2023 Coordinated Enforcement Action

Designation and Position of Data Protection Officers

Adopted on 16 January 2024

EXECUTIVE SUMMARY

In October 2020, the European Data Protection Board (EDPB) decided to set up a Coordinated Enforcement Framework (CEF) with a view to streamlining enforcement and cooperation among supervisory authorities, consistently with the EDPB 2021-2023 Strategy. A first CEF was conducted in 2021 on the Use of Cloud Services by Public Bodies.

For the second CEF, the EDPB selected in September 2022 'the Designation and Position of Data Protection Officers' for its 2023 Coordinated Enforcement Action.

Throughout 2023, 25 supervisory authorities ('SAs') across the EEA launched coordinated investigations into the role of Data Protection Officers ('DPOs'). The CEF was implemented at national level in one or several of the following ways: (1) fact-finding exercise, (2) questionnaire to identify if a formal investigation is warranted, and/or (3) commencement of a formal enforcement investigation, or follow-up of ongoing formal investigations.

Between November 2022 and February 2023, these supervisory authorities discussed the aims and the means of their actions in the context of the CEF. In this context, the SAs drafted a questionnaire in a neutral way so that it would be possible for either the controller/processor or the DPO to fill it in. While doing this, they ensured that it would be possible for SAs to adjust the questionnaire or to draft their own, based on (or inspired by) the commonly drafted questionnaire. The present report aggregates the findings of all the supervisory authorities participating in the CEF. Particular attention is paid to challenges identified by supervisory authorities and/or respondents during the CEF action. These include issues such as insufficient resources allocated to DPOs, insufficient expert knowledge and training of DPOs and risks of conflicts of interests.

This report provides, among other things, a list of recommendations that organisations, DPOs and/or SAs may take into account to address the challenges identified, without prejudice to the provisions of the GDPR/EUDPR and the powers of supervisory authorities.

List of recommendations / Points of attention
Absence of designation of a DPO, even if mandatory
• More initiatives by SAs could raise awareness among organisations regarding their obligation to designate a DPO, including as to whether or not a DPO is actually required. Further guidance from SAs on the applicable requirements to designate a DPO, further awareness campaigns to promote existing guidance on this topic and enforcement actions can be part of the solution to educate controllers and processors.
Insufficient resources allocated to the DPO
• More initiatives and actions by SAs could incentivise organisations' management to dedicate more resources to DPOs and their team. • At all times, controllers and processors must be performing an appropriate, case-by-case analysis of what resources a DPO needs. We recommend that controllers take this obligation seriously and are ready to show their work. • Controllers and processors must carefully verify that the DPO has sufficient resources to properly exercise their functions. In some cases when employing an external DPO, this may require controllers and processors to verify how many clients that DPO has, to ensure that they have sufficient time and capacity to fulfil the relevant GDPR obligations. • Further guidance from SAs as well as additional training materials could help DPOs to navigate complex issues and save time.

Insufficient expert knowledge and training of the DPO
• SAs and/or the EDPB could provide further guidance and training sessions for DPOs. These trainings (and the amount of trainings necessary) can be customised according to the specific needs of each Member State. • Controllers and processors should ensure that they are documenting their organisations' knowledge and training needs and progress. This can also be important to ensure compliance with Articles 24 and 5(2) GDPR, and Articles 26 and 4(2) EUDPR. • Controllers and processors should ensure that DPOs are given sufficient opportunities, time and resources to refresh their knowledge and learn about the latest developments, including, if it is relevant to their activities, on new EU digital- and AI-related legislation. • Increased use of certification mechanisms and initiatives where relevant. • Increased cooperation from stakeholders with universities and market-led training courses.
DPOs not being fully or explicitly entrusted with the tasks required under the GDPR/EUDPR
• More initiatives and actions by SAs could incentivise controllers and processors to maintain a proper separation between, on the one hand, the controller/processor obligations and, on the other, the DPO's own obligations and duties as set out under the GDPR/EUDPR. • Controllers should make sure to promote the role of their DPO internally. • Controllers should work together with their DPOs to build up their roles in an appropriately comprehensive and independent way. • SAs could include DPOs and/or their opinions in a structural fashion into the SA's processes when contacting a controller and/or processor, which will help to enable and promote DPOs in their roles. • All stakeholders should promote the role of the DPO within organisations to ensure that the DPO is seen as necessary and given effective support by the controller (processor) in accordance with the GDPR/EUDPR. • SAs can support and encourage initiatives to protect and enhance a DPO's independence regardless of the form of the contract under which they perform their function, so that DPOs feel safe to fulfil all aspects of their role. • Controllers and processors should ensure that they are actively reviewing and (where necessary) improving the DPO's involvement within the organisation. Such review may, among other things, consider the Guidelines on DPOs, an annual report of the DPO's activities, and general good practices.
Conflict of interests and lack of independence of the DPO
• SAs recall that the term 'conflict of interests' was already clarified in the Guidelines on DPOs and more recently by the Court of Justice in its *X-Fab Dresden* Judgment. Despite this, the results of the CEF action showed risks of possible conflicts of interests. Based on this, the Guidelines on DPOs should be developed further, also taking into account the new roles taken on by DPOs in certain organisations under the new pieces of EU legislation in the digital field**.** • More initiatives and actions by SAs could verify that controllers and processors have appropriate safeguards in their procedures to ensure that the DPO is not responsible for carrying out tasks that lead to a conflict of interests. • More awareness-raising activities, information and enforcement actions on the independence of the DPO could be envisaged (including on the prohibition on penalising and dismissing DPOs for performing their DPOs' tasks), either by SAs or internally by organisations themselves. • Organisations and DPOs could formalise the DPO duties and conditions for performing the DPO's duties in an 'engagement letter'. • DPOs should be able to collect evidence in the event of interferences with their independence.

Lack of reporting by the DPO to the organisations' highest management level
• The legal obligation to have the DPO report to the organisation's highest management level may benefit from further guidance to help controllers and processors implement it in practice. SAs could encourage the drafting and adoption of industry standards, internal data protection policies and best practices to better define the conditions, frequency, content and effectiveness of the direct reporting of the DPO to the highest management level. • SAs/the EDPB could adopt 'best practise'-based recommendations or/and a template for DPO reporting (e.g. for at least annual reporting), setting out modular and adaptable content to take into account the specificities of the organisations and the industry. • SAs could initiate more actions and initiatives with respect to the direct access of the DPO to top management, which is an important guarantee of the independence of the DPO.
Further guidance from supervisory authorities
• In addition to the existing guidance at national and EEA levels, further guidance could help empower DPOs and address some of the challenges identified above. • In particular and as mentioned above, the Guidelines on DPOs should be developed further based on the survey results.

Some of the actions undertaken by supervisory authorities in the CEF are still ongoing at national level, especially when formal investigations were launched. Accordingly, this document does not constitute a definitive statement of the actions carried out within the CEF and the purpose of this report is not to conclude on the measures to be adopted but to reflect on the actions undertaken by competent supervisory authorities and identify the possible points of attention. It may need to be updated in the course of 2024 to take into account the progress of the procedures which have not yet been completed to date and given the issues identified, if the Guidelines on Data Protection Officers are further developed by the EDPB.

Table of contents

1 INTRODUCTION

In October 2020, the European Data Protection Board (**EDPB**) decided to set up a Coordinated Enforcement Framework ('**CEF**')[1]. The CEF is a key action of the EDPB under the second pillar of its 2021-2023 Strategy[2], together with the creation of a Support Pool of Experts ('**SPE**'), aiming at streamlining enforcement and cooperation among supervisory authorities (collectively '**SAs**', or individually '**SA**').

The EDPB selected in September 2022 the topic of '**the Designation and Position of Data Protection Officers**' for its 2023 Coordinated Enforcement Framework. The EDPB decided to prioritise this topic given the position of Data Protection Officers ('**DPOs**') under Regulation (EU) 2016/679 ('**GDPR**')[3] as intermediaries between SAs, individuals and the business units of an organisation. More specifically, this topic was chosen taking into account:

(i) the fact that the role of DPOs is crucial in ensuring that data protection law is applied and complied with within organisations since the DPO is a 'key player in the new data governance system'[4]; and

(ii) the fact that, under the GDPR, the DPO is a person with expert knowledge of data protection law and practices. By bridging the gap between EU data protection law and its practical application, DPOs help to promote the effective protection of individuals' fundamental right to data protection.

Even though designating a DPO was already an obligation for the EU institutions under the previous legal framework[5] (and now under Regulation 2018/1725 or the '**EUDPR**'[6]), the DPO was a new requirement introduced into the GDPR[7] and, before the GDPR, many Member States' laws had no provisions on mandatory DPO designation. Despite this, in 2023, an IAPP research indicated that more than 700,000 organisations have registered DPOs across the European Economic Area (EEA) under the GDPR[8].

[1] EDPB Document on Coordinated Enforcement Framework under Regulation 2016/679 (EDPB, 20 October 2020), https://edpb.europa.eu/sites/default/files/files/file1/edpb_documents_20201020_coordinatedenforcementframework_en.pdf.
[2] EDPB Strategy 2021-2023, adopted on 15 December 2020.
[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation (OJ L 119, 4.5.2016, p.1).
[4] Guidelines on DPOs (as defined below), page 5.
[5] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1–22).
[6] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39). As regards the EDPS, any references to 'organisations', 'controllers/processors' and - depending on the context - 'Member States' should be understood as referring to the European Union Institutions, bodies, offices and agencies . In addition, as regards the EDPS, any reference to the GDPR should be understood as corresponding references to the EUDPR, where the latter is not explicitly referred to. More specifically, Articles 43-45 of Regulation (EU) 2018/1725 relate to DPOs.
[7] However, in some EU Member States, an equivalent of the DPOs existed before the GDPR.
[8] 'GDPR at FIVE', IAPP, May 2023, available at https://iapp.org/media/pdf/resource_center/gdpr_at_five.pdf.

The GDPR sets out specific rules regarding the designation, knowledge and experience of DPOs, the tasks and resources allocated to them as well as on their actual role and position[9]. One of the goals of this CEF was to generate deeper insight for SAs on the compliance of organisations with the applicable GDPR provisions and identify potential difficulties that DPOs are facing when conducting their tasks.

Building on common preparatory work, the EDPB announced the initiation of the action on 15 March 2023[10]. Throughout 2023, 25 supervisory authorities across the EEA launched coordinated investigations into the role of DPOs. The CEF was implemented at national level in one or several of the following ways: (1) fact-finding exercises, (2) a questionnaire to identify if a formal investigation is warranted, and/or (3) commencement of a formal enforcement investigation, or follow-up of ongoing formal investigations. More specifically, eighteen SAs stated that the initial procedural framework of their action was fact-finding. Out of these, thirteen indicated that such fact-finding could serve to determine follow-up action based on the results. In practice, ten SAs have initiated – or are planning to initiate – new formal investigations, or have been continuing ongoing investigations as part of this CEF action. The PL SA already had ongoing investigations on the matter; it therefore did not participate in the questionnaire but decided to join the CEF to exchange on its findings. Finally, NL SA's survey at national level took place during the writing of this report; the rapporteurs did their best to include these results in all statistical aspects, however the qualitative analysis of their reports could not be considered in the general discussion presented here.

The present report aggregates the findings of supervisory authorities participating in the CEF, and provides a state of play of their work. In particular, the first part of this report presents statistics regarding the stakeholders' answers for each SA, while the second part analyses the challenges faced by DPOs and organisations (controllers or processors) that have designated a DPO, and how these may impact compliance with GDPR/EUDPR. For each identified challenge, we present a short description of the issue at hand, which provisions of the GDPR apply and why this has been an issue for the participating stakeholders. In addition, we present an overview of the actions already implemented or ongoing, including guidance, enforcement actions or potential actions by SAs.

The SAs' national reports are attached as appendices to this report and provide further detail on the results obtained and the analyses and observations made at national level.

With this second CEF action, the EDPB intends to:

- **obtain insights regarding the profile, position and work of DPOs in practice to guide enforcement actions of SAs,**
- **collect the experience and conclusions of the supervisory authorities that have initiated or planned formal investigations or have continued investigations under this CEF action for analysis,**
- **raise awareness of the requirements applicable to DPOs within organisations (in particular within the highest management level of organisations),**
- **ensure that DPOs fulfil the key role assigned to them by data protection law to facilitate compliance and promote the role of the DPO and**
- **evaluate DPOs' and organisations' needs on further guidance and other form of support.**

[9] Articles 37 to 39 and recital 97 GDPR.
[10] Launch of coordinated enforcement on role of data protection officers, EDPB, 15 March 2023, https://edpb.europa.eu/news/news/2023/launch-coordinated-enforcement-role-data-protection-officers_en.

2 BACKGROUND AND METHODOLOGY

2.1 *Legal background*

The GDPR did not invent the concept of a data protection officer. However, it did impose, among other things, new EU-wide requirements setting out conditions under which such an officer must be appointed,[11] the powers that such an officer should have, and several conditions relating to their position within an entity's structure and processes. Prior to the entry into force of the GDPR, the Article 29 Working Party hailed the role of DPOs as 'a cornerstone of accountability', and its Guidelines on Data Protection Officers from 2017 (**'Guidelines on DPOs'**), which were endorsed by the EDPB following the GDPR's entry into force, stated that they would be 'the heart of this new legal framework for many organisations'.[12]

Under Article 43 EUDPR, all EU institutions or bodies must appoint a data protection officer. Meanwhile, Article 37(1) GDPR states that a controller and processor shall designate a DPO if:

a. the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
b. the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
c. the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 GDPR and personal data relating to criminal convictions and offences referred to in Article 10 GDPR.

Once appointed, Article 38(1) GDPR and Article 44(1) EUDPR require that controllers and processors keep the DPO 'involved, properly and in a timely manner, in all issues which relate to the protection of personal data', with Article 38(2) GDPR and Article 44(2) EUDPR obliging controllers and processors to 'support' the DPO 'by providing resources' for their tasks, and Article 38(3) GDPR and Article 44(3) EUDPR requiring that the officer be independent of influence from those controllers and processors. Article 39 GDPR and Article 45 EUDPR, meanwhile, set out a number of tasks for the DPO, including that they must monitor and advise on GDPR compliance, and cooperate with supervisory authorities. DPOs are also intended to be visible figures that can interact with data subjects; Articles 13(1)(b), 14(1)(b) and 37(7) GDPR, and Articles 15(1)(b), 16(1)(b) and 43(3) EUDPR require controllers to make the DPO's contact details available, so that they can be contacted if needed.

EU data protection law also provides solutions to adapt the appointment and functioning of the DPO to the specific needs of the controller or processor concerned, taking into account the complexity of their processing of personal data. Under Articles 38(6) GDPR and 44(6) EUDPR, the role can be included as part of another position (provided that the role's other tasks and duties do not result in a conflict of interests) and, per paragraph (3) of both provisions, that the DPO 'shall directly report to the highest management level of the controller or the processor'. Further, Articles 37(2) and (3) GDPR, and 43(2) EUDPR, allow multiple controllers or processors (whether undertakings or public bodies under the GDPR or EU institutions and bodies under the EUDPR) to appoint a single data protection officer, provided that the DPO is easily accessible for all. Meanwhile, Article 37(6) GDPR and Article 43(4) EUDPR state that a DPO does not necessarily have to be a full member of staff and can instead fulfil their tasks on the basis of a service contract. Notably, unlike the GDPR, the EUDPR does not consider

[11] Although, as noted above, the obligation to appoint a DPO did already exist for EU Institutions and Bodies under Regulation 45/2001, Article 24, as well as in the national laws of some Member States.

[12] EDPB, Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01, revised and adopted 5 April 2017, page 4.

these two options on an equal footing, as Article 43(4) provides that the DPO shall be a staff member of the EU institution; it is only when taking into account their size, and if the option to have a shared DPO with another EU institution is not exercised, that an EU institution may designate a DPO on the basis of a service contract. Each of these provisions are particularly useful for smaller controllers and processors who may wish to employ a DPO but do not have the resources to bring on a dedicated, permanent member of staff. However, it is very important that, even where the DPO has other roles or operates on a part-time basis, the DPO's tasks remain the same – and, as set out above, controllers and processors must ensure that they provide adequate time, training and resources for the DPO to do their job properly.

