Deloitte.

DPO Benchmark
Beltug Survey Report

MAY 2022

About Beltug

With over 2000 members from 490+ organisations, Beltug is the largest Belgian association of CIOs & Digital Technology leaders. We cover their priorities such as vendor and software asset management, 5G, hybrid IT, cyber security, artificial intelligence, the hybrid workplace, IoT, privacy, data governance, and many more.

We defend the interests of our members, develop positions, and support knowledge exchanges between our members. Each year, we organise more than 50 events for sharing experiences. Beltug also represents the business ICT users at the European and international levels, in close cooperation with organisations in other countries.
www.beltug.be

DPO survey

As explained below, now is the time to have a meaningful look at how organisations have administered the Data Protection Officer (DPO) role and how this position is being handled by various organisations. Therefore, it became clear there is a need for DPOs of larger organisation to have some benchmarking information. To this end we decided to organise a small survey, to share the experiences from privacy specialists from different sectors.

Foreword

The General Data Protection Regulation (GDPR) drastically altered the regulatory landscape not only for processing the personal data of individuals located in the European Union (EU), but also the specific requirements for the appointment and specific mandate of the data protection officer (DPO) in practice.

Indeed, due to the wide scope of the definitions and requirements contained in Article 37 of the GDPR as well as the so-called 'WP 29 Guidelines on Data Protection Officers', many organisations are now required to appoint a DPO as mandated by the GDPR (including implicitly an appropriate data protection governance structure to support such DPO).

Because the GDPR mandated these 'improved' DPO obligations already a few years ago, the time has come to take a more insightful look into how organisations across Belgium have dealt with these new requirements and how the DPO role is being fulfilled in practice.

The Beltug Privacy Council

As privacy is an important subject for companies, Beltug launched the Privacy Council. The Council provides a platform for experts to exchange experiences and best practices. This high-level, multidisciplinary Council meets, discusses and makes suggestions and recommendations to Beltug regarding issues, activities and lobbying efforts that can be undertaken in the area of privacy.

In this Council, it became clear there is a need for DPOs of larger organisations to have benchmarking information. That is why it was decided to organise a small survey, to share the experiences from privacy specialists from different sectors.

We therefore invited the members of the Privacy Council DPOs from organisations based in Belgium to participate in this qualitative survey, covering the major industry sectors, such as finance, banking & insurance, healthcare & pharmaceuticals, and the public sector. These individuals comprise of full-time and part-time DPOs appointed from large and mid-sized corporations that operate in one or several countries. In other words, the DPOs questioned represented a wide range of organisations with different operational environments **(see fig. 1 to 3 on pages 6 and 7)**. 28 DPOs responded. To provide these insightful observations, the survey included 44 targeted questions pertaining to not only the strengths and weaknesses of an organisation's data protection compliance programme, but specifically to DPO-related items such as e.g., how the DPO functions within the organisation, what the DPO's main challenges are, and what skill sets are considered most important to be a successful and effective DPO. The main purpose of this report is to highlight the key survey findings about how Belgian organisations have fulfilled their DPO obligations, an evaluation of recent trends regarding how the DPO position has evolved as well as to hear from DPOs directly themselves regarding their priorities and views on their role within their organisation.

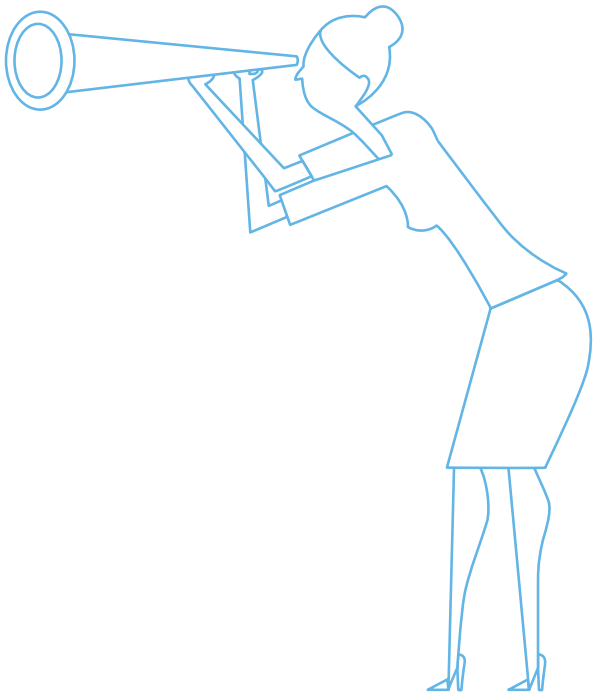
In summary, this report aims to present a holistic 'in the field' viewpoint from DPOs across a range of organisations varying in size and industry. We hope it provides some insightful key takeaways that organisations can leverage to improve both the effectiveness of their DPO function, as well as the overall maturity level of their data protection initiatives.

Our main findings are divided into five focus areas:

1. **The DPO role is as unique as the organisation that has employed it.**
Each organisation has its own operational environment and personal data processing activities. Due to these unique characteristics the survey shows a very diverse result regarding the manner in which reporting lines, resources, budget allocation as well as required DPO competences and way of working, have been implemented. This finding highlights that the uniqueness of each industry and organisation still necessitates a thorough internal reflection to determine whether its DPO mandate and allocated resources are appropriate for the data protection risks they face.

2. **An effective data protection governance structure is often lacking.**
Although, from a formal point of view, some form of a data protection governance structure often exists, our survey highlighted that the DPOs consider that much more needs to be done to render governance more effective and sustainable. Three areas of lack of effective data protection governance were identified in the survey. They are (i) lack of awareness and support at top management level (while also a need to improve awareness amongst employees), (ii) no clear assignment of privacy accountability or policy enforcement throughout the organisation, and (iii) lack of workable policies and procedures. To better help the DPO fulfill his/her obligations effectively and to ensure a collaborative approach throughout an organisation, there needs to be a strong overall governance structure (and not just limited to the DPO function) which exemplifies and explains the importance of assigning correct and sustainable data protection accountability throughout the entire organisation.

3. **Money talks – selective prioritisation.**
It is no secret that organisations are greatly concerned about their bottom line and will ensure taking necessary actions to preserve their reputation and financial wellbeing. The survey highlights how certain specific areas of data protection compliance are prioritised over implementing a holistic data protection approach. Therefore, it appears that organisations are first most concerned about financial penalties when prioritising data protection initiatives. As



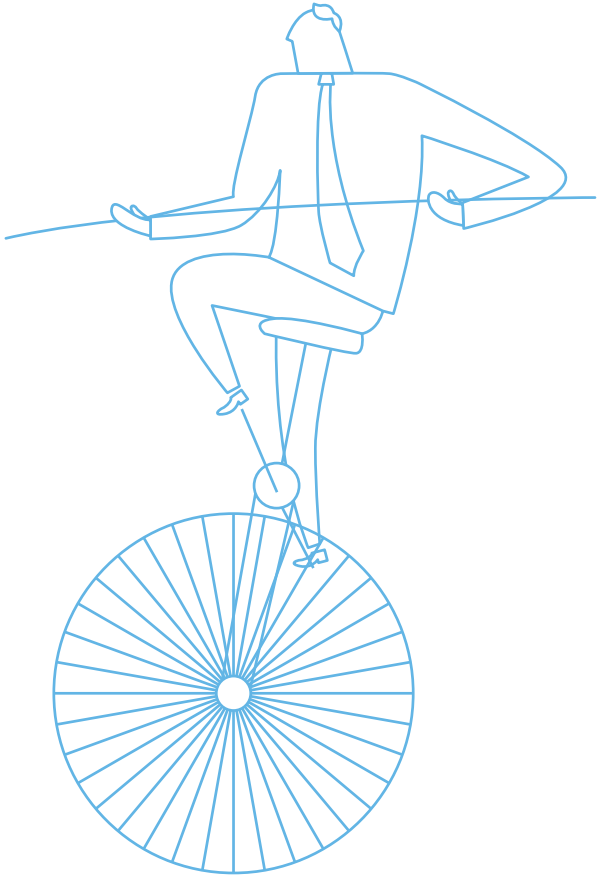
such, data protection obligations that have more outward looking elements, such as data subject rights management and data breach management, were prioritised over other obligations that were less visible or more complex because of e.g lack of legal certainty such as privacy by design, third-party data transfers (e.g., Schrems II) or document retention. While we understand why organisations have prioritised certain areas for the above stated reasons, both regulatory and operational focus has meanwhile evolved and organisations should pay more attention to other data protection compliance areas that would promote longer term benefits.

