Appendix 1.2: National Reports on the CEF DPO

Table of Contents

AT SA

Austrian Supervisory Authority – Österreichische Datenschutzbehörde

Part I - Statistics

Please see the consolidated figures in Appendix 1.1. The answers below may refer to the questions included in Appendix 1.1.

General information: It should be taken into account that all answers were given by the data controllers, but not by the data protection officers.

Part II – Substantive issues

Please select five main issues (you may choose to list between 5 and 10 issues at most) you have identified in your investigations. These issues may be related, for instance, to one of the categories and sub-categories below:

- **the designation, knowledge and experience of the DPO,**
- **the tasks and resources of the DPO,**
- **the role and position of the DPO,**
- **guidance of the Supervisory Authority.**

For each of the 5 to 10 main issues you identified[1]:

1. **Name the issue and briefly describe the main issue(s) identified.**
2. **Which provision(s) of the GDPR (or national laws) does this concern?**
3. **Explain why this has been an issue for the organisation?**
4. **What are differences that you have encountered between organisations in your Member State?**
5. **What are possible solutions to this issue?[2]**

The investigation of the Austrian banking sector did not identify any significant problems with regard to the role of DPOs.

Part III – Actions by the SA

1. **Have you already published general guidance (e.g. guides, guidelines, etc.) regarding DPOs (including before launching the coordinated action)?**
   If yes, please provide the date, link to the guidance, and a short description of the guidelines

The guidelines of the EDPB on the DPO have been available on the website of the Austrian Data Protection Autority since they existed.

2. **Have you taken action (i.e., fact finding exercises, informal contact, prior consultation, investigation) towards any of the organisations concerning the designation, tasks and/or role of**

[1] Note: for each issue, the five questions above are answered in approximately 1 page (and up to 2 pages) for each identified issue.

[2] Please note that the wording of this question has not been included in full in the following national reports. Many authorities have used the order of the subquestions 1 to 5 to respond to this question.

the DPO *prior to* launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).

In recent years - especially before the GDPR came into force - there has been a lot of informal contact with controllers regarding the design of the role of the DPOs. It is no longer possible to determine today whether the eleven controllers we examined were involved.

3. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**

This is not decided yet, but since no significant problems could be identified concerning the DPOs of the banking sector, no major actions by the Austrian Supervisory Authority will probably be necessary in this regard.

Part IV – Other

1. **What is your general impression of the levels of awareness and compliance of the organisations you consulted concerning the designation, tasks and/or role of the DPO?**

Essentially, the investigations revealed that all eleven banks examined take the role of the DPO very seriously. Those controllers provide sufficient funds to enable them to carry out their tasks independently. The DPOs are also regularly involved in the relevant decision-making processes of the controller. The impression is also given that the advice of the DPOs is listened to and that their regular reports are taken seriously by the management level.

2. **Are there any other issues or topics that you would like to flag?**

N/A

3. **Are there any leading practices of the organisations you have contacted that you would like to share?**

N/A

BE SA

Belgian Supervisory Authority – Autorité de protection des données – Gegevensbeschermingsautoriteit

Part I - Statistics

Please see the consolidated figures in Appendix 1.1. The answers below may refer to the questions included in Appendix 1.1.

Part II – Substantive issues

1) DPO for multiple organisations

Nearly half of the respondents indicated that they act as the single DPO for a group of undertakings or for several authorities or bodies.

According to Article 37(2) of the GDPR, 'a group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment'. Article 37(3) of the GDPR provides that 'Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size'.

Given the high proportion of DPOs acting as single DPO for a group of undertakings or for several public authorities or bodies, it is important to stress that the DPO must nevertheless remain accessible to data subjects, the supervisory authority and within the organisation itself and be able to fully carry out the tasks the GDPR assigns to the function for each of the organisations it has been appointed to.

It is essential that the contact details of the DPO be easily available to data subjects, the supervisory authority and to employees of the organisation and the DPO should also, in some circumstances, be able to rely on a team or a deputy.

2) Expertise in data protection

10% of the respondents indicated that no particular expertise on data protection was set as a requirement for the role of DPO but that the designation was compulsory. In addition, 19.2% of the respondents indicated that the DPO has less than 2 years' experience on the application and the interpretation of data protection requirements. Finally, only 73.32% of the respondents indicated that 'expert knowledge of data protection regulation' was set as a requirement for the role of DPO.

Article 37(5) of the GDPR stipulates that 'The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39'.

Recital 97 provides that the necessary level of expert knowledge should be determined according to the data processing operations carried out and the protection required for the personal data being processed.

The DPO should be chosen carefully, with due regard to the complexity, sensitivity and number of data protection issues that arise within the organization. In any event, as specified in the Article 29 Working

Party Guidelines on data protection officers[3] (hereafter, 'Guidelines on DPOs'), 'Although Article 37(5) does not specify the professional qualities that should be considered when designating the DPO, it is a relevant element that DPOs must have expertise in national and European data protection laws and practices and an in-depth understanding of the GDPR. It is also helpful if the supervisory authorities promote adequate and regular training for DPOs'.

3) Insufficient resources / Training

46.88% respondents indicated that the resources allocated to the DPO are not sufficient.

There is a considerable difference between the answers of the public and the private sector as 61.3% of the respondents from the public sector consider that their resources are not sufficient while 33.3% of the respondents from the private sector regard that their resources are not sufficient.

In addition, the respondents indicated that they have the following hours of training per year in order to develop and/or maintain their professional qualities and expert knowledge on data protection law and practices:

a. 0 hours: 16 (3.99%)
b. 1–8 hours per year: 33 (8.23%)
c. 9–16 hours per year: 50 (12.47%)
d. 17–24 hours per year: 32 (7.98%)
e. 25–32 hours per year: 55 (13.72%)
f. >32 hours per year: 174 (43.39%)
g. I do not know or wish to answer 41 (10.22%)

58.85% of the respondents answered that the organisation has not allocated a budget to the DPO.

Article 38(2) of the GDPR stipulates that 'The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks (…), and to maintain his or her expert knowledge'.

As indicated in the Guidelines on DPOs, depending on the nature of the processing operations and the activities and size of the organisation, the following resources should be provided to the DPO:

- Sufficient time for DPOs to fulfil their duties.
- Adequate support in terms of financial resources, infrastructure (premises, facilities, equipment) and staff where appropriate.
- Continuous training in data protection and other forms of professional development, such as participation in privacy fora, workshops, etc.
- Given the size and structure of the organisation, it may be necessary to set up a DPO team.

Particular attention should be awarded to this issue by public sector organisations, given the high number of DPOs in the public sector who consider that the resources allocated are insufficient.

4) Independence of the DPO / Conflict of interests

[3] Guidelines on Data Protection Officers ('DPOs') (wp243rev.01) of 13 December 2016, last revised and adopted on 5 April 2017.

The respondents indicated that the DPO also has the following additional tasks/roles:

a. Management: 47 (11.72%)
b. IT or information security: 75 (18.7%)
c. Legal or compliance: 95 (23.69%)
d. Other expert role: 72 (17.96%)
e. Any other office worker: 14 (3.49%)
f. Other: 90 (22.44%)
g. I do not know or wish to answer: 75 (18.7%)

In addition, the respondents answered that the following additional tasks are committed or assigned to the DPO:

a. Decision-making on the processing of personal data: 75 (18.7%)
b. Developing the organisation's data protection processes: 196 (48.88%)
c. Drafting and/or carrying out data protection impact assessments: 202 (50.37%)
d. Fulfilling the data subjects' requests on their data protection rights: 290 (72.32%)
e. Drafting and/or negotiating contracts (e.g., data processing agreements): 248 (61.85%)
f. Responsibility for the lawfulness of the processing of personal data: 102 (25.44%)
g. Other: 42 (10.47%)
h. I do not know or wish to answer: 31 (7.73%)

Article 38(6) of the GDPR provides that 'The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests'.

The Guidelines on DPOs clearly indicate that 'The absence of conflict of interests is closely linked to the requirement to act in an independent manner. Although DPOs are allowed to have other functions, they can only be entrusted with other tasks and duties provided that these do not give rise to conflicts of interests'. Organisations are called upon to be particularly cautious when combining the DPOs function with other roles and tasks, in particular senior management positions (but also other positions, depending on the organisational structure of the organisation). More than 11% of the respondents answered that they also had a management role.

The Court of Justice of the European Union recently held in its judgment of 9 February 2023 in case C-453/21 that 'The determination of the existence of a conflict of interests, within the meaning of Article 38(6) of the GDPR, 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'[4].

It is striking here that more than 18% of the respondents indicated that they take part in the decision-making on the processing of personal data. In Case C-453/21, the Court held that 'a DPO cannot be entrusted with tasks or duties which would result in him or her determining the objectives and methods of processing personal data on the part of the controller or its processor. Under EU law or the law of the Member States on data protection, the review of those objectives and methods must be carried out independently by the DPO'[5].

[4] Case C-453/21, *X-FAB Dresden GmbH & Co. KG v FC*, para. 45.
[5] Case C-453/21, *X-FAB Dresden GmbH & Co. KG v FC*, para. 44.

The organisations should take appropriate measures to ensure that DPOs may carry out their tasks independently and without conflicts of interests. Good practices in relation to this requirement are included in the Guidelines on DPOs (section 3.5).

5) Involvement of the DPO

57.11% of the respondents stated that the DPO is consulted on all processes relevant to processing of personal data, while 28.93% respondents indicated that they are consulted in some of processes only, and 10.22% indicated that they are not consulted on issues concerning data protection.

Additionally, the respondents stated that the DPO has access to and provided with sufficient information on issues relating to data protection and personal data processing operations in the organisation:

a. All the time: 88 (21.95%)
b. Most of the time: 203 (50.62%)
c. Sometimes: 75 (18.7%)
d. Rarely: 26 (6.48%)
e. Never: 5 (1.25%)
f. I do not know or wish to answer: 4 (1%)

38.4% of the respondents indicated that the DPO is involved and/or consulted in handling and solving issues relating to the processing and protection of personal data in the organisation less than 49% of the time.

The respondents answered that the level at which DPOs' opinions are being followed within the organisation is intermediate (22.44%), poor (3.49%) or very poor (1.25%).

Article 38(1) of the GDPR provides that the controller and the processor shall ensure that the DPO is 'involved, properly and in a timely manner, in all issues which relate to the protection of personal data'. Article 38(2) stipulates that the controller or processor shall 'shall support the data protection officer in performing the tasks referred to in Article 39 by providing (…) access to personal data and processing operations (…)'.

Organizations should ensure that DPOs are systematically informed and consulted before processing of personal data takes place as this eases compliance with the GDPR and promotes a privacy by design approach.

The Guidelines on DPOs indicate that organizations should ensure that:

- The DPO is invited to participate regularly in meetings of senior and middle management.
- His or her presence is recommended where decisions with data protection implications are taken. All relevant information must be passed on to the DPO in a timely manner in order to allow him or her to provide adequate advice.
- The opinion of the DPO must always be given due weight. In case of disagreement, the WP29 recommends, as good practice, to document the reasons for not following the DPO's advice.
- The DPO must be promptly consulted once a data breach or another incident has occurred.

6) Reporting to the highest management level

17.71% of the respondents answered that the DPO is not expected to regularly report to the highest management level of the organisation.

Article 38(3) of the GDPR stipulates that 'The data protection officer shall directly report to the highest management level of the controller or the processor'.

Given that the DPO's tasks is to inform and advise the controller or the processor of their data protection obligations pursuant to Article 39 of the GDPR, regular reporting to the highest management level of the organisation should take place and organisations are expected to implement this.

Part III – Actions by the SA

1. **Have you already published general guidance (e.g. guides, guidelines, etc.) regarding DPOs (including before launching the coordinated action)?**
   If yes, please provide the date, link to the guidance, and a short description of the guidelines

The Belgian Commission for the Protection of Private Life (the BE SA's predecessor) published the Recommendation n°04/2017 of 24 May 2017 on the appointment of a data protection officer in accordance with the General Data Protection Regulation (GDPR), in particular the admissibility of combining this function with other functions, including that of security advisor[6] (only available in French and in Dutch).