The GDPR sets out the conditions under which a DPO must be appointed, but controllers or processors may also choose to appoint one voluntarily. As a compliance method, this can be extremely useful; having a data protection expert who is tied into planning and decision-making processes helps with not only the principle of accountability under Article 5(2) GDPR, but also the Article 24(1) obligation to implement appropriate technical and organisational measures to ensure compliance with the GDPR, the Article 25 obligations towards Data Protection by Design and by Default, among many others.

2.2 *Methodology*

Participating supervisory authorities first drafted a questionnaire together in English, which would then be translated into the relevant EU languages and to be sent to the stakeholders of each SA's choice at national level. The questionnaire was drafted to allow SAs to apply different strategies in their choice of target for this questionnaire. One authority (EDPS) chose not to use the commonly-built questionnaire as such, but rather used a set of questions inspired from this questionnaire, which was adapted to take into account the EDPS realities (different legal framework, public sector only). PL SA participated in the effort through ongoing investigations that started before the launch of this CEF, and therefore did not use the questionnaire but rather its own set of questions. In these circumstances, the statistics given in this report based on the commonly-built questionnaire do not include PL SA. However, PL SA provided the preliminary results of its ongoing formal investigations as part of this CEF.

The following information may be relevant to analyse the results of the survey.

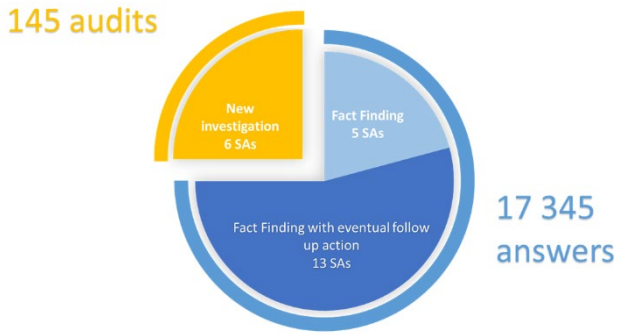
<u>Cultural and language differences:</u>
The questionnaire has been translated in 24 languages and answered in those target languages. While translations have been proofread by SAs, the wording of the questions may have been understood or interpreted differently depending on language or cultural differences.

This difficulty is particularly visible for Question 7 regarding the average duration of the DPOs appointment to the role. Some answered the time they foresee in the role (i.e. based on their type of contract) and others based on their seniority in the role.

<u>Qualitative or quantitative?</u>
Each participating supervisory authority developed its own strategy for the recipients of this commonly-built questionnaire. Overall, they sent their CEF questionnaire to 61,962 recipients (42,875 organisations and 19,087 DPOs). Out of the contacted stakeholders, 17,490 responded and completed the questionnaire: 15,108 organisations and 2,382 DPOs, providing valuable global results that can be considered significant.

However the volume and profile of contacted stakeholders vary at national level. To analyse the results it is necessary to identify their strategies, in particular those who adopted the most different ones:

- On the one hand, the Austrian, Bavarian, French, Greek, Latvian, and Swedish authorities provided qualitative oriented results built upon formal investigations of a small number of stakeholders.
- On the other hand, the Belgian, Croatian, Cyprian, Dutch, Liechtenstein, Maltese, Portuguese, Slovenian and Spanish SAs aimed at quantitative results, sending their questionnaires to hundreds (for the smaller countries) to tens of thousands (for the biggest) of organisations and DPOs. For example, the Belgian, Dutch, Liechtenstein, Portuguese, Slovenian and Spanish SAs contacted all DPOs whose contact details had been notified according to Article 37(7) GDPR.



These various strategies have to be taken into account when comparing the answers as this context might have an impact. In particular, questions regarding compliance are globally more positive for the first group (i.e. formal investigation) compared to the opposite group (i.e. anonymous massive survey).

Considering that each authority processed between 10 and 10,257 answers of the 17,490 answers collected, and to be able to see EU-wide trends, we chose to compute Average and Median based on the percentage of respondents per authority. The same indicators built on the sum of answers would give different numbers.

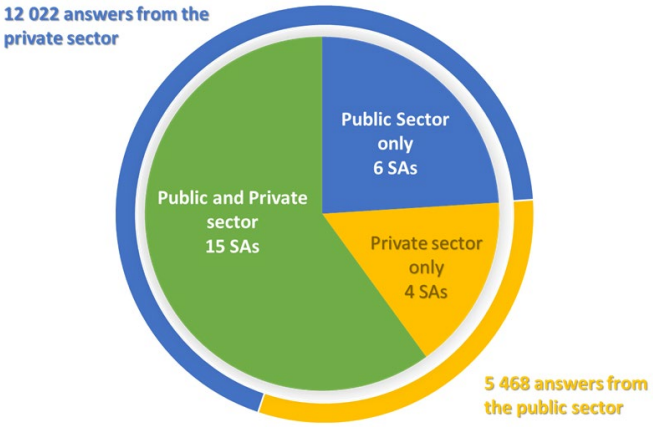
Who answered?

Sixteen SAs contacted organisations (either data processors or data controllers) while seven SAs reached out to DPOs directly, and two SAs did both. Overall, SAs contacted 61,962 recipients: 42,875 organisations and 19,087 DPOs. Out of those, 17,490 responded and completed the questionnaire: 15,108 organisations and 2,382 DPOs.

This might have two foreseeable consequences:

- When a DPO was shared by several organisations, it is possible that he or she responded only once to the survey (as opposed to completing one survey per organisation for which he/she is acting as DPO).
- The survey was mostly completed by organisations (controllers or processors), which may have presented their compliance under a more positive light than if filled out by their DPO.

Certain SAs decided to contact a specific sector or category of organisations. Public-sector organisations were contacted by the CZ SA (ministries), DK SA (municipalities), the EDPS (all the European Union (EU) institutions[13] and their DPOs), EL SA and HU SA. LV SA chose to contact the public sector and associations. Other SAs decided to only contact private-sector organisations (DE SA Bavaria for the private sector, LT SA, MT SA, entities operating in the financial sector for AT SA) or organisations across sectors (BE, CY, EE, ES, FI, FR, HR, IE, IT, LI, LV,NL, PT, SI and SE SAs).



The results obtained at national level are consolidated in **Appendixes 1.1 and 1.2**. Appendix 1.1 sets out the statistical results obtained in each Member State. The means and median of national statistics are displayed, along with the minimum and maximum percentage obtained across Member States. Appendix 1.2 displays the qualitative feedback provided by participating SAs with respect to the CEF action carried out at national level.

For those wishing to analyse the results in Appendixes, the following final elements of context would need to be taken into account:

- SAs who sent the commonly-built questionnaire sometimes added more questions or possible answers to the common questionnaire or sometimes removed or slightly modified certain questions.
- The questionnaire sent by SAs included a limited number of possible answers and no open-field questions.
- The questionnaire did not ask for the size of the contacted organisations, the type of processing carried out nor the categories of personal data processed.

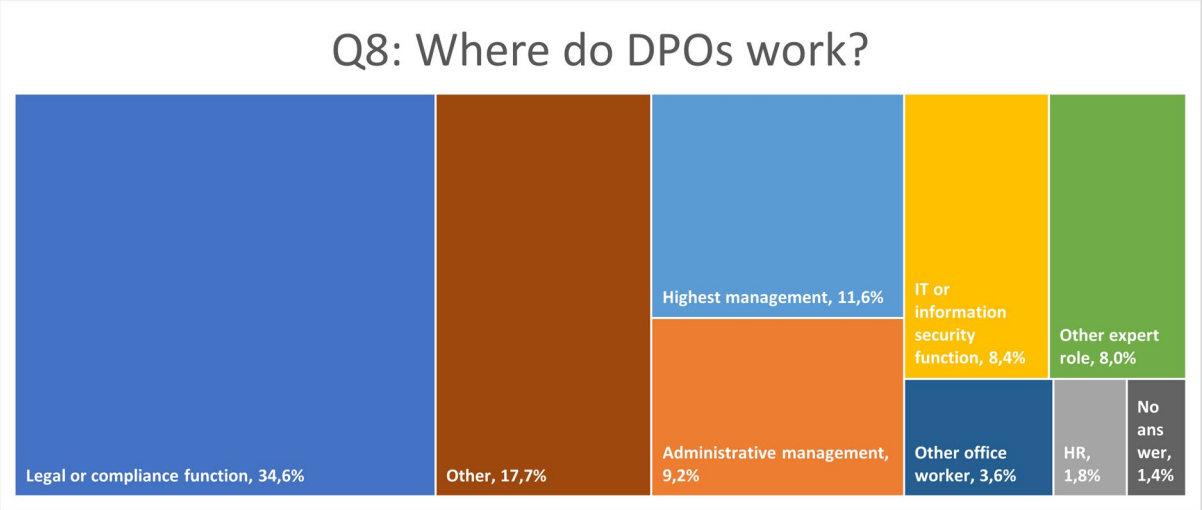
In the current report, except when specifically stated, all statistics given at the EU level are means of the national results.

[13] This refers to EU institutions, bodies, offices and agencies.

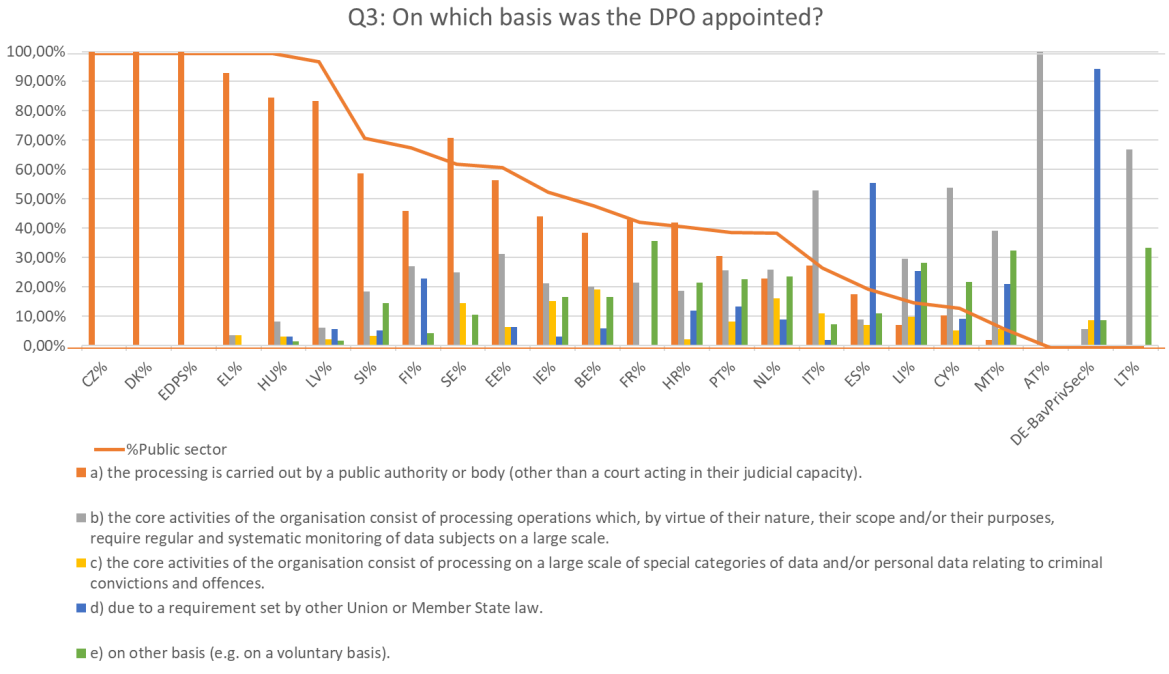
3 SURVEY FINDINGS

3.1 *The DPO in the organisation*

70% of DPOs are staff members of the contacted organisations. They can be included in very different units, in practice the legal and compliance function[14] is one of the main departments cited. Then, depending on national differences, DPOs mainly worked in the 'administrative management' or 'highest management'.



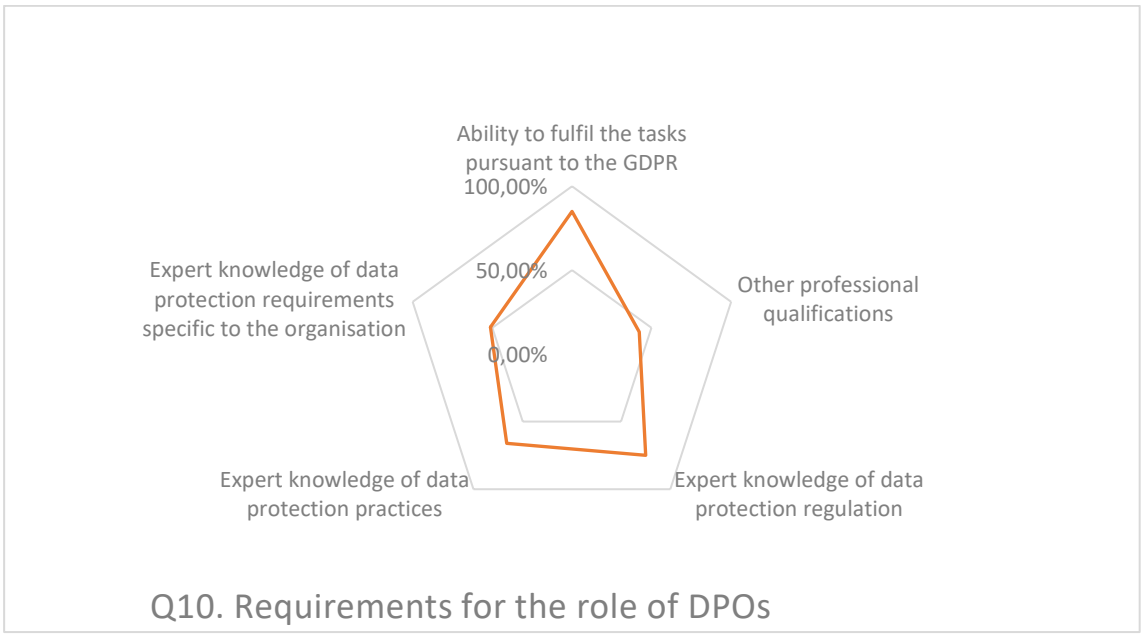
2,482 answers (around 14% of the overall answers) state that a DPO has been appointed without any legal obligation. Considering that DPOs are mandatory in the public sector, there is a strong correlation between the percentage of DPOs from the public sector interviewed and the percentage of appointment made based on 'processing carried out by a public authority or body'.



[14] For the sake of comparison, Spanish answers 'data protection' have been counted under 'legal and compliance'.