4. Different levels of maturity for different data protection initiatives.

Building off finding 3 piecemeal approach to the data protection risks, the survey found that there are significant variations in terms of maturity levels between the different data protection initiatives within each organisation. At the same time, the data protection regulatory landscape is continuously changing through new regulations, court opinions and regulatory guidance. Due to these factors, the so-called 'baseline' compliance expectations are shifting. This will require organisations to start focusing more on lesser mature data protection initiatives such as e.g., third-party data transfers (e.g., Schrems II and Cloud), document retention, privacy by design etc.

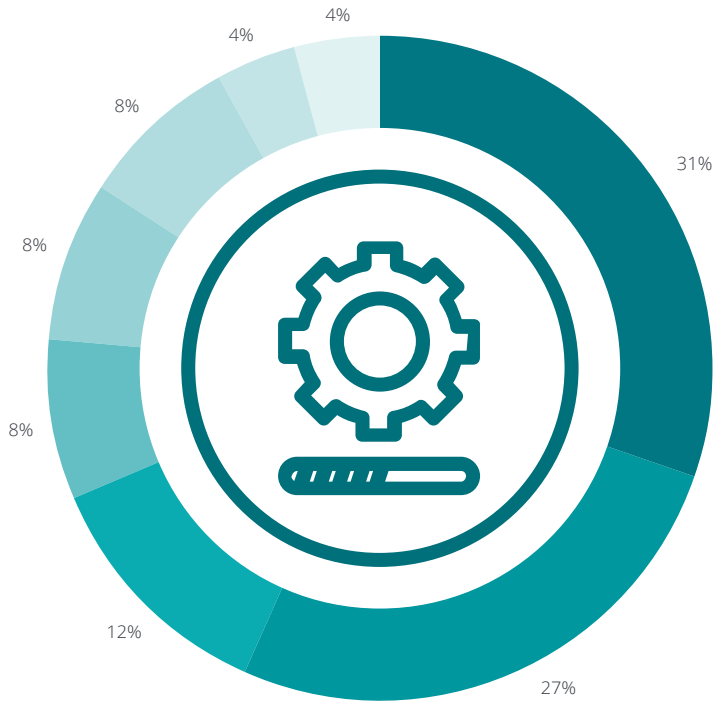
5. What organisations need from a DPO and vice versa: need for a two-way street.

The role of the DPO is clearly evolving from a 'firefighter' to more that of a 'facilitator'. This finding looked at what characteristics and resources are vital for an efficient and successful DPO such as e.g., excellent communication and interpersonal skills, helicopter view, balancing compliance and business interests, etc. Similarly we looked at what a DPO needs from the organisation. As such, the survey shows that the DPO's main asks for management are (i) more resources, (ii) more management support and (iii) correct assignment of (data protection) accountability within the organisation.



Demographic

Figure 1a. Industries



- g) Public Sector (Including state-owned companies)
- i) Other, i.e., entertainment, airport services, research institute
- b) Technology, Media & Telecom
- d) Consumers & Retail Goods and Services
- f) Healthcare & Pharmaceuticals
- h) HR staffing and related services
- a) Finance, Banking & Insurance
- c) Industrials & Manufacturing
- e) Energy, Mining & Infrastructure

Figure 1b. Full-Time/Part-Time

- Full-time
- Part-time. If part-time combined with what function(s) and what percentage of time is spent on privacy?

Figure 2. Geographical Operational Landscape

54%
Operate in one European country

12%
Operate in several European countries

35%
Operate in several EU countries and globally or outside of Europe

Figure 3. Size of Organisation

12%
Less than 100 employees

0%
100-500 employees

15%
500-1000 employees

35%
1000-5000 employees

38%
More than 5000 employees

01

The DPO role is as unique as the organisation that has employed it

01 The DPO role is as unique as the organisation that has employed it

The primary role of a data protection officer (DPO) is to assist the organisation in ensuring that IT processes the personal data of its staff, customers, suppliers, partners or any other relevant individuals, in compliance with the applicable data protection rules. This first finding will provide some insights regarding the role (and mandate) of a DPO within an organisation, how they function within the wider organisation as well as the resources that they have been equipped with to fulfill their role.

The survey illustrates a very diverse result on the way that resources and budget have been allocated to privacy teams (see fig. 5 and 6). While this finding on the one hand is not so surprising (as each organisation has its own distinct operational landscape and data protection risks), it is a finding that cannot be understated. It highlights already that one of the lessons learned from this survey is that the uniqueness of each sector and each organisation necessitates a thorough internal reflection of an organisation's personal data processing activities, in order to determine whether its allocated resources are appropriate for the data protection and privacy risks they face. By conducting an internal analysis which looks to balance the scales of the regulatory risks and the risk mitigating resources available, an organisation will be able to assess more accurately the DPO mandate as well as the actual resource needs of a DPO in relation to assisting in obtaining an organisation's 'ideal' GDPR compliance maturity level.

It was found that DPOs are leveraged in various sectors and industries, and therefore, successful DPOs should have strong competencies that go beyond specific subject data protection knowledge. DPOs (and their roles) are not 'one size fits all' and organisations must evaluate what other skill sets are needed or be willing to allocate resources to help train on industry specific issues. Again, organisations must internally reflect on the specific needs of their operational landscape and must apply this rationale to the DPO role.

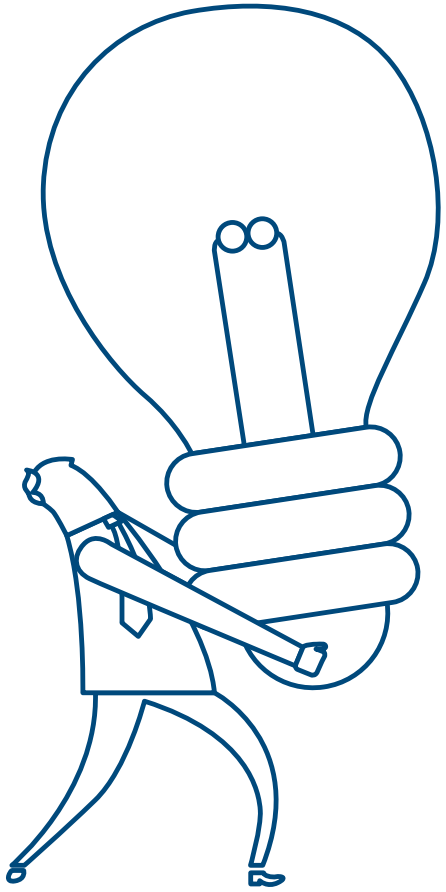
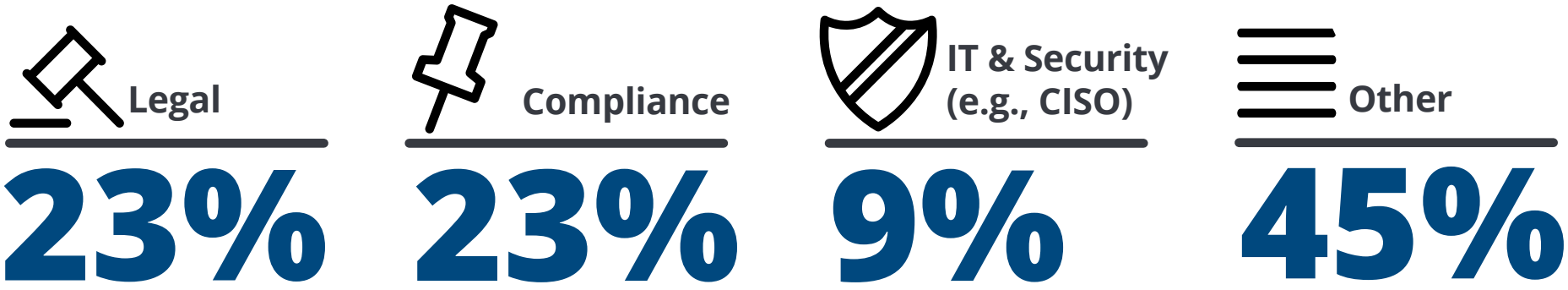


