Role of DPOs in Organisations

KPMG. Make the Difference.

KPMG International | kpmg.com

Introduction

Being a **Data Protection Officer (DPO)** has never been an easy task. The increase in regulatory requirements, as well as the interconnection and globalisation of organisations, demands that privacy officers have greater regulatory and sectoral knowledge to respond to the different privacy requirements they may encounter in the countries where they operate. In addition to the regulatory complexity, is the rapid advancement of new technologies, such as AI and digital transformation, which requires, on the one hand, the involvement of the DPO and their teams in initiatives and project design from their conception, and on the other hand, the continuous updating of skills and competencies in these areas.

All of this occurs in a context where citizens are increasingly aware of their rights: they request and demand more information about their data and are concerned about their privacy. The report "*Responsible data use at a crossroads: European citizens' perspective on privacy*" by KPMG highlighted that **72% of Irish citizens surveyed were more aware of privacy than 5 years ago.** The promotion of regulatory compliance, awareness campaigns within and outside organisations, and other aspects related to information and current affairs would explain this phenomenon.

Consequently, the role of the DPO is gaining greater relevance within corporate structures, playing a fundamental role in generating trust; they are the person responsible for driving data protection within organisations where data is one of the most valuable assets.

At KPMG, we have set out to analyse in this report how the role of the DPO is evolving in Ireland and Europe, focusing on aspects such as their position within the organisational structure, their involvement in the design of organisation projects and processes, the functions they perform, or the teams and technology they work with. The conclusions of the report were drawn from a survey conducted with 50 organisations operating in European Union countries, where the General Data Protection Regulation (GDPR) applies.

Key findings

Enhanced Role of the DPO in Strategic Decisions

The DPO's role has become more prominent and involved in the organisation's strategic decisions. This increased visibility is due to the DPO's comprehensive understanding of data protection risks and opportunities, enabling more informed and aligned decisions with corporate objectives

Interdepartmental Collaboration: CISO, DPO, IT, and More

Effective risk management and regulatory compliance have been greatly enhanced by the collaboration between information security (CISO), data protection (DPO), and technology (IT) departments. This teamwork facilitates better identification and mitigation of risks, as well as a faster response to incidents

Resource Constraints Amid Growing Demand

The rising demand for privacy and data protection necessitates additional resources that are often scarce within organisations. This can result in the DPO team being able to innovate while simultaneously facing significant limitations due to insufficient personnel or budget to fully meet their responsibilities.

How are the Objectives and Strategies Addressed?

The relationship between privacy and security in organisations

At a time when digitalisation has become integrated into the lives of every individual, personal data has become one of the main assets for organisations. Although advanced data analysis enables the provision of products and services that cater to consumer needs and generate new business opportunities, it is also true that a security breach exposing personal data can negatively impact the organisation's reputation and, more importantly, the security of the stakeholders (customers, employees, third parties, etc.). Therefore, privacy and security teams must work closely together.

54% of respondents indicate that as DPO, they work closely with the CISO and IT Security, conducting periodic reviews to align both strategies and objectives. In organisations where this occurs, privacy and security are understood as interconnected disciplines that work together to mitigate risks.

However, a significant **46%** of organisations report that collaboration between these areas is only occasional. In such instances, the operational aspects of the privacy function tend to take precedence.

Effective collaboration between the DPO and the CISO is crucial. When DPOs possess a thorough understanding of the IT and cyber environment within their organisation and can work seamlessly with the CISO, it fosters trust and significantly reduces the time spent on inquiries. This synergy not only enhances the efficiency of privacy and security operations but also strengthens the overall security posture of the organisation, ensuring the protection of sensitive data and the trust of stakeholders.

Where the DPO collaborates closely with the CISO, especially in those operating in multiple markets, there is a strategic alignment between the DPO and CISO functions, resulting in a more robust data protection practice and an integrated approach to risk management and regulatory compliance.

Today, it is universally acknowledged that privacy and cybersecurity are intrinsically linked. Privacy professionals must collaborate closely with teams dedicated to implementing security measures, especially as systems integrate increasingly complex technologies.

Is the DPO's real involvement sufficient and visible?