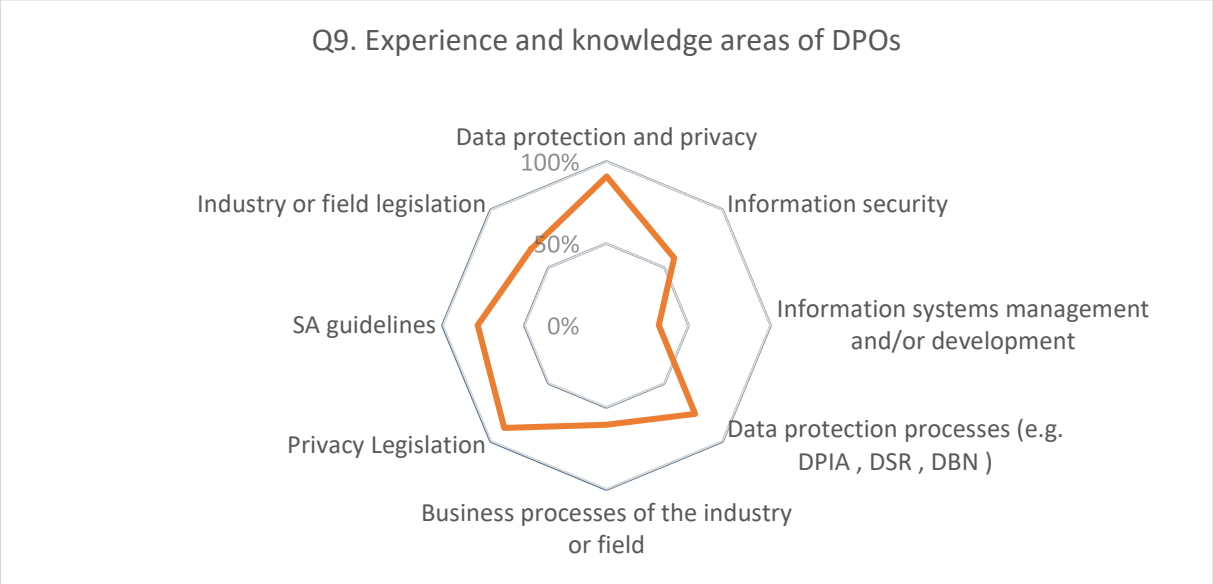
For more than a third of answers, the DPO is the single data protection officer for a group of undertakings or for several authorities or bodies.

The DPO's job requires not only an expertise on general data protection practices and regulation but also, often, a knowledge of the specific field as well as others qualifications.

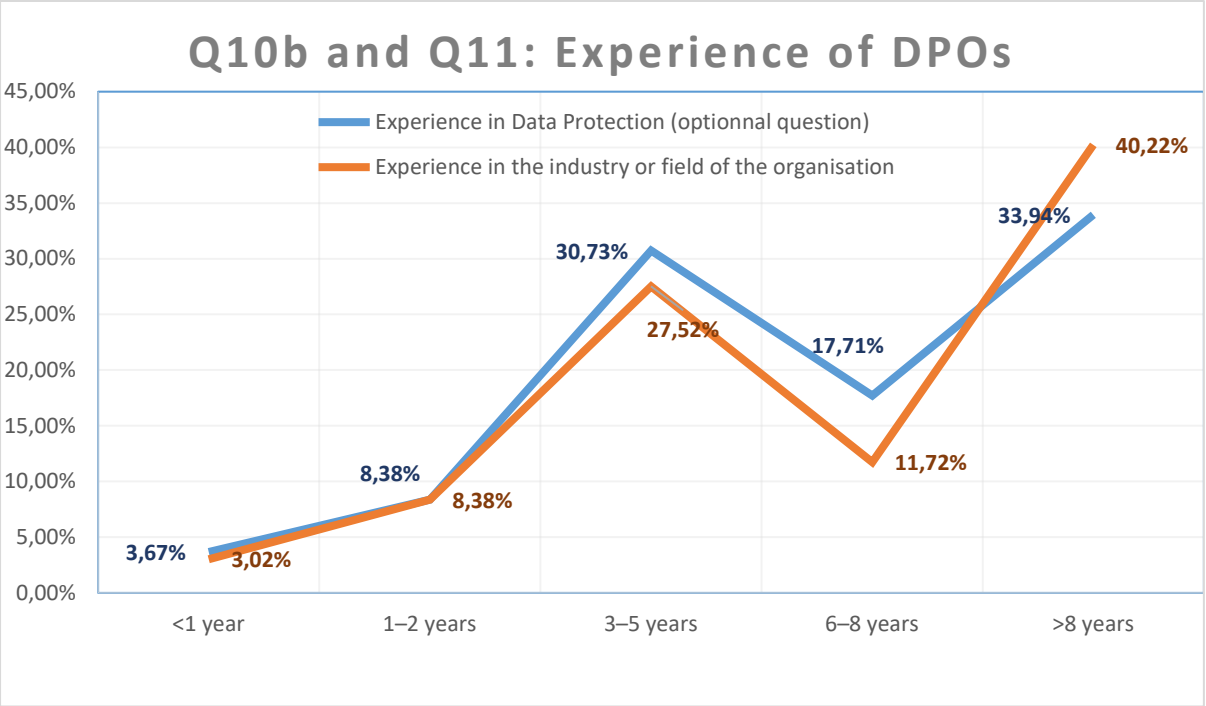


3.2 *The DPOs profile*

DPOs interrogated have a wide set of competences in different domains, on top of their data protection related skills. They also are knowledgeable in the specificity of their industry from a legal (63.89%) and business process perspective (58.3%), and in information security (39.3%).



Most of the DPOs interrogated have experience in the field and as DPOs. Fewer than 13% of them have less than 3 years of experience both as DPOs or in the given industry. About half[15] of them had more than 5 years of experience as DPOs and in the field.



4 CHALLENGES IDENTIFIED DURING THE CEF ACTION AND RECOMMENDATIONS / POINTS OF ATTENTION

This section analyses some of the challenges identified during the CEF action, either by the participating SAs or by respondents. For ease of reference, the analysis below refers to the specific question in the survey attached to this report as **Appendix 1.1** (e.g. 'Question 5').

For each challenge identified below, a list of non-binding recommendations or points of attention is included for organisations, DPOs and/or SAs, without prejudice to the provisions of the GDPR/EUDPR and to supervisory authorities' powers under data protection law. It is also worth noting that these recommendations are not exhaustive.

4.1 *Absence of designation of a DPO even if mandatory*

Of the organisations which responded to the survey, the vast majority had appointed a DPO (Question 1(A)(3)). This is a relatively unsurprising finding, given the nature of the investigation. Nevertheless, it is noteworthy that some organisations had not appointed a DPO, even though they may be required to do so under Article 37(1) GDPR (Question 4). For example, one SA noted that several data controllers in the public sector were under the false impression that Article 37(1) did not apply to them, possibly because they were unaware that they were actually performing public tasks.

[15] 47.4% had at least 6 years of experience as DPO, 52.25% had at least 6 years of experience in the industry or field of the organisation.

This is more than just an awareness problem. 12 respondents from seven Member States (out of 15,108 organisations interrogated) admitted to not appointing a DPO, even though designation was compulsory in those cases (Question 4). Some controllers attempted to provide a justification for this lack of appointment, for example by stating that the organisation outsourced the function as and when they considered it necessary, or because the DPO had quit and they were unable to find a replacement.

Nevertheless, it is also important to remember the methodological limitations of the questionnaire, as it is highly unlikely that these numbers reflect the true extent of noncompliance with Article 37(1).

Suggested recommendations to address this challenge:

- More initiatives by SAs could raise awareness among organisations regarding their obligation to designate a DPO, including as to whether or not a DPO is actually required. Further guidance from SAs on the applicable requirements to designate a DPO, further awareness campaigns to promote existing guidance on this topic (including the SMEs Guide[16]) and enforcement actions can be part of the solution to educate controllers and processors.

4.2 *Insufficient resources allocated to DPOs*

Even where a DPO was appointed, the surveys raised some concerns as to the resources that were being made available to those officers. As noted above, Article 38(2) GDPR requires that controllers and processors give adequate resources to their DPO. In some cases, as noted by the Guidelines on DPOs, it may even be necessary to set up a DPO team, depending on the size and structure of the organisation.[17] Unfortunately, these resources may not be allocated in all cases.

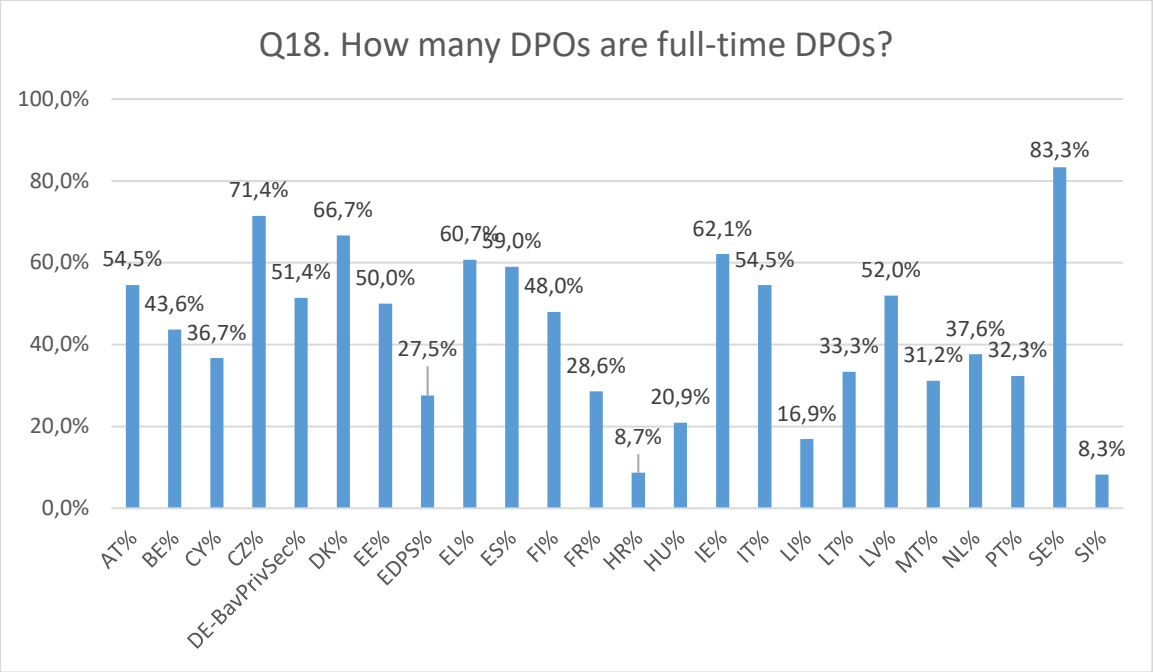
Many of the responding SAs commented in their national report that they had seen a lack of sufficient resources. Of those SAs, many highlighted a lack of human resources, with some expressing concern about organisations' lack of deputy DPOs. This is problematic, both in terms of active compliance today (e.g. because a DPO is expected to perform more work than they can actually handle, so that some matters must then be neglected) and in terms of preserving long-term compliance (e.g. ensuring continuity when a DPO is on leave, becomes sick or resigns, or if the DPO burns out from trying to manage everything on their own).

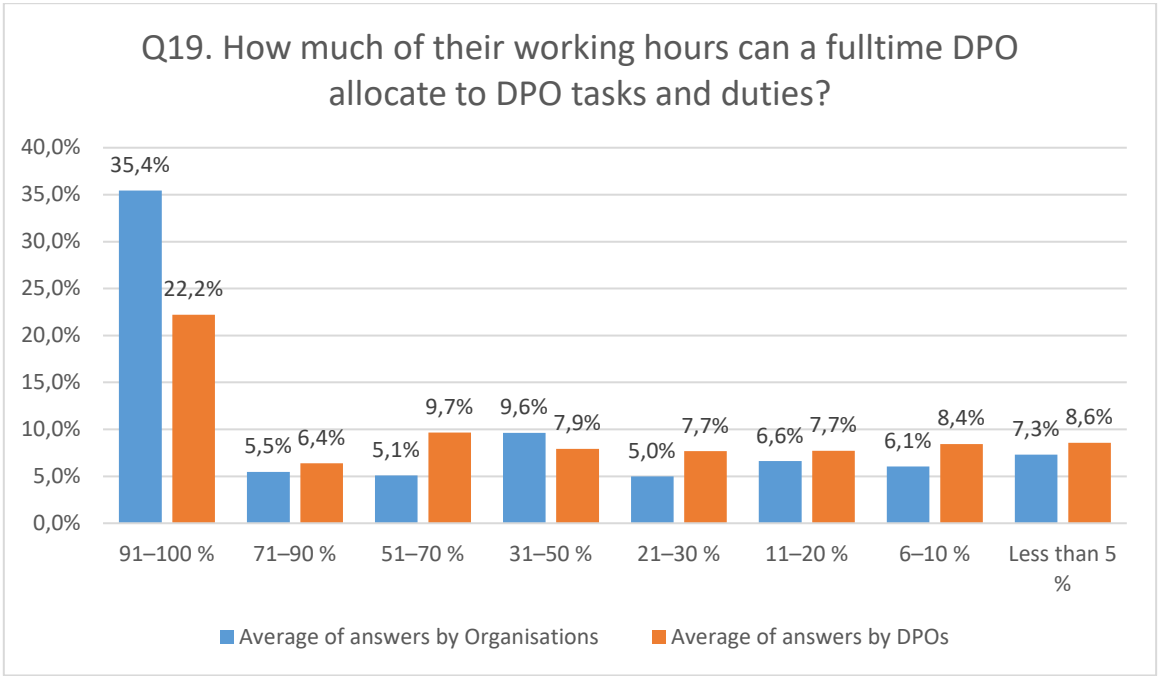
Another concern, raised by several SAs, was that external DPOs acting for multiple controllers or processors may end up spreading themselves too thinly, representing too many clients and so being unable to spend appropriate time on each one. Similar concerns were expressed for in-house DPOs, with many controllers hiring DPOs on a part time basis, or diverting at least some of their DPO's time to other tasks.

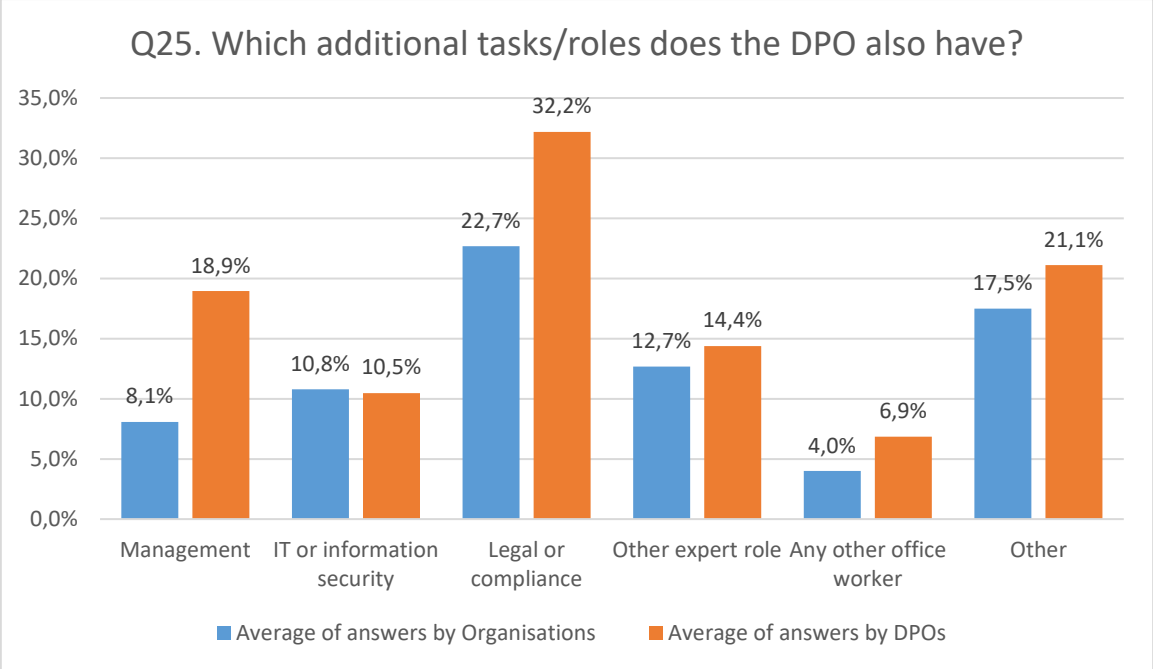
It must be remembered that the GDPR does not strictly require controllers or processors to have a deputy DPO, nor does it prohibit part-time DPOs, DPOs with multiple duties or the sharing of DPOs. However, even when a DPO is appointed under these conditions, Article 38(2) GDPR still requires that the DPO has sufficient resources necessary to carry out their tasks. Ensuring compliance with this provision will be significantly easier with a dedicated, full-time DPO, supported by a team and deputy DPO where appropriate. Equally, while also not strictly required by the GDPR, providing the DPO with control over their budget, it will be easier for that officer to manage their resources in an appropriately responsive and independent manner.