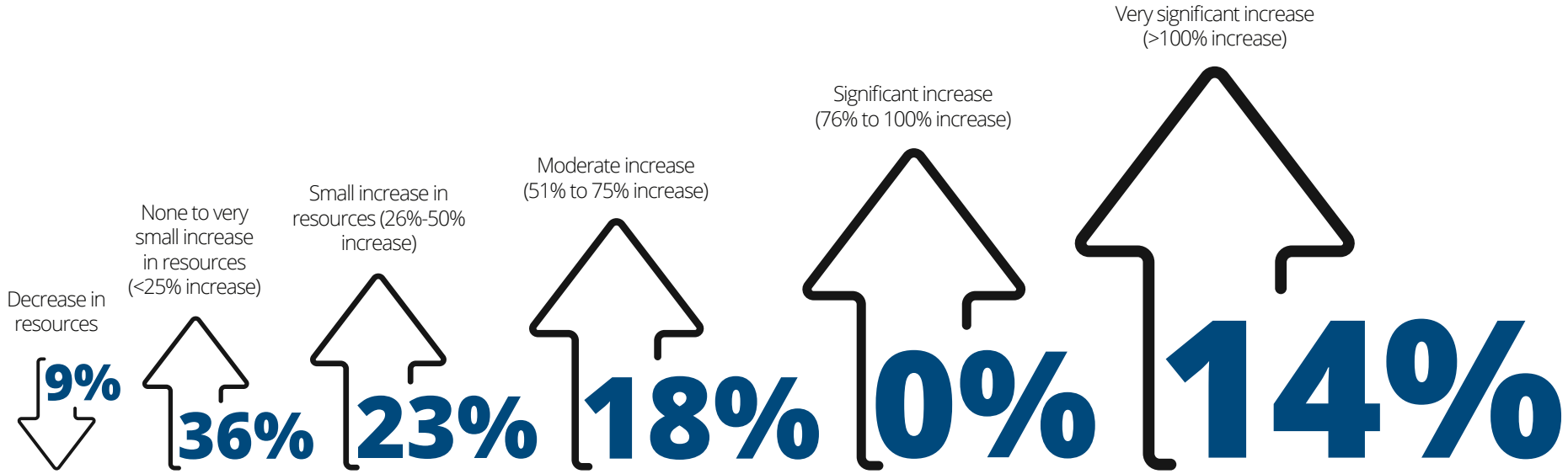
Figure 4. In which business unit does the DPO sit?



The survey also highlighted a big difference in how organisations employ DPOs. It was found that a bit more than half the organisations leverage a full-time DPO and external staff to help support privacy related issues (see also fig. 1b). However, the survey also illustrated that some organisations have only employed a part-time DPO with no external support. These differences further demonstrate that there is not one particular preferred DPO model that is currently used.

The implementation of the GPDR in 2018 has impacted the participating organisations in different ways with respect to resources and capacity for their privacy team. The majority of the respondents have shared that the increase of resources since 2018 was 'non-existent to very small (<25% increase)', this is vastly different from a small number of respondents that shared that they experienced a very significant increase of resources (>100% increase) (see fig. 5).

Figure 5. Increase in capacity today (2021) compared to before GDPR implementation (2017)



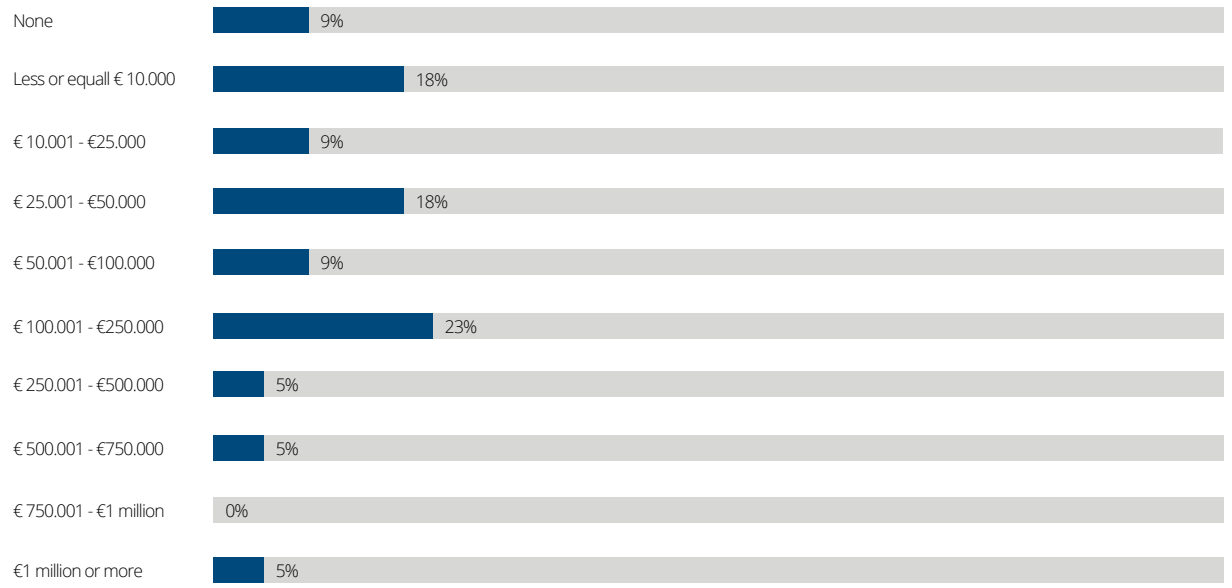
The discrepancy between these available resources is remarkable, as the legislative privacy landscape has changed substantially with the introduction of the GDPR, increasing the operational impact on any organisation (and its DPO role).

Aside from making capacity available for the privacy mandate, the respondents have shared that their organisation provides them with a yearly budget for data protection compliance costs that mainly ranges between less than 10.000 euros (18% of respondents) up to 250.000 euros (23% of respondents).

This budget excludes salaries of DPO staff and privacy and security technology licensing fees. The budget available for data protection compliance costs should be in line with the risk awareness of the business lines and the size of the organisation. We noticed that, if the business line has a high level of privacy awareness, the required budget shall be on the lower spectrum, as less budget will be necessary for costs such as external counsel fees, internal/external hired resources, and training & awareness sessions. In order to determine a suitable budget to address their concerns, the organisation should internally reflect on their operational landscape and personal data processing activities. A DPO can also assist with providing a budget estimation by examining the effectiveness of the organisation's privacy programme and the overall compliance with data protection regulations. Organisations can explore new ways in which they can allocate their budget by looking at how other organisations have allocated their data protection and privacy compliance budget. However, this should not be considered as a main guideline to follow as it cannot portray a clear benchmark for their organisation.

In summary, with respect to the DPO role, the survey has provided clear insights into how organisations employ the DPO and how they provide resources in support of its mandate. It is apparent that each organisation has its own needs and requirements regarding the DPO and how they should be utilised. The insights provided by the survey show that the organisations have made a broad range of budgets available for data protection and privacy compliance costs. This range indicates a drastic difference in how organisations handle their data protection and privacy compliance concerns.

Figure 6. Total yearly budget/fees spent for data protection/privacy compliance costs



Deloitte point of view

We do not find it surprising that organisations across Belgium have varied in how they allocate resources and budget and how they staff their data protection programmes. Each organisation is unique in its operational landscape, revenue, and risk appetite. However, it is noteworthy to also highlight the DPO role in its very nature is unique and is still a relatively new position. It also highlights that one of the lessons learned from this survey is that the uniqueness of each sector and each organisation necessitates a thorough internal reflection of an organisation's personal data processing activities in order to determine whether its allocated resources are appropriate for the data protection and privacy risks they face. By conducting such an analysis, an organisation will be able to assess more accurately the DPO mandate as well as the actual resource needs of a DPO in relation to assisting in obtaining an organisation's 'ideal' GDPR compliance maturity level. Coupling these facts together, it becomes even more important for organisations to understand how the DPO role should be fulfilled in practice and especially how DPO support and overall accountability for data privacy compliance should be further disseminated throughout the organisation.