The BE SA's website contains a page dedicated to DPOs[7], with information relating to the designation and the role of the DPO.

The BE SA published a toolkit for DPOs in 2020 that includes the following documents:

- The 10 ground rules regarding the DPO[8]: these rules are intended to support controllers and and processors in fulfilling their DPO duties.
- Checklist for the DPO[9] : a list intended to assist DPOs in their advisory role.
- A template to request the DPO's opinion[10]: a template at the disposal of DPOs in order to seek comprehensive information from the controller or processor before providing an opinion.
- A general GPDR presentation[11] that may be used by DPOs as a starting point to inform employees on data protection.

The BE SA collaborated with a DPO organization and a university on an EU-funded project to set up an online platform to support DPOs (DPO-Connect). This project was successfully completed in 2022.

[6] Available here : https://www.autoriteprotectiondonnees.be/publications/recommandation-n-04-2017.pdf
[7] Available here : https://www.autoriteprotectiondonnees.be/professionnel/rgpd-/delegue-a-la-protection-des-donnees
[8] Available here: https://www.autoriteprotectiondonnees.be/publications/les-10-regles-de-base-concernant-le-delegue-a-la-protection-des-donnees-dpo.pdf
[9] Available here: https://www.autoriteprotectiondonnees.be/publications/check-list-avis-dpo-general.pdf
[10] A simplified version is available here: https://www.autoriteprotectiondonnees.be/publications/demande-pour-le-delegue-a-la-protection-des-donnees-dpo.docx. A more detailed version is available here : https://www.autoriteprotectiondonnees.be/publications/demande-d-avis-ou-demande-d-informations-pour-le-delegue-a-la-protection-des-donnees-dpo.docx
[11] Available here: https://www.autoriteprotectiondonnees.be/publications/principes-rgpd.pptx

2. **Have you taken action (i.e., fact finding exercises, informal contact, prior consultation, investigation) towards any of the organisations concerning the designation, tasks and/or role of the DPO *prior to* launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**

The Inspection Service of the BE SA systematically enquires on the designation and the role of the DPO in the context of its formal investigations.

Several decisions relating to the designation and the role of the DPO have been adopted by the BE SA. Below is a non-exhaustive list of decisions that broach this topic:

- **Decision n°15/2020 of 15 April 2020**[12]: the Litigation Chamber notably finds a violation of Article 37 of the GDPR, given that the defendant does not demonstrate that the DPO fulfils the quality requirements imposed by the GDPR, and a violation of Article 38 of the GDPR because the defendant cannot demonstrate that it guarantees that the position of the DPO is sufficiently independent and able to report to the highest level of management.
- **Decision n°18/2020 of 28 April 2020**[13]: in this case, the DPO was also responsible for the audit, risk and compliance departments. The Inspection Service had found in this case that the DPO was not in a position that was sufficiently protected from a conflict of interests (Article 38(6) of the GDPR) and that the DPO was not sufficiently associated in discussions relating to data breaches (Article 38(1) of the GDPR). The Litigation Chamber of the BE SA found that there was no violation of Article 38(1) of the GDPR in this case but that there was a violation of Article 38(6) of the GDPR due to the multiple functions of the DPO, thus entailing a conflict of interests. This decision gave rise to numerous reactions and questions, both in Belgium and abroad, concerning the possibility of combining DPO duties with other functions within an organization.
- **Decision n°41/2020 of 29 July 2020**[14]: although it is not the object of the complaint, the Litigation Chamber of the BE SA recalls that Article 38(2) of the GDPR requires that organizations support their DPOs by providing resources necessary to carry out [their] tasks and access to personal data and processing operations, and to maintain his or her expert knowledge. The Litigation Chamber lists various aspects that should be taken into consideration, notably active support of the DPO's function by the management, sufficient time being allocated to the DPO to carry out their tasks, sufficient financial resources and infrastructure, etc. The Litigation Chamber also insists on the fact that the more complex and sensitive the processing operations are and the more data processed, the greater the resources that should be allocated to the DPO. The DPO must be able to carry out their duties effectively, and be provided with adequate resources in relation to the data processing carried out and the risks involved.
- **Decision n°24/2021 of 19 February 2021**[15]: the Litigation Chamber of the BE SA found that given that the DPO provides its opinions to a contact person within the defendant's

[12] Available here: https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-15-2020.pdf. See in particular paras 143-155.

[13] Available here: https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-18-2020.pdf. See in particular Section 3.d).

[14] https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-41-2020.pdf. See in particular paras 87-89. This decision has been appealed and annulled by the Market Court.

[15] Available here https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-24-2021.pdf. See in particular paras 153-156.

organization and not to the highest management level, there is a violation of Article 38(3) of the GDPR.

- **Decision n°21/2022 of 2 February 2022**[16]: the Litigation Chamber of the BE SA considered that the defendant should have appointed a DPO, in accordance with Article 37 of the GDPR, given that regular and systematic observation of identifiable users on a large-scale was being performed by the defendant. It concluded that there was a violation of Article 37 GPDR in the case at hand.
- **Decision n°162/2022 of 16 November 2022**[17] the Litigation Chamber of the BE SA concluded that the controller had violated Articles 38(1) and 39(1) of the GDPR due to the fact that the DPO had not been sufficiently involved in several issues relating to data protection.
- **Decision n°81/2023**[18] **of 22 June 2023**: the Litigation Chamber of the BE SA noted that the function of DPO and security advisor are performed by the same person. The Litigation Chamber pointed out that in the case C-453/21, the CJEU held that there may be a conflict of interests within the meaning of Article 38(6) of the GDPR when a DPO is entrusted with other missions or tasks that would lead them to determining the purposes and means of the processing of personal data with the data controller or processor. This must be verified on a case-by-case basis, with an assessment of all the relevant circumstances.
- **Decision n°110/2023 of 9 August 2023**[19]**:** the Litigation Chamber of the BE SA found that the defendant, a local municipality that had used the services of an external DPO, was in breach of Article 37(1)(a) and Article 37(7) of the GDPR due to the way in which the DPO was appointed, the manner in which the appointment was monitored and due to absence of notification of the DPO to the BE SA. The Litigation Chamber also concluded that there had been a breach of Article 39(1) of the GDPR given the lack of an adequate working framework for the DPO. Several issues were identified, notably: insufficient time allocated to enable the DPO to perform its tasks (120 hours per year), absence or lack of direct contact with the highest management level. This was especially problematic given the large volume of personal data processed from a large number of data subjects by the controller.

3. What action(s) are you planning to undertake based on the results of this coordinated action, if any? (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)

Update of the thematic page relating to DPOs on the BE SA's website as well as organizing a seminar for DPOs.

[16] Available (in English) here: https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-21-2022-english.pdf. See in particular paras 517-524. This decision was appealed before the Market Court and the latter rendered an interim ruling on 6/09/2022 in which it referred preliminary questions to the Court of Justice of the European Union (case C-604/22).

[17] Available here: https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-162-2022.pdf. See in particular paras 67-75.

[18] Available here: https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-81-2023.pdf. See in particular para 28.

[19] Available here: https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-110-2023.pdf. See in particular paras 57-63.

Part IV – Other

1. **What is your general impression of the levels of awareness and compliance of the organisations you consulted concerning the designation, tasks and/or role of the DPO?**

There seem to be disparities in the level of compliance with the obligations relating to the DPOs position and tasks among the respondents.

In any event, there is still a lot of room for improvement and organisations should be made aware of the crucial role played by the DPO and encouraged to provide the necessary resources to their DPOs in order for them to be able to carry out their tasks and missions in compliance with the relevant provisions of the GDPR.

2. **Are there any other issues or topics that you would like to flag?**

No other issues or topics.

3. **Are there any leading practices of the organisations you have contacted that you would like to share?**

16.46% of the respondents indicated that the DPO was not appointed on the basis of Article 37(1) of the GDPR or in accordance with an obligation arising from another legislation of the Union or of a Member State, but 'On another basis, for example on a voluntary basis'.

As indicated in the Guidelines on Data Protection Officers adopted by the Working Party 29, the appointment of a DPO on a voluntary basis is to be encouraged.

CY SA

Cyprus SA – Office of the Commissioner for Personal Data Protection

Part I - Statistics

Please see the consolidated figures in Appendix 1.1. The answers below may refer to the questions included in Appendix 1.1.

Part II – Substantive issues

1) The designation, knowledge and experience of the DPO

- Deputy DPO

1. 53% of the respondents have not appointed a deputy DPO.
2. Art. 38(1), (4), Art. 39(1) GDPR
3. In case where the DPO cannot perform their duties, for a certain period of time and there is no deputy DPO, then both the communication with the data subjects for the exercise of their rights and the cooperation with the Supervisory Authority are significantly affected.
4. –
5. Designation of deputy DPO.

2) The tasks and resources of the DPO

- DPO to multiple organizations

1. Some companies provide DPO services to multiple organizations.
2. Art. 38(1) GDPR
3. There are concerns whether the DPOs are able to fulfil their duties effectively for each one of these organizations.
4. –
5. Dedicated person in the company for each organization.

3) The role and position of the DPO

- Position in the management of the organization

1. 13% of the designated DPOs belong to the highest management or the administrative management of the organization.
2. Art. 38(6) GDPR
3. DPOs cannot be in a position to determine the scope and means of processing. Such case may cause a conflict of interest.
4. –
5. Employees who belong to the administration of the organization must be excluded from being designated as DPOs.

4) Publication of the contact details

1. 14% of the respondents have not made public the contact details of their DPOs nor have communicated them to the Supervisory Authority.
2. Art. 37(7) GDPR
3. Both the communication with the data subjects for the exercise of their rights and the cooperation with the Supervisory Authority are adversely affected.
4. –
5. Provision of specific guidelines by the Supervisory Authority.

Part III – Actions by the SA

1. **Have you already published general guidance (e.g. guides, guidelines, etc.) regarding DPOs (including before launching the coordinated action)?**
   If yes, please provide the date, link to the guidance, and a short description of the guidelines

Yes, our Supervisory Authority has published guidance on its website regarding DPOs, in the form of questions and answers and other supporting material, including explanation of the provisions of the relevant Articles of the GDPR and based on the EDPB Guidelines. The aim was the understanding of the obligations of the data controllers, derived from the GDPR, including the tasks of the DPOs.

This guidance has been published prior to the launch of this coordinated action at the following link: https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page2b_gr/page2b_gr?opendocument.

2. **Have you taken action (i.e., fact finding exercises, informal contact, prior consultation, investigation) towards any of the organisations concerning the designation, tasks and/or role of the DPO *prior to* launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**

Through the years, many seminars/presentations have been held in both private and public sector, regarding the GDPR in general, including the role and tasks of the DPOs.

Also, we contact many organizations and requested to provide the contact details of their DPOs, in order to update our database.

Furthermore, in 2022, at the Ministry of Finance, a special training on the GDPR, for DPOs in public sector was organized.

The same year, the Commissioner organized two seminars/presentations in which more than 200 officials, supervisors and high-ranking officials of the House of Representatives, Ministries, Deputy Ministries, Departments, Services, Independent Offices and Authorities participated.

In 2020, in order to assess the level of compliance of the private sector (supermarkets, insurance companies and private hospitals) our Office started conducting sector audits through a questionnaire. The aim of these controls was, inter alia, the designation and tasks of the DPOs.

In 2019, our Office conducted audits, through a questionnaire, in public sector (Departments, Services, Public Law Legal Entities, Local Government Organizations). The main objective of the audit was to investigate whether the public sector has responded sufficiently in their obligations regarding the designation of the DPOs and if they have been given to the person designated to carry out the due duties, the appropriate resources for the exercise of their duties, with full independence.

3. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**

Our Office aims to communicate, with both public and private organizations in order to provide specific guidelines regarding the main issues identified based on the results of the coordinated action. Although we have already provided guidelines on the designation and the role of the DPO, the results of the questionnaire showed specific topics that need further guidance. The said guidance will be published after the final report by the EDPB.

Part IV – Other

1. **What is your general impression of the levels of awareness and compliance of the organisations you consulted concerning the designation, tasks and/or role of the DPO?**

From the responses given, we observe that a significant percentage of organizations seem to comply with the definition, duties and/or role of the DPO.

