Data Protection Officer survey

On working conditions for Data Protection Officers and compliance with data protection legislation in Norwegian enterprises

September 2021

Datatilsynet

Content

INTRODUCTION 3

THE BACKGROUNDS OF DATA PROTECTION OFFICERS AND WHERE THEY WORK 6

ABOUT THE ROLE OF THE DATA PROTECTION OFFICER 11

THE DATA PROTECTION OFFICERS RELATIONSHIP WITH THE MANAGEMENT 14

THE OFFICER'S ROLE IN THE ENTERPRISE 21

COMPLIANCE WITH THE DATA PROTECTION LEGISLATION 24

FIVE RECOMMENDATIONS FOR STRENGTHENING THE WORK OF THE DATA PROTECTION OFFICERS WITHIN THE ENTERPRISE 299

Introduction

In recent decades, few regulations have affected Norwegian enterprises as much as the General Data Protection Regulation (GDPR) from 2018. This regulation strengthened the rights of individual consumers, while holding enterprises more accountable. In order to ensure compliance with this regulation, both public and private organizations have had to review all procedures and practices relating to the processing of personal data.

Norwegian enterprises are becoming increasingly data-intensive. Most enterprises collect large quantities of data about various groups of people, such as employees, customers, members, and citizens, and the public's trust in how different enterprises process personal data varies. The Norwegian Data Protection Authority's privacy survey (2019/2020) showed that Norwegians, in general, have a high level of trust in the way public sector organizations process personal data, but that there is much greater uncertainty associated with the way in which private sector organizations process this type of data.

The GDPR imposes a wide range of requirements on the processing of personal data by an enterprise. In addition to making sure the enterprise has a legal basis for even processing the data in the first place, it must protect personal data security. The enterprise must also handle requests from users and citizens who seek to exercise their rights.

Data Protection Officers are central to the enterprises' compliance with data protection legislation. The officer's role is to advise on how best to protect data protection interests, as well as to ensure compliance with relevant legislation.

The Data Protection Officer (DPO) system has existed in Norway since 2001, but with the implementation of the GDPR, the contents of this role has significantly expanded. Having a DPO became mandatory for most public sector agencies and authorities, as well as for a wide range of private sector enterprises and organizations. By year-end of 2020, 1,341 Data Protection Officers had been registered, representing 1,891 Norwegian enterprises.

However, there is little knowledge about the Data Protection Officers' experiences with this work. That is why the Data Protection Authority conducted a survey among Norwegian Data Protection Officers in November and December 2020.

About the survey

Market analysts Opinion performed the survey on behalf of the Data Protection Authority, between 25 November and 17 December 2020. The survey was distributed to 1,082 Data Protection Officers in Norway, and we received 632 responses. The respondents submitted their responses online.

The Data Protection Authority last mapped the working conditions of Data Protection Officers in 2011, through a survey conducted by market analysts Synovate.

What we wanted to know:

- Who are the Data Protection Officers, and how do they experience their working conditions?
- How would Data Protection Officers rate enterprise compliance with data protection legislation?

We present the main findings from the survey in this report. Finally, we also outline some recommendations for how the Data Protection Officer role can be handled and taken care of in the enterprises.

Summary

The General Data Protection Regulation has strengthened the role of the Data Protection Officer in Norwegian enterprises

68 percent of DPOs who responded to the survey, have between one and three years' experience of the Data Protection Officer role, which means that their appointment can be seen in relation to the implementation of the General Data Protection Regulation.

Considerable variation in how much time is spent on the role

Of all of the DPOs who responded, only 17 percent work full-time as Data Protection Officers. As many as half of all DPOs state that they spend less than 20 percent of their time on the role, and more than one in ten (11 percent) state that they spend no time on this role at all.

Many experience a lack of commitment on the part of management and a lack of resources

Almost three in ten DPOs find that they do not have sufficient time to dedicate to their responsibilities as Data Protection Officers. More than half of the DPOs who responded, do not have regular meetings with management. Many DPOs find that management does stay informed of and express interest in their roles and responsibilities, but still, 31 percent of DPOs find that management, to a small or very small extent, stays informed and expresses interest. This could indicate that the managements in many Norwegian enterprises are not up to date on the activities of their Data Protection Officers and their enterprise's data protection efforts.

Officers find that enterprises are compliant with data protection legislation

On average, almost eight in ten Data Protection Officers (77 percent) report that their enterprise complies with data protection legislation to a large or very large extent. The DPOs who experienced the greatest extent of compliance work in consulting or law firms. Officers in local and regional public authorities most commonly found their organizations to be the least compliant.

Specific legal requirements have often been implemented, but many struggle with a lack of competence-building and training of staff

It appears that most enterprises have implemented formal, legal requirements, such as data processing agreements, protocols, procedures for access and systems to report data security violations. The enterprises are less likely to have taken steps to provide employees with competence-building and training in data protection and privacy. The consequence of this may be that control systems for data protection and information security have been formally implemented, but employees may not be aware of them.

Human resources and functional procedures and processes are among the biggest challenges, whereas few find the legislation itself to be an impediment to good solutions

Around half of the officers found that the lack of human resources and functional procedures and processes to a large extent constitutes a challenge in terms of compliance with today's data protection legislation. However, the data protection legislation itself was generally not seen as a challenge for innovation and the establishment of good technical solutions.

Data Protection Officers in Norway

Norway has had Data Protection Officers since 2001. Statistics Norway was among the first organizations to appoint a Data Protection Officer in 2002. Several municipalities were also among the first to appoint a Data Protection Officer.

In the previous Personal Data Act, all enterprises were required to report all processing of personal data to the Data Protection Authority. If an enterprise applied for the appointment of a Data Protection Officer, it also applied for an exemption from this reporting obligation. Appointing a Data Protection Officer was a voluntary system, where having a Data Protection Officer was a sign that the enterprise took on a greater responsibility.

Norway was one of few countries with such a system prior to 2018. Historically, the system did not have a very strong link to data protection legislation, but with the implementation of the General Data Protection Regulation (GDPR), the system became mandatory for many enterprises, both in Norway and in Europe. The regulation includes several provisions on who is required to have a Data Protection Officer, the role of the Data Protection Officer, and the Data Protection Officer's tasks. The number of Data Protection Officers in Norway increased from 173 in 2010, to 1,341 by the end of 2020.

According to the GDPR, the Data Protection Officer must work with management to ensure compliance with the GDPR. This also entails that the Data Protection Officer will serve as an ambassador for data protection within the enterprise. But even if the Data Protection Officer is central to compliance with data protection legislation, the enterprise itself is responsible for any violations.

The tasks of the Data Protection Officer are described in Article 39 of the General Data Protection Regulation:

> 1. The Data Protection Officer shall have at least the following tasks:
>
> a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member States data protection provisions;
>
> b) to monitor compliance with this Regulation, with other Union or Member States data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
>
> c) to provide advice where requested as regards to the data protection impact assessment and monitor its performance pursuant to Article 35;
>
> d) to cooperate with the supervisory authority;
>
> e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.
>
> 2. The Data Protection Officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

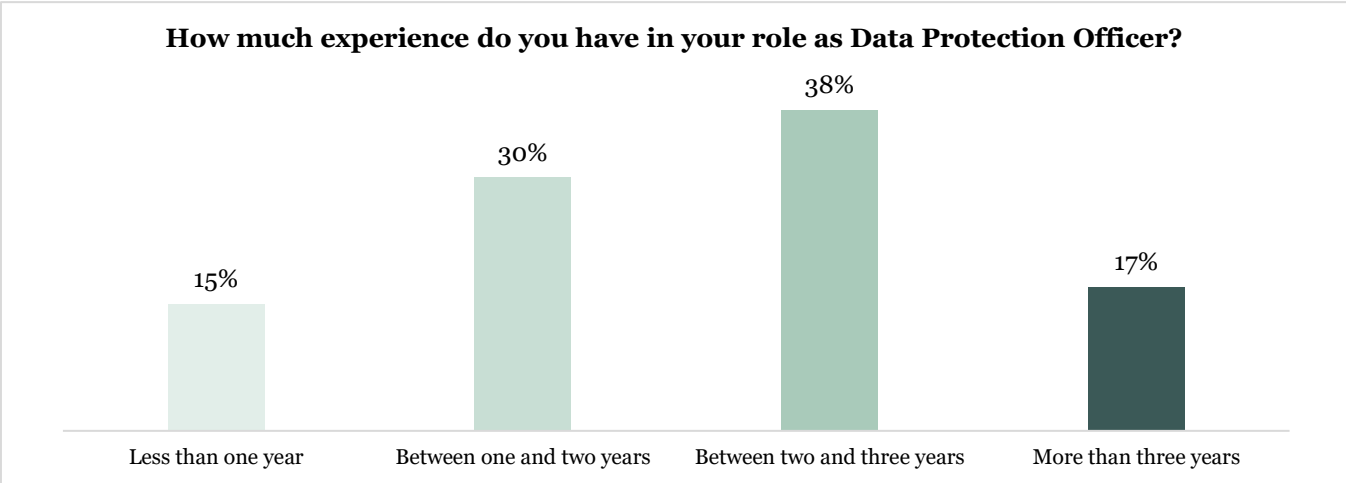
The backgrounds of Data Protection Officers and where they work

The General Data Protection Regulation lays down constraints on who can serve as Data Protection Officers. The individual must be designated on the basis of professional qualities and expert knowledge of data protection law and practices. There is no formal requirement for education, authorization or certification. Nevertheless, there is an expectation that the individual has the appropriate ability and motivation for the role, as well as appropriate knowledge of the enterprise and its processing of personal data.

Once the enterprise has designated a Data Protection Officer, the officer must be registered with the Data Protection Authority. Since the entry into force of the GDPR, the Data Protection Authority has seen the number of registered officers double many times over. This increase in numbers means that it is not only the most data-intensive enterprises that designate a Data Protection Officer; officers represent a wide range of enterprises and industries. The Data Protection Officer register shows an even gender distribution among officers, with a small majority of women (52 percent).

Experience in the role as Data Protection Officer

Some officers have prior experience of data protection-related activities, whereas others have very little experience with data protection work when they assume their roles. We asked respondents how much experience they have in their roles.