Organisations that take a proactive role in 'right-sizing' the DPO mandate and resources, will be in a much better position regarding compliance with current data protection obligations such as e.g., better oversight of processing activities, quicker response times regarding new or amended regulatory obligations, etc.

Organisations must also think strategically on how the DPO will interact with other workforce members and business units. While DPOs are leading the charge for data protection initiatives within an organisation, they cannot ensure compliance alone. Privacy accountability must be borne by the organisation as a whole. This requires clearly defined roles and responsibilities for all business and support units within the organisation.

It is not easy to determine the 'appropriate' level of privacy related resources, staffing and budget as the GDPR and data protection obligations have been implemented recently and are evolving over time. We do believe that the survey shows that organisations must take a more active role in determining how much resources should be spent on the DPO and data privacy compliance. The majority of the respondents stated that their resources have decreased, increased only slightly or remained the same since 2018. Meanwhile, with the increasingly rapid evolution of (digital) data management, we have seen an increased shift in global data protection regulations and other (digital data) regulations that interact with data protection. This (digital data) trend will only continue to increase and organisations that fail to accurately determine how to deploy the DPO role and allocate appropriate resources, will be at risk of falling seriously behind with their data protection obligations.

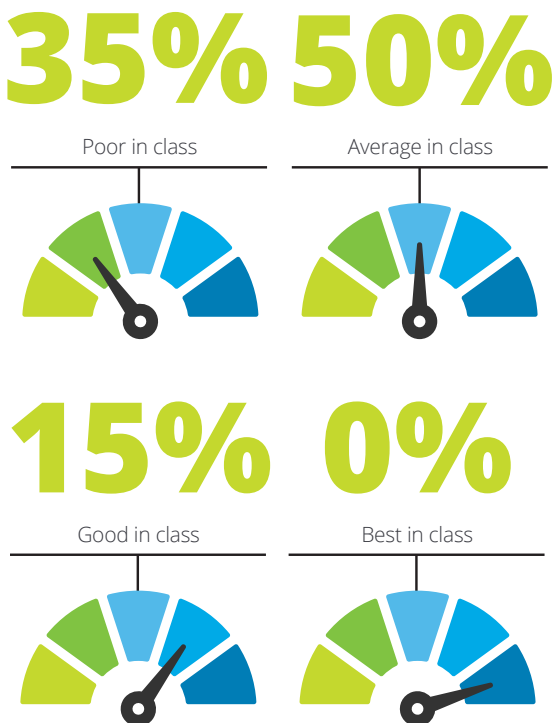
02

An effective data protection governance structure is often lacking

02 An effective data protection governance structure is often lacking

The governance structure and responsibilities regarding data protection and information security have significantly evolved in recent years. Due to new emerging technologies, such as the cloud, big data and artificial intelligence initiatives, there are increased risks for individuals' rights. Now organisations must take steps to ensure that they provide adequate protection to personal data across their entire organisation and its partners. One of the most significant measures that should be put in place, is a strong governance structure that champions data protection and information security.

Figure 7. Company privacy governance structure is often lacking



The DPO survey highlights how DPOs largely believe that the governance regarding personal data and information security can be improved and consider these areas to be more paramount in the operational landscape of their organisation. There are three central areas where there is a lack of governance. They are:

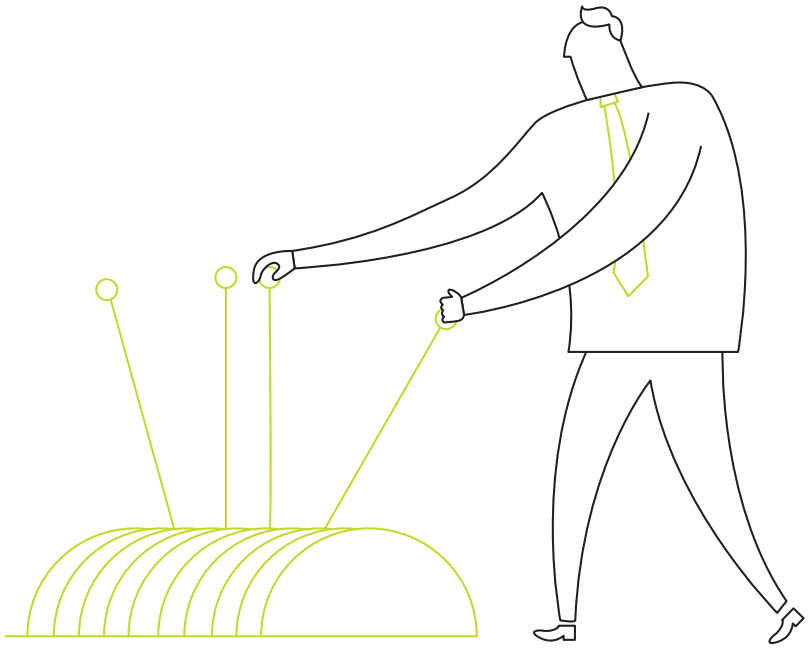
- Lack of awareness and support at the top management level
- No clear assignment of privacy accountability or policy enforcement
- Lack of workable policies and procedures

This is a very important – and often underestimated – finding of the survey resulting in potentially important risk of non-compliance. Top level management will not know how the organisation processes data, and therefore, the organisation will not be able to adequately determine whether appropriate measures are in place to safeguard the data and ensure that there is a lawful basis for processing. Additionally, when data and DPOs are not championed within an organisation, their importance is lost on its workforce members. This lack of understanding can lead to workforce members not fully understanding their role in privacy governance and therefore potentially processing personal data in a non-compliant way.

A similar result can happen when there is a lack of workable policies and procedures or when such policies and procedures are not properly enforced. Employees need to know how they are supposed to process personal data in their daily jobs and how to react or escalate when certain events arise. Without clear procedures, proper awareness and clear support from the top, employees will often work in an ad hoc manner exposing the organisation to potential non-compliance risk.

Ultimately, with respect to privacy governance, the survey provided some significant insights into the nature and structure of privacy governance within an organisation. Most meaningfully, in the survey, almost all DPOs felt like there is significant room for improvement in terms of actual governance as opposed to a theoretical governance structure. They indicated that such improvements are necessary and would benefit the effectiveness of their data protection initiatives and the DPO's role, as a better governance structure would further champion the importance of data protection throughout the organisation.

Organisations should evaluate how they govern personal data and what messages they are sending out to their employees. Most importantly it must be noted that if top level management does not take the protection of personal data seriously, neither will the rest of the staff.



Deloitte point of view

Personal data is a unique thing. It is valuable, very transient, and can be difficult to manage, especially if the boundaries of its processing and sharing are not clear. Additionally, it was not until relatively recently that organisations have been clearly mandated by the GDPR and subsequent guidelines to provide more protections for personal data in a sustainable and integrated manner ('privacy by design').

Working with a DPO and ensuring the right level of data protection is a question of culture and change management because, in order to achieve compliance, data protection must be effectively embedded within the entire organisation's processes, internal rules and way of working. The DPO alone should not and cannot make this happen.

It is a fact that data privacy and data protection have historically often been considered a strictly 'legal' or 'IT issue' that would be solely handled by an organisation's Legal or IT team. These factors combined provide a clear rationale for why organisations tend to lack a strong integrated governance structure versus a more siloed and 'theoretic' one.

However, organisations must now take more efforts to ensure that personal data protection is handled adequately and holistically at the governance level. We see the negative consequences when key stakeholders lack awareness of the data protection issues and regulatory obligations, and do not know how their organisations' privacy compliance obligations actually translate into their daily tasks. Without such an overall privacy governance (and awareness) structure, data protection initiatives will most likely fail or significantly fall short of their primary aim: ensuring that data management can be done in a compliant and effective manner.