2. **Are there any other issues or topics that you would like to flag?**

No.

3. **Are there any leading practices of the organisations you have contacted that you would like to share?**

Not at the moment.

CZ SA

Czech Supervisory Authority – Office for Personal Data Protection

Part I - Statistics

Please see the consolidated figures in Appendix 1.1. The answers below may refer to the questions included in Appendix 1.1.

Part II – Substantive issues

Question 17

1. The survey has shown that three out of fourteen ministries stated that their DPOs were tasked with drafting and carrying out a Data Protection Impact Assessment (DPIA) as an additional task.
2. Art. 35(2), Art. 38(6) GDPR.
3. The survey has shown that three out of fourteen ministries stated that their DPOs were tasked with drafting and carrying out a Data Protection Impact Assessment as an additional task. For clarity the SA would like to point out that the Czech version of the questionnaire featured a question with phrasing that explicitly implied a creation of a DPIA. Considering the fact that DPOs are supposed to merely provide assistance, in the form of providing advice, to the controller who carries out a DPIA it could be said that if they were to simultaneously draft-up DPIA itself and carry it out instead of the controller they would end up in a conflict of interest. As was stated in Guidelines on Data Protection Officers ('DPOs'), controllers are the ones obliged to carry out a DPIA, not DPOs themselves. This finding could indicate a violation of Article 38(6) GDPR.
4. In the remaining responses the ministries haven't stated that their DPOs were tasked with drafting and carrying out a DPIA as an additional task.
5. It is not possible to conclude that GDPR has been violated purely based on the answers provided in the survey. The solution to indicated violation of GDPR could lay in utilising the investigative powers bestowed upon SA by Article 58(1)(d) GDPR and notifying the controller of an alleged infringement of GDPR, especially in cases where a DPIA was actually carried out.

Question 27

1. The survey has shown that eleven out of fourteen of responding ministries do not include their DPO in every issue concerning personal data protection.
2. Art. 38(1) GDPR.
3. The survey has shown that eleven out of fourteen of responding ministries do not include their DPO in every matter concerning personal data protection. Any answer other than that the DPO is included in all matters concerning personal data protection indicates a violation of Article 38(1) GDPR. One ministry even stated that their DPO is involved in less than 5 % of matters concerning personal data protection. Such answer indicates a general lack of effectiveness of DPO's position within the ministry and a question arises as to whether this lack of effectiveness shows up in the level of personal data protection provided by the ministry in question.
4. Three ministries have stated that their DPO is involved in all matters concerning personal data protection.

5. It is not possible to conclude that GDPR has been violated purely based on the answers provided in the survey. A possible solution would be to hold an audit focused on the inclusion of DPOs in matters concerning personal data protection.

Question 28

1. The survey has shown that three out of fourteen responding ministries do not require a consultation with the DPO on the issues concerning data protection, such as cases of personal data breaches, in their internal processes.
2. Art. 38(1) GDPR.
3. The survey has shown that three out of fourteen responding ministries do not require a consultation with the DPO on the issues concerning data protection, such as cases of personal data breaches, in their internal processes. Even if this is not an obligation explicitly required by GDPR it is recommended by Guidelines on Data Protection Officers ('DPOs'). It should be noted that this group of three ministries includes a ministry that stated that their DPO has access to all information in relation to personal data protection only rarely in a follow-up question. In context of this situation the answer may indicate that their DPO isn't included in all matters concerning personal data protection. This can therefore indicate a violation of Art. 38(1) GDPR. Other five respondents have stated that their internal processes require a consultation with DPO only in certain cases, which can also indicate that their DPO isn't included in all matters concerning personal data protection.
4. The survey has shown that the remaining six out of fourteen respondents have stated that their internal processes require a consultation with DPO in all matters concerning personal data protection.
5. SA will probably approach ministries through a letter that will aim to advise ministries to take best practise included in Guidelines on Data Protection Officers ('DPOs')in mind.

Question 29

1. The survey has shown that twelve out of fourteen responding ministries have stated that their DPO does not always have a sufficient access to information on issues relating to data protection and personal data processing operations in the organisation.
2. Art. 38(1)(2) GDPR.
3. The survey has shown that twelve out of fourteen responding ministries have stated that their DPO does not always have a sufficient access to information on issues relating to data protection and personal data processing operations in the organisation. Ten of the responding ministries have stated that their DPO has access to all information regarding personal data processing most of the time for the most part. These answers already indicate a possible violation of Article 38 (1)(2) GDPR because the DPO should always be included in matters relating to personal data protection in a proper and timely manner by the organisation. Especially in a case of one answer out of this group of twelve which included that their DPO has access to all information regarding personal data processing only rarely a flagrant violation GDPR is alluded to and this raises the question of how well is their DPO capable of performing their tasks. It should be noted that in the case of this ministry the questionnaire was not actually filled out by a DPO.
4. The survey has shown that only two ministries have stated that their DPO always has access to all information regarding personal data protection. It should be noted that in these two cases the questionnaire was filled out by a DPO.

5. The solution to the indicated violation of GDPR could lay in utilising the investigative powers entrusted to supervisory authorities in Article 58 (1)(d) GDPR or in performing an audit with focus on the DPO's access to information relating to personal data protection and personal data processing and possibly in ordering the ministries to ensure the necessary conditions for the DPOs to perform their duties independently. Precise course of action will be determined in due time.

Question 31

1. The survey has shown that nine of the fourteen responding ministries have stated that their reasons for not following their DPO's advice is not documented.
2. Art. 38(1) GDPR.
3. The survey has shown that nine ministries have stated that they don't document in any way their reasons for not following their DPO's advice in matters concerning personal data protection. Even if this is not an obligation explicitly required by GDPR it is recommended by Guidelines on Data Protection Officers ('DPOs'). An absence of such procedure can be indicative of the possible fact, that other interests of the organisation are preferred instead of fully adhering to provision of GDPR regarding DPO. On the other hand, it is necessary to say that the survey has also shown that seven ministries have stated that they follow their DPO's opinions, and seven ministries have stated that their DPO's opinions are followed most of the time. It is not possible to get a clear picture of the number of times the ministries have decided not to follow their DPO's opinions from the survey alone.
4. The survey has shown that no ministry documents their reasons for not following their DPO's opinions in all cases. One ministry has answered that their reasons for not following their DPO's advice are documented most of the time.
5. SA will probably approach ministries through a letter that will aim to advise ministries to take best practise included in Guidelines on Data Protection Officers ('DPOs') in mind.

Question 32

1. The survey has shown that one of the fourteen responding ministries has stated that they give their DPO instructions regarding the exercise of their tasks.
2. Art. 38(3) GDPR.
3. The survey has shown that one of the fourteen ministries has stated that they give their DPO instructions regarding the exercise of their task. According to Article 38 (3) GDPR the controller shall ensure that the DPO does not receive any instructions regarding the exercise of those tasks. The requirement of independence associated with DPOs position is not any different for employees of ministries. This finding indicates a violation of the duty to ensure DPO's independence and therefore indicates a violation of Article 38 (3) GDPR. It can be said that all ministries have answered that none of their DPOs has been dismissed or penalised for performing their tasks and duties.
4. In the remaining thirteen cases the ministries have answered that they do not give their DPOs instructions regarding the exercise of their tasks. The singular exception in this group of thirteen was an answer stating that the ministry does so in area of cyber security. It is not clear whether the DPO in question of this ministry isn't also entrusted with a different task or a role within the organisation, however it should be noted that the ministry in question has also stated that their DPO performs their role as a full-time job.
5. The solution to the aforementioned violation of GDPR could lay in utilising the investigative powers entrusted to supervisory authorities in Article 58 (1)(d) GDPR or in performing an audit

with focus on independence of the DPO's position and after answering the questions of fact ordering the ministry to ensure that their DPO will not receive any instruction regarding the exercise of their tasks. Precise course of action will be determined in due time.

Part III – Actions by the SA

1. **Have you already published general guidance (e.g. guides, guidelines, etc.) regarding DPOs (including before launching the coordinated action)?**
   If yes, please provide the date, link to the guidance, and a short description of the guidelines

The Supervisory authority (SA) has not published any general guide focused on DPOs. The most important information is available on SA's web page in form of an FAQ.

SA started to organise a series of specialised educational events during the year 2018, seven of which were meant specifically for DPOs employed by public authorities and bodies. These educational activities were eventually halted due to COVID-19 pandemic. SA resumed organising such events in June 2023. The topic of last-held event so far was Data Protection Impact Assessment.

2. **Have you taken action (i.e., fact finding exercises, informal contact, prior consultation, investigation) towards any of the organisations concerning the designation, tasks and/or role of the DPO *prior to* launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**

SA has also concerned itself with DPO's position and conditions for fulfilling their duties during audits of ministries in cases where it related to the subject of the audit itself.

Specifically in case of an audit that SA has held at Ministry of foreign affairs, which finished in the year 2021, during which SA discovered a violation of Article 38(1)(2) GDPR.

3. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**

Action of SA is going to be derived from findings acquired from individual ministries. SA presumes that individual ministries will be informed according to investigative power bestowed by Article 58 (1)(d) GDPR about the fact that their answers in the questionnaire indicate a possible violation of GDPR. At the same time, they will be ordered to relay more concrete information in accordance with Article 31 GDPR. In some cases, it will be possible to think about initiating an audit in accordance with Art. 58 (1)(b) GDPR instead of the previously mentioned approach. As a response to further findings, the SA will then start to give corrective orders. It needs to be said that due to Article 83(7) GDPR and section § 62 subsection 5 Act No. 110/2019 Coll., on personal data processing, it's impossible to impose an administrative fine on public authorities and bodies for violating GDPR.

Part IV – Other

1. **What is your general impression of the levels of awareness and compliance of the organisations you consulted concerning the designation, tasks and/or role of the DPO?**

Based on results of the questionnaire SA has an opinion that it is possible to observe significant differences within a relatively homogenous group of entities such as ministries in terms of how they create an environment for their DPO's position and related affairs. SA believes that these differences can exist partially due to different ways these ministries fulfil their various agenda and from which varying parameters of personal data processing may stem. Nonetheless, vast majority of requirements have their origin in GDPR itself and are therefore same for all ministries, such as the requirement to involve DPOs in every matter concerning personal data processing, and their lack of proper implementation cannot be substantiated solely by a possible difference in parameters of personal data processing. As can be concluded from information mentioned above the answers of ministries often indicate a violation of GDPR's provisions focused on DPOs in itself or in sum of their parts. In SA's opinion the position of DPO and ensuring resources for their tasks in ministries is not aided by the fact that the Czech legislative in Act No. 110/2019 Coll. in its section § 62 subsection 5 in accordance with Article 83(7) GDPR has utilised the possibility of exempting public authorities and bodies from sanctions by not allowing the SA to impose an administrative fine.

2. **Are there any other issues or topics that you would like to flag?**

Not applicable.

3. **Are there any leading practices of the organisations you have contacted that you would like to share?**

Not applicable.

DE SA

DE SA Bavarian Supervisory Authority for the non-public sector – Bavarian State Office for Data Protection Supervision (BayDSG)

Part I - Statistics

Please see the consolidated figures in Appendix 1.1. The answers below may refer to the questions included in Appendix 1.1.

Part II – Substantive issues

We are still in an ongoing process of investigation and asking further explanations from the organisations, where we identified possible violations.

Therefore the listing of the substantive issues we identified should be considered as the current state of which issues we're expecting as the final main issues after our investigation is fully done.

1) DPO's tasks do not meet the minimum tasks defined by the GDPR

1. A significant number of organisations did not respond that all of the tasks in Question 16 are committed/assigned to the DPO, despite we would consider them all as tasks which should be committed/assigned to the DPO.
2. Art. 39(1) and 38(4) GDPR.
3. This is an issue as the DPO should be committed/assigned to all of the tasks the GDPR is defining.
4. Other organisations did respond that all of the tasks in Question 16 are committed/assigned to the DPO.
5. The organisations must ensure that all the tasks the GDPR is defining are committed /assigned to the DPO.