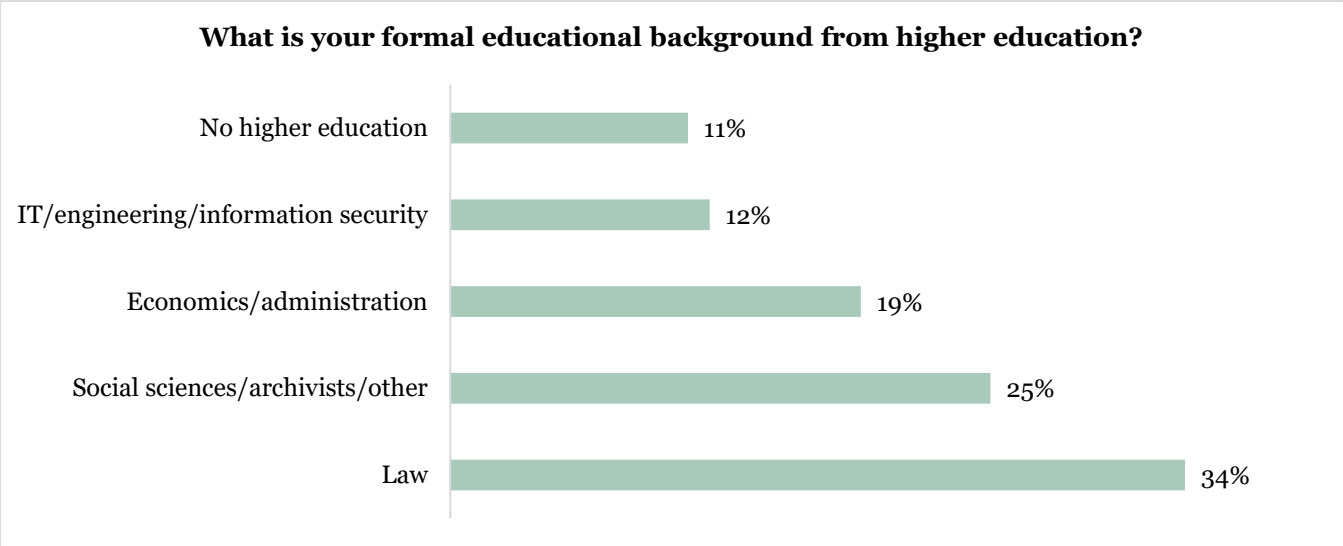


Responses show that 68 percent of officers have between one and three years of experience. This suggests that many officers were designated around the time the General Data Protection Regulation was implemented. It is fair to assume that this coincides with the regulation making it clear which enterprises should have a Data Protection Officer, and the regulation became mandatory for many at the same time. The responses indicate that the General Data Protection Regulation has promoted the designation of Data Protection Officers in Norway.

Education

The law does not require any formal requirements for the officers' educational background. Nevertheless, the Data Protection Officer is expected to have in-depth knowledge about GDPR, as well as a sound understanding of the enterprise's processing activities and ICT systems, and of information security and practices. The Data Protection Officer does not need to be an expert in all of these areas, but it is important to be able to establish a good collaboration and dialogue with experts within the enterprise. Even so, educational background may be of relevance to the approach

adopted to the role of Data Protection Officer. We have therefore asked officers questions about their educational background.



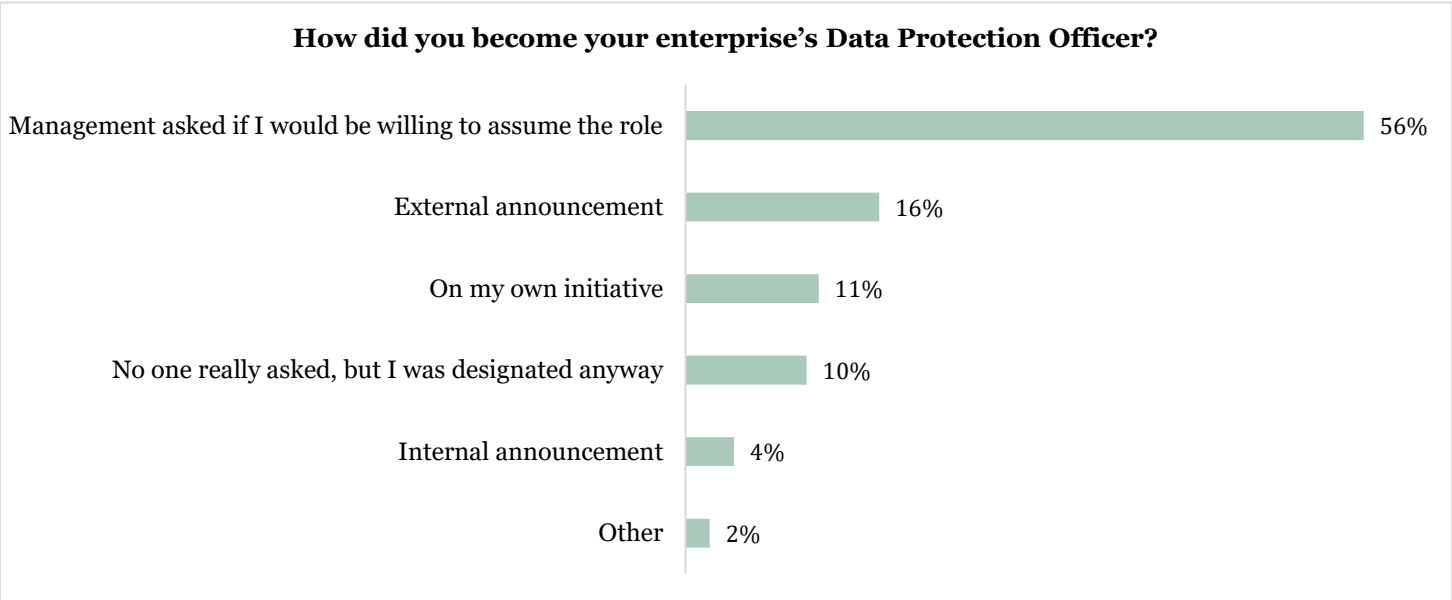
The responses show that officers come from a variety of different backgrounds, but that lawyers make up the largest group (34 percent of all officers). This could be because lawyers have traditionally handled issues of compliance. The responses also indicate that it is more common for larger enterprises to designate a lawyer as their Data Protection Officer. In enterprises with more than 250 employees, 43 percent of Data Protection Officers are lawyers.

Public administration has the highest share of lawyers (64 percent), whereas only 13 percent of officers in consulting and law firms are lawyers. In telecommunications and IT enterprises, however, the majority of officers have a background in IT/engineering/information security (39 percent). Thus we see that the educational background of officers varies with the industries in which they operate.

One in four Data Protection Officers comes from the social sciences/archives/other, and one in ten comes from IT, engineering or information security. One in ten does not have a background from higher education.

How did they become Data Protection Officers?

We also asked the officers how they fell into the role.



The responses show:

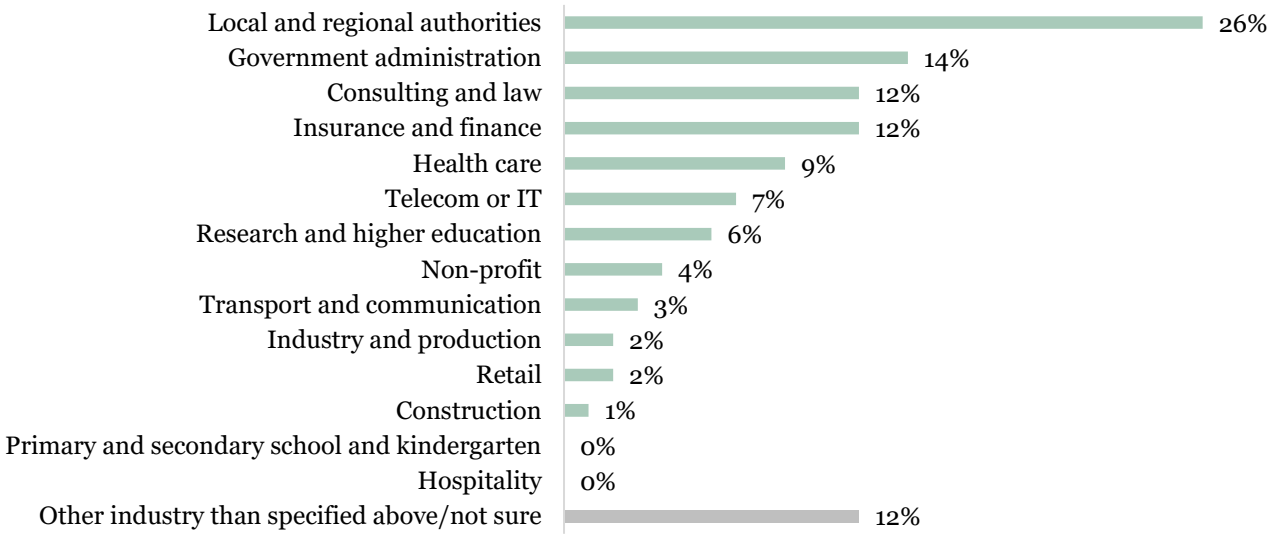
- More than half (56 percent) were asked by management if they would assume the role.
- One in ten officers were designated without anyone asking them directly.
- Many designations took place without competition. Only two in ten officers were designated after an internal or external announcement.

It is a concern that one in ten Data Protection Officers were designated without being asked if they were willing to assume the role. When an employee is allocated the role of Data Protection Officer without being asked, it may negatively affect the officer's motivation for fulfilling the tasks defined by law, and for promoting data protection in the workplace.

Sector affiliation

In order to learn more about the sectors in which officers operate, we asked which type of enterprise or sector they worked in.

Which industry does the enterprise for which you are a Data Protection Officer operate in?



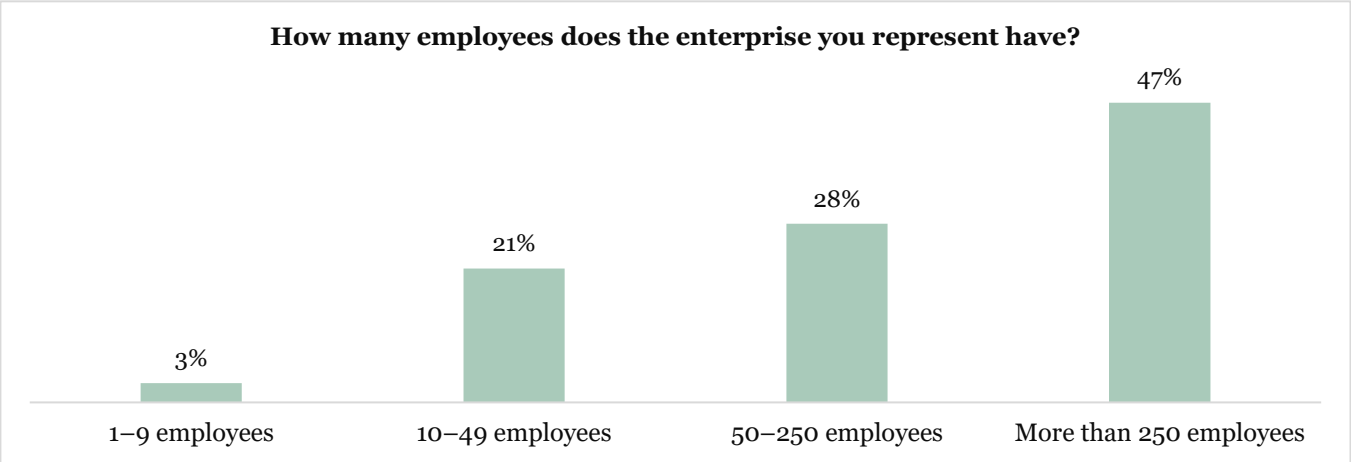
The responses show:

- Four in ten officers who responded to the survey, represent public sector undertakings, at the local, regional or national level.
- There is relatively fewer Data Protection Officers in trade and service industries, such as construction, retail, industry and production, and hospitality.

According to the law, all public authorities and bodies must designate a Data Protection Officer. It is therefore not surprising that four in ten Data Protection Officers work in the public sector, at the municipal, county or national level. The statistics also show that there are relatively fewer Data Protection Officers in the retail and construction sectors. The reasons for this may be complex, but a key factor is probably that many enterprises in these sectors process relatively less personal data, which means it is not mandatory for most of these enterprises to designate a Data Protection Officer.