Lastly, personal data compliance in practice is still relatively new to many employees and they lack comprehensive understanding of its importance and its regulatory obligations. In order to promote better buy-in from employees, data protection needs to be championed from the top down. Board and management level employees should help explain its importance and foster a culture of data protection compliance and culture throughout the entire organisation, not just within the Privacy team. Indeed, the survey results show that management's accountability for privacy compliance is often lacking, as the DPO is often seen as the sole responsible figure for data protection within an organisation. Tasks such as performing DPIAs (Data Protection Impact Assessment), TIAs (Transfer Impact Assessment) or fulfilling the ROPAs (Records of Processing Activities) are typical tasks that managers deem as 'tasks for the DPO'. Reinforcing awareness and accountability at the top level will not only improve the quality of employees' compliance, but also benefit the role and effectiveness of the DPO.

We believe that organisations must (re-)evaluate their own governance structure regarding data protection. Times have changed, and (personal) data has become more central to a company's operational landscape. Given the current and future reliance on, and importance of, (digital) data management, it would be negligent for organisations to ignore these changes and not examine how they holistically should deal with data protection. We believe that organisations that take the effort now will be best suited to deal with successful data management in the future and be ready to adopt new business ventures or further incorporate additional emerging technologies.

03

Money talks – selective prioritisation

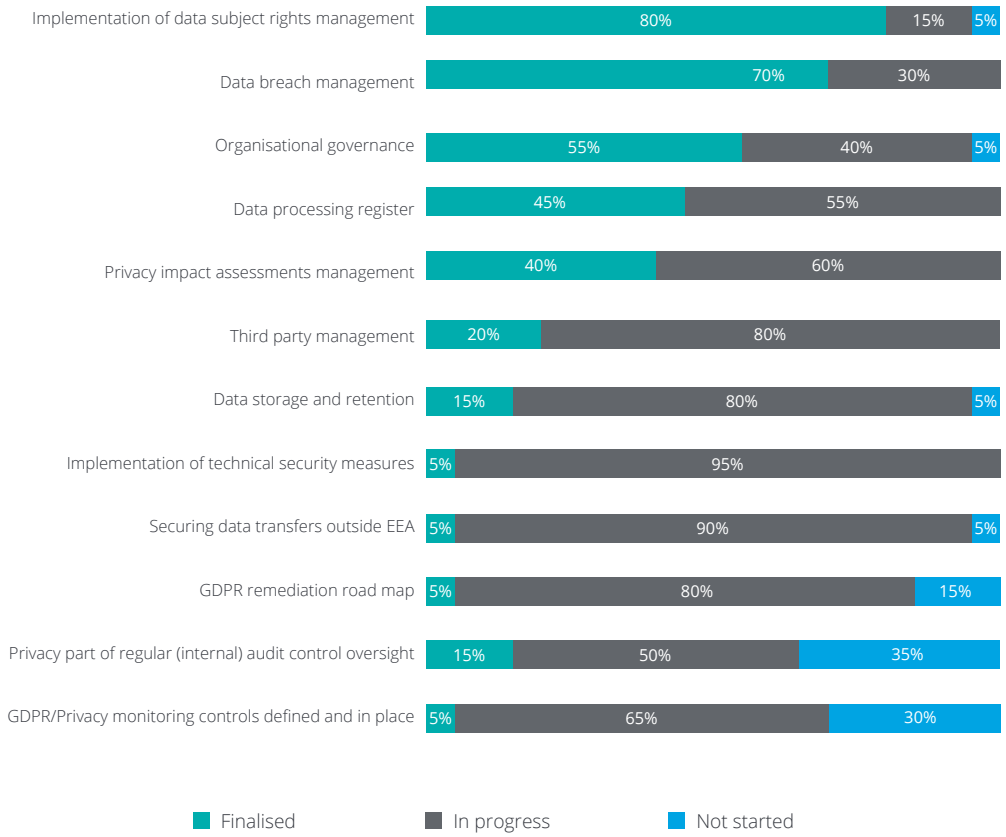
03 Money talks – selective prioritisation

It is no secret that organisations are greatly concerned about their bottom line and will ensure taking necessary actions to preserve their reputation and financial wellbeing. The survey highlights how certain specific areas of data protection compliance are prioritised over implementing a holistic data protection approach. As such, the DPO's responses explain how organisations were primarily motivated by financial and reputational harm. While there are many factors that could contribute to how and what areas organisations prioritised for their GDPR compliance (e.g., so-called low hanging fruit, some areas are dependent on the maturity of others, their operational landscape), there was a clear indication that financial and reputational harm were the most motivating factors.

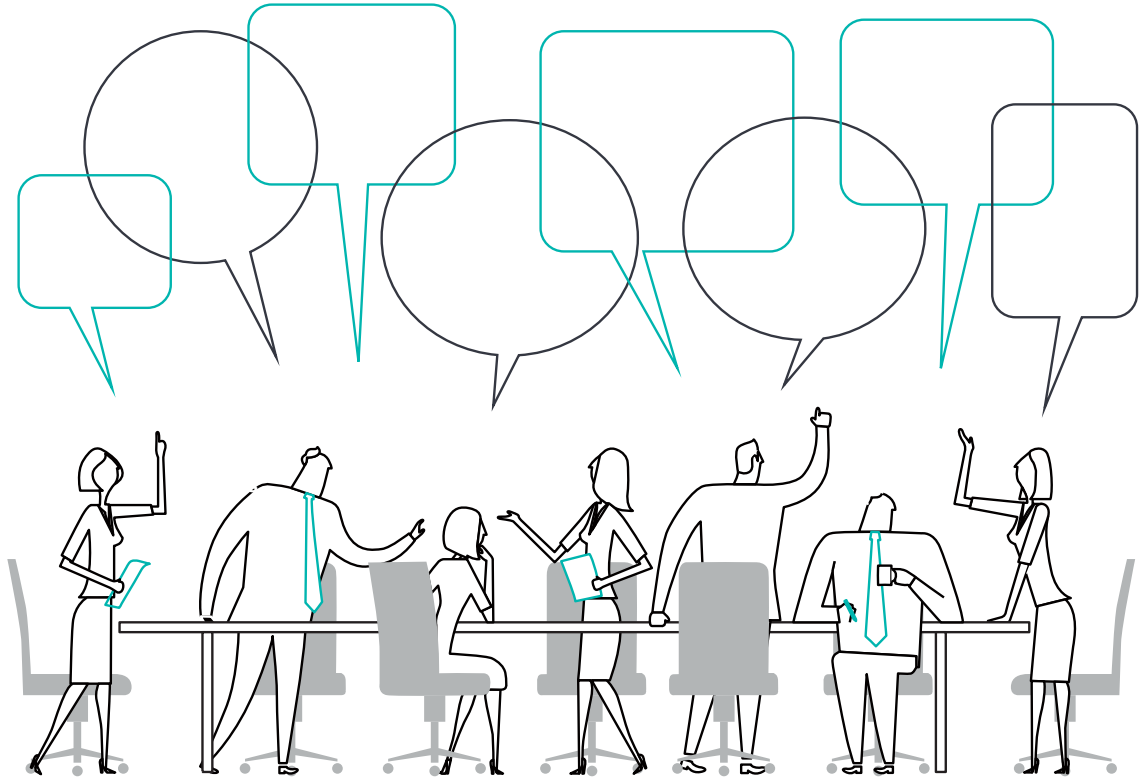
The responses to 'Why did your organisation appoint a DPO?' provide a clear pattern that demonstrates that organisations appointed a DPO because it was a mandatory legal requirement. While some DPOs in the survey were able to provide up to three reasons for their appointment, most DPOs only provided one reason, a mandatory legal requirement. Additionally, when the DPOs provided multiple reasons, the mandatory legal requirement was consistently considered the first reason.