2) Additional tasks are committed/assigned to the DPO, which are causing a conflict of interests

1. A significant number of organisations did respond to Questions 17 and 25 that tasks are committed/assigned to the DPO, which we would consider as a conflict of interests.
2. Art. 38(6) GDPR.
3. This is an issue as tasks which are causing a conflict of interests are forbidden to be committed/assigned to the DPO.
4. Other organisations did not reply with such tasks.
5. The organisations must ensure that additional tasks of the DPO are free of conflicts of interests.

3) DPO has no designated deputy

1. Many organisations did respond to Question 21 that the DPO does not have a designated deputy. Despite this is not an obligation the GDPR explicitly demands, it is at least questioning, if the tasks of the DPO are sufficiently taken care of in case of the DPO being absent.
2. See response under point 1.
3. See response under point 1.
4. Other organisations stated that a deputy is designated.

5. The matter requires further investigation on what other arrangements the organisations have established for the case of the DPO being absent.

4) No independent budget allocated to the DPO

1. Many organisations responded to questions 23 and 24 that there is no budget allocated to the DPO or that the DPO cannot manage such budget independently.
2. Art. 38(2) GDPR.
3. While there might not automatically be a violation with those answers given, not having such budget or having limitations in managing it is at least questioning if the DPO is provided with sufficient resources.
4. There were also several organisations which answered that an independent budget is allocated.
5. The matter requires further investigation on how the DPO is requesting financial resources from the organisation and how the processing of such requests is organised.

5) Insufficient consultation, access and documentation

1. The answers of several organisations to questions 27, 28, 29 and 31 are indicating that the consultation of the DPO and its documentation is insufficient and the DPO does not have the required access to fulfil his tasks.
2. Art. 38(1) and (2) GDPR.
3. The DPO only can fulfil his tasks when he has the required access to do so and when he is getting involved in questions regarding the protection of personal data.
4. Most organisations might have at least one of these issues but there are also several which do not seem to have a problem here.
5. The matter requires further investigation on how the DPO is involved within the organisation but the aim must be that the organisations involve the DPO and grant him access like the GDPR demands.

6) Overall resources

1. For several organisations we are in doubt if the overall resources (especially human resources) of the DPO are sufficient when we take a look for example at the number of employees and customers, the industry/sector of the organisation or the number of organisations he is assigned to as a group DPO.
2. Art. 38(2) GDPR.
3. Sufficient resources are a key element of a DPO who is actually capable of action. If the organisation limits those resources below the actual requirements, the DPO cannot fulfil his tasks sufficiently.
4. It is not yet foreseeable how many organisations actually have a problem here but there definitely also are organisations where we would consider the resources in a sufficient proportion.
5. The matter requires further investigation for each individual organisation where we are in doubt of sufficient resources.

Part III – Actions by the SA

1. **Have you already published general guidance (e.g. guides, guidelines, etc.) regarding DPOs (including before launching the coordinated action)?**
   If yes, please provide the date, link to the guidance, and a short description of the guidelines

We do not have general guidelines yet but only some FAQ and a general landing page on our website. This publication however requires revision and addition, which both is planned in the course of the coordinated action.

2. **Have you taken action (i.e., fact finding exercises, informal contact, prior consultation, investigation) towards any of the organisations concerning the designation, tasks and/or role of the DPO *prior to* launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**

Prior to launching the coordinated action, some of the contacted organisations in the past have received individual advice to specific DPO-related questions or supervisory notices on specific matters like publication of the DPO's contact data. We are not aware of more serious actions according to Article 58(2) GDPR.

3. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**

We have not yet decided, what kind of further actions will be the most appropriate ones to promote the results of the CEF. We receive many questions on this aspect claiming that the Guidelines on DPOs should be updated as one of the key outcomes - a wish we strongly support. In the meantime, we will work on guidelines or FAQ's published by our authority or - in best case - supported by the other German SA's taking also into account current questions like the role of DPO's in the implementations of whistleblowing-systems (currently a question because the national implementation of Directive 2019/1937 just entered into force; see below Part IV Nr. 2). Regardless of these measures, we are aiming at finishing our formal investigations case by case, expecting that this will take at least until mid-year 2024.

Part IV – Other

1. **What is your general impression of the levels of awareness and compliance of the organisations you consulted concerning the designation, tasks and/or role of the DPO?**

Notwithstanding further investigations, at first sight we look at structures and implementations of the concept of the DPO as an internal monitoring and advisory body that seem in line with the GDPR-requirements. Looking at specific elements like resources, tasks, budget, additional tasks and functions or the way, the DPO is able to report to the highest management level reveals in several cases misunderstandings and shortcoming of awareness, how a DPO should be integrated in the compliance mechanisms of companies.

2. Are there any other issues or topics that you would like to flag?

We recently received several questions regarding recital 56 of so called Whistleblowing Directive (EU) 2019/1937, which states in the German translation of the Directive that the DPO of smaller organisations is considered a suitable choice to be designated as competent to receive and follow up on reports under this this Directive. We however think that performing this specific task in relation to whistleblowing together with the tasks of a DPO is likely to lead to a conflict of interests on a regular basis. We would be interested to hear the opinions of other authorities about this matter.

3. Are there any leading practices of the organisations you have contacted that you would like to share?

Not yet. We will analyse carefully the findings of our colleagues and try to contribute relating findings if possible.

DK SA

Danish Supervisory Authority – Danish Data Protection Agency

Part I - Statistics

Please see the consolidated figures in Appendix 1.1. The answers below may refer to the questions included in Appendix 1.1.

Part II – Substantive issues

1) Conflict of interests
The DK SA noticed a relatively large number of controllers outsourcing the DPO-role to external organisations, such as law firms. These law firms act as DPO for multiple different municipalities, and sometimes they take on advisory roles as well as handle legal cases for the municipalities. There is a risk that this could compromise the DPO's independence and ability to act without a conflict of interests, cf. Article 38(6) GPDR.

2) Other tasks and duties
Related to the first issue. A number of controllers mentioned that they had additional tasks beyond what was required by the GDPR. This is not in itself an issue, however, several indicated that they had tasks that would necessarily interfere with their other tasks as DPO's, such as making decisions on the controller's processing of personal data. This would also relate to Article 38(6) GPDR.

3) Providing necessary resources
Another issue identified is a lack of necessary resources relating to the condition in Article 38(2) GDPR. 17% of the respondents said that they do not have the necessary resources to carry out the tasks of the DPO.

4) Involvement of the DPO
The survey has shown that only 4% of the respondents involve their DPO in all issues relating to the protection of personal data. Additionally, 16% responded that, according to their internal procedures, they are not required to involve the DPO in questions regarding data protection. These issues concern Article 38(1) GDPR.

The final identified challenges will be part of our ongoing considerations for starting own-volition investigations.

Part III – Actions by the SA

1. **Have you already published general guidance (e.g. guides, guidelines, etc.) regarding DPOs (including before launching the coordinated action)?**
   If yes, please provide the date, link to the guidance, and a short description of the guidelines

Indeed, the Danish SA published guidelines on DPO's in December 2017. The guidelines have a broad scope, and issues guidance on what a DPO is private organisations' obligation to appoint a DPO, public authorities' obligation to appoint a DPO as well as the role of the DPO. The Danish SA also has a link on its website to the EDPB guidelines on DPO's. Link to the guidelines (only available in Danish unfortunately): https://www.datatilsynet.dk/Media/B/E/Databeskyttelsesr%c3%a5dgivere.pdf.

2. **Have you taken action (i.e., fact finding exercises, informal contact, prior consultation, investigation) towards any of the organisations concerning the designation, tasks and/or role of the DPO *prior to* launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**

Yes, we opened some own-volition inquiries into a couple of chosen municipalities regarding their DPO's resources, tasks and qualifications. The inquiries were opened in 2019. In the end, the Danish Supervisory Authority did not consider the municipalities to have breached the GDPR, and thus no corrective measure was imposed upon the municipalities.

3. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**

Based on the results of the coordinated action, the Danish SA initiated an investigation on the outsourcing of the DPO-role. The aim is to make an overall assessment of whether the municipalities have implemented the necessary organizational structures in order to ensure that the DPO's are able to perform their tasks, including ensuring the independence of the DPO.

The investigations are initiated and will continue throughout the spring.

The other issues could be alleviated either by more focused guidance on this matter, or by opening investigations. This will be considered by the Danish SA going forward.

Part IV – Other

1. **What is your general impression of the levels of awareness and compliance of the organisations you consulted concerning the designation, tasks and/or role of the DPO?**

Our general impression is that the levels of awareness and compliance among Danish municipalities is quite high. We have primarily seen positive answers to the questionnaire. However, there are some areas that obviously could be improved.

2. **Are there any other issues or topics that you would like to flag?**

No.

3. **Are there any leading practices of the organisations you have contacted that you would like to share?**

No.

EDPS

European Data Protection Supervisor

Part I - Statistics

Please see the consolidated figures in Appendix 1.1. The answers below may refer to the questions included in Appendix 1.1.

Part II – Substantive issues

Issue No 1 - Tasks and resources

1. *Brief description of the issue identified*

The main issue for DPOs seems to be a lack of resources. This translates both as a lack of time to perform their DPO duties, in particular for part-time DPOs, and as lack of additional staff resources. Almost half of the 69 respondents estimate that their resources are insufficient to fulfil their tasks. Less than half of the DPOs have a deputy and less than 30% have their own budget. 30% indicate that they do not have any full time equivalent (FTE) at their disposal for fulfilling their tasks and 40% only have a part-time resource.

2. *Relevant provisions*

The relevant provisions of 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 (EUIs) and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (EUDPR) are Article 44(2) and (6)[20].

3. *Why this has been an issue for EUIs*

If the DPOs do not have sufficient time and resources to perform their duties, there is a risk that data protection is not perceived as a priority by their EUI, and that the data protection culture must be further fostered. Even where this is not a conscious choice or a result of negative prioritisation by EUIs, it will inevitably have a negative impact on the internal application of the EUDPR.

4. *Differences between EUIs*

The difference in size of the EUIs entails significant differences in resources; larger EUIs naturally have more staff to devote to DPO tasks and may even have a whole team supporting the DPO, whereas smaller EUIs often only have part-time DPOs that carry out other tasks in parallel to their DPO tasks. The largest EUIs (European Commission, European Parliament, etc.) also have appointed Data Protection Coordinators who advise and assist a particular directorate-general or service in all data protection aspects, acting as delegated DPOs. Furthermore, there is a large disparity between the type of personal data processed by the different EUIs. While they all process administrative data relating to HR matters, contracts, etc., not all of them process personal data in their core business. Others, such as Europol and Frontex, process large amounts of sensitive data within the framework of their mandate. The workload and expertise required of DPOs therefore vary a lot from one EUI to another and are not necessarily related to the size of the EUI.

5. *Possible solutions*

EUIs can be encouraged to allocate more resources to the DPO function. Having a strong and independent DPO function that is capable of taking action and ensuring the internal application of the

[20] Equivalent to Article 38(2) and (6) GDPR.

EUDPR, should be seen as an asset, an insurance against future problems. DPOs should also be encouraged to inform the EDPS where there is an issue linked to resources, so that the EDPS can intervene if needed, for example by formally addressing the matter with senior management of the EUI in question.

Issue No 2 - The role and position of the DPO

1. *Brief description of the issue identified*

Independence of the DPO. A very small number, 3 out of 69 respondents, reported that they have been dismissed or penalised for performing their tasks and duties.

2. *Relevant provisions*

Articles 44(3)[21], 44(8) second sentence[22] and 45(1)(b) first sentence[23] EUDPR.

3. *Why this has been an issue for EUIs*

Although the number of DPOs reporting having suffered serious negative consequences for carrying out their tasks and duties is small (4%) this is still cause for concern since the independence of the DPO cannot be guaranteed if they risk retaliation for performing their tasks.

4. *Differences between EUIs*

N/A

5. *Possible solutions*

More awareness-raising activities and information on the importance of the independence of the DPO could be envisaged, in particular directed at senior management. This could be followed by audits or investigations on the matter, possibly resulting in corrective measures if needed.