Enterprise size

The size of the enterprise may play a considerable role in the working conditions of the Data Protection Officer. Larger enterprises often need key persons to oversee activities involving the processing of personal data. We therefore asked the officers how many employees the enterprise they represent has.



The responses show that almost half of all Data Protection Officers work in enterprises with more than 250 employees. The largest enterprises are also where we most commonly find full-time Data Protection Officers (33 percent), as well as officers who came to the role after it was advertised externally or internally (31 percent).

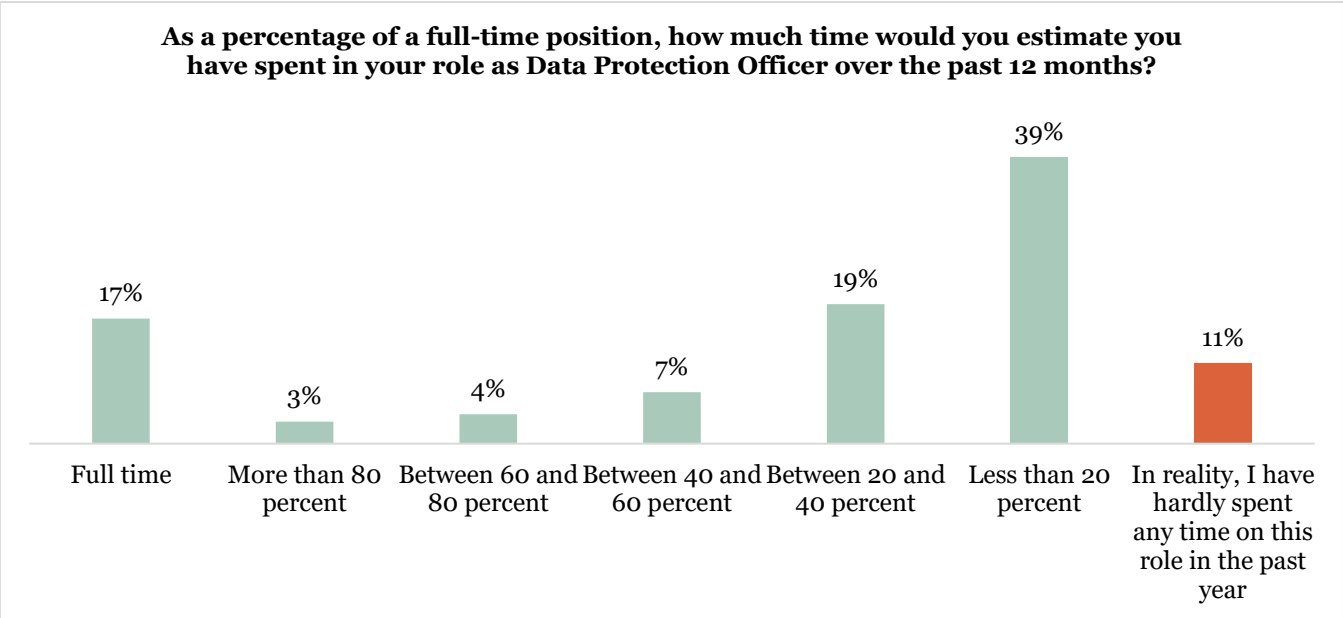
Large enterprises face different challenges than do small and medium-sized enterprises, and they are more often dependent on having good systems in place to ensure compliance and to view different processes in context. A Data Protection Officer can be a key resource in these types of enterprises.

About the role of the Data Protection Officer

How much time is spent on the Data Protection Officer role?

How much time a Data Protection Officer spends on their role may vary. The scope and type of personal data, as well as the complexity of the activity (such as the type of processing or number of IT systems) can affect how much resources an enterprise allocates to the Data Protection Officer role. Some enterprises need a full-time Data Protection Officer, whereas others may not need a Data Protection Officer who dedicates all of their time to this work.

We asked the officers how much of a full-time position they have dedicated to their role as a Data Protection Officer in the past 12 months.



The responses show:

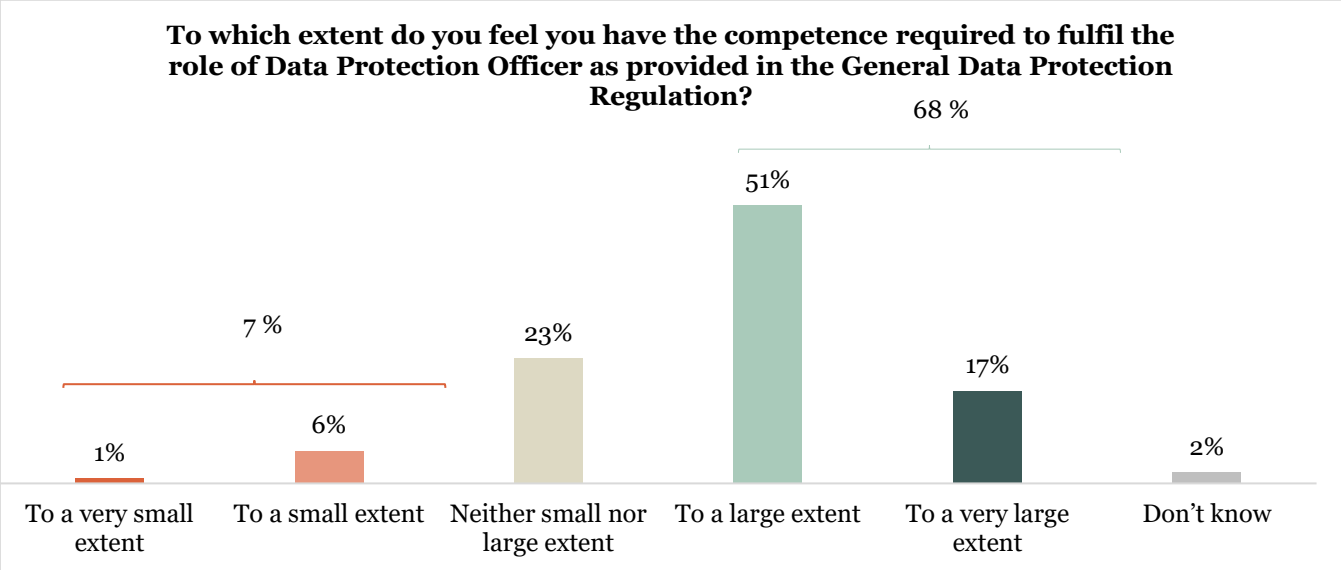
- 17 percent of officers work full-time in their role as Data Protection Officer.
- 50 percent of officers spent less than the equivalent of 20 percent of a full-time position on their role as Data Protection Officer.
- As many as 11 percent of officers report that, in reality, they have barely spent any time at all on their role as Data Protection Officer in the past year.

The responses show considerable variation in the amount of time spent on the role as Data Protection Officer, but as many as half of all Data Protection Officers spend less than the equivalent of 20 percent of a full-time position on the role.

The enterprises that have designated a Data Protection Officer have done so either because they process personal data on a large scale, or because they are a public body. In this context, therefore, seeing that more than one in ten officers who responded has not spent time on this role in the past year is quite alarming. It could indicate that compliance with data protection law within the enterprises is less than full, and also that Data Protection Officers may not play an active role in the processing of personal data within these enterprises.

Do officers find they have the appropriate competence?

Data Protection Officers need a certain level of competence in order to be able to fulfil their roles. We therefore asked the officers whether they felt they had the competence required to fulfil the role of Data Protection Officer as provided for in the General Data Protection Regulation.



The responses show:

- Seven percent respond that they, to a small or very small extent, have the competence required to fulfil their role as Data Protection Officer.
- 68 percent respond that they, to a large or very large extent, have the competence required.

In other words, an overwhelming majority responds that they feel they do have the competence required to fulfil the role of Data Protection Officer, to a "large" or "very large" extent. However, we do see that some officers feel they do not have the competence required.

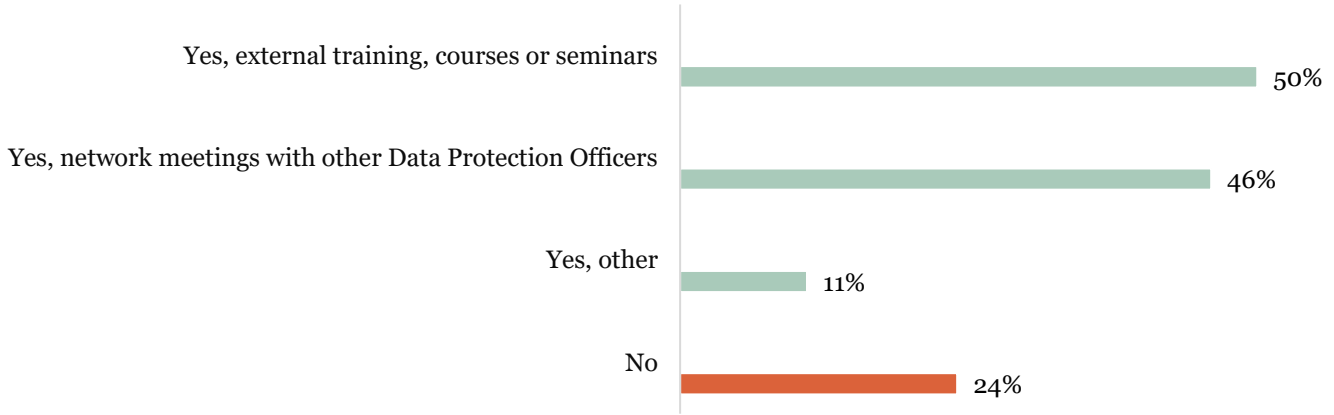
Of course, the Data Protection Officer does not need to be an expert in every area. It is, however, important that the officer has the ability to establish good collaboration and communication with the people who do have this competence, and that the officer is interested in acquiring new knowledge. Participation in courses and network events may therefore be useful.

The survey also shows that the processes involved in the designation of the officer, play a role in whether the officer feels they have the competence required. Among those who came into the role after an external recruitment process, no fewer than 88 percent respond that they to a large or very large extent have the competence required. Similarly, 85 percent of those who came into the role after an internal recruitment process respond the same way. However, less than half (46 percent) of those who were designated without anyone even asking them directly, report that they have the competence required.

Competence-building

In order to build competence and to meet other people with whom they can discuss data protection issues, it might be useful to participate in external courses, seminars or network events. This provides officers with an opportunity to update their knowledge of privacy and information security, and to gain insights into how other officers handle their roles. We therefore asked the officers if they had participated in any such events in the past year.

In the past year, have you participated in external courses, seminars or network events that have provided you with an opportunity to build your competence or update yourself on data protection law and/or information security? *(You may select more than o*



Half of the responding officers have participated in external training programmes, courses or seminars, and just under half have participated in network events with other Data Protection Officers. Officers working in enterprises in the research and higher education sectors most commonly report having participated in external education programmes, courses or seminars (83 percent), whereas officers in non-profit organizations and associations most commonly report having attended network events (70 percent).

One in four officers had not participated in any activities in the past year. Among officers representing consulting and law firms, more than half (53 percent) responded that they had not participated in any such activities.