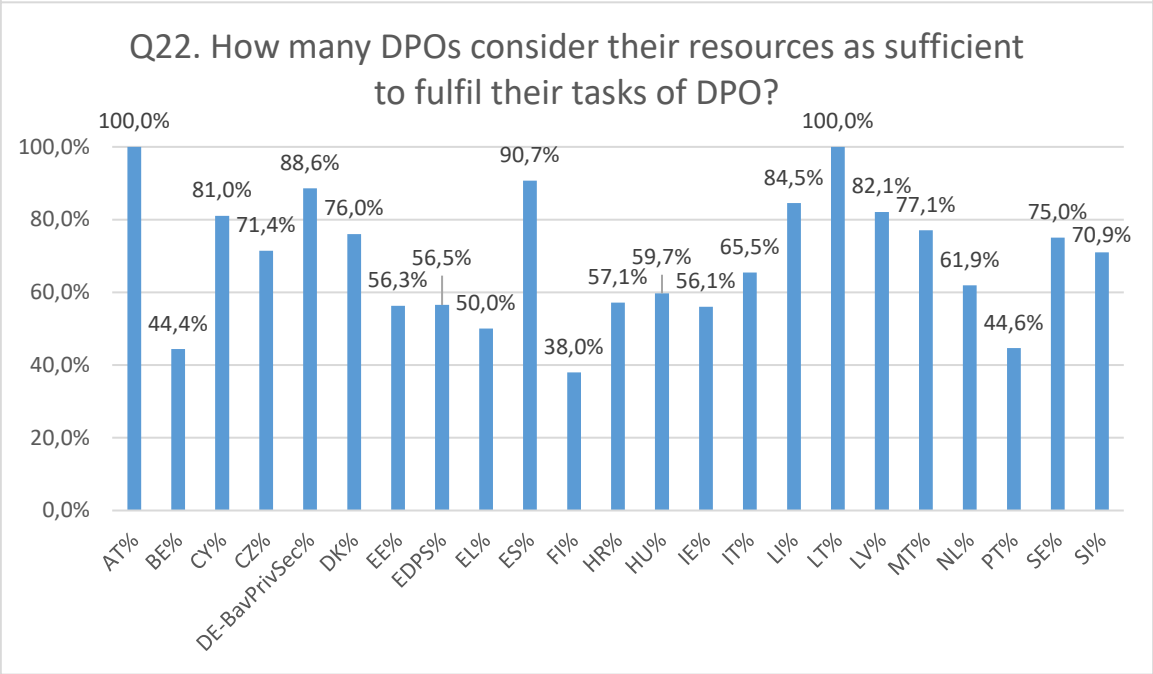
[16] The EDPB data protection guide for small business, available at https://edpb.europa.eu/sme-data-protection-guide/home_en.
[17] Guidelines on DPOs, page 14.

Interestingly, some SAs noted that there was a difference between answers relating to DPOs in the public sector and those relating to DPOs in the private sector. Indeed, BE SA noted that 61.3% of respondents in the public sector indicating that they had insufficient resources, while only 33.3% of that SA's respondents in the private sector indicated the same. This is also confirmed at the EU level: in the 4 SAs interrogating the private sectors, in average, resources were deemed sufficient 91% of the time, while for the 6 SAs interrogating the public sector it was sufficient only in 66% of the cases. We can only note that DPOs from the public sector were significantly less likely to have a deputy DPO (36.4% vs 56.3%), to have a budget (26.6% vs 56.8%) and to manage it when they had one (36.3% vs 53.4%). This is a concerning observation, given that DPOs are often mandatory for public-sector bodies and the importance that they play in protecting the rights of data subjects.









Suggested recommendations to address this challenge:

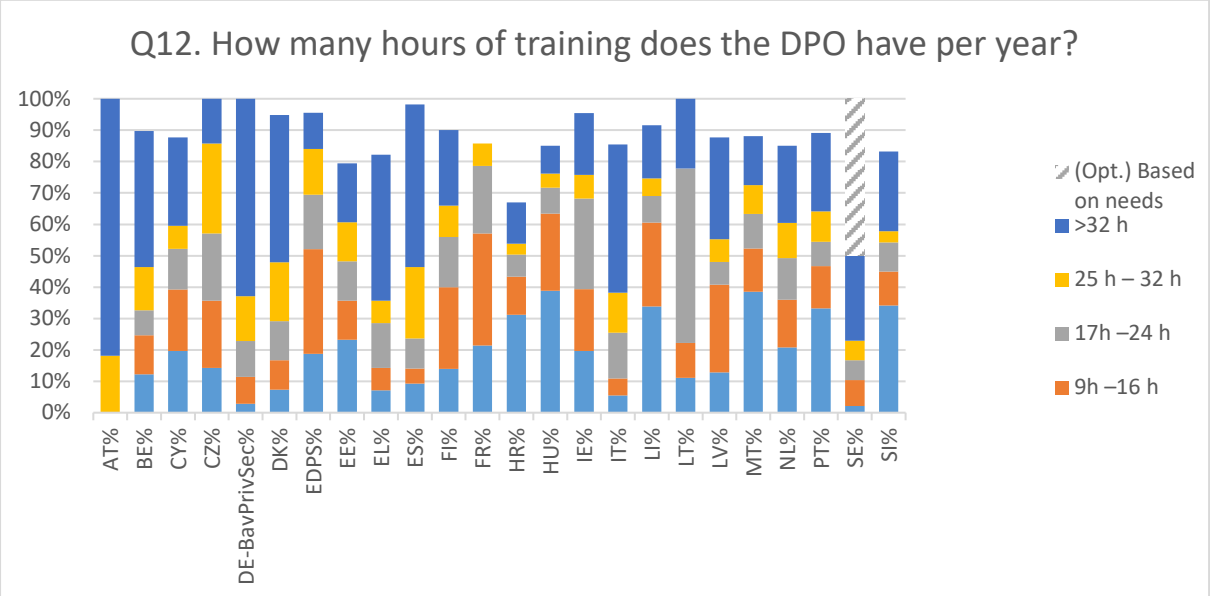
- More initiatives and actions by SAs could incentivise organisations' management to dedicate more resources to DPOs and their team.
- At all times, controllers and processors must be performing an appropriate, case-by-case analysis of what resources a DPO needs. We recommend that controllers take this obligation seriously and are ready to show their work.
- Controllers and processors must carefully verify that the DPO has sufficient resources to properly exercise their functions. In some cases when employing an external DPO, this may require controllers and processors to verify how many clients that DPO has, to ensure that they have sufficient time and capacity to fulfil the relevant GDPR obligations.
- Further guidance from SAs, as well as additional training materials, could help DPOs to navigate complex issues and save time.

4.3 *Insufficient expert knowledge and training of DPOs*

Alongside human and financial resources, SAs also identified concerns relating to DPOs' levels of training and expert knowledge. This included both the level of training and knowledge required when entering the position, and the level of training and knowledge provided to support DPOs once they had been hired.

Under Recital 97 GDPR, the necessary level of expert knowledge required for a DPO varies on the nature of the relevant processing operations. Nevertheless, it is notable that, across all surveys, only a median of 74.97% of respondents indicated that an expert knowledge of data protection regulations was a requirement for the role of DPO, with only a median of 66.12% requiring expert knowledge of data protection practices (Question 10). A median of 90.91% of respondents did state that their DPO (or members of their staff) had data protection and/or privacy experience or expert knowledge (Question 9), but questions still remain as to whether the training provided is enough to fill the gap. It must be noted that the most common single response was that DPOs received more than 32 hours of training a year, with a median of 24.7% (Question 12). However, with only a median of 9.5% DPOs receiving between 25–32 hours a year, this still leaves a strong majority of DPOs receiving 24 hours or less of training a year, with a median of 4.3% receiving none (additional option to Question 12).

While these statistics cannot be used to draw hard-and-fast conclusions as to the adequacy of DPOs' knowledge, a few areas of concern must be identified. First, Article 37(5) GDPR explicitly requires that the DPO have 'expert knowledge'; mere 'experience' is not enough to fulfil the legal requirements. The fact that a median 90.9% of respondents have experience or expert knowledge does not, therefore, mean that all of those respondents are compliant with the GDPR. Secondly, data protection and privacy are rapidly developing fields which require DPOs to receive consistent and continuous education. Even leaving aside the time necessary to develop and maintain expertise in the GDPR, CJEU case law, EDPB's guidelines and national data protection laws and practices (which, by itself, is a task which must be given adequate time and resources), the new developments relating to the European Data Strategy and the so-called Big Five laws (the Digital Services Act, the Digital Markets Act, the Data Governance Act, the Data Act and the Artificial Intelligence Act) may themselves take up more education time than currently granted to many DPOs. This therefore reflects an area of genuine concern, as DPOs can only properly fulfil their roles and provide their full benefits if they are adequately trained.



Suggested recommendations to address this challenge:

- SAs and/or the EDPB could provide further guidance and training sessions for DPOs (e.g. as in France with free online MOOC courses, or as in Poland by publishing answers to DPOs' questions regarding both status and tasks of DPOs, or as at the EDPS by offering a welcome package of information to newly appointed DPOs). See also the subsection below on 'further guidance by SAs', which indicated a clear need for more guidance. These trainings (and the amount of trainings necessary) can then be customised according to the specific needs of each Member State. For example, an extensive data protection training programme for DPOs was launched in Croatia as part of the EDPB's Support Pool of Experts (SPE) initiative[18].
- Controllers and processors should ensure that they are documenting their organisations' knowledge and training needs and progress. This can also be important to ensure compliance with Articles 24 and 5(2) GDPR, and Articles 26 and 4(2) EUDPR.
- Controllers and processors should ensure that DPOs are given sufficient opportunities, time and resources to refresh their knowledge and learn about the latest developments, including, where relevant to their activities and/or purposes, on new EU digital- and AI-related legislation.
- Increased use of certification mechanisms and initiatives where relevant (e.g. as in France).
- Increased cooperation from stakeholders with universities and market-led training courses.

4.4 *DPOs not being fully or explicitly entrusted with the tasks required under the GDPR*

4.4.1 DPOs not being given key roles as required under the GDPR

Article 39 GDPR sets out a number of tasks which must be performed by a data protection officer. However, based on the survey results, these tasks may not always be being properly assigned.

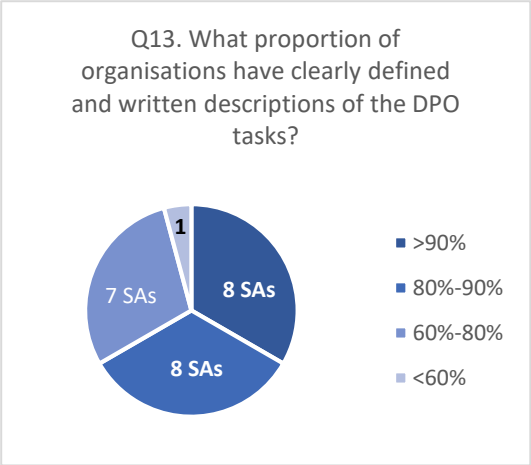
As a starting point, it is clear from the responses that most respondents do not assign all of the required responsibilities to their DPOs. It is not possible to say from the data whether this is because some of those tasks have never arisen in practice. Nevertheless, the data does raise serious questions, with some dramatic variations in the frequency with which different tasks are undertaken by or assigned to DPOs. For example, the most commonly performed or assigned task was for DPOs to inform and advise on obligations pursuant to data protection law, with a median reported rate of 96.51% (Question 16). Given that this would seem to be core to the role of the DPO, it is slightly concerning that even this task was not universal, with one Member State reporting that just 78.23% of respondents had performed or been assigned this task (Question 16). Meanwhile, the task with the lowest reported score (both in terms of median from all Member States and the lowest percentage of respondents from any particular Member State) was monitoring the performance of data protection impact assessments[19], with a median of 69.66% and a Member State low of 31.38% respondents

[18] 'Data Protection Training Programme for DPOs in Croatia', HR SA's website, available at https://azop.hr/edpb-support-pool-of-expert-project-data-protection-training-programme-for-dpos-in-croatia/;
also see EDPB Support Pool of Experts initiative, available at https://edpb.europa.eu/support-pool-experts-spe-programme_en

[19] The EDPB Report on the CEF on the Use of cloud-based services by the public sector (available at https://edpb.europa.eu/our-work-tools/our-documents/other/coordinated-enforcement-action-use-cloud-based-services-public_en) already noted on page 11 that in most cases, the controllers' DPOs were not closely involved in the process of the data protection impact assessments. This raised concerns amongst some of the participating SAs. This Report highlighted that 'Close involvement of the DPO can in fact aid public bodies to implement cloud applications in a way that is compliant with the GDPR'.

(Question 16). It is also notable that a median of 1.75% of respondents stated that they either did not know or did not wish to answer this question, with one SA reporting that 8.25% of respondents selected this response.

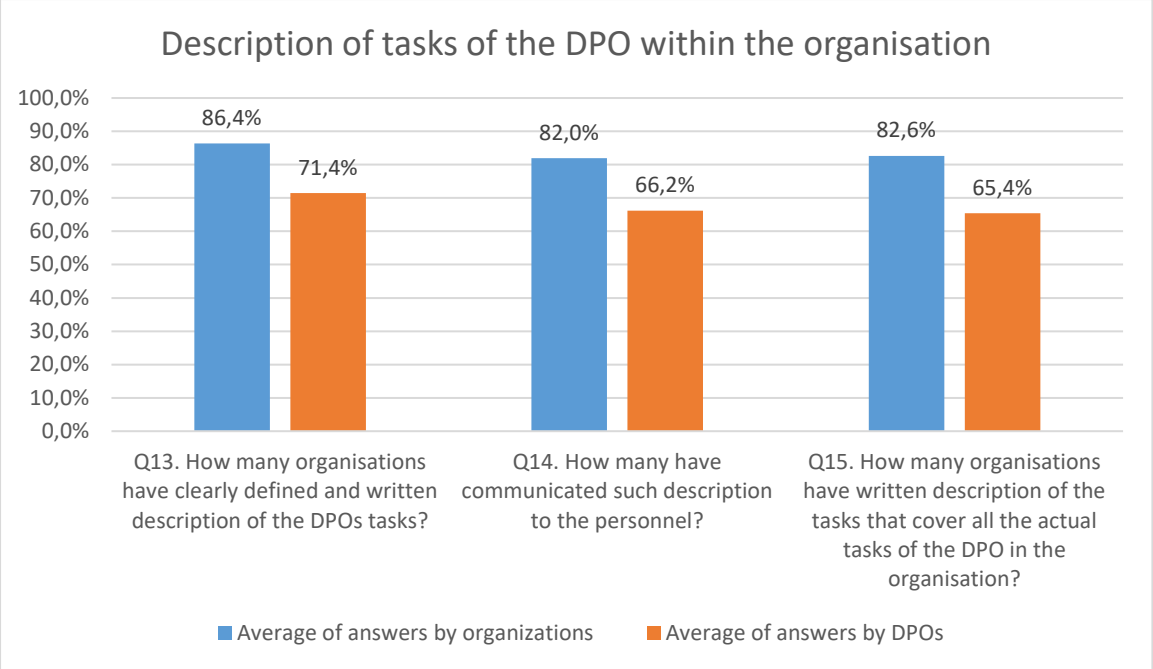
Potentially compounding this problem is that many organisations did not have a clearly defined and written description of the DPO's tasks. Moreover, while a median of 85.57% respondents had such a description (Question 13), only a median of 84.40% of those organisations responded that the written description actually covered all of the DPOs tasks (Question 15) and only a median of 78.79% organisations communicated that description to its personnel (Question 14). Some SAs have suggested that this may both cause and be caused by a lack of understanding and/or awareness as to exactly what a DPO should be doing within the organisation, and highlighted the importance that controllers and processors familiarise themselves with their obligations under the law – possibly together with DPOs themselves.