One of the primary functions of the DPO is to ensure regulatory compliance and act as a liaison for individuals in relation to their rights. However, according to the survey only around **10%** of European DPOs sit in the highest management of a organisation, compared to **24.2%** of Irish DPOs. While Ireland is ahead of many European counterparts, the importance of commitment to privacy emanating from the highest levels of the organisation, promoting a culture of responsibility in the protection of personal data through visible leadership needs to still be a key area of focus for both DPOs and senior management.

According to the survey, **65%** of European DPOs identify as having moderate involvement, participating in some key organisation decisions. Only **16%** of European DPOs indicate that they have little or no visibility, a figure that is lower for national DPOs (**10%**).

However, there is still room for improvement in increasing involvement. The results show that only **24%** of surveyed DPOs participate from the beginning in new technological projects, **35%** are notified but do not actively participate, and more than **40%** get involved once the deployment has started. Additionally, **16%** indicate that there are no formal procedures for their participation.

The involvement of the DPO from the beginning of projects and strategic opportunities is key to building decisions that take privacy into account, increasing awareness, and promoting a corporate culture.

Where can there be roadblocks?

One of the main functions of the DPO is to ensure regulatory compliance and data protection within organisations. To be effective, they need to collaborate closely with all internal areas of the organisation. The department with the greatest challenge for DPOs encountering resistance is Marketing, followed by Operations and Human Resources.

32% of respondents hold periodic meetings with different project teams to learn about new organisation initiatives, while **25%** identify that it is the departments that involve them directly through internal mechanisms.

25% of survey respondents agree that there can be sometimes a lack of structured collaboration, as in some cases these occur through ad hoc requests, reflecting a reactive rather than proactive approach to privacy management, which does not allow the data privacy team to anticipate needs.

The consequences of this approach can lead to gaps in privacy protection, increased risk of non-compliance, and potential data breaches. To mitigate these risks, it is crucial to integrate privacy as a core business objective, ensuring that all areas of the organisation are involved in privacy management continuously, rather than only responding to immediate needs. This proactive integration fosters a culture of responsibility and enhances the overall effectiveness of privacy protection measures.

How is privacy measured and reported?

Although **70%** of respondents report to the highest level of the organisation, a significant percentage report to the CISO or the security department (**13%**), and a minimal percentage report to other roles (Compliance, Legal, or Risk mainly). This indicates that in some organisations, privacy is embedded within functional areas, potentially compromising the DPO's ability to operate independently, as mandated by regulations

It is recommended that reporting to senior management is prioritised to ensure both the independence of the DPO and the strategic alignment of privacy with the organisation's objectives.

Regarding frequency of reporting to senior management, more than **90%** of respondents report at least once a year. Various frequencies are interspersed, with **43%** only reporting annually, which may mean that senior management considers it sufficient to receive updates occasionally, therefore indicating the perception that the DPO and privacy more broadly can make little strategic impact.

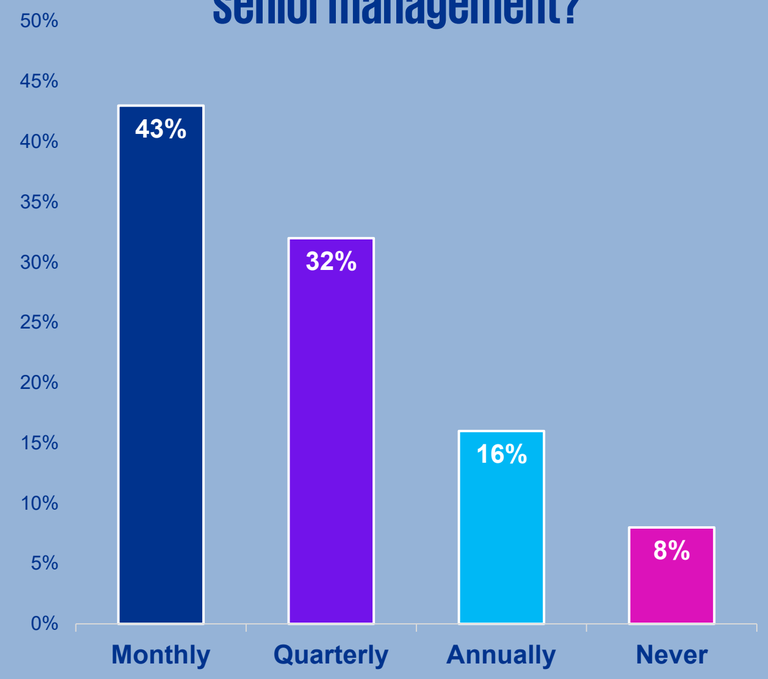
A second group **(12%)** reports quarterly to senior management. These organisations, often with an international presence, enable frequent monitoring of data protection status, highlighting its strategic importance for growth.