Issue No 3 - Further guidance from EDPS

1. *Brief description of the issue identified*

Almost all the DPOs requested further guidance from the EPDS, not specifically as to their tasks and role, probably because the awareness of these matters is already high within EUIs (the previous legal framework on data protection from 2001 also included an obligation to appoint a DPO).[24] DPOs are in fact more interested in guidance to help them fulfil their tasks more efficiently and provide advice that is more impactful to data subjects and controllers within their organisation. The DPOs reported that they would like to receive such guidance both for themselves and for internal distribution within their EUI.

2. *Relevant provisions*

Articles 45(1)[25] EUDPR.

[21] Equivalent to Article 38(3) GDPR.

[22] No equivalent in GDPR. This provision reads as follows: '(...) The data protection officer may be dismissed from the post by the Union institution or body which designated him or her if he or she no longer fulfils the conditions required for the performance of his or her duties and only with the consent of the European Data Protection Supervisor.'

[23] No equivalent in GDPR. it reads as follows: '1.(b) to ensure in an independent manner the internal application of this Regulation; (...)'.

[24] In light of the entry into force of the EUDR, the EDPS issued a Position Paper on the role of DPOs in EUIs on 30 September 2018. This Position Paper built on the principles and recommendations in a previous paper from 2005.

[25] The list of tasks of the DPO in Article 45 EUDPR is more elaborated than in Article 39 GDPR (see italics): '1.The data protection officer shall have the following tasks:

3. *Why this has been an issue for EUIs*

As many DPOs struggle with a lack of resources, they often find it difficult and time-consuming to set up procedures and create templates (for instance for DPIAs), whilst providing guidance on a wide range of complex data protection issues. As a large majority of DPOs report that they are involved in almost all the data protection related tasks listed in the questionnaire, they are required to be experts in many different aspects of data protection, both legal and IT-related. Many DPOs have also reported that they are asked to take on additional tasks, such as developing the organisation's data protection processes, dealing with data subjects' requests to exercise their rights, or drafting and negotiating contracts (e.g., data processing agreements).

4. *Differences between EUIs*

Additional guidance is an almost unanimous request from DPO. There does not seem to be any difference between EUIs, although the issues encountered would logically be more accentuated for DPOs with little resources.

5. *Possible solutions*

In addition to the Position Paper on DPOs, the EDPS has already issued extensive guidance for controllers and DPOs, such as thematic guidelines. Other tools made available to DPOs include: an annotated EUDPR (wiki); training sessions (including training targeted to newly appointed DPOs); workshops; DPO roundtables (where a small number of DPOs and the EDPS discuss specific topics of interest for DPOs); factsheets; podcasts; Quick News for DPOs (a short monthly newsletter covering topics of interest for DPOs with a practical focus); periodical publications (EDPS newsletter, TechDispatch, TechSonar), etc.[26]

Furthermore, the EDPS organises biannual meetings with the EU DPO network. Certain items on the agenda of these meetings are prepared in cooperation with the small group of DPOs (DPO Support Group). At these meetings, the EDPS organises workshops and case studies, together with the DPO Support Group, aimed at giving DPOs practical guidance on different topics. All the above tools and initiatives, contribute to provide support and guidance to DPOs. The EDPS intends to issue further guidance based on converging requests from DPOs on specific topics. This guidance could be given in the form of Q&As and FAQs, training material and documentation, both for the DPOs themselves and for internal distribution within their EUI, as well as guidelines and online and dynamic tools. To

(a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union data protection provisions;
(b) *to ensure in an independent manner the internal application of this Regulation*; to monitor compliance with this Regulation, with other applicable Union law containing data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, the raising of awareness and training of staff involved in processing operations, and the related audits;
(c) *to ensure that data subjects are informed of their rights and obligations pursuant to this Regulation*;
(d) *to provide advice where requested as regards the necessity for a notification or a communication of a personal data breach pursuant to Articles 34 and 35*;
(e) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 39 *and to consult the European Data Protection Supervisor in case of doubt as to the need for a data protection impact assessment*;
(f) *to provide advice where requested as regards the need for prior consultation of the European Data Protection Supervisor pursuant to Article 40; to consult the European Data Protection Supervisor in case of doubt as to the need for a prior consultation*;
(g) *to respond to requests from the European Data Protection Supervisor; within the sphere of his or her competence*, to cooperate *and consult* with the European Data Protection Supervisor *at the latter's request or on his or her own initiative*;
(h) *to ensure that the rights and freedoms of data subjects are not adversely affected by processing operations*.

[26] See EDPS website : www.edps.europa.eu (please note that the wiki on the EUDPR and the Quick News are only available to DPOs).

facilitate this action, the EDPS has recently appointed a dedicated contact person who will coordinate such requests and act as the entry point between the DPO network and the EDPS.

Part III – Actions by the SA

1. **Have you already published general guidance (e.g. guides, guidelines, etc.) regarding DPOs (including before launching the coordinated action)?**
   If yes, please provide the date, link to the guidance, and a short description of the guidelines

Yes, the Position Paper on the role of Data Protection Officers of the EU institutions and bodies was published on 30 September 2018 (replacing the Position Paper of 2005)[27]. This paper covers the following aspects: designation, position, and tasks of the DPO, and relations between the DPO and the EDPS.

2. **Have you taken action (i.e., fact finding exercises, informal contact, prior consultation, investigation) towards any of the organisations concerning the designation, tasks and/or role of the DPO *prior to* launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**

EDPS actions include: fact-finding exercises (i.e. regular surveys sent to EUIs including questions on the DPO role, consultation of the DPOs on the draft DPO Position Paper), informal contacts, investigations in the context of complaints and consultations.

Outcome of these actions include: survey reports, letters, decisions, recommendations and general guidance.

No corrective measures in this context have been taken so far.

3. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**

The EDPS will use the results to feed into our ongoing discussion with the network of EUI DPOs on actions needed to further strengthen the role of DPOs and ensure their independence. A discussion on the survey results already took place at the EDPS-DPOs meeting of 30 November 2023. The DPOs discussed the results in workshops divided into three main areas: 1) designation and resources (including externalisation of tasks); 2) tasks; and 3) role and position (including conflicts of interest). The request from DPOs to receive more guidance from the EDPS, including the envisaged update of the DPO Position Paper, was also part of this discussion. The updated version will draw on the experience gained throughout the year to give more hands-on guidance, with practical examples, for both EUIs and DPOs.

[27] Available at https://edps.europa.eu/sites/default/files/publication/18-09-30_dpo_position_paper_en.pdf.

Overall, the outcome of the survey does not seem to warrant any corrective measures or investigative actions by the EDPS. Nevertheless, the EDPS may look into whether the reported cases of dismissal/penalisation require further action at this stage.

Part IV – Other

1. **What is your general impression of the levels of awareness and compliance of the organisations you consulted concerning the designation, tasks and/or role of the DPO?**

The level of awareness and compliance of the EUIs is high. Most DPOs seem to have a real impact in their EUI as they report that their advice is generally followed. The level of experience and expertise of EUI DPOs is high, a clear indication that the DPO function is becoming more and more professionalised. Most DPOs also benefit from regular training, which contributes to a high level of professionalism. Furthermore, a very large majority report that there is a written description of their tasks and that they are involved in almost all the data protection related tasks listed in the survey. Many DPOs are asked to take on additional tasks, such as developing the organisation's data protection processes, dealing with data subjects' requests to exercise their rights, or drafting/negotiating data processing agreements.

As many as 19 DPOs are full time DPOs, which implies that not only the larger institutions have a full time DPO, but also certain smaller EUIs. Involvement of DPOs is also very satisfactory, with a large majority reporting that they are consulted in 75-100% of all data protection related issues and their opinions are followed in most cases. The majority of EUIs also documents the reasons for not following the DPO's advice where applicable. Independence of DPOs seems to be respected in almost all EUIs, with only a few reporting that they receive instructions. The large majority replied that they had access to sufficient information all the time or most of the time.

Further guidance from the EDPS is requested by almost all the DPOs - Q&As/FAQs, training material and documentation, both for themselves and for internal distribution within their EUI, as well as guidelines and online tools, could be means to satisfy this demand. The recent designation of an EDPS contact point for the DPO network will also be an asset in this respect: it will not only foster efficiency and cohesion among the existing collaborative frameworks (DPO Support Group, Roundtable for DPOs, regular bilateral meetings with the DPOs of the largest EUIs, etc.), but also develop other mutually beneficial initiatives, such as training (including a possible DPO certification).

2. **Are there any other issues or topics that you would like to flag?**

As expected, the main issue for (in particular part time) DPOs seems to be a lack of resources. This translates both as a lack of time to perform their DPO duties and as lack of additional staff resources. As indicated earlier, almost half of the DPOs estimate that their resources are insufficient to fulfil their tasks. Only half of DPOs have a deputy and less than 30% have their own budget. It is potentially a cause for concern that 18 DPOs did not reply to the question how much working time they can allocate to DPO tasks and duties. If this result is caused by a reluctance to reply, this could be an indication that the DPOs fear that their honesty could have a negative impact for them. Even if retaliation in form of dismissal or penalisation remain rare cases, it is still a cause for concern that three DPOs report having been victim of such measures.

3. **Are there any leading practices of the organisations you have contacted that you would like to share?**

In accordance with Article 45(3) EUDPR, all EUIs have to adopt further implementing rules concerning the DPO. The implementing rules should in particular concern the tasks, duties and powers of the DPO. Although this is a legal requirement for all EUIs and thus not merely a practice, the EDPS believes that it may be useful also for organisations under the GDPR to adopt a written policy for defining the role and tasks of their DPO. This is also reflected in the replies where almost all of the respondents indicated that the organisation's management has clearly defined and given a written description of the DPOs tasks.

Similarly, most of the DPOs indicate that the written description of the DPO's tasks have been communicated to the personnel of the EUI.

Finally, many of the EUI DPOs issue annual activity reports that detail their work and contribute to enhancing transparency and raising awareness.

EE SA

Estonian Supervisory Authority – Data Protection Inspectorate

Part I - Statistics

Please see the consolidated figures in Appendix 1.1. The answers below may refer to the questions included in Appendix 1.1.

Part II – Substantive issues

1) The role and position of the data protection officer.

In most cases, the data protection officer is not subordinated to the highest level of management, in some cases the data protection officer is, for example, an office worker performing other tasks. Half of the respondents also stated that they do not report regularly to the management level, nor are they required to do so.

The controller or processor shall be responsible for, and be able to demonstrate, compliance with data protection requirements. Where the data controller takes decisions that do not comply with the GDPR and the data protection officer's advice, the data protection officer must be given the opportunity to make his or her dissenting opinion clearly known to the highest level of management and decision-makers. In this regard, Article 38(3) states that the data protection officer 'shall be directly subordinated to the highest level of management of the controller or processor'. Such direct subordination shall ensure that the senior management is aware of the advice and recommendations of the data protection officer that are part of the data protection officer's tasks of informing and advising the controller or processor. In situations where a person performing the duties of a data protection officer is located in an entirely different department and is directly subordinate to, for example, the head of the department, it is doubtful whether he or she will always be able to convey his/her messages to the management board. If, for example, a data protection officer tasks has been assigned to some office worker, it is also doubtful that he/she would be regularly involved, for example, in highest management meetings and that his or her presence will be ensured when decisions with data protection implications are taken.

Among other things, this kind of work management and organisational structure raises doubts as to how the autonomy of the data protection officer is guaranteed and that the data protection officer does not receive instructions for the performance of his/her duties. If a data protection officer is several steps below the highest level of management in the organisation's structure, it is doubtful that he/she will not receive instructions in his/her activities and will be able to perform his/her duties with sufficient autonomy. Of course, only the fact that a data protection officer is located in the middle or lower level of the structure may not immediately indicate that the data protection officer has no autonomy. However, the fact that half of respondents do not report to management suggests that an officer is actually reporting to someone else or not at all.

Possible solutions to the issue starts with raising awareness. Organisations need to understand what a data protection officer is doing and his/her role and responsibilities within the organisation. By understanding this, organisations will also better understand why a data protection officer's autonomy is crucial and why a data protection officer needs to be subordinated to a higher level of management.

2) The role and position of the data protection officer.