The Data Protection Officers relationship with the management

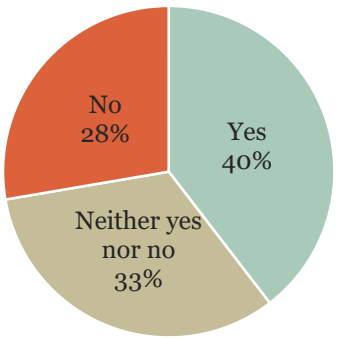
Tension may arise between privacy and other considerations in enterprises. Among other issues, management and the Data Protection Officer may disagree on key considerations that affect work on data protection and information security. Both sides, however, may benefit from maintaining a good relationship. The officer needs sufficient time and resources in order to fulfil their role, and management is dependent on the officer's professional expertise, advice and control to ensure the best possible compliance with data protection legislation.

In enterprises processing vast quantities of data, the management needs basic data protection competence in order to properly consider the Data Protection Officer's recommendations and weigh such considerations against other considerations. This competence is especially important when one considers that management, and not the Data Protection Officer, is ultimately responsible for compliance with the law.

Is the officers given sufficient time and resources at their disposal?

Data Protection Officers need sufficient time and resources to do their jobs well. We therefore asked the officers whether they feel they are provided with sufficient time and resources to fulfil their role as Data Protection Officer in a satisfactory manner.

Do you find that management provides you with sufficient time and resources to adequately fulfil your role as Data Protection Officer in a satisfactory manner?



The responses show:

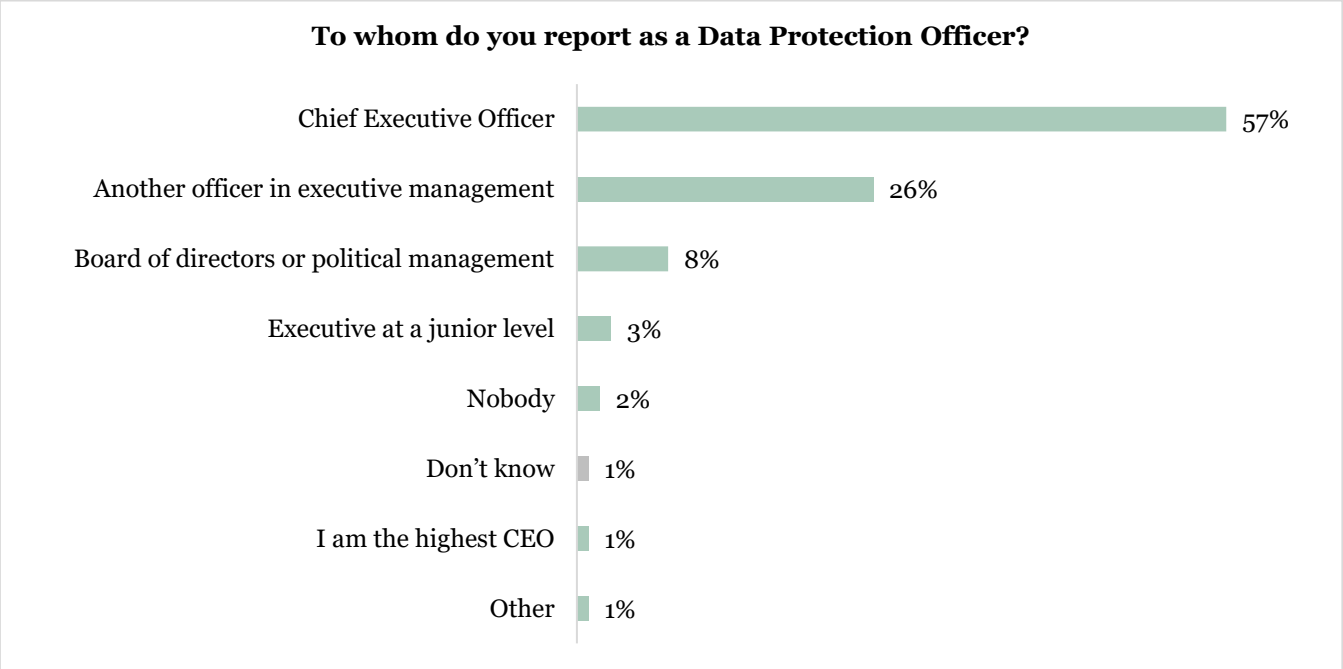
- Only 40 percent of officers feel they are provided with sufficient time and resources.
- 28 percent claim they are not provided with this.

That almost three in ten officers feel they are not provided with sufficient time and resources, indicates that many officers are not able to fulfil their tasks as a Data Protection Officer to the extent they would prefer. At the same time, all enterprises must consider how best to allocate internal resources, and different needs must be balanced against each other. This is particularly true for situations where management has to deal with a shortage of human resources and many tasks to be fulfilled; data protection work may become less of a priority as a result. It is nevertheless essential that Data Protection Officers are able to fulfil their tasks and fill the supportive role they were intended to have in protecting privacy concerns and ensuring compliance.

There may be many different reasons why 33 percent of officers responded with “neither yes nor no” to this question. One explanation may be that the enterprise does not have clear definitions of roles and expectations for how time is spent. In many enterprises, privacy-related concerns are handled whenever the need arises, and there may not be well-established procedures for the allocation of time and resources.

To whom do Data Protection Officers report?

According to data protection law, the Data Protection Officer reports directly to executive management. In order to determine how this reporting is handled in practice, we asked to whom the officers report within their enterprise..



The responses show:

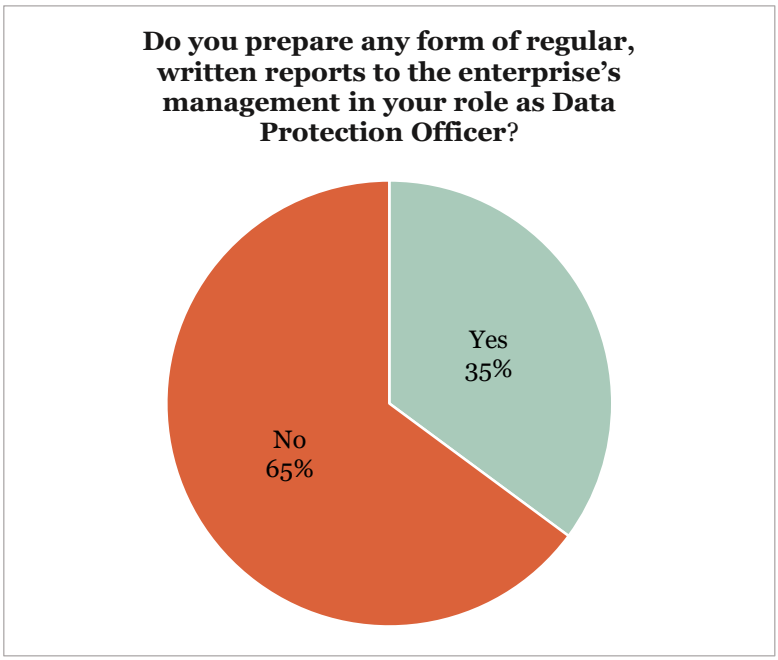
- More than half of officers (57 percent) report to the Chief Executive Officer (CEO) in the enterprise.
- 26 percent report to another officer in the enterprise’s executive management.
- Eight percent report to the enterprise’s board of directors or political management.
- Three percent of officers report to an executive at a junior level. This is not in line with the requirements of the General Data Protection Regulation.
- A total of five percent of officers do not have a clear reporting line — they have no one to report to, they do not know to whom to report, they report to “others”, or they are the CEO.

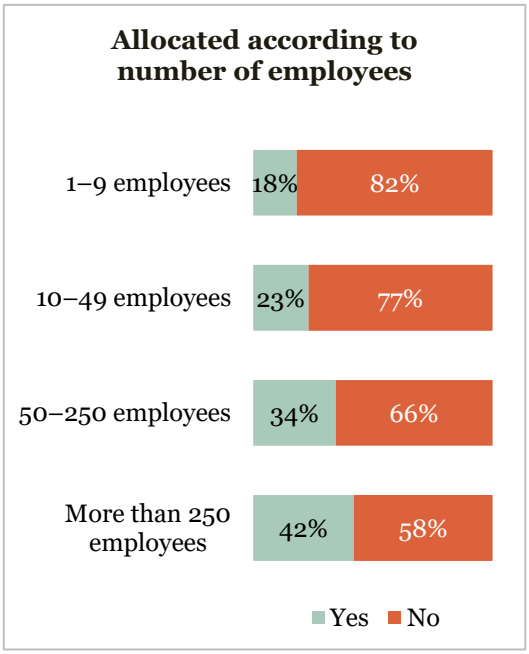
As the enterprise’s senior management has the final and formal responsibility for ensuring compliance with data protection legislation, it is important that they are presented with the Data Protection Officer’s recommendations, so that they can consider these recommendations and weigh them against other considerations. To whom the Data Protection Officer reports is therefore important. Responses show that a majority of officers report to executive management, which indicates that management is often kept informed of the Data Protection Officer’s work.

However, it is problematic that so many officers do not report to executive management. The consequence of this may be that the executive management is not informed of work related to legislation in which they are responsible for ensuring compliance. This also means that the executive management may not necessarily have the knowledge required to make informed decisions about the use of personal data within the enterprise.

Reporting to and meetings with the management

Good communication between the Data Protection Officer and management is essential for prioritizing data protection measures within the enterprise. Reporting and meetings are indications of the extent to which the enterprise is conscious of the tasks and significance of the officer's role. Formal reporting procedures may be necessary to establish a good framework for dialogue. We therefore asked the officers if they have any form of regular, written reports to the enterprise's management.





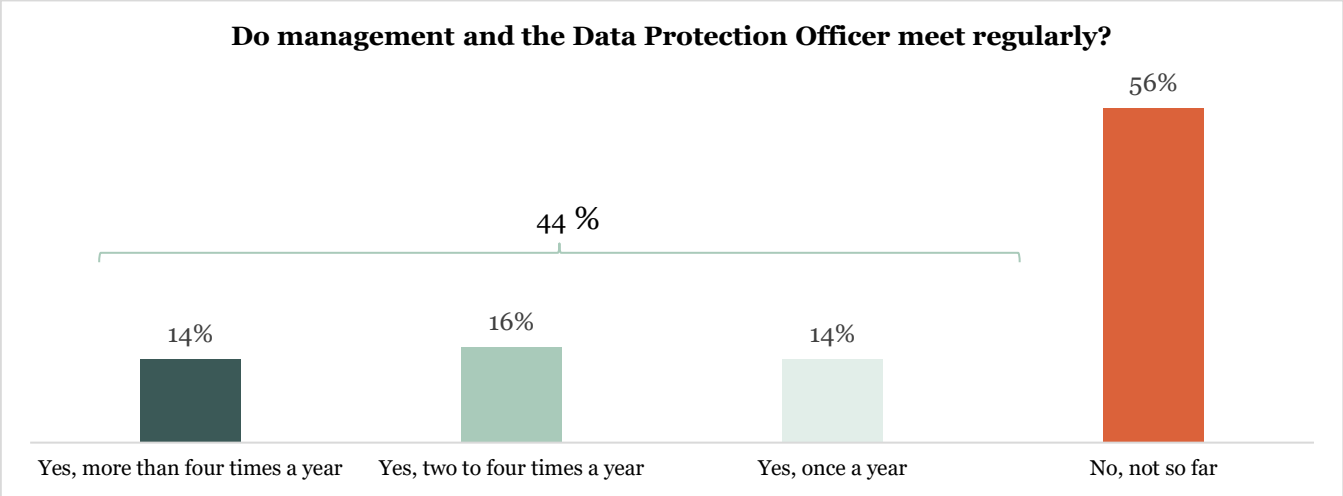
The responses show:

- Most Data Protection Officers do not prepare any form of regular, written reports to the enterprise's management, but there are considerable differences between sectors.
- While written reports are more common among large enterprises than among smaller ones, only 42 percent of officers representing enterprises with more than 250 employees report that they prepare regular, written reports to management.