Having more frequent reporting than annually allows our DPOs to actively involve senior management. The implementation of monthly or quarterly reporting processes creates structures that integrate privacy into the business strategy.

Further, organisations often rely on lagging risk indicators for monitoring privacy activities. For example, DPOs report on periodically on the number of reported data breaches and data incidents. However, lagging risk indicators do not identify root cause early enough to prevent harm. Leading risk indicators can enhance privacy reporting. For example, percentage of IT assets processing personal information, percentage of personal information records/ processes without a defined retention period, length of time since last external privacy notice review/update.

While many organisations try to align with compliance standards, the lack of effective metrics and frequent reporting to senior management limits the strategic impact of the DPO.

How often is the report made to senior management?



Success indicators: are they measured?

Monitoring and assessing the maturity of privacy programs remains a challenge for some organisations, revealing a diverse landscape. While over **40%** of organisations have established methods to measure their programmes against tailored internal standards, many still need to define and implement effective metrics

24% of organisations are in the process of implementing metrics, while **27%** lack effective measures to evaluate their entire privacy program

Not having metrics to measure the effectiveness of the privacy programme can result in greater difficulties when requesting a larger budget or resources for the function, as in addition to demonstrating the value of privacy in the organisation. Metrics and monitoring can drive out clear privacy objectives in accordance with the data and the reality faced by each organisation.

41%

Key Performance Indicators (KPIs) based on an internal control framework

27%

Working on implementing indicators

24%

Updating the activity log

5%

No standardised parameters to measure the privacy programme

3%

External Audits

Privacy needs: are they covered?

More than half of the respondents consider that they have a team with enough participants to carry out their work **(57%),** but they report a lack of other types of resources or find limitations in some areas, compared to **22%** who indicate that they do not have the necessary personnel in their team for privacy management.

This may indicate that, although organisations are investing resources in privacy, they do not fully meet the current demands, which can pose a challenge for effective compliance or achieving the set objectives.

Only **19%** of DPOs indicate that the budget they receive is sufficient to fulfil the obligations assigned to their role and teams. According to the information provided, these organisations also report to senior management more frequently, and the measurement of their privacy programme is based on metrics built and implemented from their own regulatory control frameworks.

What tools are used?

An extended use of well-known office tools, e.g. Excel, **(36%)** has been identified. The prevalent use of these typical office tools suggests that technology is not being leveraged strategically in privacy management. One of the risks we can identify in this case are limitations in terms of scalability, security, and in some cases efficiency.