The results from the survey state that the most mature areas of compliance are data subject requests and data breach management (see fig. 8). The maturity of these compliance areas further supports the notion that organisations have chosen to prioritise those privacy compliance obligations that have a clear 'external' component such as e.g., data subject requests.

Figure 8. The most mature areas of compliance



However, organisations in the survey seem to be less mature regarding compliance for areas that are less visible and more 'inward facing', such as e.g., privacy by design. Implementing controls for privacy by design (e.g., for data subject requests) require significant resources that must be implemented across the entire organisation. However, it seems likely that organisations prioritised data subject requests due to the fact that it is easier to prove non-compliance which leads to more financial penalties. According to the DPOs in the survey, another decisive factor influencing an organisation's priorities is legal certainty. When there are clear cut rules applying to a certain area of compliance, it is easier for an organisation to make choices. When this is not the case and certain rules may still be subject to interpretation, organisations tend to be reluctant, postpone their action and potentially challenge their DPO's advice on these uncertainties (e.g., on what is proportionate, legitimate, a reasonable expectation, etc.).



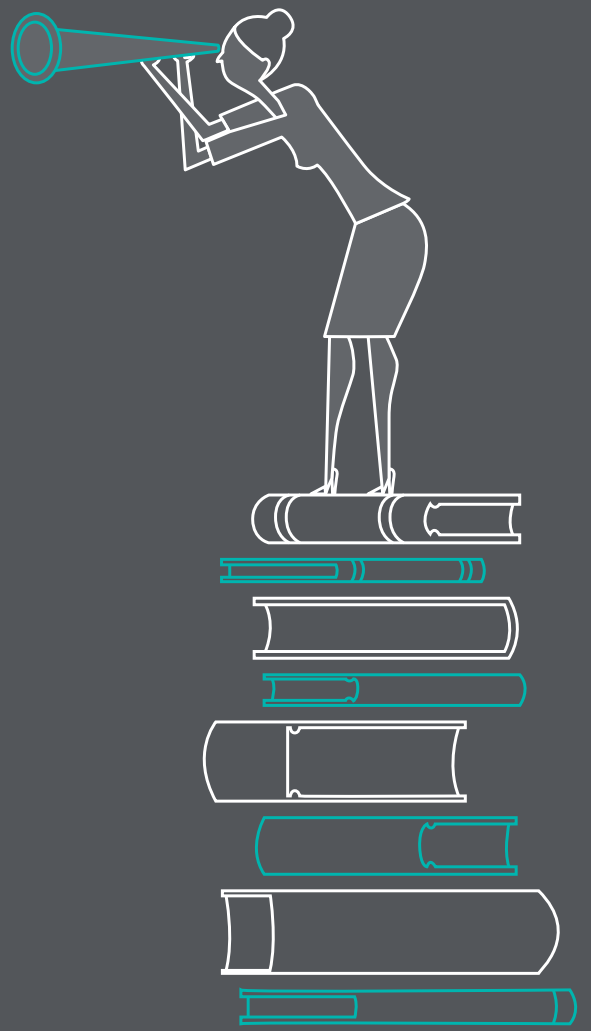
Deloitte point of view

While we understand why organisations prioritise certain areas of compliance due to higher chances of receiving a monetary fine or suffer reputational harm, organisations should pay significant attention to other compliance areas that would promote long term benefits. For example, a strong privacy by design initiative would reaffirm privacy and data protection obligations that employees are trained on, it would also help organisations look holistically at their data, what third-party vendors are leveraged, and what technical and organisational measures would help reduce risks to data subjects. In other words, privacy by design forces organisations to (re)examine their personal data processing activities and implement measures as they are developing their (data) initiatives.

In addition to the above, it must also be kept in mind that, when starting an investigation on a specific apparent violation (following a complaint, press release, or breach notification), the Data Protection Authority usually requires organisations to fill in a thorough questionnaire (of approximately 50 questions) whereby it assesses the organisation's compliance in all areas. This is indeed an in-depth investigation in which the DPA's intention is that of digging into less visible areas of compliance as well. It is therefore crucial for an organisation to refrain from neglecting those areas of compliance that would normally fall outside the scope of its priorities.

Moreover, these 'forced' assessments bring other benefits such as troubleshooting technical issues that arise with personal data before certain investments are made and provide more clarity for the organisation on what data is being processed and where it is stored. Numerous organisations are currently spending considerable monetary resources and manpower to determine what data they are processing and where it is being stored due to the lack of oversight.

Ultimately, while it is understandable that organisations have prioritised initially certain privacy compliance areas for the above stated reasons (e.g., data breach and data subject access requests), both regulatory and operational focus has meanwhile significantly evolved. Therefore organisations should pay more attention to other data protection compliance areas that would promote longer term and more structural benefits (e.g., privacy by design, document retention, sharing of data internationally etc.). As such a realistic and integrated 'privacy by design' approach throughout the entire organisations' processes is no longer a 'nice to have' but has become a 'must-have' for effective and sustainable data protection compliance.



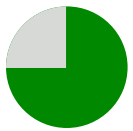
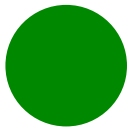
04 Different levels of maturity for different data protection initiatives

04 Different levels of maturity for different data protection initiatives

As concluded in the third main finding (3. Money talks – selective prioritisation), organisations tend to prioritise strict legal requirements due to the fear of reputational and/or financial harm. Consequently, there is a clear variety in maturity levels between different areas of data protection within such organisations.

In the survey, such maturity levels, that range from 1-5, are labelled as: ad hoc (1), repeatable (2), defined (3), managed (4), and optimised (5) (see fig. 9 below).

Figure 9. Levels of maturity

Ad hoc Level 1	**Repeatable** Level 2	**Defined** Level 3	**Managed** Level 4	**Optimised** Level 5
				
Capability is typically undocumented and in a state of dynamic change, tending to be driven in an ad-hoc, uncontrolled and reactive manner. Basic/Early level of implementation.	Capability is performed on a regular basis, but is not formalised or consistent. Coverage is not agreed or comprehensive. Mostly at a standard level of implementation, but still basic in places.	Capability is formally documented, with an agreed ownership and scope, and is used throughout the majority of the organisation. Standard level of implementation.	Capability is actively maintained and performance is regularly reported in a format that can be actioned. Advanced level of implementation in places, with almost full coverage.	Capability is continually improved trough both incremental and innovative changes. Advanced/industry leading implementation and full coverage.

Thus, while the DPOs in the survey defined their organisations' general maturity level as either 'defined' (45% of respondents) or 'repeatable' (35% of respondents), with only a minority responding with 'ad hoc' (10% of respondents) or 'managed' (10% of respondents), and none deeming it as 'optimised', it is clear that significant differences exist between the (perceived) maturity levels of the individual GDPR related projects (fig. 10, fig. 11).

Figure 10. Maturity of the Privacy by Design initiative

Figure 11. Training and Awareness initiative

As stated in the third main finding above on selective prioritisation, it seems that the more visible an area is – increasing the ability to assess its (non-)compliance and levy administrative fines – the higher its maturity is. Implementation of data subjects rights management (the handling of a subject's rights and requests) and data breach management, therefore, rank at the top. On the other end of the spectrum, the more inward facing areas – ranging from data storage and retention, to third-party management – are largely considered only 'in progress'.

When asked about what is keeping the DPOs in the survey mostly awake at night, they listed cross border data transfers, allocating (enforcing) appropriate accountability at business level and finding where data are within the organisation, as the most important challenges for data protection compliance today.

Indeed international data transfers (in particular, the security of transfers outside the European Economic Area or EEA), have become a significant point of attention. Following the Court of Justice of the European Union's Schrems II decision of July 2020, the European Data Protection Board (EDPB) adopted new GDPR guidelines in November 2019 (on the territorial scope of the GDPR) and November 2021 (on the interplay between the GDPR's territorial scope and international data transfers) reflecting the changes in their prioritisation. This was also signalled by the DPOs, noting that they perceive international data transfers to be the most challenging remediation item to their organisation (fig. 12).