The preparation of written reports to management outlining the status of data protection efforts and reporting on challenges that have been identified and the officer's considerations and recommendations, is a way to hold both the officer and management accountable. Such reports are also a way to keep other parts of the enterprise informed of what the Data Protection Officer is doing and the recommendations provided by the officer, promoting increased awareness throughout the entire enterprise of the officer's tasks and the significance of the Data Protection Officer role. When as many as 65 percent of officers responded that they do not prepare regular, written reports for management, this could be an indication that many enterprises do not sufficiently emphasize or document the work of the Data Protection Officer.

The survey also indicates that within the research and higher education sectors, 67 percent of officers prepare written reports, as do 61 percent of officers in the insurance and finance sectors. Written reports are the least common in consulting and law firms (13 percent).

Written reports may be used in preparation for and execution of regular meetings with management. We therefore also asked whether the Data Protection Officer regularly meets with management.



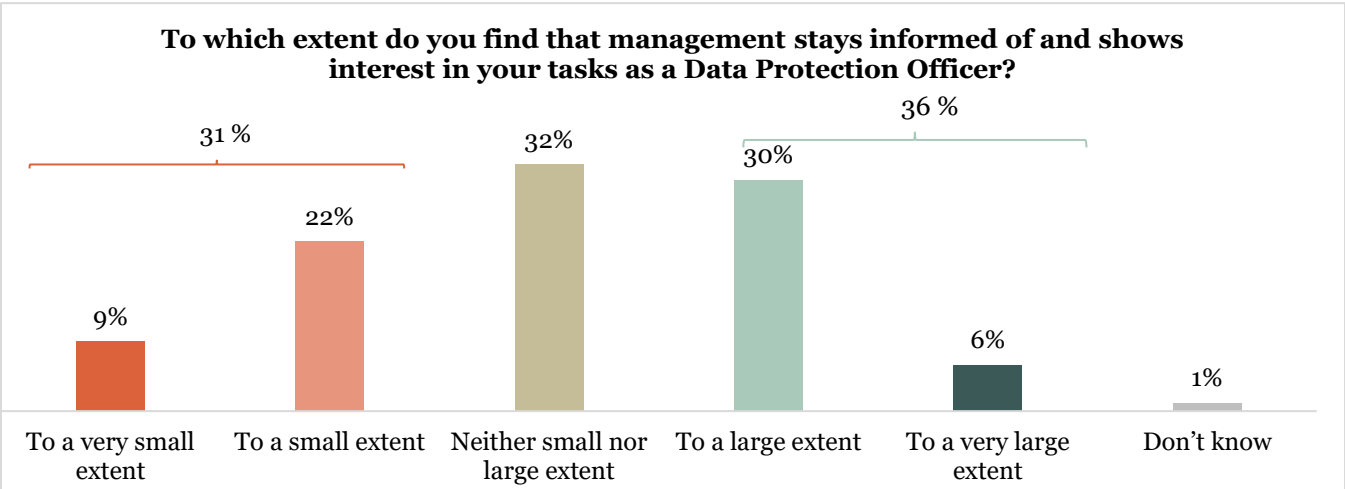
The responses show:

- More than half of officers who responded (56 percent) do not meet with management regularly.
- 30 percent of officers have two to four meetings a year with management.
- 14 percent report meeting with management once a year.

When seen in light of the fact that many officers do not prepare regular, written reports to management, this is an indication that many enterprises may not have satisfactory procedures in place for dialogue between the officer and management. The consequences of inadequate reporting and meetings between management and the officer may be that management does not have sufficient insight into the enterprise's data protection efforts, or that management do not take into consideration central issues related to the enterprise's personal data processing. This is problematic, as management is ultimately responsible for compliance with data protection legislation. In order for management to stay informed of the enterprise's data protection activities, it might be useful to schedule either quarterly or semi-annual meetings.

Engagement and interest from management

Engagement and interest from management is important to ensure a healthy exchange of views and promote a positive data protection culture within the enterprise. A lack of engagement and interest, on the other hand, may lead to deprioritization of data protection work to other issues, as well as to less motivated Data Protection Officers. We therefore asked to which extent officers find that management stays informed and shows interest in the Data Protection Officer's tasks.



The responses show:

- Only 36 percent of officers find that management stays informed of and shows interest in their tasks as a Data Protection Officer.
- 31 percent of officers find that management to a small or very small extent stays informed and show interest.

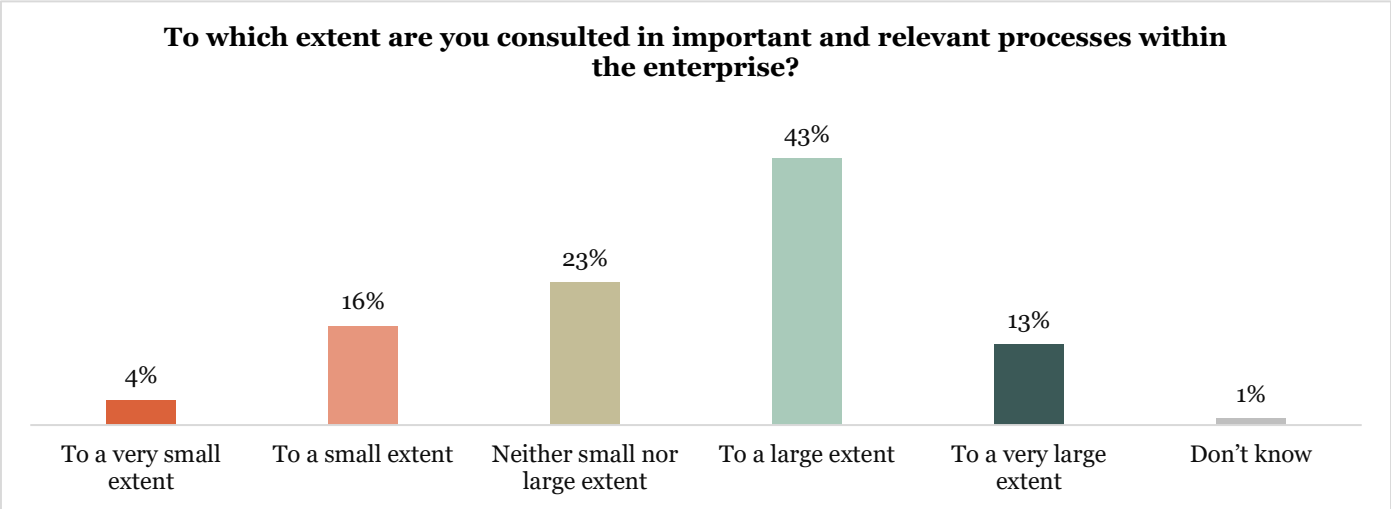
In order to ensure that a systematic and continuous effort is put into information security and data protection, management involvement is essential. Management largely sets the standard for how an enterprise works. If management does not prioritize and take ownership of data protection issues, this lack of interest is often reflected in the rest of the organization. Strong signals from the top are not only a prerequisite for compliance but is also essential in building trust among employees, customers and citizens, making them willing to adopt solutions and share data in a safe and secure way. Results from the survey indicate that officers experience varying levels of interest from management. The fact that only 36 percent of officers find that management stays informed of and shows interest is an ominous sign.

Responses from officers in the insurance and finance sectors are the most positive in this area. 58 percent of responding officers from these sectors report that they to a large or very large extent find that management shows an interest in their work. These are industries where the processing of personal data must be good in order to maintain a high level of trust with customers. These external incentives may contribute to making data protection more of a priority within the enterprise.

Responses from some of the public sector organisations are the least encouraging. Only 26 percent of officers from national public bodies report that management shows an interest, whereas in local and regional authorities, 27 percent of officers report the same. In these sectors, 41 percent of officers report that management to a small or very small degree shows an interest.

Are officers consulted?

A lack of interest on the part of management or other parts of the enterprise may ultimately lead to the officer not being consulted in important processes related to data protection, excluding them of the opportunity to present key considerations and recommendations. We therefore asked to which extent the officers find that they are consulted in important and relevant processes within the enterprise.



The responses show:

- More than half of officers (56 percent) find that they are consulted in important and relevant processes.
- Two in ten (20 percent) find that they are consulted to only a small or very small extent.
- In addition, 23 percent responded “neither small nor large extent”.

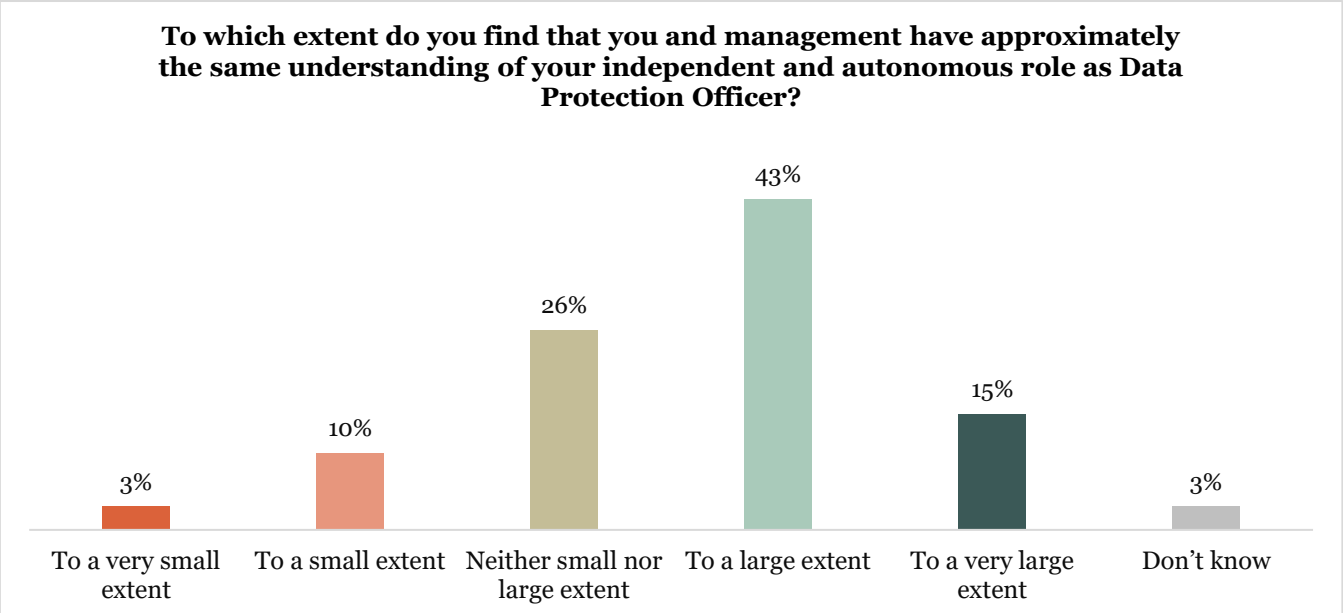
The survey shows that a relatively high percentage of Data Protection Officers feel they are not consulted on important and relevant processes. This is, of course, unfortunate, as one of the Data Protection Officer’s core tasks is to advise on the use of personal data within the enterprise. If the enterprise is in the process of making decisions that may be in conflict with data protection legislation, the officer should be provided with an opportunity to present their views to the people making the decision, and if necessary, the executive management of the enterprise.