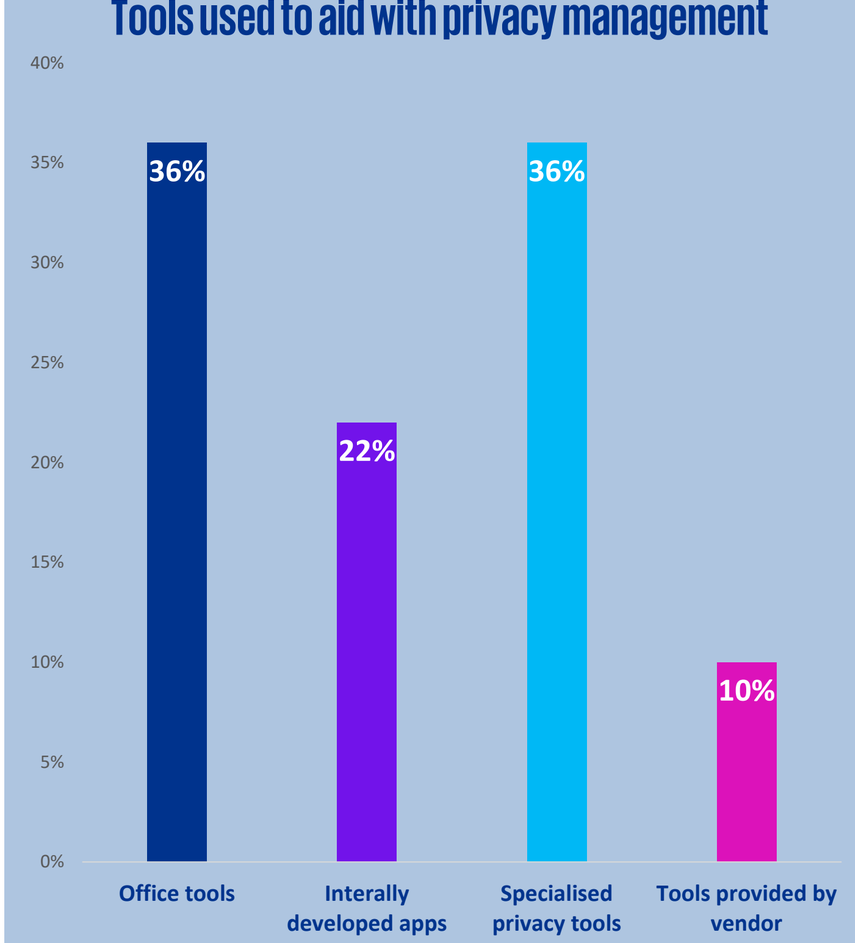
22% of surveyed DPOs identify that they have developed their own internal applications for privacy management, thus facing the challenges posed by these types of developments, such as the lack of integration with other organisation processes, generating duplications if done in isolation.

In both cases, their use is combined with third-party tools specialised in privacy. In some organisations, a significant percentage of DPOs **(36%)** have opted for the use of specialised tools to manage privacy. A smaller percentage **(10%)** of this group prefers to centralise their efforts using exclusively a tool provided by a vendor.

The priority now is to facilitate the management of routine processes such as ROPA updates and addressing data subject rights that are essential to comply with accountability duties, allowing time and resources to be dedicated to activities that demand greater collaboration across different areas. This ensures that new products or services that organisations want to launch consider privacy as a differentiating factor.

It is important to consider the objectives and goals of each organisation to decide whether it is convenient to unify processes through more integrated solutions that optimise compliance management.

46% of respondents agree that regulatory compliance is the key piece to consider when choosing a tool to manage privacy, closely followed by usability for the team and the management of the programme itself, which implies that the tool allows for the collection of various privacy processes.



The DPO's agenda

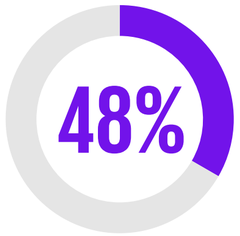
The activity that consumes the most time in the DPO's schedule is the management of the privacy programme and the verification of its effectiveness, followed by continuous work to ensure its alignment with the organisation's strategic objectives. The day-to-day activities of the DPO are complemented by resolving queries, responding to requests from teams that require advice, and actions aimed at training and awareness. DPOs are highly committed to privacy through accountability activities, dedicating a large part of their time to contract reviews, third-party management, and privacy by design processes through involvement in new projects or initiatives.

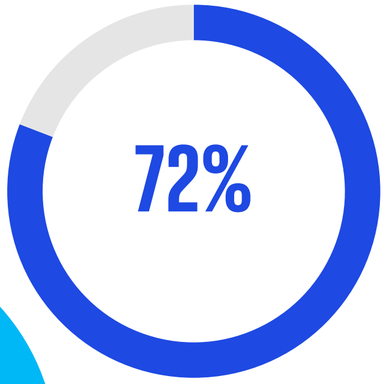
To improve data protection and privacy, it is crucial to integrate privacy into the business strategy and consider the implementation of more advanced technological tools and structured processes that facilitate proactive and efficient collaboration between different areas of the organisation.

What does Privacy Resourcing look like?