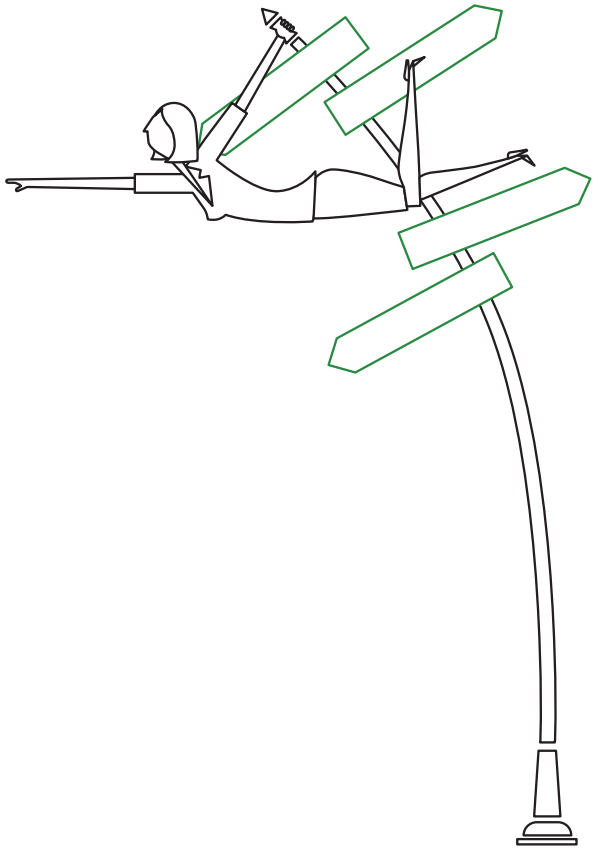
Figure 12. Most difficult data privacy concerns according to DPOs

Another area with room for development according to the DPOs in the survey, is data protection by design and default. The approach (to ensure data protection through technology design) is regulated in the GDPR, stating that it should consider the state of the art, the cost of implementation, and the nature, scope, context, and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing activities.

Hence the EDPB published guidelines in October 2020 on its Article 25, regulating data protection by design and by default.

In this area too, the DPOs' replies highlight the lack of maturity of their organisations' privacy by design approaches as the majority scored them to be 'ad hoc' (45% of respondents) and 'repeatable' (20% of respondents) – to reiterate, these are the lowest levels. Security measures to protect personal data, the identification of internal data flows, and training and awareness, moreover remain challenging remediation items. The latter's maturity level was scored as 'repeatable' (40% of respondents) or 'defined' (30% respondents).

The reason behind these results (especially privacy by design/default) is that the DPO is often consulted when a project has already started. Because the DPO is not given the opportunity to intervene from the very beginning, it will be more difficult for him/her to issue an opinion on a project that has already received other internal approvals or recommend changes which might heavily impact the project. In some cases, this absence of early involvement, according to the DPOs in the survey, is due to the managers/colleagues' lack of understanding of the DPO's role and, in other cases, because the DPO is simply avoided on purpose.



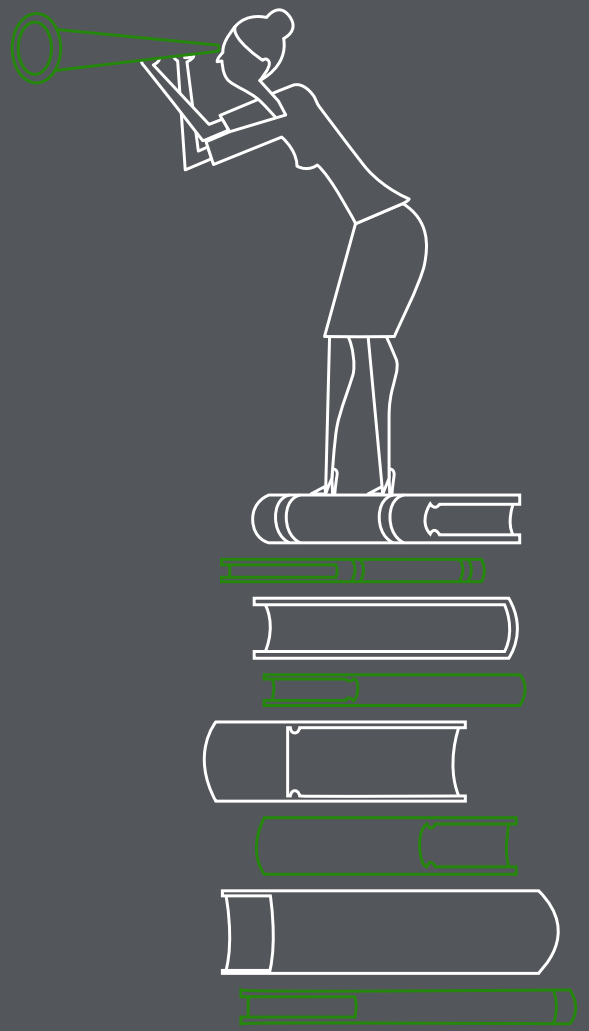
Deloitte point of view

Building off finding 3, i.e., the often piecemeal approach by organisations to the data protection risks, the survey found that there are significant variations in terms of maturity levels between the different data protection initiatives within each organisation. At the same time, the data protection regulatory landscape is continuously changing through new regulations, court opinions and regulatory guidance. Due to these factors, the so-called 'baseline' compliance expectations are shifting. This will require organisations to start focusing more on lesser mature data protection initiatives such as e.g., third-party data transfers (e.g., Schrems II and Cloud), document retention, privacy by design, etc.

We fully understand that determining what compliance areas to focus on can be complicated. Furthermore, we know that these decisions require informed stakeholders that are about to effectively communicate on the topic of personal data. While the DPO should help facilitate these discussions, they are dependent on their co-workers' input. The DPO should also inform management and employees of the current maturity levels for the various compliance areas.

It is also important to develop clear roadmaps to help determine next steps in the compliance process and which measures should be taken and when. As we have seen with the Schrems II case, new obligations can develop and drastically alter the regulatory landscape. These roadmaps better situate DPOs and their organisations to continue their compliance measures, while incorporating new obligations.

In conclusion, it is likely that these increased expectations from DPAs and recent court rulings holding new obligations, will cause a shift in what organisations will focus on. It is, therefore, essential for DPOs to have their finger on the pulse of current events and for organisations to be agile and ramp up different compliance measures to manage the fluidity of the data regulatory landscape.



05

What organisations need from a DPO and vice versa: need for a two-way street

05 What organisations need from a DPO and vice versa: need for a two-way street

As a concluding finding, and reflecting the uniqueness of the role of DPO, we will discuss here the results of the survey related to what organisations need in a DPO, and vice versa.

Balancing, complexity, management, and reconciliation between compliance constraints and business interests; these are some of the key expressions DPOs in the survey use to describe their main roles. The explanation behind this lies in the fact that successful DPOs must have, in addition to their privacy subject matter expertise, also domain knowledge of several different areas, such as legal (both internationally as well as local level), (information) security, technology (IT), and risk management. They must also have a good understanding of the business operations and processes, as well as the sector/organisation itself.

In addition to this, DPOs are sometimes asked to provide advice on other regulatory obligations and perform duties beyond data privacy and protection. It seems that a so-called 'helicopter view' is really required to better facilitate the DPOs' performance as they must be able to wear many different hats – ranging from acting almost as a CISO to being the Head of Risk & Compliance.

Operating under the above-mentioned different hats inherently leads to the question of where the DPO's position should be inserted within the organisational governance structure. The survey demonstrates that, as it relates to DPO reporting lines, DPOs do report to senior management in some fashion, but not all in the same manner. While almost half of the organisations' DPOs report directly to the CEO (45% of respondents), others report to – among others – the Head of Legal (27%), the Chief Compliance Officer (9% of respondents) or the Chief Financial Officer (5% of respondents). An equally small minority (5% of the respondents) report to the Head of IT. This falls quite in line with the respondents' answers to the question "in which business unit does the DPO sit?" to which the answers equally varied from legal (23%), compliance (23%) or IT & Security (9%). Of the remaining 45% of respondents, half marked themselves as a separate and/or independent department or function, who still had the obligation to report.