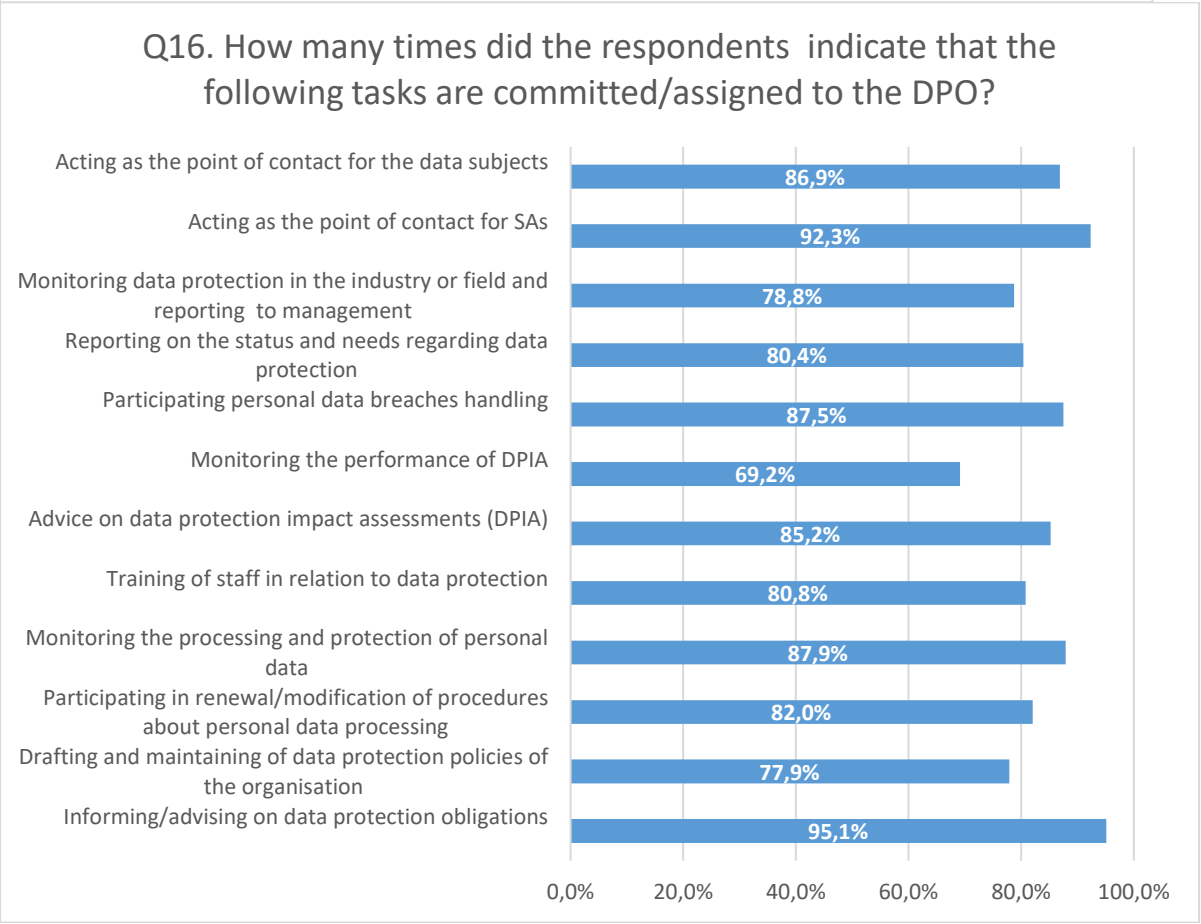


The survey also considered some extra tasks which may be assigned to DPOs in addition to those mandated by the GDPR. While the survey was not comprehensive in this regard, two SAs did note the conflicts of interest in these tasks (e.g. where DPOs are required to carry out the controller's duties), while another reiterated the concerns as to resources discussed above. When assigning tasks to DPOs, the distinction between the controller (processor) and the data protection officer should be clearly respected. Three SAs also highlighted that some organisations had improperly assigned tasks to their DPOs, burdening DPOs with the duties that the controller should perform.

In that regard, a median of 32.88% of respondents indicated that DPOs are tasked with drafting and carrying out a DPIA in addition to their other tasks (Question 17). However, in this context, it is important to recall that Article 35(2) GDPR specifically requires that the controller 'shall seek advice' of the DPO when carrying out a DPIA. Further the Guidelines on DPOs state that 'it is the task of the controller, not of the DPO, to carry out, when necessary, a [DPIA]' (Article 35(1) GDPR). In particular, the Guidelines recommend that the DPO's advice should be sought 'whether or not the [DPIA] has been correctly carried out and whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with the GDPR'[20]. While the DPO can be significantly involved in the drafting of a DPIA, they should have the sufficient independence to evaluate the DPIA and its outcomes.

[20] Guidelines on DPOs, page 17.





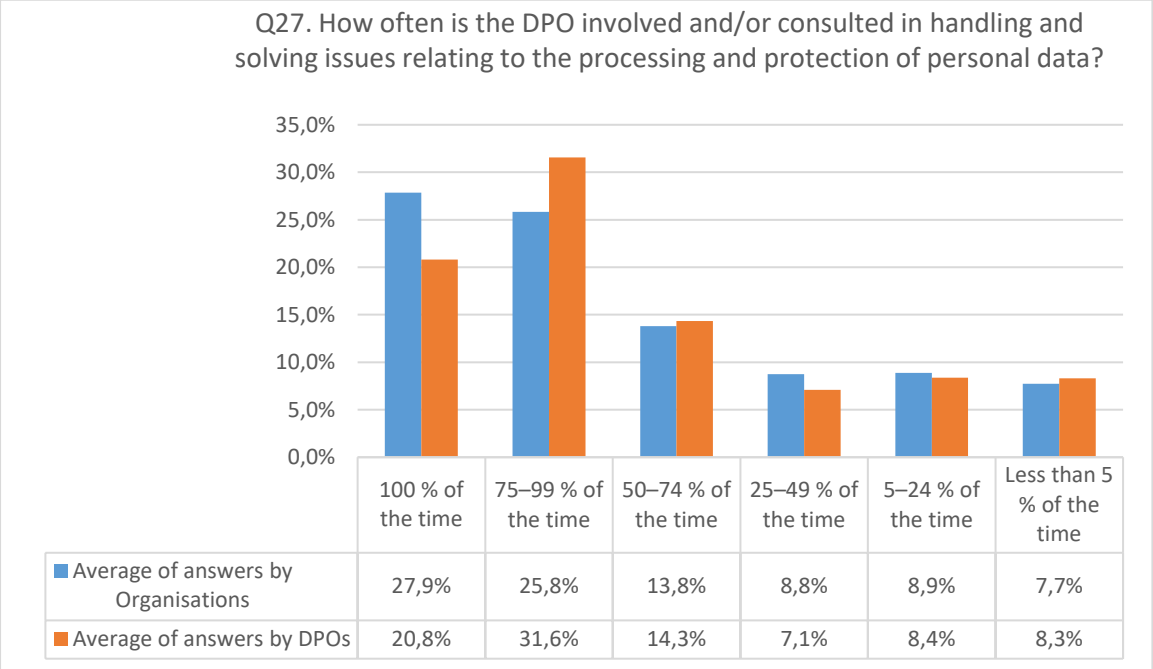
<u>Suggested recommendations to address this challenge</u>:

- More initiatives and enforcement actions by SAs could incentivise controllers and processors to maintain a proper separation between, on the one hand, the controller/processor obligations and, on the other, the DPO's own obligations and duties as set out under the GDPR.
- Controllers should make sure to promote the role of their DPO internally.

- Controllers should work together with their DPOs to build up their roles in an appropriately comprehensive and independent way.
- SAs could include DPOs and/or their opinions in a structural fashion into the SA's processes when contacting a controller and/or processor, which will help to enable and promote DPOs in their roles.

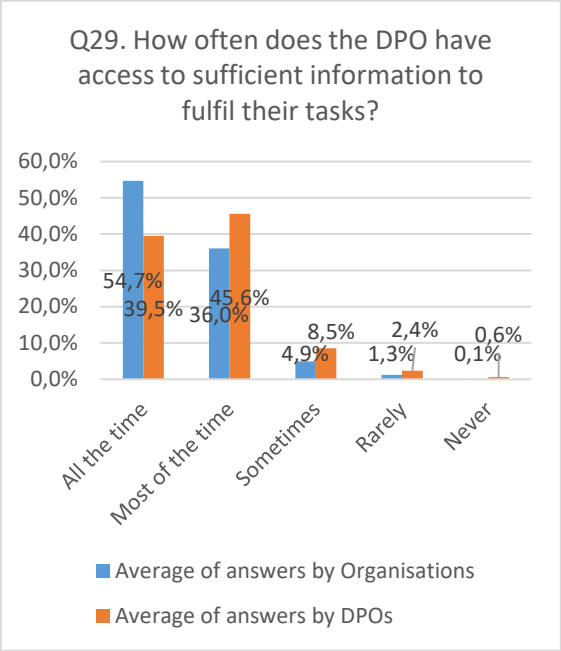
4.4.2 Lack of systematic involvement of the DPO within organisations

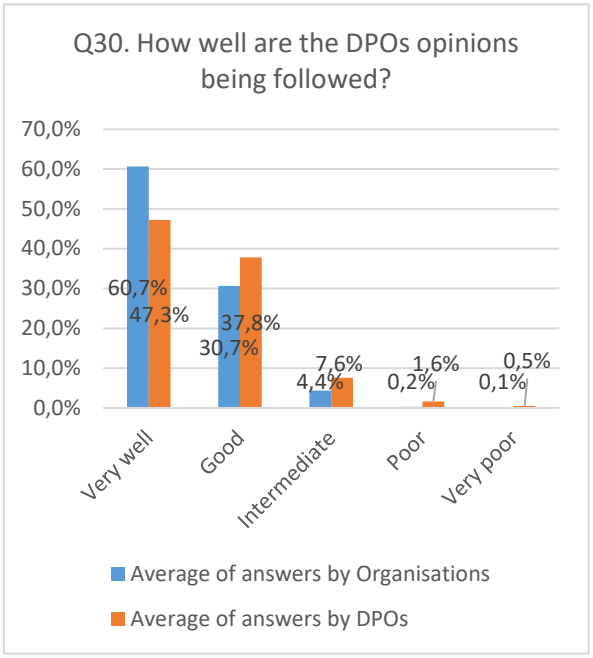
The survey also revealed that there were some serious deficiencies and inconsistencies as to the roles that DPOs played in practice. Five SAs noted concern about DPOs being insufficiently consulted on data protection issues, but similar issues could be seen in most responding Member States. When asked about how frequently the respondent's DPO was 'involved and/or consulted in handling or solving issues relating to the processing and protection of personal data in the organisation', only a median of 22.54% of respondents stated that the DPO was consulted all of the time (Question 27). Meanwhile, a median of 28.00% stated that the DPO was consulted 75% – 99% of the time, and a median of 13.95% were consulted 50% – 74% of the time (Question 27).



	100 % of the time	75–99 % of the time	50–74 % of the time	25–49 % of the time	5–24 % of the time	Less than 5 % of the time
Average of answers by Organisations	27,9%	25,8%	13,8%	8,8%	8,9%	7,7%
Average of answers by DPOs	20,8%	31,6%	14,3%	7,1%	8,4%	8,3%

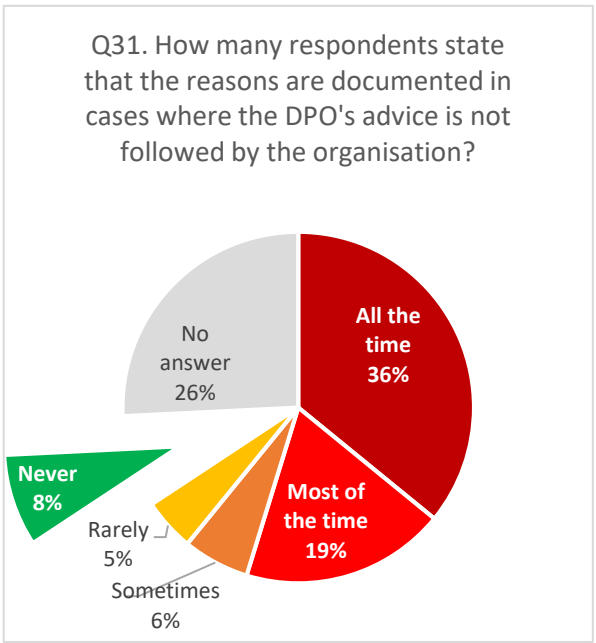
It must be noted that the survey did not define 'handling or solving issues' and, due to the survey design, we therefore cannot be sure how each respondent calculated their consultation rates. As noted in the Methodology section above, different respondents may have interpreted the questions in different ways and this will affect the conclusions which can be drawn from the responses, particularly where (as here) the responses appear to show significant differences between Member States. For example, under some interpretations of this question, a response of 100% involvement may actually be a negative if the respondent counted tasks which would result in a conflict of interests for the DPO (e.g. those noted in the previous section) as 'handling or solving issues relating to the processing of personal data in the organisation'. Nevertheless, these answers do still demonstrate a point of interest. Fundamentally speaking, Article 38(1) GDPR requires that the data protection officer 'is involved, properly and in a timely manner, in all issues which relate to the protection of personal data' and, as noted by several SAs, DPOs cannot do their job unless they are consulted on these issues. This issue was also seen elsewhere in the survey, with only a median of 41.92% of respondents stating that the DPO always had access to sufficient information on issues relating to data protection and personal data processing operations to fulfil their tasks (Question 29). While a median of 44.17% said that the DPO had such access 'most of the time' (Question 29), this lack of comprehensive access will





inevitably have a knock-on effect on all areas of the DPOs' competences, hampering their ability to support controllers, protect data subjects and fulfil their role under the GDPR.

Moreover, it is concerning that, even when Data Protection Officers were consulted, that consultation did not always bear fruit. When asked how well the organisation followed the DPO's opinions, only a median of 53.86% of respondents responded that their organisation did 'very well' on this issue (Question 30). It must be noted that, of the other respondents, a median of 36.43% of respondents described themselves as doing 'good' and a bare minority described themselves as doing 'poorly' or 'very poorly', with a median of 2.53% stating that they do not know or do not wish to answer (Question 30). Nevertheless, given the methodology of the surveys, it would be surprising if a significant number of respondents described their performance as poor or very poor. Moreover, when asked how frequently the reasons for diverging from the DPO's advice was documented, only a median of 34.59% stated that this was done 'all the time', while a median of 18.23% stated that it was done 'most of the time' and a median of 21.43% responded that they do not know or do not wish to answer (Question 31). Read together, these responses paint a clear picture of controllers failing to take full advantage of their data protection experts.



Suggested recommendations to address this challenge:

- All stakeholders should promote the role of the Data Protection Officer within organisations to ensure that the DPO is seen as necessary and effective support of the controller or processor in accordance with the GDPR/EUDPR.
- SAs can support and encourage initiatives to protect and enhance a DPO's independence regardless of the form of the contract under which they perform their function, so that DPOs feel safe to fulfil all aspects of their role.
- Controllers and processors should ensure that they are actively reviewing and (where necessary) improving the DPO's involvement within the organisation. Such review may, among other things, consider the Guidelines on DPOs, an annual report of the DPO's activities, and general good practices.

4.5 *Conflict of interests and lack of independence of the DPO*

Based on the survey results, up to 15 participating SAs reported in their qualitative analysis that certain DPOs are likely to be in a situation of conflict of interests and/or identified risks to the DPOs' independence.