According to the results of this survey, **72%** of the respondents' privacy offices consist of a team of between 5 and 10 members or full-time equivalents (FTE). We also found that **48%** of the surveyed DPOs have been in their position for more than 5 years. However, regardless of the territorial scope, **81%** of the DPOs responded that their budget is either insufficient or does not fully meet the demands of their function.

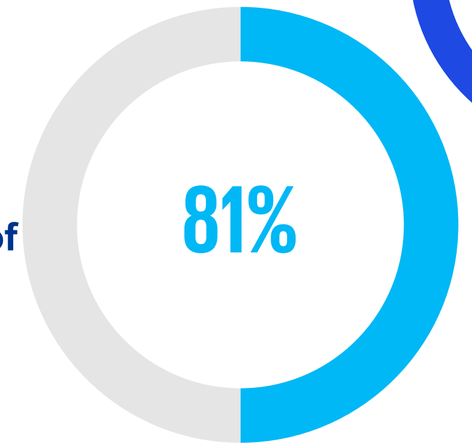
48% of DPOs have been in their position for more than 5 years





72% of privacy offices consist of teams with 5 to 10 members

81% DPOs believe their budget is insufficient of inadequate



Challenges in resourcing

As previously identified, generally, **70%** of respondents indicate that they have small teams for privacy management **(<5 members).** In these cases, they may face difficulties in addressing the growing complexity of privacy, especially in larger organisations or those operating in multiple jurisdictions. Privacy teams skillsets are multidisciplinary; more than **55%** of the profiles correspond to professionals specialised in privacy and data protection. With compliance specialists **(26%)** and engineers **(10%),** they create a balance between technical, legal, and compliance skills.

The teams are multidisciplinary, thus balancing the technical, organisational, and compliance skills necessary to effectively tackle tasks.

Percentage of Outsourced Privacy Management Activities

How are Obligations Addressed ?

With regard to the various obligations within the office, let us examine how the principal tasks are executed to ensure compliance with regulatory requirements.

01

Records of Processing Activities

Regarding **updating of the record of processing activities** and who is responsible for this function, **37%** state that it is a task delegated to the business. On the other hand, **63%** of DPOs indicate that it is carried out directly by the areas assigned to data protection tasks, sometimes with their own entity and other times within specific departmental areas, which are mainly Compliance or Legal.

02

Data Protection Impact Assessment

In the **execution of data protection impact assessments (DPIA) or PIA**, we found disparity in the responses. While **48%** of respondents state that they are carried out by the DPO and dedicated personnel from their office, **52%** share that they are managed by various areas such as risk, business, security, or others.

03

Incident Management

According to the survey, the **management of incidents** affecting personal data is usually a shared task among IT, security, business, and DPO in **65%** of cases, and only in **35%** are they managed and led directly by the DPO, who takes the initiative.

