consistent questions across every business function, you'll gain access to a meaningful gap analysis, and already possess the tool with which to delegate privacy tasks efficiently to close gaps.

Trying to manage a privacy agenda without a software is similar to trying to manage a marketing and sales funnel without a CRM-system. There are too many moving parts to keep track of in a way that drives progress and efficiency and enables collaboration.

This is how you involve your colleagues in your privacy management work, by providing them with a system to make their contribution easy and measurable.

REPORT WITH CONFIDENCE AND DRIVE PRIVACY KPI

For privacy heroes like you, reporting on privacy efforts in the absence of effective collaboration was (and may still be) hard. Afterall, how could you show progress on a privacy agenda where many were unwilling to contribute information that would make the project a success?

With a privacy management tool like DPOrganizer, tracking and reporting on core privacy concerns is finally a reality.

From DPIAs and high risk processing analysis, to scheduled reviews on processing activities and even incident management, you gain direct access to dashboards showing the overall status of data processing at your organisation.

This allows your colleagues to measure and appreciate the extent that they impact privacy efforts. It also enables board-level privacy leaders to turn legal confusion and technical complexity into measurable progress.

Integrate collaboration and measure the impact of privacy with DPOrganizer, your key to transforming privacy work-flows at your business.

DPOrganizer

DPOrganizer is a Software as a Service platform, designed by privacy professionals, for privacy professionals. From layout and structure to reporting and visualization, we create and update our software with the privacy professional in mind, covering the legal as well as the technical requirements for GDPR compliance.

We are based in Stockholm, Sweden, with an expert board of privacy professionals and customers in 18 countries across the globe.

At DPOrganizer, we believe privacy management can be made easier.

Contact information

HQ - Stockholm

📍 Centralplan 15, 1tr | 111 20 Stockholm
☎ Phone: +46 8 121 480 25
✉ Email: hello@dporganizer.com

London Office

☎ Phone: +44 7990 506332
✉ Email: hello.uk@dporganizer.com