This dispersity can have an effect on the internal communication and governance of the organisation. Namely, almost half of the DPOs indicated – as far as the effectiveness of their companies' privacy/GDPR compliance programme is concerned – the following items as 'most important risks': (i) not being (timely) involved in matters of relevance or brought in on new (data processing) initiatives, (ii) frequent reorganisations and (iii) the lack of a solid foundation in the form of policies and procedure to fall back on.

This lack of effective and timely involvement prohibits DPOs from accurately manoeuvring through their variety of tasks. According to the DPOs in the survey, their tasks consist mainly in the following: (i) advising on privacy and data protection, monitoring compliance, (ii) developing and implementing policies, procedures and associated business processes, (iii) risk analysis, (iv) handling of data flows and data transit issues, or (v) the creation of Data Protection Impact Assessments (DPIAs), Privacy Impact Assessments (PIAs) and Legitimate Interest Assessments (LIAs) – as required under the GDPR, in addition to Records of Processing Activities (ROPAs).

To duly perform these tasks, 50% of the DPOs pointed out that knowledge of different areas beyond privacy subject matter expertise, is required. Moreover, interpersonal skills are considered essential. First, excellent communication skills were mentioned by 10% of the respondents. Namely, DPOs have interactions with both internal and external stakeholders and must facilitate compliance among several actors. Second, good diplomatic and pragmatic skills were marked as essential by 15% of the respondents as DPOs often request employees to engage in what appears to be extra, but often regarded as 'burdensome' work. These skills in particular are needed to engage other members of the organisation to contribute to the success of achieving compliance. Finally, 20% of the respondents highlighted that a DPO is needed to raise privacy and data protection awareness within the organisation and across all management levels. DPOs must be able to come up with inspiring or captivating ways of informing employees. Otherwise, training initiatives will not adequately provide employees with the knowledge required for organisation-wide compliance.

Equally interesting is the DPOs take on the other side of the story: what does a DPO need from an organisation? In line with what has been mentioned above, the survey shows that DPOs have a 'balancing' role between competing priorities. Indeed the reality today is that in many organisations data protection issues are often still low on the priority list unless their (financial and/or reputational) impact is or can be felt. Therefore, and as mentioned under the second main finding above on governance, there is a clear expectation from the DPOs for data protection and privacy to be championed from the top down.

To achieve a higher level of accountability within the business, board and management level employees should take data protection initiatives more seriously, emphasise their importance and help foster a culture of compliance. This can then result in better buy-in from across the organisation. In turn, it can also improve both the role of the DPO as well as the quality of the employees' compliance.

DPOs in the survey also stressed the need for adequate privacy management technologies for the oversight and optimisation of data compliance issues. The survey indicates that, after most of the surveyed organisations invested in such tools, such as in-house and/or market GDPR solutions, the organisations' GDPR compliance efforts became more efficient. Concretely, such solutions were invested in by 75% of the respondents. Among these, 40% of respondents invested in in-house solutions while the remaining 35% of respondents invested in market solutions.

The DPOs indicated as main benefits of these privacy management tools in relation to GDPR obligations the following: (i) providing a more sustainable clear and global overview, (ii) establishing an audit trail and (iii) assuring a more efficient follow-up of actions. Redundancy was, thereby, avoided, and the administrative burden lessened.

Lastly, the survey demonstrated that organisations must make more efforts to adequately train and increase awareness. DPOs indicated that such training should also extend to themselves, especially in the area of communication and interpersonal skills. Simply understanding the regulatory obligations is not considered sufficient as DPOs must be able to obtain effective buy-in from other departments. Additionally, personal data is present among almost all business units within an organisation, and therefore, DPOs must be able to effectively communicate to a variety of different employees.

Figure 13. Maturity of the overall GDPR compliance programmes

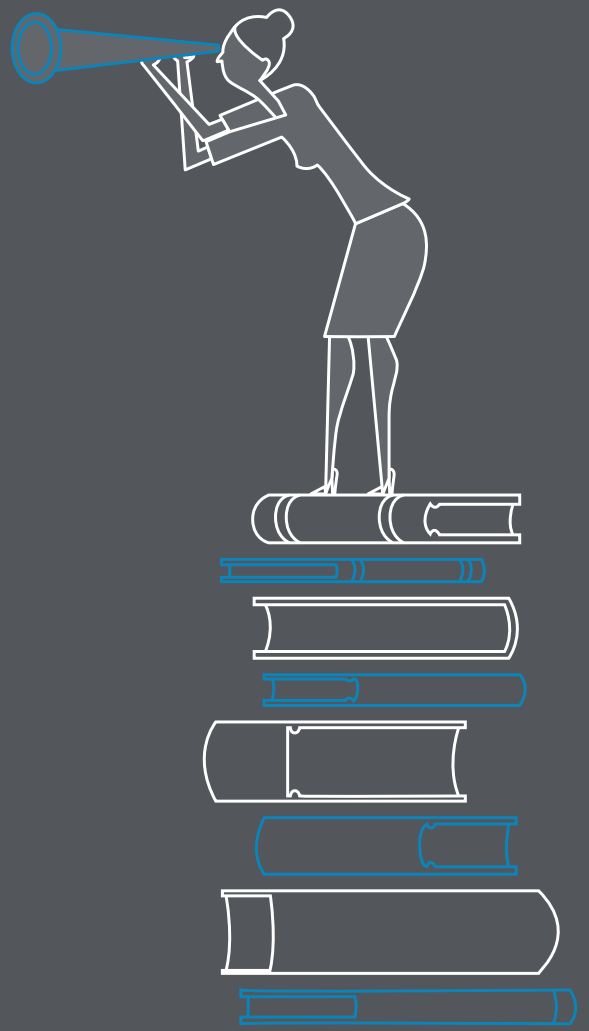
Deloitte point of view

The role of DPOs within an organisation is uncompared. Their role requires often a balancing act of many hats, knowledge areas and interpersonal skills and puts them in a complicated position.

The survey results clearly demonstrates that DPOs need to wear many hats and to have an adequate understanding of a variety of legal, technical, and compliance matters. This should not come as a surprise. The DPO role has really only come into focus in recent years and it would make sense for organisations to try to fulfil this role in a variety of ways. However, given the evolved regulatory expectations, especially as it relates to the role of the DPO, organisations must adopt a more active role and determine not only where the DPO sits within the organisation but how they can be effectively integrated and mandated, in the organisations' overall governance structure. It is also similarly unsurprising that DPOs are more and more expected to be knowledgeable in many areas as regulatory obligations are rooted in various laws, standards and sector specific requirements. Organisations need to employ someone with these various expertise, and must implement a recruitment process that reflects this need.

Additionally, we concur with the overall responses from DPOs that they believe their employers should better support their roles. In this regard, the DPO should not be considered a stand-alone function but integrated in a more wider and multi-disciplinary governance structure. This would, moreover, assist in creating a more effective governance structure in which everyone contributes (and has clear accountability) to championing data protection and privacy compliance, as well as generating more visibility and respect for DPOs.

In summary, the role of the DPO is clearly evolving from an ad hoc 'firefighter' to more that of a clearly mandated 'facilitator'. This final finding of the survey looked at what characteristics and resources are considered vital for an efficient and successful DPO. As such excellent communication and interpersonal skills, helicopter view, balancing compliance and business interests, are considered crucial elements. Similarly we looked at what a DPO needs from the organisation. In this regard, the survey shows that the DPO's main asks from management are (i) more resources, (ii) more management support and (iii) correct assignment of (data protection) accountability within the organisation.



Contact us about this report

Contact Beltug:

CEO

Danielle Jacobs
Industriepark-West 75
9100 Sint-Niklaas
Mobile +32 495 10 88 51
danielle.jacobs@beltug.be

Contact Deloitte:

Partner
Consulting & Advisory

Erik Luysterborg
Gateway Building, Luchthaven Nationaal 1J
1930 Zaventem
Direct: +32 2 800 23 36
Mobile: + 32 497 51 53 95
Fax: +32 2 800 24 01

Deloitte.

Designed by CoRe Creative Services. RITM0994293