In organisations, other employees still do not understand exactly what data protection is, everything with the word 'data' in it is believed to be within the competence of the data protection officer.

The answers of some respondents showed that sometimes there is not enough knowledge about what is exactly is data protection and which questions are dealt with by a data protection officer. One of the

respondents specifically pointed out that in an organisation the role of a data protection officer is understood differently and also incorrectly. Data protection officer explained that he/she also performs tasks in the field of IT and information security, legal and compliance, and in other expert role and receives on his/her desk all tasks which, even briefly, contains the word 'data'. However, not everything related to data does not belong to the field of personal data protection, and therefore the data protection officer is expected to carry out tasks that are not actually part of his/her duties.

Such problems may concern Article 38(2) of the GDPR, which provides that the controller and processor shall support the data protection officer in the performance of his/her tasks by providing him or her with the necessary resources to carry out those tasks. Giving the data protection officer sufficient time to perform his/her duties can also be understood as a necessary resource. Otherwise, the inconsistency of priorities may result in the data protection officer's critical tasks being neglected. Giving the data protection officer sufficient time to delve into his/her duties is essential. In a situation where a data protection officer is overburdened with tasks that do not actually fall within his/her competence, it is possible to create a situation in which he/she is unable to carry out his/her duties. This, in turn, increases the risk of infringements and is detrimental to the organisation as a whole. Not to mention, it also contributes burnout.

In most cases, data protection officers also have many other tasks and data protection officers must be involved in the various processes of the organisation, but in practice, the employees of the organisation face difficulties in distinguishing between areas related to the protection of personal data and other areas related to data processing. Which may lead to the fact that the data protection officer is not involved in the necessary processes.

The awareness of data protection in organisations varies. There are also data protection officers in organisations who perceive that there has been an increase in employees and management awareness of data protection officers work what they do. The nature and necessity of data protection appears to be clearer in the public sector. However, this is not a rule of thumb either, because in the monitoring we also discovered organisations that did not have a data protection officer at all, even though the designation was mandatory for them.

It is probably still necessary, as a supervisory authority, to inform about what falls within the scope of the GDPR and what is personal data and so. But also about the duties and competences of the data protection officer.

3) The role and position of the data protection officer / the tasks and resources of the data protection officer.

Around 30 % of respondents stated that the tasks of the data protection officer have not been clearly and in written form defined by management and that the description of the tasks of the DPO has not been communicated or made known in any other way to other employees.

This may indirectly conflict with Article 38(2) of the GDPR, according to which the organisation must support the data protection officer by providing him or her with the means necessary to perform his/her duties and maintain the level of expertise and access to personal data and personal data processing operations. It is important that the appointment of a data protection officer is officially notified to all staff members and that his/her presence and duties are known throughout the organisation. The information provided to staff could clearly indicate the exact tasks and scope of the data protection officer's tasks. The formal notification of the appointment of a data protection officer to all staff members ensures that his/her presence and duties are known throughout the organisation. A lack of knowledge and understanding within the organisation of what a data protection officer is doing, what his/her tasks and the fact that a data protection officer has been appointed at all makes it difficult for the DPO to carry out his/her work and perform the assigned tasks.

As a positive fact, it can be pointed out that in most cases, the tasks of data protection officers are still defined in the employment contract. A more problematic issue in general is how the information about the tasks and their scope is communicated to, for example, other employees and management. Several working parties have also recommended that the data controllers should clearly indicate the precise

tasks and scope of the data protection officers' tasks, both in the data protection officers' contract, but also in the information provided to staff and management (and, where appropriate, to other stakeholders).

To the extent that data protection officers perform tasks other than data protection, it is particularly important that tasks are defined in writing. Otherwise, the inconsistency of priorities may result in the data protection officer's tasks being neglected. In addition, this increases the risk of a data protection officer not being involved in the necessary processes early enough.

It is also worth determining how much time is needed to perform the tasks of the data protection officer and what is the priority level of the data protection officer's tasks. According to that, a work plan should be also drawn up.

In particular, this problem could be solved by more communication at the level of society and the state. The role of the data protection officer still needs to be clarified. In most cases, however, it all starts from the management and how the need for a data protection officer in the management is perceived. The problem could also be solved by improving intra-organisational communication.

4) The designation, knowledge and experience of the data protection officer.

Only half of respondents replied that expert knowledge of data protection regulation and expert knowledge of data protection practices were also critical when hiring a data protection officer. However, almost all respondents said that ability to fulfil the tasks in accordance with the GDPR was required to appoint a data protection officer. 12 % of respondents said that no particular expertise on data protection was required, but the appointment of data protection officer was compulsory.

However, this may also be related to the fact that half of the respondents' data protection officers had 3-5 years of experience in the organisation's field of activity and 70 % of respondents had 3-5 years or more in the field of data protection. This means that they were hired when the General Data Protection Regulation came into force or some time after that. It was probably more difficult to find competent people back then, and the threshold was set lower. The necessary level of professional knowledge is not directly determined by the General Data protection Regulation and it should be determined in accordance with the data processing operations. The level of knowledge must be commensurate with the sensitivity, complexity and amount of the data processed by the organisation. Otherwise, the data protection officer may not be appointed under the conditions set out in Article 37(5) GDPR. As said, where the processing of data is particularly complex or involves a large amount of sensitive personal data, the DPO may need more expertise. Nearly half of the respondents had worked in the organisation's field of activity for 3-5 years. 18 % of respondents had worked for 1-2 years and the same number (18 %) for over 8 years. This kind of long-term work experience is positive, as knowledge of the business sector and organisation is always beneficial. The data protection officer should also be well aware of the data processing activities, information systems, data security and data protection needs of the controller. In general, mostly the tasks of the data protection officers are assigned to some existing staff members, which is positive in the sense that they have experience, but a lack of data protection knowledge may make it more difficult for the data protection officers to work, as this is a rather complex and specific area.

The number of top specialists working in the field of data protection in Estonia may still be limited due to the lack of training for high-level data protection officers. In addition, such training is mostly expensive and would mostly require financial support from the employer. This, on the other hand, puts employers in a situation where they may not have enough choice in the labour market. The best solution is to hire an existing employee. This is a bigger and more complex problem, but as one possible solution would also be to provide a high level of data protection education at national level.

5) The tasks and resources of the data protection officer.

While working on a full-time basis, less than half can fully focus on the tasks of the data protection officer, and 40 % of the data protection officers who replied to the questionnaire considered that the

resources allocated (number of subordinates, number of working hours) are not sufficient to perform the tasks assigned to the data protection officer.

Article 38(2) GDPR provides that an organisation must support the data protection officer by providing him/her with the necessary resources to carry out his/her tasks. Depending on the processing operations and the activities and size of the organisation, the necessary means can be understood, inter alia, as sufficient time to perform the tasks of the data protection officer, as well as adequate financial support hiring personnel. On the one hand, it is not surprising that we received such answers and results because the workload of data protection officers is enormous.

Only about half of the data protection officers working in the public sector feel that the resources allocated are sufficient to carry out their tasks. In the private sector, therefore, data protection officers feel somewhat greater support from the management of the organisations. Public sector institutions are mostly large, with a wide variety of sectors of activity and a higher number of data subjects, as services are mostly aimed at all country citizens.

In order for data protection officers to be fully committed to their work tasks and to be able to perform them at sufficient level, larger organisations should hire another data protection officer in addition to already working data protection officer. As a positive example, one of the monitored organisations, which is a large public sector institution and therefore also a very large data controller, already has two data protection officers working. One ministry also pointed out that they are hiring an additional person to help the data protection officer. As a side note, it should be kept in mind that Estonia is a small country and the number of public employees is always kept low here, so this is a positive example where, despite this trend, the need for a data protection officers has been understood.

As one idea and option, there could be some kind of questionnaire or indicator, by answering which, based on the result, it would be possible to assess how likely the organisation needs more than one data protection officer. The Estonian Data Protection Inspectorate has made similar control questions to data controllers, for example regarding privacy policies, and on the basis of this, data controller can check whether their privacy policy covers everything necessary. It may be that in those organisations where the data protection officers themselves feel that it is necessary to hire more personnel, but the management has not done it, the management does not understand the workload of the data protection officer, and the data protection officer alone obviously cannot convince them of this either. Such questionnaire would allow the managements of the organisations to get a so-called external opinion, which may seem more impartial to them.

Part III – Actions by the SA

1. **Have you already published general guidance (e.g. guides, guidelines, etc.) regarding DPOs (including before launching the coordinated action)?**
   If yes, please provide the date, link to the guidance, and a short description of the guidelines

Circular letter. In this circular letter, we briefly pointed out why a data protection officer is essential and which organisations must definitely appoint one. This circular letter was sent to public sector data processors who did not have a designated data protection officer according to the e-business register. Date of publication of the circular letter 23.08.2023 https://www.aki.ee/sites/default/files/ringkiri_i.pdf.

Guide/article on our website ('Data protection officer'). On this page, we describe the tasks of the data protection officer, who can be in this role, and what his/her competencies and skills should be. You can also read on the same page as (clicking to the red flag) how to notify of data protection officer and also read about the trainings offered by different higher education institutions. Date of publication or amendment of the guide 30.07.2019 - https://www.aki.ee/et/eraelu-kaitse/andmekaitsespetsialist.

Guide/article on our website ('Who must appoint a data protection officer?'). In this article, we describe who is obliged to appoint a data protection officer under the GDPR. What is a 'core activity', what is a 'regular and systematic monitoring of data subjects', which data processing can be understood 'as on a large scale', etc. Date of publication or amendment of the guide 14.05.2020 - https://www.aki.ee/et/eraelu-kaitse/andmekaitsespetsialist/kes-peavad-maarama-andmekaitsespetsialisti.

Guideline 'General instructions for the controllers or processors'. The general guideline is – as the name suggests – a collection of explanations about GDPR overall. It is aimed at all processors and controllers. Date of publication or amendment of the guideline 13.03.2019/02.12.2019 - https://www.aki.ee/sites/default/files/dokumendid/isikuandmete_tootleja_uldjuhend.pdf (PDF file), https://www.aki.ee/et/isikuandmete-tootleja-uldjuhendi-veebitekst (web text).

2. **Have you taken action (i.e., fact finding exercises, informal contact, prior consultation, investigation) towards any of the organisations concerning the designation, tasks and/or role of the DPO *prior to* launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**

We do not have specific statistics on such actions. But we have had an investigation where we inspected whether the data protection officer had been granted independence in the performance of his/her duties and whether the data protection officer was released from the workplace in violation of the GDPR (for performing his/her tasks and duties). We terminated the investigation with a warning.

3. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**

Specific actions are not planned yet. We plan actions in more detailed after the results of the monitoring have been consolidated. We are probably planning to publish articles and guidelines, perhaps we plan to organise some kind of meetings for data protection officers.

Part IV – Other

1. **What is your general impression of the levels of awareness and compliance of the organisations you consulted concerning the designation, tasks and/or role of the DPO?**

Based on answers we have received, level of awareness and the position of data protection officers could be better.

2. **Are there any other issues or topics that you would like to flag?**

No.

3. Are there any leading practices of the organisations you have contacted that you would like to share?

No.

EL SA

Hellenic Supervisory Authority – Hellenic Data Protection Authority

Part I - Statistics

Please see the consolidated figures in Appendix 1.1. The answers below may refer to the questions included in Appendix 1.1.

Part II – Substantive issues

The Hellenic Supervisory Authority at this point can identify mainly issues relating to the above highlighted categories[28] and more precisely issues that arise from a prima facie analysis of the replies to questions is 12, 13, 14, 24, 25, 26, 29, 30, 32, 33 and 37 of the questionnaire. In other words, the emerging issues stem from the application of Articles 37 – 39 GDPR and corresponding Articles 6-8 of national Law 4624/2019 on measures for implementing 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 transposition of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016, on data protection. Since the Hellenic Supervisory Authority is participating in this coordinated action by conducting also a formal investigation in 31 public bodies, an in depth analysis as well as the required follow up with letters and requests for documentation in order to substantiate the replies provided to the questionnaire are necessary both for the formal investigation and for providing answers to this Part II – substantive issues. The process of the formal investigation is still on early stage and therefore we are currently unable to relay more information.