The highest percentage of officers who respond that they are consulted to a small or very small degree represent local and regional authorities (29 percent). The same applies to officers from the transport and communications sector (25 percent). By cross-referencing responses from the survey, we see that the officers who were designated by management without having requested the role, are the ones who are least likely to be consulted in their capacity as Data Protection Officer (35 percent selected small or very small extent).

At the same time, a considerable majority (56 percent) find they are consulted in important and relevant processes. These figures should, of course, be even higher, but they do nevertheless reflect that while some enterprises lack procedures for regular reporting and meetings, the majority of enterprises do want to hear what the Data Protection Officer has to say.

Officers’ independence and autonomy

Data Protection Officers must not be instructed on how to perform their tasks, be it from the enterprise itself or other parties. This means that the officer must not be instructed on which tasks to prioritize, how to interpret the law, or what the outcome of a matter under consideration by the officer should be. This independence and autonomy is essential for the officer to be able to perform in accordance with the intentions of the law. We therefore asked to which extent the officers find that management understands the independent and autonomous role of the Data Protection Officer.



The responses show:

- Most officers find that management to a large or very large extent has a similar understanding of the independent and autonomous role of the officer (58 percent).
- 13 percent of officers, however, report that management to a small or very small degree understand this role.

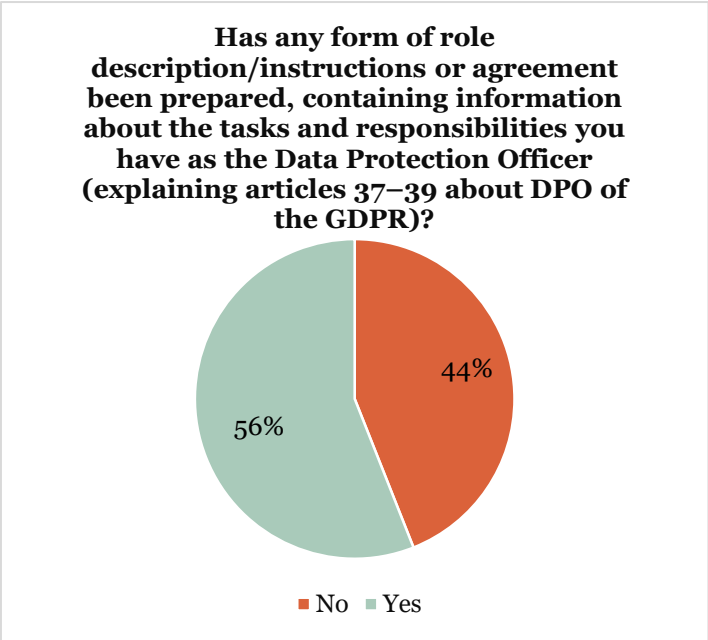
The responses show that enterprises generally have a good, shared understanding of the officer's independence and autonomy. There are, however, a significant number of enterprises (13 percent) that do not share this understanding. This could create problems for the officer in their fulfilment of the tasks of their role.

The highest extent of shared understanding is found in research and higher education, as well as in health and care services. In these sectors, seven in ten officers say they find a shared understanding to a large or very large extent. The lowest extent of shared understanding is found among Data Protection Officers who fell into the role "without anyone directly asking them". Almost one in four of these officers (24 percent) chose "to a small or very small extent" on this question.

The officer's role in the enterprise

The enterprise is responsible for taking the appropriate steps to ensure that the Data Protection Officer is able to fulfil their tasks. To prevent a situation where the officer's role or tasks are unclear, it is wise to have a role description or instructions clearly outlining the officer's tasks and how responsibilities are distributed between them and the enterprise.

We asked officers whether they have any role descriptions, instructions or agreements in place that define their tasks and responsibilities.



The responses show:

- 44 percent of officers say they have no role description/instructions or agreement.
- Among enterprises with 1–9 employees, almost six in ten officers lack a role description/instructions or agreement.

The fact that less than half of officers have a role description or instructions onhow to fulfil their role as a Data Protection Officer is concerning. We see that the share of officers with a role description is highest in large enterprises (61 percent), whereas in enterprises with less than 10 employees, only four in ten officers have a description of this kind. It is a fair assumption to believe that this may be because larger enterprises require more clearly defined procedures and responsibilities.

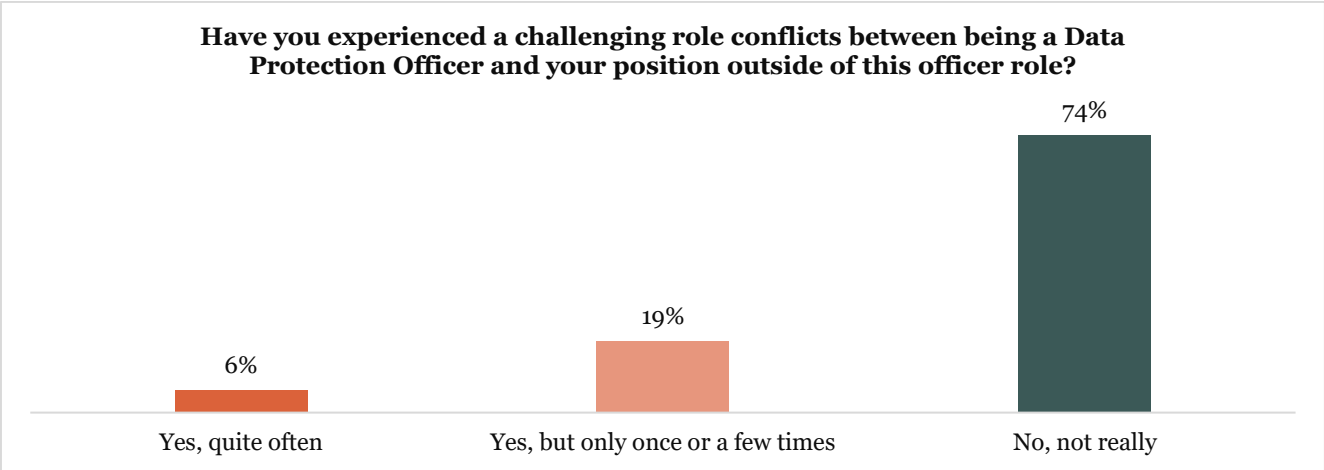
Officers are most likely to have a role description in the finance and insurance sectors (87 percent), followed by public administration and non-profit organizations (61 percent). Officers without a role description are most likely to work in consulting and law firms.

Of officers who say they became officers following an external announcement, 72 percent have a role description that both they and management can consult. For those officers who say they became officers without having been asked directly, the share is 45 percent. This could be because they work in enterprises that have not focused as strongly on the role that Data Protection Officers play and what tasks this role requires.

Role conflicts

A Data Protection Officer may also have other tasks and roles within the enterprises, in addition to their tasks as a Data Protection Officer. As this survey has shown, 83 percent of officers combine their role as Data Protection Officer with other tasks. In these cases, the enterprise must make sure that these other tasks and roles do not lead to a conflict of interest. This is related to the requirement that the officer must be able to fulfil their role independently.

We asked the Data Protection Officers whether they have experienced challenging role conflicts between their position and the role as Data Protection Officer.



The responses show:

- Most officers have not experienced role conflicts (74 percent).
- One in four officers has experienced a difficult role conflict at least once (25 percent).

Provided that the officers who responded have a good understanding of their role, the survey shows that most officers rarely find themselves in situations where their independence in relation to other tasks within the enterprise is challenged.

Role conflicts may, for example, occur in situations where the officer also has other roles, such as determining the purpose of personal data processing, or the way in which such data is processed. This type of situation may occur if the officer personally heads or is responsible for IT security or compliance in other areas. Clear role descriptions and procedures for how the enterprise handles conflicts of interest are essential for handling this type of situation in a satisfactory way.

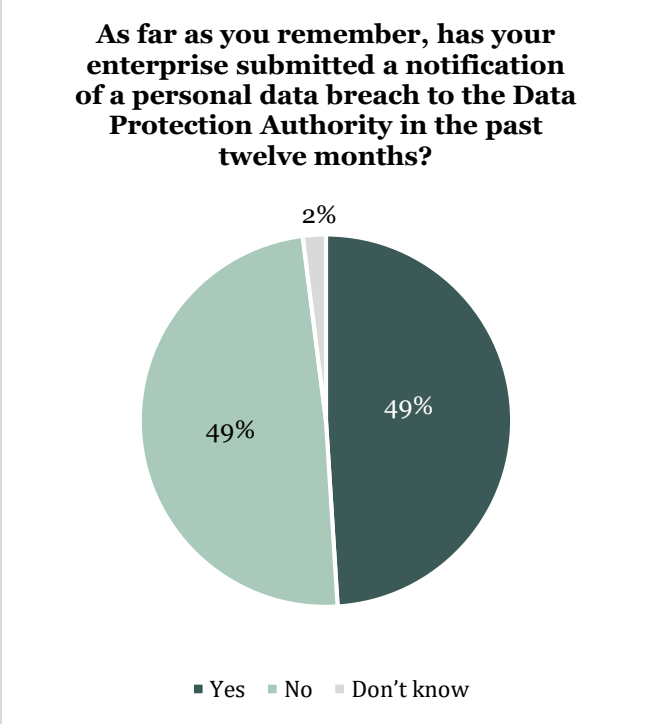
The officer's role in connection with a breach of personal data security

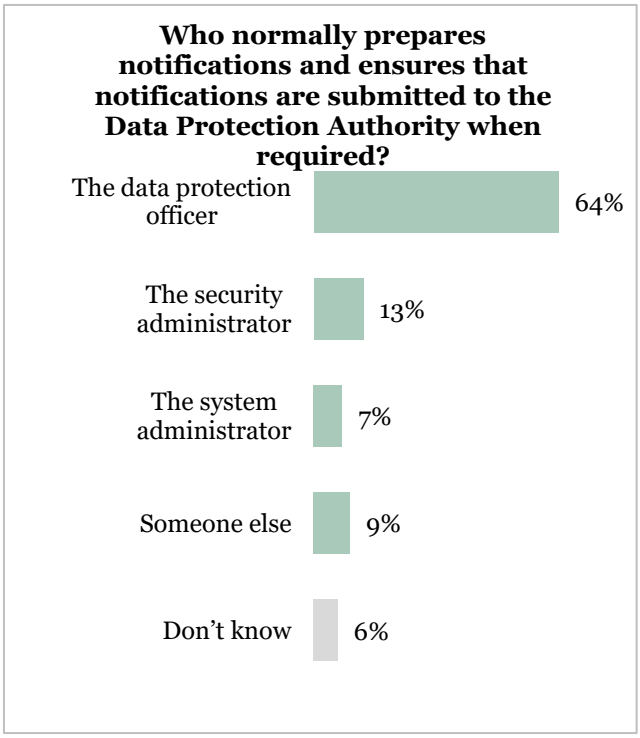
If a breach of personal data security (discrepancy) is identified, the data controller must notify the Data Protection Authority (discrepancy notification), unless the breach is not likely to entail a risk for the rights and freedoms of natural persons.