04

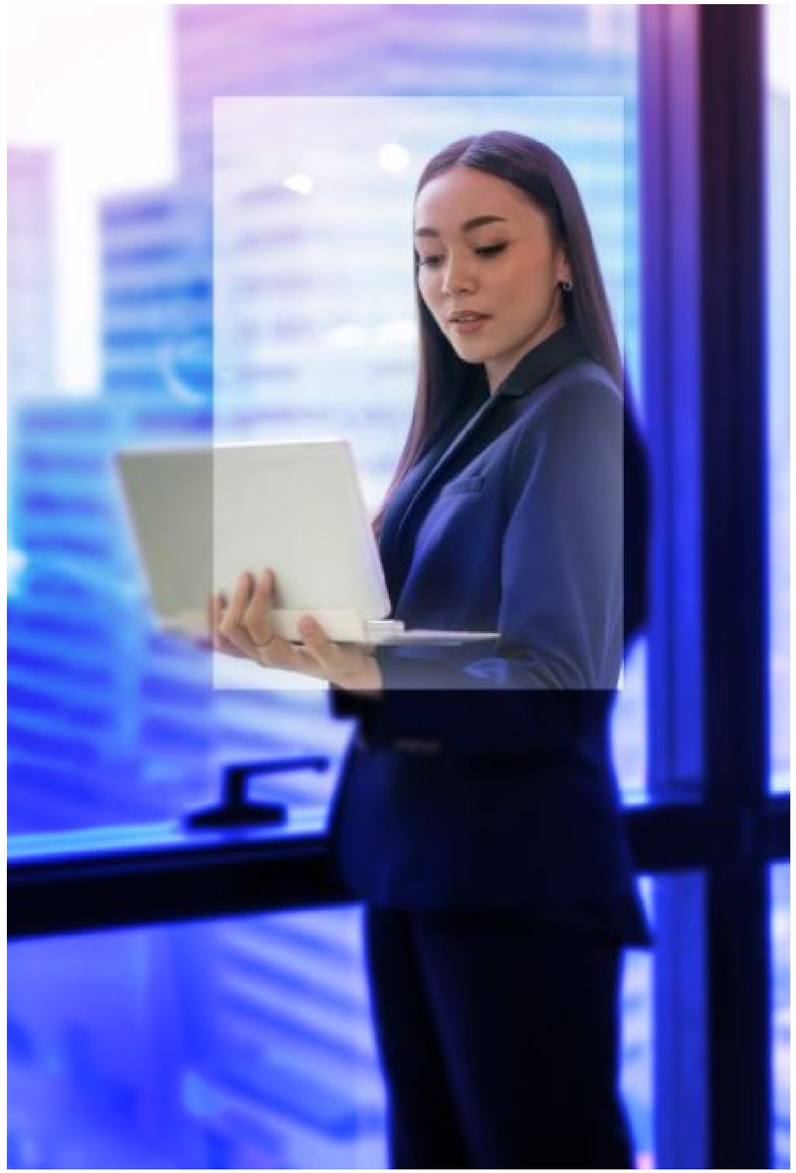
Security Measures

Regarding **security measures**, we found that in almost **60%** of cases, security measures are delegated to the Information Security area with limited supervision by the DPO or their office.

05

Retention, Deletion and Purging of Information

The formulation of **internal policies for the retention, deletion, and purging of information** is predominantly undertaken by the DPO in collaboration with business areas, as indicated by **60%** of respondents. Additionally, **30%** of respondents report that in their organisation, these policies are defined by business areas with the DPO's involvement on an as needed basis, while **10%** state that these policies are driven by external areas without the DPO's involvement.



Proactive Responsibility

Managing proactive responsibility and establishing technical and organisational measures to ensure regulatory compliance can be achieved through activities such as evaluating privacy programmes. In this regard, **18%** of DPOs have a dedicated internal audit team for regulatory compliance. **38%** of respondents indicate that internal audits are carried out annually and **43%** in other departments, such as internal control.

More than half of surveyed DPOs use **awareness campaigns** to communicate privacy policy changes and promote proactive responsibility. Specifically, **45%** use email, **31%** prefer face-to-face meetings, and some communicate solely through the corporate portal. Additionally, **54%** trust these campaigns for proactive responsibility, marking a rise from **45%** last year, with a **27%** decrease in paper use. Communications with suppliers are conducted only when necessary.

It is essential that the DPO involves other departments in the execution of tasks such as updating the Records of Processing Activities, delegating DPIAs, or managing data access rights.

In this regard, it is important to remember Article 39 of the GDPR: **The DPO's role is to inform and advise the controller or the processor and the employees who carry out the processing of their obligations pursuant to the GDPR.** Additionally, DPOs must have sufficient resources to carry out their functions (Article 38). Among these resources, we can find specific technological tools to execute DPIAs, manage ROPA, or address security breaches.

According to the survey the main concern of DPOs is equally divided between the lack of budget and the collaboration of areas. These are areas that need to be addressed across all organisations to ensure compliance with regulation.

What do DPOs see as the key Opportunities and Challenges of their Role?

The perception of the DPOs opportunities and challenges pivot in two main directions:

01

50% of DPOs demand increased involvement in the strategic decisions of the organisation.

02

42% of DPOs seek greater recognition of the value that the privacy and data protection function brings to business management.

8% of DPOs surveyed indicate that they will need access to better technological resources to perform their work

These percentages reflect how different activities are managed within privacy offices

40%

Claim lack of resources

20%

Focus on staying up-to-date with regulations and new technologies

40%

Face difficulties involving other departments in projects

Challenges for Irish DPOs

The DPC participated in the EDPB Coordinated Enforcement Framework, focusing on the position and designation of DPOs.