4.5.1 Conflict of interests due to conflicting roles or tasks

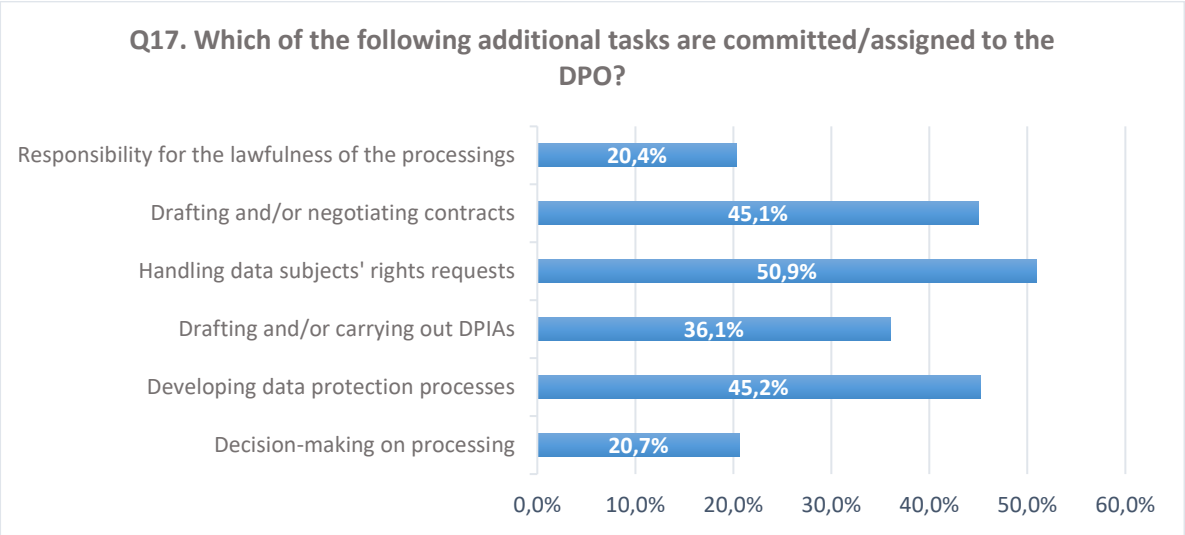
Only a median of 45.82% of contacted DPOs worked full time (Question 18). In addition, the survey revealed that a wide range of additional tasks or roles were entrusted to the DPOs, irrespective of whether these are linked to those assigned to them in their role as DPO (Questions 17 and 25). A median of 33.97% of DPOs were also shared among several organisations (Question 5). While Article 38(6) GDPR does allow DPOs to fulfil other tasks and duties, it is up to the controller or processor to ensure that they do not result in a conflict of interests[21]. Based on the survey results, many SAs have identified situations that could potentially give rise to conflicts of interests, subject to an evaluation on a case-by-case basis[22].

First, in-house DPOs sometimes hold positions or have duties related to the (highest) management level of their organisation. In seven Member States, more than 20% of the respondents answered that the DPO belonged to the highest management (Question 8). This means that these DPOs may act as directors (e.g. Chief Financial Officer or Chief Executive Officer) or heads of departments, where they are likely to take decisions on the purposes and the means of the data processing activities of their organisation. Corroborating this finding, a median of 17% of the respondents specified that the DPO takes part in the decision-making processing for personal data processing (Question 17). However, the

[21] CJEU Judgment of 9 February 2023, C-453/21, *X-Fab Dresden GmbH & Co. KG*, ECLI:EU:C:2023:79 ('**CJEU *X-Fab Dresden* Judgment**'), paragraph 40: 'the GDPR does not establish that there is a fundamental incompatibility between, on the one hand, the performance of DPO's duties and, on the other hand, the performance of other duties within the controller or processor. Article 38(6) [GDPR] specifically provides that the DPO may be entrusted with performing tasks and duties other than those for which it is responsible under Article 39 [GDPR].'

[22] CJEU *X-Fab Dresden* Judgment, paragraph 45: 'The determination of the existence of a conflict of interests [...], must be carried out, case by case, on the basis of an assessment of all the relevant circumstances, in particular the organisational structure of the controller or its processor and in the light of all the applicable rules, including any policies of the controller or its processor'. Also see Guidelines on DPOs, page 16.

CJEU has recently concluded that a 'conflict of interests' may exist when a DPO holds a role or position within an organisation that involves determining the purposes and the means of the processing of personal data[23], as DPOs have to evaluate, scrutinise and possibly criticise such processing independently under Article 39(1)(b) GDPR.



Secondly, as also noted in Section 4.4.1, the survey indicates more generally that some DPOs are in charge of contradictory tasks requiring them to act simultaneously in two roles (Question 17). This may prevent the DPOs' tasks that are required under data protection law from being properly carried out. As mentioned above, the list of tasks of the DPO is not exhaustive; however, when assigning other tasks to the DPO, the controller or processor needs to ensure that these tasks cannot cause a conflict of interests.

Thirdly, the above issues are also relevant for external DPOs, who may also be entrusted with both the regular tasks of the DPO and additional tasks which may lead to situations where the outsourced DPOs monitor their own activities. For example, as pointed out by one SA, law firms designated as external DPOs are also sometimes entrusted with tasks that can conflict with their DPO tasks. They may be asked to represent their clients in court for data protection cases despite acting as their DPO, even though this practice may lead to conflicts of interests as already pointed out by the Guidelines on DPOs[24].

A similar situation of conflict of interests may arise in another case examined in the CEF, where, according to the findings of one SA, the external DPO also acted as the DPO of the controller and the processor. Even if the controller itself is obliged to monitor the processor (see Articles 28(1) and 28(3)(h) GDPR), the simultaneous performance of monitoring tasks vis-à-vis the controller and the processor leads to a conflict of interests for the DPO, due to their different responsibilities and interests, which weakens the fulfilment the DPO's role.

The above findings are problematic given that, as recently emphasised by the CJEU, the purpose of Article 38(6) GDPR is to 'preserve the functional independence of the DPO and, consequently, to ensure the effectiveness of the provisions of the GDPR'[25].

Lastly, while it was not included in the survey as such, one SA noted the lack of procedures within organisations to ensure that conflicts of interest are avoided (as soon as the phase of designation of

[23] CJEU *X-Fab Dresden* Judgment, paragraph 44.
[24] Also see Guidelines DPOs, page 16.
[25] CJEU *X-Fab Dresden* Judgment, paragraph 42.

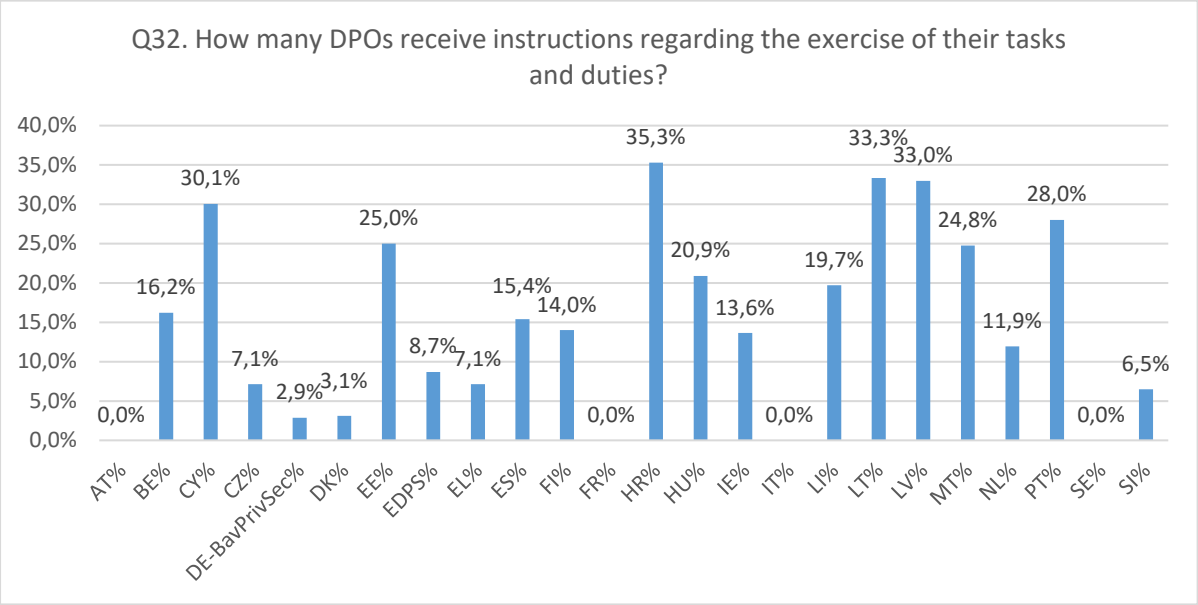
the DPOs). It should also be recalled that the Guidelines on DPOs include a number of good practices to prevent conflicts of interests.

Suggested recommendations to address this challenge:

- Supervisory authorities recall that the term 'conflict of interests' was already clarified in the Guidelines on DPOs and more recently by the Court of Justice of the EU in its *X-Fab Dresden* Judgment. Despite this, the results of the CEF action showed risks of possible conflicts of interests. Based on this, the Guidelines on DPOs should be developed further, also taking into account the new roles taken on by DPOs in certain organisations under the new pieces of EU legislation in the digital field**.**
- More initiatives and actions by supervisory authorities could verify that controllers and processors have appropriate safeguards in their procedures to ensure that the DPO is not responsible for carrying out tasks that lead to a conflict of interests.

4.5.2 Lack of independence due to instructions received by DPOs or contractual or budgetary setup

In light of Article 38(3) GDPR, it is very concerning that some of the contacted respondents reported that their DPO receives instructions on how to carry out their tasks and duties, namely with a median of 13.82% in each Member State (Question 32). While this represents a minority of DPOs, eight Member States displayed results above 20%. According to one SA, there appears to be a lack of comprehensive understanding regarding the DPO's role as an independent advisor.



Interferences to the DPO's independence may also derive from the contractual and budgetary set up. For example, controllers and processors that use an external DPO will need to be very mindful of the contractual relationship between themselves and their DPO to ensure that it does not entail, either directly or indirectly, instructions as to how to carry out the DPO's tasks; indeed, one SA encountered a data processing agreement between an organisation and its external DPO and pointed out that considering the DPO as a data processor could lead to a breach of the independence requirements under Article 38(3) GDPR.

In addition, the survey results indicated that a median of 47.04% of the DPOs who have an allocated budget actually manage it independently, raising questions about the DPO's operational

independence (Question 24). One SA pointed out that, where a DPO lacks control over its own budget, the DPO's ability to prioritise critical tasks is significantly hindered, which may lead to insufficient or delayed responses to urgent data protection issues and undermine compliance efforts. Further, according to the same SA, when the budget allocated to the DPO is managed by the organisation, the DPO's lack of financial autonomy could make the DPO hesitant to criticise the organisation's data protection practices, fearing budget cuts or resource limitations as a form of retaliation.

Although the number of DPOs reporting having suffered serious negative consequences for carrying out their tasks and duties, i.e. dismissal or penalisation, is very low (ranging from 0% to 4.35% depending on the Member State for Question 33), this is still cause for concern since the independence of the DPO cannot be guaranteed if they risk retaliation for performing their tasks. In addition, the methodology of the survey has to be borne in mind, as an overwhelming majority of respondents are organisations themselves (see Section 2 on Methodology). Furthermore, where a conflict of interests does exist, this may have lowered the reporting of negative consequences in the survey. Lastly, another SA highlighted that even though no dismissal or penalisation had been reported, no safeguards had been put in place to prevent such a decision from occurring. While this is not in itself a breach of GDPR, it is problematic that no protections against unlawful dismissal or penalisation are preventively put in place, even though some protection may be provided for by national labour-law provisions in some Member States[26].

Suggested recommendations to address this challenge:

- More awareness-raising activities, information and enforcement actions on the independence of the DPO could be envisaged (including on the prohibition on penalising and dismissing DPOs for performing their DPOs' tasks), either by SAs or internally by organisations themselves.
- Organisations and DPOs could formalise the DPO's duties and conditions for performing the DPO's duties in an 'engagement letter'.
- DPOs should be able to collect evidence in the event of interferences with their independence.

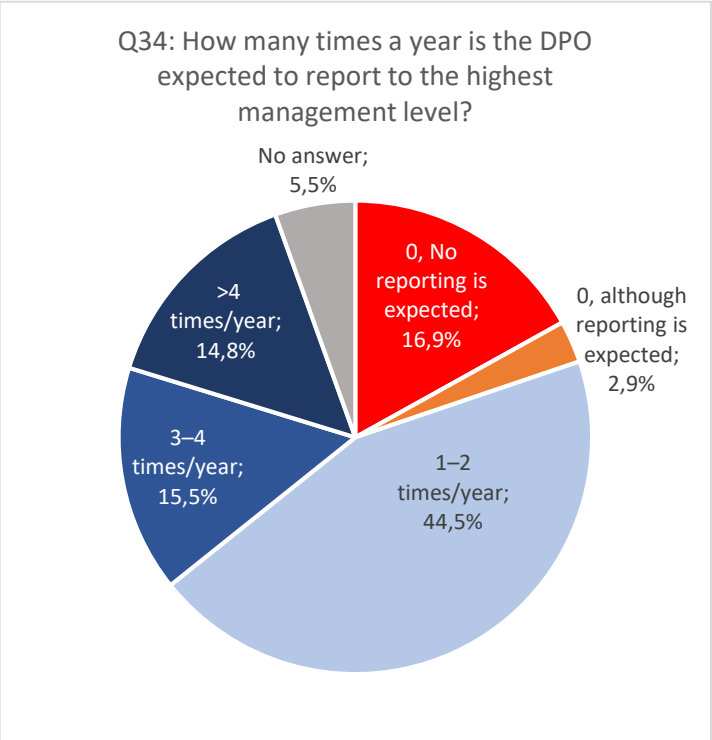
4.6 *Lack of reporting by the DPO to the organisations' highest management level*

Article 38(3) GDPR requires DPOs to report to the organisation's highest management level. Therefore it is concerning that, in some cases, DPOs are not expected to regularly do such reporting, or do not do so on a voluntary basis, or that some of the contacted organisations/DPOs have selected the response in the survey 'do not know or wish to answer the question' (Question 34). In four Member States, 30% or more of respondents have even indicated that the DPO is not expected to carry out such reporting at all. These results reveal that DPOs may not have a direct access to the highest management level. In that regard, three SAs found the DPO was expected to report to other functions in the lower levels of management. More specifically, at least one SA reported that some of the contacted organisations assigned the DPO to a subordinate role at the lower management level. Furthermore, their organisational chart only showed a 'dotted line' between the DPO and the highest management level, instead of a 'strict line', indicating an unclear relationship with the highest management level. These findings require further investigation to ascertain whether the DPO has an explicitly guaranteed and unrestricted opportunity to report to top management when needed.

It is noteworthy that the most common answer across the EEA concerning the frequency of DPO reporting was only 'one to two times per year', with a median of 45.64% (Question 34). While the GDPR and the Guidelines on DPOs do not specify how frequent the reporting should be, infrequent or

[26] CJEU Judgment of 22 June 2022, Leistritz, case C-534/20.

irregular reporting by DPOs to the highest management level raises significant concerns about effective oversight and governance. This issue is also linked to the insufficient involvement of DPOs that is set out above.



As recalled by the Guidelines on DPOs, direct reporting 'ensures that senior management (e.g. board of directors) is aware of the DPO's advice and recommendations as part of the DPO's mission to inform and advise the controller or the processor' under Article 39(1)(a) GDPR[27]. The lack of direct access therefore prevents DPOs from making their voice heard, especially in the event of a dissenting opinion. This ultimately undermines the DPO's effective role under the GDPR; if regular reporting is not done to the highest management level of an organisation, the management is unlikely to receive sufficient information on the work carried out by the DPO or on data protection issues in general, thereby affecting the organisation's overall compliance. This is also problematic given that organisations may be held responsible in case of GDPR infringements.