Part III – Actions by the SA

1. **Have you already published general guidance (e.g. guides, guidelines, etc.) regarding DPOs (including before launching the coordinated action)?**
   If yes, please provide the date, link to the guidance, and a short description of the guidelines

No.

2. **Have you taken action (i.e., fact finding exercises, informal contact, prior consultation, investigation) towards any of the organisations concerning the designation, tasks and/or role of the DPO *prior to* launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**

No.

3. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If**

[28] Please see the full wording of this question.

possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)

As mentioned above, the Hellenic Supervisory Authority is conducting a formal investigation and consequently it is not possible to give an overall indication of the actions to be taken as a result of the outcome of the investigation. Still, it is high likely that measures such as recommendations and possible corrective ones will be issued.

However, we can inform you at this stage that in three cases out of the 31 questionnaires that the Hellenic Supervisory Authority sent out to public bodies, where the Hellenic Supervisory Authority did not receive replies, the Hellenic Supervisory Authority's Board will convene in order to issue a decision where the application of corrective measures for the infringement of Article 31 GDPR (cooperation with the supervisory authority), according to Article 58 (2) GDPR will be considered. In two out of the these three cases there is no appointment of DPO and therefore this infringement will also be considered by the Hellenic Supervisory Authority's Board resulting in these cases too in the application of correctional measures or even an administrative fine. Please note that this also relates to the replies provided in question 4, in the sense that it explains why there was no organisation replying that they had not designated a DPO, as two public bodies that had not appointed DPO did not reply to the questionnaire at all.

Furthermore, due to the high number of public bodies that are formally being investigated, it is not possible to provide you at this point with a time frame of the conclusion of the investigation.

Part IV – Other

1. **What is your general impression of the levels of awareness and compliance of the organisations you consulted concerning the designation, tasks and/or role of the DPO?**

Even though it is – as mentioned above - still early stages of the ongoing formal investigation, the general impression is that in many aspects of the DPO's role, position and tasks awareness and compliance is rudimentary. There is definitely plenty of room for improvement.

2. **Are there any other issues or topics that you would like to flag?**

No.

3. **Are there any leading practices of the organisations you have contacted that you would like to share?**

No.

ES SA

Spanish Supervisory Authority – Agencia Española de Protección de Datos (AEPD)

Part I - Statistics

Please see the consolidated figures in Appendix 1.1. The answers below may refer to the questions included in Appendix 1.1.

Part II – Substantive issues

1) The designation, knowledge and experience of the DPO

According to the answers provided, 86% of respondents were not staff members, which confirm the figures ES SA have following the communication procedure of DPO contact information. In our view this figure could be a confirmation that a significant number of organisations contract external DPOs, which in some cases could show a weakness since some designated DPO could be in charge of several entities sharing resources among them and increasing the risk that the role of DPO can be consider as a formality to be accomplished instead a real and proactive involvement of the DPO in the data processing carried out by the organisations.

Regarding the duration of DPOs appointments, the pool shows that 58% of respondents have a permanent relationship with the controller which shows an important number of temporary appointments which could correlate with the numbers of external DPO. This issue about temporary appointments can correlate with the fact explaining in the previous paragraph and may reinforce one of our greatest concerns in this field in relation to the risk that controllers prioritize a formal designation of the DPO in order to cover the legal requirement instead a true proactive commitment on their part.

The rest of the responses to the questions raised in this section show answers that can be qualified as 'expected'.

2) The tasks and resources of the DPO

At first glance, most of the responses shown in this section show a fairly positive situation of the DPOs in terms of availability of resources that may also have its not so positive aspects.

3) The role and position of the DPO

The responses given in this section show, perhaps, a more realistic panorama with some aspects to be improved such as the participation of the DPO in all issues in which the processing of personal data is involved.

4) Guidance of the Supervisory Authority

As stated in our comment to question 41, just a few answers have been provided indicating that in general terms respondents considered appropriate the guidance, Q&A/FAQs, online tools, guidelines as well as the publication of the opinions and decisions provided in the web page of the ES SA.

Part III – Actions by the SA

1. **Have you already published general guidance (e.g. guides, guidelines, etc.) regarding DPOs (including before launching the coordinated action)?**
   If yes, please provide the date, link to the guidance, and a short description of the guidelines

No actions have been taken prior to launching the coordinated action.

2. **Have you taken action (i.e., fact finding exercises, informal contact, prior consultation, investigation) towards any of the organisations concerning the designation, tasks and/or role of the DPO *prior to* launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**

For the moment no actions have been planned based on the results of this coordinated action beyond those that are already planned, such as holding sectoral meetings with the DPOs of those most relevant sectors from the point of view of the processing of personal data and that the Spanish SA carries out on a regular basis: education, health, assurance and financial, telecommunications, etc.

In addition, Spanish SA will continue to develop guidelines and tools in several data protection fields in order to assist controllers, processors and DPOs to fulfil their obligations under GDPR.

3. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**

The Spanish SA will continue to develop the tools, meetings, and consultation channels it has been promoting since the entry into force of the GDPR to support DPOs so that they can develop their work with the appropriate resources and means in order to ensure their independence.

Part IV – Other

1. **What is your general impression of the levels of awareness and compliance of the organisations you consulted concerning the designation, tasks and/or role of the DPO?**

In general terms, we consider the results shown in the survey very positively and we trust that it has also served to make controllers, processors and also DPOs aware of the importance and scope of the obligations under GDPR. At the same time, the Spanish SA considers that it is necessary to continue insisting that data controllers become aware of the importance of the DPO's role in ensuring compliance with data protection regulations as well as the necessity to provide resources, in terms of training and budget, in the fulfilment of their tasks.

To this end, the Spanish SA will continue to develop guidelines and tools to assist those controllers and DPOs in order to comply with the GDPR.

In addition, the Spanish SA will continue to respond to queries directly raised by DPOs in the query channel established for this purpose.

2. Are there any other issues or topics that you would like to flag?

No issues or topics to flag at this moment.

3. Are there any leading practices of the organisations you have contacted that you would like to share?

No additional comments.

FI SA

Finnish Supervisory Authority – Office of the Data Protection Ombudsman

Part I - Statistics

Please see the consolidated figures in Appendix 1.1. The answers below may refer to the questions included in Appendix 1.1.

Part II – Substantive issues

1) The tasks and resources of the data protection officer

In many cases the organisation's management hasn't made a clearly defined and written description of the data protection officer's tasks. In addition, there seemed to be failures in the organization'' personnel being made aware of the tasks and duties of the data protection officer via the written description or otherwise.

- Relates to Articles 39(1) and 38(6) GDPR.
- The tasks and duties of the data protection officer in the organisation should be clearly defined in a written document. This document can be used to clarify the cases in which the data protection officer can be consulted.

The data protection officer has often been entrusted with other tasks in addition to those under the GDPR. This may lead to potential conflicts of interest.

- Relates to Article 38(6) GDPR.
- The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.
- Based on the questionnaire's replies, conclusions cannot be drawn directly from the assignment of other tasks to the data protection officer, but the examination of potential conflicts of interest must be carried out on a case-by-case basis.

Based on the questionnaire, the resources allocated to fulfil the tasks of the data protection officer are often deemed insufficient. A deputy is also not always designated for the data protection officer.

- Relates to Article 38(2) GDPR.
- Insufficient resources allocated to the tasks of the data protection officer and absence of deputy can contribute to weakening e.g. the timely exercise of data subjects' rights.

2. The role and position of the data protection officer

Based on the questionnaire, the organisations have challenges and deficiencies in making sure the data protection officer is involved and/or consulted when the organisation is handling and solving issues relating to the processing and protection of personal data.

- Relates to Article 38(1) GDPR.
- The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues that relate to the protection of personal data.
- In the questionnaire, there is a variation between the data protection officers' views on how they are involved and/or consulted on the aforementioned issues. Some of the data protection

officers feel that the consulting is done very well, while others feel they are not consulted in a sufficient way.

- If the data protection officer is not consulted and/or involved in the handling and solving issues relating to the processing and protection of personal data, the decisions being made might not take into account all the requirements set out in the GDPR or other data protection legislation.

Based on the questionnaire, all data protection officers are not required to report regularly to the highest management level of the organisation, nor does it always report on a voluntary basis.

- Relates to Article 38(3) GDPR.
- If regular reporting is not done to the highest management level of the organisation, the management is unlikely to receive sufficient information on the work carried out by the data protection officer within the organisation or on data protection issues in general.

Part III – Actions by the SA

1. **Have you already published general guidance (e.g. guides, guidelines, etc.) regarding DPOs (including before launching the coordinated action)?**
   If yes, please provide the date, link to the guidance, and a short description of the guidelines

The FI SA publishes general guidance for data protection officers on its website (https://tietosuoja.fi/tietosuojavastaavat):

- Tasks of the data protection officer -section
- Designating a data protection officer -section
- Instructions for organisations that have designated a data protection officer
- Instructions for communicating the contact details of the data protection officer to the FI SA
- Frequently asked questions (FAQ) on data protection officers -section
- Internet links for more information outside the FI SA website.

In addition, the FI SA publishes an electronic newsletter (https://tietosuoja.fi/uutiskirje) about six times a year, aimed at data protection officers.

In addition to the written material the FI SA provides telephone guidance for data protection officers (https://tietosuoja.fi/puhelinneuvonta): Telephone guidance service provides general guidance and support in matters involving data protection and lets you know if the case requires more detailed investigation and processing at the FI SA Office.

2. **Have you taken action (i.e., fact finding exercises, informal contact, prior consultation, investigation) towards any of the organisations concerning the designation, tasks and/or role of the DPO *prior to* launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**

Discussions with organisations and data protection officers providing general advice.

The FI SA participates and lectures in seminars and training sessions in which data protection officers also participate.

3. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**

The FI SA has not yet decided what actions will be taken in this matter. The option of taking actions related to the Coordinated Enforcement Action is still open.

The FI SA does recognise the importance of sufficient knowledge of the data protection officer's role and tasks in the designating organisation and the compliancy to the legislation concerning data protection officer.

It should be noted that an administrative fine cannot be issued to public authorities in Finland at the moment. However, the Programme of the Finnish Government (2023) states that provisions on administrative fines for breaches of information security will be laid down in such a manner that they will apply equally to both the public and private sector.

Part IV – Other

1. **What is your general impression of the levels of awareness and compliance of the organisations you consulted concerning the designation, tasks and/or role of the DPO?**

The organisations of the data protection officers who responded to the questionnaire represent different sectors. Organisations differ from one another and e.g. the number of their employees varies considerably.

The resources for data protection work in organisations vary. This may contribute to a variation between organisations and sectors in the level of data protection work on the designation, tasks and role of data protection officers as well as in the overall information on data protection.

Generally, shortcomings in data protection work carried out by data protection officers can often be identified. Based on the questionnaire, only in few replies was the level of data protection work with regard to data protection officers considered to be completely unproblematic.

2. **Are there any other issues or topics that you would like to flag?**

N/A

3. **Are there any leading practices of the organisations you have contacted that you would like to share?**

N/A

FR SA

French Supervisory Authority – Commission Nationale de l'Informatique et des Libertés (CNIL)

Part I - Statistics

Please see the consolidated figures in Appendix 1.1. The answers below may refer to the questions included in Appendix 1.1.

Part II – Substantive issues

Issue 1: Sufficient time to fulfil DPO's duties

1. One issue identified in our investigations is the fact that several DPOs do not have sufficient time to fulfill their duties.
2. This issue concerns Article 38(2) of the GDPR, that requires the organization to support its DPO by 'providing resources necessary to carry out [their] tasks'.
3. In certain cases, it would have been appropriate for the DPO to be supported with a team, but the organizations decided not to hire data protection specialists other than the DPO.
4. This issue can take very different forms in the different organizations: for instance, a DPO can work full-time, receive the assistance of a team, and still lack the necessary time resources to manage their missions. However, we noted that this issue was more frequent when the DPO was shared between organizations.
5. Possible solutions to this issue are:

- For data protection authorities: To remind data controllers of their obligations under the GDPR (in particular Article 38 of the GDPR).
- For data protection authorities: To publish an 'engagement letter' template. Such document could be given by organizations to the DPO when they take up their post. This document should stipulate in particular that the organization must support its DPO by providing resources necessary to carry out their tasks, and specify what these resources are. The CNIL already published such document; this document is available at https://www.cnil.fr/sites/cnil/files/atoms/files/cnil-gdpr_practical_guide_data-protection-officers.pdf (Appendix 2: mission statement template to be given by the organization to the DPO).
- For organizations/DPOs: To formalize the DPO duties and conditions for performing the DPO's duties in an 'engagement letter'.
- For organizations/DPOs: establishment of an internal network of 'data protection intermediaries' that can report data protection issues to DPO.
- For organizations/DPOs: To draft a work plan, presented by the DPO to the data controller in order to agree on the DPO's objectives and DPO's resources, and to prioritize the DPO's tasks.