Identifying and following up on potential breaches of personal data security is an important part of an enterprise's internal control and information security work. The Data Protection Officer should play a central role in this work. For this reason, the General Data Protection Regulation includes a requirement that contact information for the Data

Protection Officer must be included in the notification submitted to the Data Protection Authority. Nevertheless, the enterprise – not the Data Protection Officer – is responsible for the assessments made in the discrepancy notification,.

We have taken a closer look at the role the Data Protection Officers play in the submission of notifications of personal data breaches to the Data Protection Authority.





The responses show:

- Every other enterprise has submitted notifications to the Data Protection Authority.
- Data Protection Officers are primarily (64 percent) behind the preparation and submission of notifications to the Data Protection Authority. In the insurance and finance sectors, the rate is 88 percent.
- Two in ten officers (20 percent) said the security administrator or system administrator was responsible for preparing and submitting the notification.
- Six percent of officers said they do not know who normally prepares and submits such notifications. This percentage was the highest in public administration, where ten percent of officers said they do not know.

If the Data Protection Officer submits a notification of a personal data breach on behalf of the enterprise, this could easily challenge the officer's integrity and independence. When a personal data breach has occurred, the officer's assessment may differ from that of the management in terms of the cause and consequences of the breach, as well as in terms of the types of measures that should be implemented. This is especially important in assessments of the risks to data subjects' rights and freedoms. However, the Data Protection Officer should always be informed that a notification has been submitted to the Data Protection Authority.

Compliance with data protection legislation

In connection with the implementation of the General Data Protection Regulation in 2018, many public and private enterprises spent considerable time and resources on reviewing and establishing procedures and practices related to the processing of personal data. At the same time, the regulation also simplified certain things — it is, for example, no longer necessary to apply to the Data Protection Authority for a licence to process sensitive personal data.

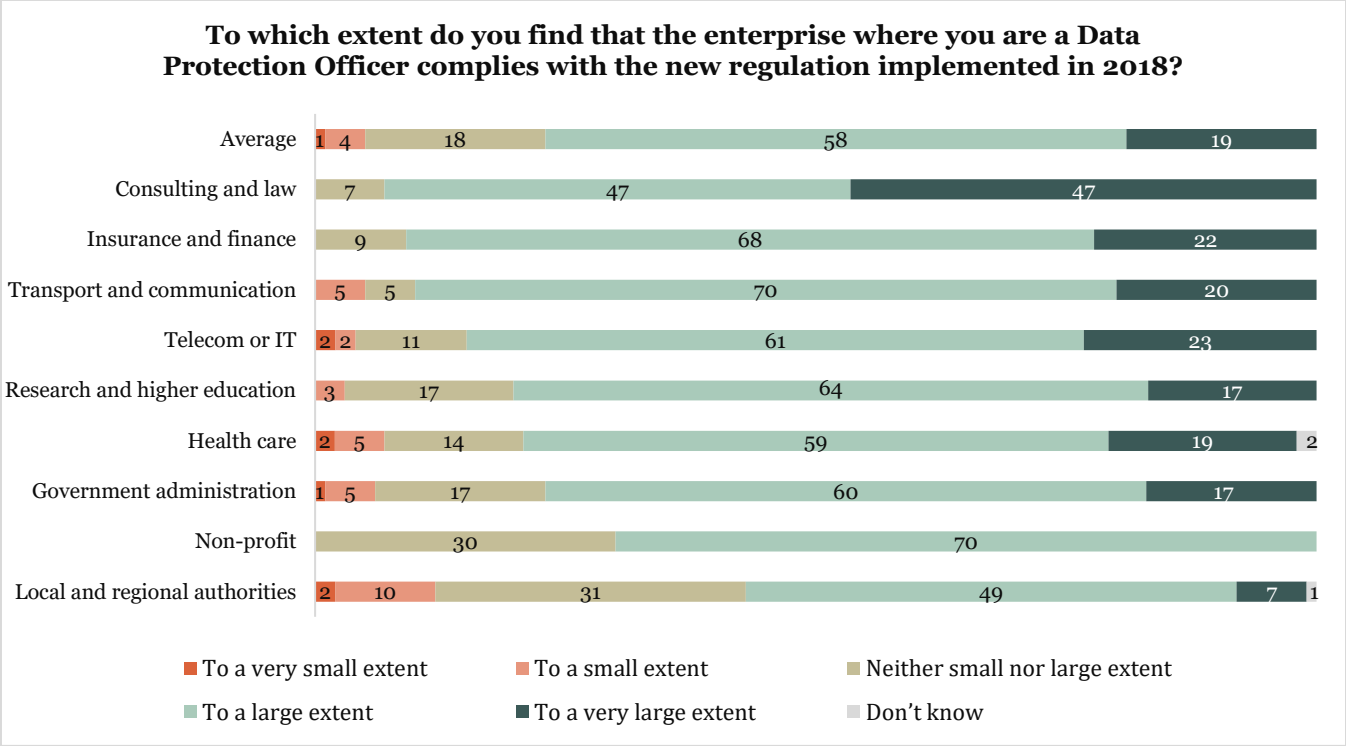
The European Commission published its first evaluation of the General Data Protection Regulation in June 2020. The Commission's assessment was that the regulation had in general successfully met its objectives of strengthening the protection of the individual's right to personal data protection and guaranteeing the flow of personal data within the EU. Nevertheless, the Commission pointed out that it was too soon to draw any definitive conclusions on the practical implementation of the General Data Protection Regulation.

Despite it being too soon to conclude on how the implementation of the regulation has affected Europe as a whole, some reports have given indications of how things have gone. The Swedish Authority for Privacy Protection (Integritetsskyddsmyndigheten) published a survey in 2019 on how enterprises and Data Protection Officers experienced the implementation of the regulation. According to this report, three in four Data Protection Officers found that the implementation of the General Data Protection Regulation in Sweden had been successful. At the same time, several enterprises reported that the biggest hurdle lay in establishing functional procedures and processes, and in interpreting the regulation.

In Norway, we see that many enterprises are actively working to ensure compliance. In the Data Protection Authority's privacy survey (2019/2020), we found that Norwegians generally have a high level of trust in the way public sector organizations process personal data, but that there is a much lower level of trust in the way many private sector organizations process and use this type of data. Also, more than half of the population has refrained from using a service or a product as a result of being uncertain about how their personal data will be handled.

What do officers think about how enterprises comply with legislation?

Data Protection Officers have a unique insight into how their enterprise processes personal data. We therefore asked the officers to which extent they feel that the enterprises they represent comply with the law. The responses have been categorized according to industry. Some industries have been omitted from the summary, because the number of respondents from these industries was not high enough to calculate a percentage. These industries are “retail”, “hospitality”, primary and secondary school and kindergarten”, and “construction”.



The responses show:

- On average, almost eight in ten Data Protection Officers (77 percent) report that the enterprise they represent complies with data protection legislation to a large or very large extent. Only five percent find that the enterprise complies with data protection legislation to a small or very small extent.
- The officers with the most favourable impression of their enterprise’s compliance, work in consulting and law firms, as well as in the insurance and finance sectors.
- Among non-profit organizations and associations, none of the respondents say their enterprises comply with legislation to a small or very small extent. Also, none of the respondents say their enterprise complies to a large or very large extent.
- The lowest rate of perceived compliance is found among officers representing local and regional authorities. 12 percent of officers from these sectors say their enterprises comply with legislation to a small or very small extent. At the same time, only slightly more than half (56 percent) say they find that their enterprise complies to a large or very large extent.

The general perception is positive. Responses show that Data Protection Officers generally find that the enterprises they represent comply with relevant data protection legislation. Some sectors, however, stand out in a negative way, especially local and regional authorities.

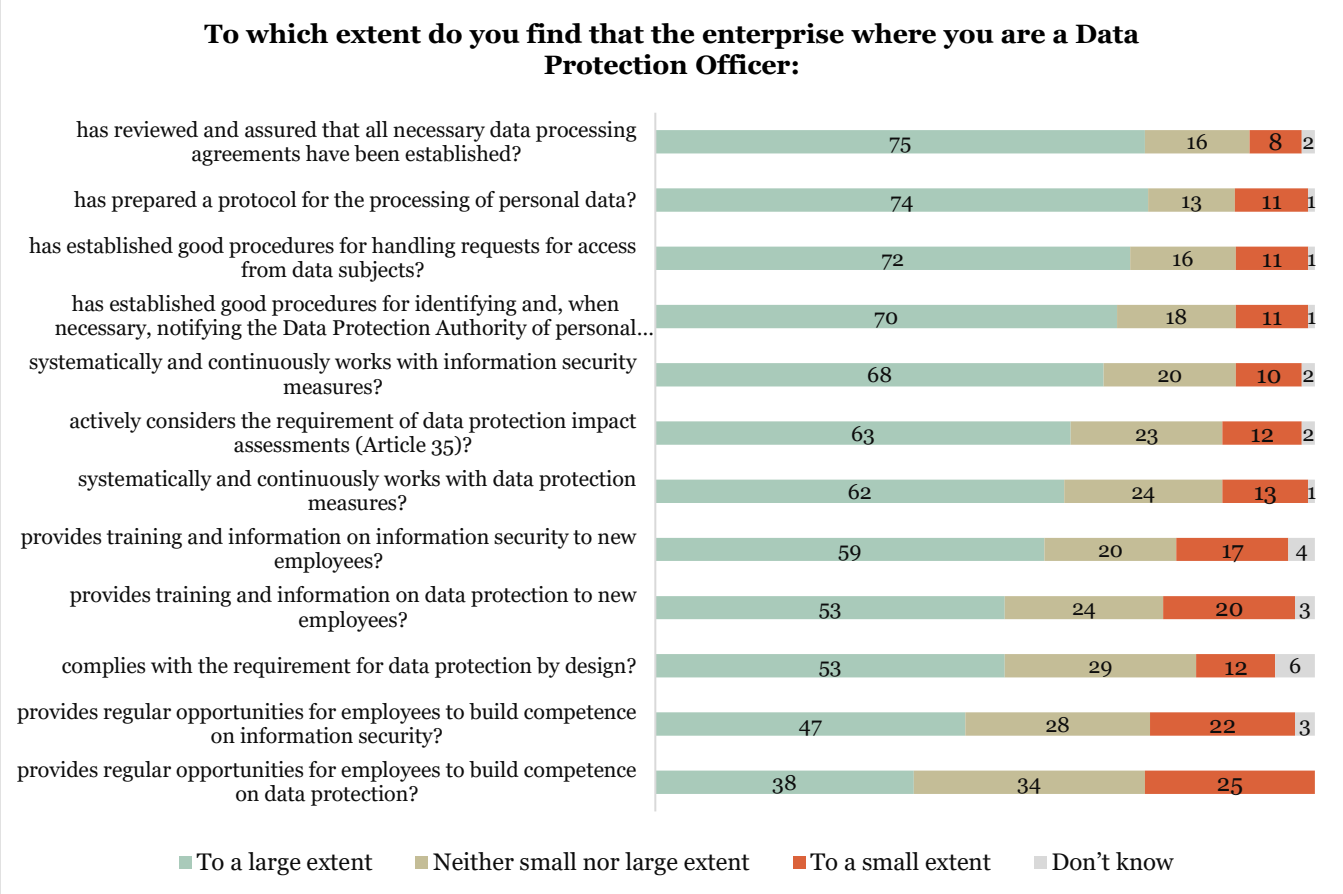
The reason why perceived compliance is lower among Data Protection Officers representing local and regional authorities is likely complex. Municipalities process vast quantities of personal data about their citizens from birth to death, including sensitive or other special categories of personal data. In addition, municipalities and counties are complex organizations, with an extremely wide range of tasks to perform. This applies both to the types of services they

provide and their exercise of authority. One should perhaps also note that while having a Data Protection Officer is voluntary for many private enterprises, all public bodies are required to have a Data Protection Officer.