The GDPR and the Guidelines on DPOs do not specify the format of the report(s), including whether they should be oral or written. It appears that a 'written report submitted and/or presented to the board' is the most common reporting across the EEA, with a median of 43.02% respondents having this form of reporting (Question 35). However, a significant share of respondents, with a median of 28.04% in the different Member States, has selected the response 'other'. This suggests inconsistent practices across organisations, with reporting that may be oral, even though written reports offer greater accountability and traceability than an oral briefing.

Suggested recommendations to address this challenge:

- This legal requirement may benefit from further guidance to help controllers and processors implement it in practice. SAs could encourage the drafting and adoption of industry standards, internal data protection policies and best practices to better define the conditions, frequency, content and effectiveness of the direct reporting of the DPO to the highest management level.
- Furthermore, SAs/the EDPB could adopt a best practise-based recommendations or/and a template for DPO reporting (e.g. for at least an annual reporting), setting out modular and adaptable content to take into account the specificities of the organisations and the industry.
- Supervisory authorities could initiate more actions and initiatives with respect to the direct access of the DPO to top management, which is an important guarantee of the independence of the DPO.

4.7 *Further guidance from SAs*

The survey results highlight a common wish on the part of the contacted organisations and DPOs to receive further guidance from SAs. One SA even mentioned having received an 'almost unanimous

[27] EDPB Guidelines on DPOs, page 15.

request from DPOs' in that regard. Overall, a median of more than 60% of the respondents in the different Member States indicated that they would like to be provided with (1) Q&As or FAQs, (2) additional guidelines, and (3) training materials or documents, both for DPOs and to be distributed within organisations (Question 41). The survey also showed a clear interest for more online tools, with a median of 50.95% of the respondents in each Member State eager to engage with such tools. To confirm this conclusion, a median of 4.81% of the respondents considered that no further guidance from their SA was necessary.

Additional guidance could help to empower DPOs and address some of the challenges identified above. It could also enable DPOs to carry out their tasks more efficiently, for example by providing them with user-friendly templates and materials for internal training of staff members (to be adjusted depending on the processing activities carried out organisations), which can save time and thus alleviate DPOs' insufficient resources[28]. Further guidance, for example in the form of online courses, workshops or certifications, could also address the insufficient expertise or training of some DPOs. Specific materials could support DPOs in maintaining and updating their expert knowledge. For example, some respondents expressed the desire to receive newsletters or updates on the decisions adopted in the field of data protection across the EEA. As pointed out by one SA and some respondents, guidance dealing with specific issues is also needed as DPOs are required to be experts in many different aspects of data protection, both legal- and IT-related, and give guidance on (sometimes) extremely complex issues. In addition, educating internal stakeholders, such as staff members and the highest management, could raise awareness as to what the DPOs' role and tasks actually are under data protection law. This would ultimately give more visibility to the DPOs at all levels of organisations and ensure the DPOs' greater involvement.

Some guidance is already available both at national and EEA levels. Section 5 maps out the existing guidance and actions carried out by SAs in relation to DPOs and shows in particular the very diverse forms of support provided by SAs to DPOs across the EEA. The nature, volume and format of the available guidance vary significantly across the EU, with a few SAs having extensive guidance in place for DPOs and/or organisations, while others primarily rely on the Guidelines on DPOs. In that regard, it is noteworthy that the respondents' call for further guidance appears also in Member States with comprehensive guidance.

As mentioned above, the Guidelines on DPOs should be developed further based on the survey results analysed in Section 4, also taking into account the new roles that might be taken on by DPOs in certain organisations under the new pieces of EU legislation in the digital field.

However, adopting further guidance will require that both national SAs and the EDPB are provided with appropriate resources to be able to analyse stakeholders' need and address it. This includes having the necessary financial and human resources, especially for smaller SAs. It is noteworthy that, as part of EDPB Support Pool of Experts initiative, an extensive DPO training programme was launched in Croatia, specifically tailored for the health and educational sectors to address the existing shortage of experienced data protection practitioners. More specifically, an external expert designed training materials and Q&A for DPOs.

4.8 *Conclusion on the levels of awareness and compliance*

There are many links between the challenges and concerns identified above. In other words, their cause(s) and consequence(s) are often intertwined. For example, where an organisation allocates insufficient resources to the DPO, this may lead to the DPO being assigned tasks that fall outside of

[28] A few SAs adjusted the questionnaire to be sent at national level and included free-text fields to open additional input from stakeholders.

the DPO's core missions under the GDPR, which in turn may lead to a conflict of interests. Another example could be that, where a DPO does not directly report to the highest level of management, this could reinforce the lack of awareness regarding the DPO's core missions within the organisation and the management could decide to allocate fewer resources than necessary to the DPO as it would not be aware of the data protection issues identified by the DPO, leading, among other things, to a reduced budget for DPO training.

These challenges hamper the key role assigned to the DPO by the GDPR as they impede DPOs from properly fulfilling their mission and all their tasks. This is particularly problematic as the DPO may not be able to foster a real data protection compliance culture within organisations nor protect data subjects' rights due to these challenges. As a result, they may not only give rise to infringements of the GDPR provisions on DPOs, but also – more generally – to the controllers' and processors' obligations under the GDPR.

Based on the survey results, participating SAs assessed the levels of awareness and compliance of the contacted organisations with the data protection law requirements on DPOs in their individual reports (**Appendix 1.2**, under Question 1 in Part IV). On the one hand, the overall levels of awareness and compliance were deemed low or insufficient by four SAs due to visible shortcomings, with only few results deemed completely unproblematic (CZ, EL, FI, HR SAs). On the other hand, despite the shortcomings identified, ten SAs were under the general impression that the survey results were overall positive or satisfactory (AT, CY, DK, ES, EDPS, IE, IT, LI, LT, MT SAs). NL SA also had the impression that the level of awareness amongst respondents was far above average.

Participating SAs observed disparities in the level of compliance with DPO requirements at national level, regardless of whether the questionnaire was completed by a homogenous (CZ SA) or heterogeneous pool of respondents (BE, FI, SE SAs). Nevertheless, the SAs' assessment also varied to some extent depending on the addressed stakeholders and the results obtained at national level. For example, according to the EDPS, the levels of awareness and compliance were high among the EU Institutions. The DK SA shared the same evaluation for the contacted municipalities. The eleven banks contacted by AT SA also took the role of the DPO very seriously. According to NL SA, the results obtained were explained by the fact that only registered DPOs (as opposed to organisations) were invited to complete the questionnaire. Adopting a nuanced approach, the PT SA concluded that there was a reasonable level of awareness but a significant deficit in the level of compliance.

Given the disparities observed across the EEA, enhanced cooperation between SAs could further improve the levels of compliance and awareness in some Member States. For example, the SAs' national reports set out in Appendix 1.2 include useful best practices that were observed by some SAs in their Member State, and which could be promoted in other Member States.

Without prejudice to the challenges above and the concerns expressed by SAs regarding compliance with certain DPO requirements, participating SAs emphasised, among other things, the following positive trends:

- In some cases, despite being a relatively new profession, the level of experience and expertise of DPOs was high (LV, MT SAs), which clearly indicates that the DPO function is becoming more and more professionalised (EDPS).
- Most of the respondents indicated that DPOs are involved or consulted in handling and solving problems related to the processing and protection of personal data in the organisation (IE SA). According to respondents, most DPOs seem to have a real impact in their organisations as the survey shows that their advice is generally followed (EDPS, IE, LV, MT SAs).
- Data subjects have the opportunity to contact the DPO in matters related to the processing of their personal data or the exercise of data subject rights.

Four SAs stressed that there was still plenty of room for improvement (EL, DK, EE, LV SAs). Further, some SAs noted a lack of full understanding of the DPO's role and a shortcoming of awareness (DE SA Bavaria, LV, PL and SI SAs). In this regard, SAs emphasised the need to strengthen the role and recognition of the DPO and to continue making organisations aware of both the importance of the DPO's role in ensuring compliance with data protection requirements and of the necessity to provide the necessary resources, in terms of training and budget, in the fulfilment of their tasks (BE, ES, IT, LV SAs).

5 ACTIONS TAKEN BY SAS

This section maps out the actions carried out by SAs at national level in relation to DPOs and summarises them depending on their nature (e.g. whether they relate to enforcement or soft-law guidance). However, this section does not aim to present a comprehensive overview of all actions conducted by SAs, nor does it list ongoing actions that are not finalised and on which SAs have not yet publicly communicated. Each individual report of the participating SA detailing their respective actions is available in **Appendix 2.2** attached to this report.

5.1 *Enforcement actions*

SAs have a number of powers at their disposal in accordance with Article 58 GDPR, including corrective powers such as issuing reprimands or orders to comply or even fines, for cases of non-compliance with the legal requirements for DPOs. In accordance with Article 83 (4) GDPR, if a controller or processor does not fulfil its obligations in line with Articles 37 to 39 GDPR, it can be subject to administrative fines up to 10,000,000 EUR or, in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher. However, in that regard, it should be noted that SAs in some Member States could not issue fines towards public authorities.

Of the participating SAs, ten have already taken action at national level to enforce DPOs' requirements under the GDPR prior to this CEF. For instance, BE SA has adopted eight decisions that notably relate to the role of the DPO from April 2020 to August 2023, on such topics as the DPO independence[29], conflict of interests with the DPO's assigned tasks[30], the level of organisations' support towards their DPOs[31], the failure to report to the highest management level[32], the failure to appoint a DPO[33] and the lack of DPO's involvement[34]. As of the date of entry into force of the GDPR, PL SA has been starting investigations to ensure compliance with DPO requirements. For instance, PL SA has taken corrective

[29] BE SA, Decision n°15/2020, 15 April 2020, available at https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-15-2020.pdf.
[30] BE SA, Decision n°18/2020, 28 April 2020, available at https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-18-2020.pdf;
Decision n°81/2023, 22 June 2023, available at https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-81-2023.pdf.
[31] BE SA, Decision n°41/2020, 29 July 2020, available at https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-41-2020.pdf.
[32] BE SA, Decision n°24/2021, 19 February 2021, available at https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-24-2021.pdf;
Decision n°110/2023 of 9 August 2023, available at https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-110-2023.pdf.
[33] BE SA, Decision n°21/2022, 2 February 2022, available at https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-21-2022-english.pdf.
[34] BE SA, Decision n°162/2022, 16 November 2022, available at https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-162-2022.pdf.

actions in relation to several breaches regarding the performance of DPO duties, including by issuing an order to appoint a DPO in a housing cooperative. PL SA also imposed an administrative fine in connection with the performance of the DPO's tasks without taking due account of the risks associated with processing operations and not involving the DPO in the processing operations carried out. Moreover, in March 2022, PL SA developed a list of 27 questions on the status and functioning of the DPO and on the basis of its powers under Article 58(1)(a) and (e) GDPR addressed it to selected controllers from both the public and private sectors[35]. Further, PT SA has opened several infringement procedures against local governments and other public bodies in relation to the lack of designation of DPO, issuing fines in this regard. CZ SA has also conducted audits of national ministries and concluded that a violation of Article 38(1) and 38(2) GDPR by the Ministry of Foreign Affairs had occurred. Similarly, IT SA has taken action against controllers in the public sector, with 11 decisions adopted between 2021 and 2022 related to topics such as the failure to appoint a DPO or to properly publish or communicate the DPO contact details to the SA, and the conflict of interests with the other tasks assigned to the DPO[36]. FR SA has also taken measures towards organisations, for example, by ordering 22 municipalities to appoint a DPO in May 2022. After assessing the compliance of public bodies in 2020, IE SA has identified 77 entities as potentially not compliant. IE SA also issued a decision against a body in respect of infringements of Articles 37(1) and 37(7) GDPR[37]. The NL SA included the position of the DPO in several administrative fines on the processing of data. However, the position of the DPO was mostly an aggravating circumstance or a secondary or unexpected finding of an investigation and no standalone decision has been taken yet[38]. The NL SA also has meetings on a regular basis with the highest level of management of controllers to convey the standards regarding the position of their DPO.

A number of actions taken prior to this CEF did not result in the issuing of fines or other sanctions. For example, after carrying out two waves of privacy sweeps in 2022, SI SA discovered that roughly 520 public bodies failed to inform the SA about their DPOs. The respective organisations, however, properly informed the SA of the same and no further sanctions were taken. Likewise, DK SA has opened own-volition inquiries into certain municipalities regarding their DPO's resources and tasks in

[35] PL SA, Verification of compliance with the provisions on data protection officer, available at https://archiwum.uodo.gov.pl/en/553/1325.

[36] Decision of 11 February 2021, n. 54, doc. web n. 9556625 available at https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9556625; Decision of 13 May 2021, n. 193, doc. web n. 9687954 available at https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9687954; Decision of 16 September 2021, n. 318, doc. web n. 9718134 available at https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9718134; Decision of 7 April 2022, n. 119, doc. web n. 9773950 available at https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9773950; Decision of 28 April 2022, n. 163, doc. web n. 9777996 available at https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9777996; Decision of 12 May 2022, n. 174, doc. web n. 9781242 available at https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9781242; Decision of 9 June 2022, n. 214, doc. web n. 9794895 available at https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9794895; Decision of 10 November 2022, n. 365, doc. web n. 9834477 available at https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9834477; Decision of 10 November 2022, n. 367, doc. web n. 9835095 available at https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9835095; Decision of 10 November 2022, n. 372, doc. web n. 9843603 available at https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9843603; Decision of 15 December 2022, n. 423, doc. web n. 9852800 available at https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9852800.

[37] IE SA, Decision IN-22-2-1, 3 May 2022, available at https://www.dataprotection.ie/sites/default/files/uploads/2022-05/IN-22-2-1%20PHECC%20Decision%20Final.pdf.

[38] The fining of the Dutch tax authorities is a prime example https://www.autoriteitpersoonsgegevens.nl/uploads/imported/besluit_boete_belastingdienst_fsv.pdf

2019, but no need for corrective measures was identified. EE SA also terminated an investigation regarding the independence of a DPO by issuing a warning.

As part of this CEF action, ten SAs have initiated – or are planning to initiate – new formal investigations, or have been continuing ongoing investigations (AT, DE SA Bavaria for the private sector, DK, EL, FR, HR, HU, PL, LT, SE SAs). This includes asking contacted organisations to substantiate their answers to the questionnaire. HR SA has also initiated 417 enforcement actions. In addition, EL SA is conducting a formal investigation with respect to 31 public bodies and has already initiated proceedings in relation to the EL SA's corrective powers, including for bodies which did not cooperate with it or which did not designate a DPO. SE SA has launched formal investigations that are still ongoing for the pool of the 48 contacted stakeholders. Further, HU SA has launched 29 new own-volition inquiries regarding the public bodies' obligation to designate a DPO, the obligation to publish the DPO's contact details and notify them to the SA.

Even though investigations are still ongoing, it is likely that – at least in some cases, where violations are identified – corrective measures will be adopted, such as orders to comply or fines. However, no further information can be shared regarding the outcome of these cases.

5.2 *Guidelines*

Several SAs refer to the Guidelines on DPOs on their respective websites, while some publish general FAQ sections and online guidance on DPOs.