In 2023, the Irish Data Protection Commission (DPC) participated in the EDPB Coordinated Enforcement Framework (CEF) focusing on the designation and position of Data Protection Officers (DPOs). This initiative supported the DPC's 2022-27 strategy to improve collaboration with other data protection authorities and enhance DPOs' roles. The DPC surveyed 100 DPOs across different sectors in Ireland.

The findings highlighted three main issues:

- Insufficient resources for DPOs;
- Conflicts of Interest; and
- Diverse tasks performed by DPOs.

Ireland

29% of DPOs consider that they have a team with enough members to carry out their work

86% of DPOs report directly to the highest level of management

71% Of DPOs report at least quarterly to senior management

86% of DPOs have moderate visibility and are involved in some key decisions

Europe

57% of DPOs consider that they have a team with enough members to carry out their work

70% of DPOs report directly to the highest level of management

55% Of DPOs report at least quarterly to senior management

65% of DPOs have moderate visibility and are involved in some key decisions

Training, Innovation and Strategy

Continuous and Cross-Functional Training

The DPO function is continuously adapting and changing due to the constant publication of privacy news and regulatory updates. This is supported by the survey results, which identified that **54%** of DPOs continuously train and participate in relevant forums and groups relating to privacy and data protection. However, **46%** acknowledge that they do not do so, or do so occasionally.

The demands of the changing regulatory landscape require privacy professionals to stay up-to-date and share their concerns with their peers, thus creating working groups that can strengthen the sector.

In February 2025, Data protection authorities from Ireland, Australia, Korea, France and the United Kingdom signed a joint declaration to reaffirm their commitment to implementing data governance that promotes innovative and privacy-protecting AI, further emphasising privacy's importance in the changing technological landscape

Innovation and Strategy

It is interesting to note that **60%** of respondents believe they should be more involved in-strategic decision-making, demanding greater involvement in such projects from the beginning and not in an incidental or accessory manner, as some participants in this study have stated.

Regarding the self-perception of the DPO function in terms of innovation and evolution, **35%** are currently involved in technology within their organisation, while **37%** expect to do so but have not yet started. The remaining **27%** have not implemented it yet and do not consider doing so in the short term. In terms of areas where they are immersed in improving the maturity of their processes, there is room for possible automation.

Regarding the implementation of new technologies for management and integration, **70%** of DPOs have already implemented some technological tool related to data & IT, compared to **30%** who have not yet done so but consider that they are working internally to comply with privacy regulations for the time being.

Conclusion

01

The DPO’s increased visibility over strategic decisions

The DPO role has gained greater visibility and participation in the organisation's strategic decisions. This is because the DPO has a comprehensive view of the risks and opportunities related to data protection, allowing for more informed and aligned decisions with corporate objectives.

02

Collaboration is critical

Collaboration between information security (CISO), data protection (DPO), and technology (IT) areas is essential for effective risk management and regulatory compliance. This collaboration allows for better identification and mitigation of risks, as well as a quicker response to incidents

03

Insufficient resources for the ever-growing demand

The increasing demand for privacy and data protection requires additional resources that are not always available in organisations. This can lead to situations where the DPO team can innovate but also face significant limitations due to the lack of adequate personnel or budget to fulfil all their responsibilities.

Methodology

The report is based on an EU wide survey conducted by KPMG Spain with DPOs or privacy officers from 50 European organisations across different sectors (financial, retail, industry, education, energy, and technology) in the last quarter of 2024.

Additional research was conducted by KPMG Ireland with Irish DPOs to give a national perspective and context to the EU data.

The percentages in the charts may not add up to 100 due to rounding of decimals.

Contacts

Michael Daughton
Risk and Regulatory
Consulting Partner
KPMG Dublin
Tel: +353 87 744 2965
E: Michael.daughton@kpmg.ie

Tom Hyland
Risk and Regulatory
Consulting Director
KPMG Dublin
Tel: +353 87 050 4223
E: Tom.hyland@kpmg.ie

Michelle Griffin
Risk and Regulatory Consulting
Associate Director
KPMG Dublin
Tel: +353 86 104 0095
E: Michelle.griffin@kpmg.ie

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com

Designed by Evalueserve.