The responses provided in this survey are in line with the trend we have observed in the Data Protection Authority's daily guidance and case processing activities. We have seen several examples of compliance with data protection legislation proving difficult for some municipalities, and there have been a number of personal data breaches — sometimes leading to hefty fines. In 2019, both the City of Bergen and the City of Oslo were fined more than NOK 1 million each (in Norwegian). Several other municipalities have also been fined and sanctioned since 2018.

Which requirements do enterprises struggle to comply with?

While many Data Protection Officers find that their enterprises generally comply with relevant legislation, the law includes several specific requirements that must actively be met. We therefore asked to which extent officers find that central requirements and conditions for compliance with data protection legislation have been met in the enterprises they represent.



The responses show:

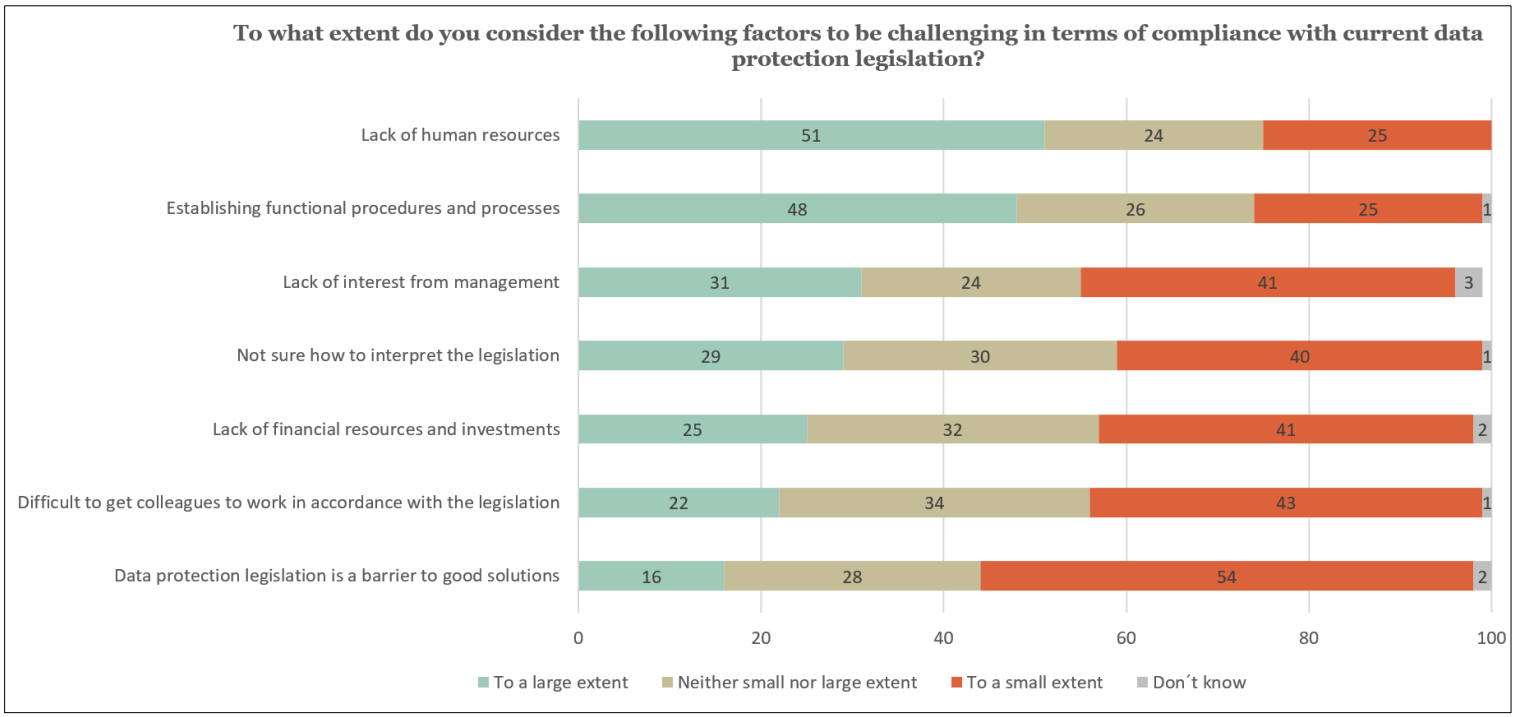
- Most officers say that their enterprise has established data processing agreements (75 percent), has prepared protocols (74 percent), and has established good procedures for handling requests for access from data subjects (72 percent).
- Seven in ten officers (70 percent) also say that their enterprise has established good procedures for identifying and giving notification of personal data breaches.
- Almost seven in ten officers (68 percent) say that their enterprise, in their opinion, systematically and continuously works with data protection measures.
- Very few officers say their enterprise has implemented measures only to a small extent. The biggest challenges, as officers see it, concern building the employees' competence on data protection and information security.

The results show that officers feel many of the statutory requirements have been met. Specific requirements, such as data processing agreements, protocols, procedures for access and systems for notification of breaches have largely been met.

The responses also give rise to some concerns, however. Some enterprises seem to fall short in areas related to competence and culture, such as regular competence-building and training. The consequence may be that systems and procedures may have been developed, but employees are not aware of them or may not have the competence to execute measures in practice. This is an impediment for good compliance.

What do officers believe to be the main challenges in terms of compliance?

The survey shows that many officers find that their enterprises generally are compliant, but that several requirements and conditions have not been met. In the survey, we also asked the officers to identify challenges they have identified in terms of compliance with current data protection legislation.



The responses show:

- Half of the officers find that a lack of human resources to a large extent pose a challenge in terms of compliance with current data protection legislation. This is seen as a major challenge in the public sector (local and regional authorities and national administration) and among non-profit organizations and associations.
- Approximately half of the officers say establishing functional procedures and processes are a challenge (48 percent).
- 27 percent experience uncertainty about how to interpret the legislation.
- Some point to a lack of competence and interest within the enterprise as a challenge for compliance. 29 percent point to the challenge of lack of interest from management, and 22 percent find it difficult to get their colleagues to work in accordance with the legislation.
- The factor that seems to pose the least problems is the data protection legislation itself.

As the Data Protection Officers see it, access to human resources and the establishment of functional procedures and processes are the two main challenges to the enterprise's compliance with legislation. The data protection legislation itself is not found to stand in the way of good solutions.

27 percent of officers, however, experience uncertainty about how to interpret the legislation. This could be attributable to the fact that this legislation is still relatively new, and the enterprises are facing legal clarifications they have not encountered before. At the same time, the survey shows that 24 percent of officers have not participated in courses or seminars or had the chance to build competence on data protection legislation and/or information security. The potential for providing Data Protection Officers with more opportunities to participate in competence-building measures could be considerable.

Five recommendations for supporting the work of Data Protection Officers within the enterprise

Data Protection Officers play a key role in the enterprise's work with privacy and information security, as well as in its compliance with the General Data Protection Regulation. At the same time, management is responsible for establishing a good framework for the officer to perform their tasks. Based on the findings from this survey, the Data Protection Authority has prepared some recommendations for Data Protection Officers and management to strengthen the role of the Data Protection Officer, and thus also the enterprise's data protection efforts.

1. **Establish a work and role description which is agreed with the enterprise's chief executive officer**
   Management is responsible for making the necessary arrangements to ensure the officer is able to perform their tasks. To prevent a situation where misunderstandings about the role or conflicts of interest may occur, it is a good idea to have a role description or instructions that clearly define the officer's tasks and how responsibilities are distributed between them and the enterprise. It is equally important to coordinate expectations concerning which tasks the Data Protection Officer is **not** expected to be responsible for. If the Data Protection Officer also has other tasks, one should clarify how much time (e.g. as a percentage of a full-time position) should be set aside for the role of Data Protection Officer.

2. **Establish formal structures that ensure involvement and dialogue between the Data Protection Officer and management.**
   Formal reporting procedures are a great way to establish a good framework for dialogue. Executive management should agree with the officer (preferably in the role description) to meet regularly, such as quarterly or semi-annually. We also recommend that the officer prepare written reports to management on the status of data protection efforts, any challenges that have been identified and the officer's assessments and recommendations. Establish procedures for which other meetings and processes within the enterprise which it is natural for the Data Protection Officer to be involved in. This work should be seen in light of the fact that management, and not the Data Protection Officer, is responsible for compliance with data protection legislation.

3. **Strengthen awareness of and competence on data protection within the enterprise**
   Competence-building, training and awareness are central to data protection efforts within the enterprise. In order for established procedures and processes to be effective, the enterprise is entirely dependent on employees being familiar with them and having the competence to follow up on them. Management and the Data Protection Officer should therefore initiate competence-building measures. Employees should be made aware of what privacy and data protection actually entail and which procedures and systems the enterprise has put in place, as well as be provided with opportunities to build their competence on information security and the role of the Data Protection Officer within the enterprise. The Data Protection Officer should also make their contact information available, so that employees (and external parties) know whom to contact if they have questions about privacy and data protection. Last, but not least, the tone is set from the top. Management must get involved and show an interest in data protection in order to promote a good data protection culture within the rest of the enterprise.

4. **The Data Protection Officer should establish contact and collaborate with other Data Protection Officers**
   Data Protection Officers should participate in networks and communicate with other Data Protection Officers. This will both build the officer's competence and provide them with opportunities to discuss data protection issues and challenges they experience in their role as Data Protection Officers with peers. For example, officers can join the Norwegian Association of Data Protection Officers (pvo.no) or one of the many networks for Data Protection Officers. To build competence, officers may also find it useful to prioritize external courses and seminars, which provide them with opportunities to update their knowledge of data protection and information security.

5. **Contact the Data Protection Authority for advice and guidance**
The Data Protection Authority offers online guidance and also has a phone guidance service, where officers can discuss data protection issues with the Authority's staff. The Data Protection Authority has also a dedicated contact person and coordinator for Data Protection Officers, who may be consulted on questions concerning the role of Data Protection Officer.

Office address:
Trelastgata 3, Oslo

Postal address:
PB 458 Sentrum
0105 Oslo

postkasse@datatilsynet.no
Telephone: +47 22 39 69 00

datatilsynet.no
personvernbloggen.no
twitter.com/datatilsynet