Additionally, certain SAs have developed their own general and specialised guidelines on the matter. For instance, IE SA has published guidance on appropriate qualifications for a DPO[39], on who needs a DPO[40], on how to notify the IE SA of a DPO[41] and an FAQ document on the DPO registration process[42]. It is noteworthy that BE SA has published an extensive toolkit for DPOs in 2020 that includes the following documents: 10 ground rules regarding the DPO[43], a checklist for the DPO[44] and a template to request the DPO's opinion[45]. Moreover, BE SA published a recommendation on the appointment of

[39] IE SA, Guidance on Appropriate Qualifications for a Data Protection Officer, July 2019,available at https://www.dataprotection.ie/sites/default/files/uploads/2019-07/190708%20Guidance%20on%20Appropriate%20Qualifications%20for%20a%20Data%20Protection%20Officer%20%28GDPR%29.pdf.
[40] IE SA, Who Needs a DPO, available at https://www.dataprotection.ie/en/dpos/who-needs-dpo.
[41] IE SA, Notify the Data Protection Commission of your DPO, available at https://www.dataprotection.ie/en/organisations/know-your-obligations/data-protection-officers.
[42] IE SA, Data Protection Officer Register - Frequently Asked Questions, available at https://www.dataprotection.ie/sites/default/files/uploads/2022-06/Data%20Protection%20Register%20FAQs%20Updated%20010622_0.pdf.
[43] BE SA, Les 10 règles de base concernant le délégué à la protection des données (DPO), available at https://www.autoriteprotectiondonnees.be/publications/les-10-regles-de-base-concernant-le-delegue-a-la-protection-des-donnees-dpo.pdf.
[44] BE SA, Check-list avis DPO, available at https://www.autoriteprotectiondonnees.be/publications/check-list-avis-dpo-general.pdf.
[45] BE SA, Demande d'avis ou demande d'informations pour le Délégué à la protection des données (DPO), available at https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.autoriteprotectiondonnees.be%2Fpublications%2Fdemande-d-avis-ou-demande-d-informations-pour-le-delegue-a-la-protection-des-donnees-dpo.docx&wdOrigin=BROWSELINK.

a DPO back in 2017[46]. DK SA also published guidelines on DPOs[47] and FR SA has a comprehensive reference guide for DPO-related questions[48]. In its own document, CY SA elaborates on the obligations and tasks of DPOs[49]. Along similar lines, SI SA has issued guidelines on recommendations and best practices regarding DPOs in 2018[50]. PL SA also provided guidelines on the designation and status of DPO (including detailed guidance on the possibility of combining the functions of DPOs with various other positions)[51], notifying the SA of the designation of a DPO (including the manner and deadline for notifying)[52] and the tasks of DPOs (in particular what tasks are assigned to the DPO and which tasks the controller is required to carry out)[53]. Likewise, EE SA provides various guidelines on their website, such as 'Who must appoint a DPO'[54]. LT SA also published a public consultation on the obligation to appoint a data protection officer[55]. The NL SA published a position paper on the designation, tasks and/or role of the DPO, which is available on the SA's website[56]. Finally, HR SA published a short brochure[57] about the role and tasks of DPOs.

[46] BE SA, Recommandation n° 04/2017, 24 May 2017,
available at https://www.autoriteprotectiondonnees.be/publications/recommandation-n-04-2017.pdf.
[47] DK SA, Vejledning om databeskyttelses-rådgivere, December 2017,
available at https://www.datatilsynet.dk/Media/B/E/Databeskyttelsesr%c3%a5dgivere.pdf.
[48] FR SA, Practical Guide GDPR: Data Protection Officers, 2021,
available at https://www.cnil.fr/sites/cnil/files/atoms/files/cnil-gdpr_practical_guide_data-protection-officers.pdf.
[49] CY SA, Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων, 5 April 2017,
available at https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/EB81BC1F868BF60DC225820A003EF39D/$file/%CE%9A%CE%B1%CE%B8%CE%BF%CE%B4%CE%B7%CE%B3%CE%B7%CF%84%CE%B9%CE%BA%CE%AD%CF%82%20%CE%B3%CF%81%CE%B1%CE%BC%CE%BC%CE%AD%CF%82%20%CE%B3%CE%B9%CE%B1%20DPO%20el.pdf.
[50] SI SA, Priporočila Informacijskega pooblaščenca glede delovanja pooblaščene osebe za varstvo osebnih podatkov, 9 November 2018, available at https://www.ip-rs.si/fileadmin/user_upload/Pdf/novice/Priporocila_IP_glede_delovanja_DPO_koncno.pdf.
[51] PL SA, Designation and status of DPO, available at https://uodo.gov.pl/pl/495.
[52] PL SA, Notifications of the President of UODO related to DPO,
available at https://archiwum.uodo.gov.pl/pl/p/zawiadomienia-prezesa-uodo-zwiazane-z-iod.
[53] PL SA, DPO Tasks, available at https://archiwum.uodo.gov.pl/pl/p/zadania-iod.
[54] EE SA, Kes peavad määrama andmekaitsespetsialisti, 14 May 2020,
available at https://www.aki.ee/et/eraelu-kaitse/andmekaitsespetsialist/kes-peavad-maarama-andmekaitsespetsialisti.
[55] LT SA, Viešoji Konsultacija dėl Pareigos Paskirti Duomenų Apsaugos Pareigūną, 2017,
available at https://vdai.lrv.lt/uploads/vdai/documents/files/Viesoji%20-%20dap_2017.pdf.
[56] Document is available via
https://www.autoriteitpersoonsgegevens.nl/uploads/imported/positionering_van_de_fg.pdf
[57] HR SA https://azop.hr/wp-content/uploads/2021/01/brosura-Zasto-je-vazno-imenovati-sluzbenika-za-zastitu-OP_2021_e_mail-version.pdf

Some SAs have issued specific guidelines for DPOs operating in the public sector, such as IT[58] and HR[59] SAs, or like the PT SA focusing on conflicts of interests[60]. The EDPS also published a position paper on the role of DPOs of the EU institutions[61]. Further, private sector-related guidance was provided by IT SA[62] and LT SA, which issued a consultation on DPO's assignment criteria[63].

5.3 *Conferences and trainings*

Four of the participating SAs noted that they offered informal individual advice on questions related to DPOs. One SA offers tailor-made training to newly appointed DPOs. Moreover, multiple SAs provide more extensive training opportunities for DPOs, organising educational and networking events on the matter. Indeed, LI SA organises an annual meeting/training for all DPOs, during which they are provided with information about the SA's work, recent legal developments and other updates. HU SA held a DPO Conference in 2019 based on the Guidelines on DPOs, with a video presentation on the tasks related to the appointment of the DPO.[64] A national conference, 'The DPO in focus', was also held recently by IT SA, with its results currently under evaluation[65]. Similarly, NL SA held the second national DPO conference in 2023 called 'Day of the DPO'. Only registered DPOs could choose from a wide variety of workshops and presentations held by NL SA and external experts. HR SA[66] in 2023 organised an international conference 'DPO-the job of the future', as a part of ongoing awareness-raising campaign, encompassing monthly trainings for DPOs. CZ SA started to organise a series of specialised educational events in 2018, seven of which were meant specifically for DPOs employed by public authorities and bodies. CY SA also noted various seminars and presentations being held for both the private and public sectors regarding the role of the DPOs, and the public sector held at the Ministry

[58] IT SA, Faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico (in aggiunta a quelle adottate dal Gruppo Art. 29), 15 December 2017,available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7322110 ; Provvedimento del 29 aprile 2021 - Documento di indirizzo su designazione, posizione e compiti del Responsabile della protezione dei dati (RPD) in ambito pubblico, 29 April 2021, available at https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9589104.

[59] HR SA, Priručnik za službenike za zaštitu podataka (SZP-ove): Smjernice za službenike za zaštitu podataka u javnom i gotovo isključivo-javnom sektoru o tome kako osigurati usklađenost s Općom uredbom o zaštiti podataka Europske unijeo zaštiti podataka Europske unije, July 2019, available at: https://azop.hr/wp-content/uploads/2023/09/DPO-prirucnik.pdf

[60] PT SA, Incompatibilidade da acumulação de funções EPD/RAI, 11 April 2023, available at https://www.cnpd.pt/media/xi5lsevz/2023-04-11_incompatibilidade-acumula%C3%A7%C3%A3o-fun%C3%A7%C3%B5es-epd-rai.pdf; Relativa à avaliação do desempenho de trabalhador que seja EPD, 18 April 2023, available at https://www.cnpd.pt/media/vy3h045x/projeto-de-orienta%C3%A7%C3%A3o_avalia%C3%A7%C3%A3o-epd.pdf.

[61] EDPS, Position paper on the role of Data Protection Officers of the EU institutions and bodies, 30 September 2018, available at https://edps.europa.eu/sites/edp/files/publication/18-09-30_dpo_position_paper_en.pdf.

[62] IT SA, Faq sul Responsabile della Protezione dei Dati (RPD) in ambito privato, 26 March 2018, available at https://www.garanteprivacy.it/faq-sul-responsabile-della-protezione-dei-dati-rpd-in-ambito-privato.

[63] LT SA, Rekomendacija dėl Duomenų Apsaugos Pareigūnų Skyrimo Viešajame Sektoriuje Ir Jų Veiklos Reglamentavimo Ypatumų, 11 June 2019, available at https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomendacija-del-DAP-viesajame-sektroiuje-2019-06-13.pdf.

[64] HU SA, Adatvédelmi tisztviselők 2019. évi konferenciája, available at https://naih.hu/dpo-konferencia-2019.html#vid3.

[65] IT SA, Privacy: i Responsabili della Protezione Dati al centro del cambiamento. Giornata di confronto organizzata dal Garante Privacy a Bologna, 23 June 2023, available at https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9901692.

[66] HR SA, https://azop.hr/data-protection-day-2023-gdpr-conference-dpo-the-job-of-the-future/

of Finance. FR SA regularly holds various workshops and webinars addressed to DPOs[67] and they can also benefit from free online training sessions.[68] From 2016 to 2019, PL SA conducted a cycle of free training for DPOs in selected sectors, focusing on new EU data protection rules and national rules applicable to data processing in a specific field of activity. The EDPS holds two meetings a year with the DPOs of all EUIs, which aim notably to approach challenges faced by DPOs through presentations and interactive workshops. At the latest meeting (November 2023), EDPS dedicated one workshop to the position of DPOs.

Notably, BE SA put forward an EU-funded project setting up an online platform to support DPOs, called 'DPO-Connect'[69]. Likewise, SI SA's works on awareness trainings and a platform for DPO networking aimed at sharing knowledge and best practices among DPOs. IT SA also held regular meetings with various stakeholders aimed at fostering networking among respective controllers. Since 2018, FR SA also offers approved organisations that issue a DPO skills certification[70], which presents certain advantages for DPO certification holders.

Lastly, as part of the EDPB Support Pool of Experts initiative, an extensive DPO training programme was launched in 2023 in Croatia, specifically tailored for the health and educational sectors in this country to address the existing shortage of experienced data protection practitioners[71].

5.4 *Study and research*

Prior to the CEF, five SAs have already conducted their own studies and questionnaires regarding DPOs. For example, FR SA held three editions of online research on the DPO functions between 2019 and 2022. The latest edition, in particular, was based on a survey of 1,811 DPOs, revealing the diversification of profiles of DPOs and a decrease in GDPR training[72]. HU SA also launched similar surveys in the past years in connection to its annual DPOs conferences. In 2019, SI SA published a report based on a survey among DPOs in public sector, covering similar issues and identifying substantial problems regarding the support provided to DPOs by the management[73]. Likewise, CY SA launched questionnaires in 2019 and 2020, aimed at first the private sector (e.g. supermarkets, insurance companies and private hospitals), and public sectors (e.g. departments, services, local government organisations). The aim of these questionnaires was, among other things, to investigate the designation and tasks of the DPOs. Between 2020 and 2021, HR SA[74] conducted research involving 732 Data Protection Officers (DPOs) across both public and private sectors. Over half of the surveyed

[67] FR SA, Agenda, available at https://www.cnil.fr/fr/actualites/agenda.
[68] FR SA, Le MOOC de la CNIL est de retour dans une nouvelle version enrichie, 27 June 2022, available at https://www.cnil.fr/fr/comprendre-le-rgpd/le-mooc-de-la-cnil-est-de-retour-dans-une-nouvelle-version-enrichie.
[69] BE SA, 'DPO-Connect' platform, available at https://www.dpopro.be/all-about-dpo-pro/dpo-connect/. This paltform was successfully completed in 2022.
[70] FR SA, Certification des compétences du DPO, available at https://www.cnil.fr/fr/certification-des-competences-du-dpo-0.
[71] Data Protection Training Programme for DPOs in Croatia', HR SA's website, available at https://azop.hr/edpb-support-pool-of-expert-project-data-protection-training-programme-for-dpos-in-croatia/; also see EDPB Support Pool of Experts initiative, available at https://edpb.europa.eu/support-pool-experts-spe-programme_en.
[72] FR SA, Délégué à la Protection des Données, 2022, available at https://travail-emploi.gouv.fr/IMG/pdf/synthese_dpo.pdf.
[73] SI SA, Anketa med DPO v javnem sektorju, 28 January 2020, available at https://www.ip-rs.si/fileadmin/user_upload/Pdf/Porocila_IP/Dan%20varstva%20OP%202020%20-%20rezultati%20DPO%20ankete.pdf.
[74] HR SA, https://hrcak.srce.hr/file/383527

DPOs (54%) reported lacking prior experience in data protection before assuming their roles, while a significant majority (82%) expressed a need for additional education in this field. The majority of DPOs revealed minimal to no prior expertise in data protection and expressed a desire for further education to enhance their understanding of fundamental concepts related to personal data protection.

5.5 *Other forms of support*

A few SAs have also employed other relevant initiatives, such as the newsletter issued cyclically by the PL SA since 2019[75] and the electronic newsletter aimed at DPOs issued by FI SA six times a year[76], by NL SA four times a year and by EDPS ten times a year. The EDPS[77], ES SA[78], FI SA[79], FR SA[80], NL SA and PL SA[81] also provide a helpline or channel addressed to DPOs to assist them.

6 CONCLUSION

Despite the shortcomings and concerns identified above, the survey results are encouraging. Nevertheless, they emphasise the need to strengthen the role and recognition of DPOs – and the need to continue promoting the importance of the DPO's role. In order for DPOs to best ensure compliance with data protection requirements, controllers and processors must provide the necessary resources, in terms of training and budget, to allow them to properly fulfil of their tasks. SAs have acknowledged the added value of the coordinated work under the CEF, reporting that it has also served to make controllers, processors and even DPOs aware of the importance and scope of the DPO requirements under GDPR. Many participating SAs are considering adopting further guidance regarding DPOs following this CEF.

The present report is the state of play, at the end of 2023, of the CEF action regarding the designation and position of DPOs. It may need to be updated in the course of 2024 to take into account the progress of the procedures which have not yet been completed to date and given the issues identified, if the Guidelines on Data Protection Officers are further developed by the EDPB.

At a time when a number of EU legislations in the digital field are being developed or have recently entered into force, the role of the DPOs seems to be changing. In practice, and to name just a few, it seems that DPOs of some organisations are internally picking up key roles under these legislations, such as the AI Act, the Digital Services Act, the Digital Market Act or the Data Act, and, more and more, are being tasked with new roles that are related to AI, ethics, data governance and data spaces. These new roles may reinforce some of the concerns identified above, such as the risk of conflicts of interests or the insufficient resources at the disposal of the DPOs. It is therefore vital that all stakeholders seriously consider how DPOs are being tasked, utilised and supported, to ensure that they can provide the best added value for everybody involved.

[75] Available at: https://archiwum.uodo.gov.pl/p/archiwum-newslettera-dla-iod and at: https://uodo.gov.pl/pl/p/archiwum-biuletynu-dla-iod.
[76] FI SA, Tietosuojavaltuutetun toimiston sähköinen uutiskirje, available at https://tietosuoja.fi/uutiskirje.
[77] https://edps.europa.eu/data-protection/our-role-supervisor_en.
[78] https://www.aepd.es/guias-y-herramientas/herramientas/canalDPD.
[79] FI SA, Puhelinneuvonta, available at https://tietosuoja.fi/puhelinneuvonta.
[80] https://www.cnil.fr/fr/saisir-la-cnil/contacter-la-cnil-standard-et-permanences-telephoniques.
[81] PL SA, Ruszyła Infolinia UODO dla IOD, available at https://archiwum.uodo.gov.pl/pl/138/720.

APPENDIX 1: NATIONAL REPORTS BY SUPERSIVORY AUTHORITIES

Appendix 1.1: Consolidated survey results of participating supervisory authorities.

Appendix 1.2: National reports of participating supervisory authorities regarding the substantive issues identified and actions taken at national level.