Issue 2 : DPO's qualifications and training

1. An issue identified in our investigations is the fact that some organizations do not seem to have designated their DPO on the basis of professional qualities, in particular knowledge of data protection law.

In addition, it was noted the insufficiency, or the absence of training for some DPOs, despite the fact that DPOs must be given the opportunity to stay up to date with regards to developments within the field of data protection.

2. These issues concern Articles 37(5) and 38(2) of the GDPR.
   Article 37(5) of the GDPR provides that 'the data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39'.
   In addition, Article 38(2) of the GDPR provides that 'the controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge'.
3. We found that companies sometimes had to choose between experts in data protection and experts in the particular field they are working in. Finding people who have expert knowledge in, for instance, aviation laws and data protection laws can still prove difficult for organizations.
4. We noted that DPOs come from varied background (technical, law, archivist, etc.) which is beneficial for the profession.
5. Possible solutions to this issue are:

- For organizations/DPOs: in France, organizations can designate DPO holding a DPO certification (even if it is not compulsory to be certified in order to be designated DPO). Since 2018, in order to support organizations in identifying the appropriate profile, the CNIL has approved organizations that issue a DPO skills certification[29] on the basis of its reference system, and keeps a list of such organizations.
- For data protection authorities: To publish an 'engagement letter' template: this document should stipulate in particular that the DPO 'must benefit from regular training allowing them to maintain their specialized knowledge in the field of data protection'. As stated above, the CNIL already published such document.
- For data protection authorities: To publish and translate tools for training (the CNIL has published numerous content, such as workshops or webinars, and online training (MOOC)). We noted that trainings provided (for free) by data protection authorities were very well received by DPOs.
- For data protection authorities: To work in connection with universities and business schools on an inventory of DPO training courses.
- For organizations/DPOs: To formalize the DPO duties and conditions for performing the DPO's duties in an 'engagement letter'.
- For organizations/DPOs: To draft a 'training plan'.
- For organizations/DPO: to provide a multi-fields team of people working with the DPO to support its activities and knowledge.

<u>Issue 3 : Involvement of the DPO in all issues relating to the protection of personal data and access to other services of the organization</u>

1. Another issue identified in our investigations is that some DPOs are not involved in issues relating to data protection, and do not have access to other services (such as HR, IT…) and consequently do not receive information and support from those services.
2. Article 38(1) of the GDPR provides that the controller and the processor shall ensure that the DPO is 'involved, properly and in a timely manner, in all issues which relate to the protection of personal data'. Article 38(2) of the GDPR provides that 'the controller and processor shall

[29] Available at https://www.cnil.fr/fr/certification-des-competences-du-dpo-0.

support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations'.

3. This issue entails that the DPO does not have sufficient information on some data processing operations put in place in their organization. It can also signify that the DPO will not be involved at the earliest stage of the decisions on data processing, for instance when he or she is not involved in strategic meeting. This is detrimental as it is easier (and, in fact, mandatory to comply with data protection by design requirement) to implement data protection principles from the start of a project.
4. We found that organizations differ on this matter in the way that they have or have not formalized how and when the DPO should be involved: in some instances, the process is very detailed and communicated to all employees, in other cases it is only an informal practice.
5. Possible solutions to this issue are:

- For data protection authorities: To publish an 'engagement letter' template: this document should stipulate that the DPO has access to processing operations and personal data within his organization. As stated above, the CNIL published such a document.
- For organizations/DPOs: To formalize the DPO duties and conditions for performing the DPO's duties in an 'engagement letter'.
- For organizations/DPOs: To implement internal procedures within the organization's governance, in order to ensure that the DPO is involved from the earliest stage possible in all issues relating to data protection (for instance, exercise of rights, data breaches…), and communicate such procedures within the organization.

Issue 4: Data protection audit and access to personal data and processing operations

1. Another issue identified in our investigations is that DPOs can have difficulties in carrying out data protection audits, in particular when he or she does not have access to processing operations and personal data within his organization.
2. This issue concerns in particular article 38(2) and article 39(1)b) of the GDPR.
   Article 38(2) of the GDPR requires the organization to support its DPO by 'providing resources necessary to carry out [their] tasks and access to personal data and processing operations'.
   Article 39(1)b) of the GDPR provides that 'the data protection officer shall have at least the following tasks: […] (b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits'.
3. We noticed that organizations very rarely formalize how their DPO can audit already existing data processing. The emphasis is commonly put on involving the DPO in the conception of new processing but the review of existing process lacks proper documentation, in particular with respects to the way DPOs can access or require access to databases.
4. N/A, this was observed across organizations.
5. Possible solutions to this issue are:

- For data protection authorities: To publish an 'engagement letter' template (see above).
- For organizations/DPOs: To formalize the DPO duties and conditions for performing the DPO's duties in an 'engagement letter'.
- For organizations/DPOs: To draft an internal document formalizing the cases and the conditions under which the DPO's access will be carried out (e.g., audit, data breaches, etc.).

Issue 5: Safeguards enabling DPOs to perform their tasks in an independent manner

1. Another issue identified during our investigations is that some organizations did not properly ensure the independence of their DPO.
2. Article 38(3) provides that controllers/processors are required to ensure that the DPO 'does not receive any instructions regarding the exercise of [his or her] tasks. He or she shall not be dismissed or penalized by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor'.
3. We did not find any cases where the DPO has been penalized or dismissed by the controller or the processor for performing their tasks. However, we found that no safeguards had been put in place to prevent such a decision to occur. While this is not in itself a breach of GDPR, it is problematic that no protections against unlawful dismissal are put in place, as this subject should be tackled before the problem arises.
4. This has been observed in a majority of organization. However, the subject was addressed in some engagement letters or deontological charters.
5. Possible solutions to this issue are:

- For data protection authorities: To remind data controllers of their obligations under the GDPR (including Article 38 of the GDPR and the independence of the DPO), in particular when a new DPO is designated.
- For data protection authorities: To publish an 'engagement letter' template (see above).
- For organizations/DPOs: To formalize the DPO duties and conditions for performing the DPO's duties in an 'engagement letter'.
- For organizations/DPOs: To draft an annual report of the DPO's activities provided to the highest management level; and to present once per year this report to the highest level of the organization.
- For DPOs: in the event of independence issues, the DPO may collect information on this independence issue.

Part III – Actions by the SA

1. **Have you already published general guidance (e.g. guides, guidelines, etc.) regarding DPOs (including before launching the coordinated action)?**
   If yes, please provide the date, link to the guidance, and a short description of the guidelines

First of all, the CNIL's website contains a 'hub' regarding DPOs topics[30]. This hub contains information concerning the designation[31], the role[32] or the certification of the DPO[33]. Moreover, some contents concern DPOs in specific sectors (for instance, the designation of a DPO in territorial authorities[34]).

It should be noted that in 2019, the French Ministry of Labour decided to work alongside several organizations, including the CNIL, in order to launch **an online research** on the function of DPO. Three

[30] Available at https://www.cnil.fr/fr/le-delegue-la-protection-des-donnees-dpo.
[31] Available at https://www.cnil.fr/fr/designation-dpo.
[32] Available at https://www.cnil.fr/fr/devenir-delegue-la-protection-des-donnees.
[33] Available at https://www.cnil.fr/fr/certification-des-competences-du-dpo-0.
[34] Available at https://www.cnil.fr/fr/designer-un-delegue-la-protection-des-donnees-dans-une-collectivite.

editions of this research took place in 2019, 2020 and 2021-2022. The 2021-2022 edition is based on a survey of 1811 DPOs designated by the CNIL, interviewed between September and October 2021[35]. This research reveals in particular the diversification of profiles of DPOs (47% of DPOs come from fields of expertise other than legal and IT) and an important decrease in training (1/3 had not received any GDPR training since 2016).

From now on, this annual study looks more like an observatory of the profession of DPOs. Many researchers join the scientific committee in order to deepen knowledge of the profession of DPOs, and interactions with their ecosystem (economic, working relationships…).

In addition, the DPOs can rely on resources available on the CNIL's website[36]. DPOs can also attend GDPR presentation days ('Journées RGPD') and thematic information workshops, including via webinars[37].

DPOs can in addition use the online training (MOOC) published by the CNIL for the first time in March 2019[38]. This training, on the fundamentals of data protection, is open to all and free of charge.

Moreover, it should be noted that since 2018, the CNIL has approved organizations that issue a DPO skills certification on the basis of its reference system, and keeps a list of such organizations. Even if it is not mandatory to be certified in order to be designated DPO, certification presents various advantages (for its holder, certification constitutes a proof of their adequacy with the level of knowledge requirement imposed by the GDPR; for organizations looking for profiles of data protection experts, certification represents a guarantee of confidence).

Finally, on March 14, 2022, the CNIL published a reference guide for questions about the data protection officer[39]. With the help of many professional associations, the CNIL has gathered in this guide the most important and useful knowledge about the DPO.

This guide is organized in four parts:

- The role of the DPO;
- Appointing a DPO;
- Performing the function of DPO;
- CNIL's support for DPOs.

Each topic is illustrated by concrete examples and answers to frequently asked questions on the subject. From their appointment to the end of their mission, this guide provides essential and precise information about the DPO. The CNIL has been particularly careful to provide clear information on how to ensure that the DPO can carry out their tasks independently, without any conflict of interest and with real efficiency for the organization.

2. Have you taken action (i.e., fact finding exercises, informal contact, prior consultation, investigation) towards any of the organisations concerning the designation, tasks and/or role of the DPO *prior to* launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the organisation, general

[35] Available at https://travail-emploi.gouv.fr/IMG/pdf/synthese_dpo.pdf.
[36] Available at https://www.cnil.fr/fr/professionnel.
[37] The agenda of these events is available at https://www.cnil.fr/fr/actualites/agenda on the CNIL's website.
[38] Available at https://www.cnil.fr/fr/le-mooc-de-la-cnil-est-de-retour-dans-une-nouvelle-version-enrichie.
[39] Available at https://www.cnil.fr/en/cnil-publishes-guide-dpos.

guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).

No actions had been taken towards the fifteen organisations prior to launching the coordinated action.

However, the CNIL has already taken corrective measures towards other organizations regarding the designation and the role of the DPO. For instance, twenty-two cities were ordered to appoint a DPO in May 2022. In another case, the CNIL found that an organisation was in violation of Article 38(4) of the GDPR because the DPO was not allowed access to the email inbox receiving data subjects' requests.

3. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**

The decisions regarding the outcome of the investigations have yet to be made by the CNIL's President.

The CNIL is currently considering an action plan to improve the conditions under which the DPO is appointed and the conditions under which he or she can carry out his or her duties.

Part IV – Other

1. **What is your general impression of the levels of awareness and compliance of the organisations you consulted concerning the designation, tasks and/or role of the DPO?**

The coordinated action cemented our opinion that conducting investigation on the compliance with Articles 37, 38 and 39 of the GDPR is more complex than for some other articles. Indeed, targeting the right organizations is challenging unless there has been a formal complaint by the (ex-)DPO.

Furthermore, establishing breaches with Articles 38 and 39 requires a thorough analysis (for instance, to prove that the resources given to the DPO are insufficient).

2. **Are there any other issues or topics that you would like to flag?**

In order for the profession of DPO to be well identified and understood, it could be interesting to launch an annual survey on the DPO role at European level across EU countries. As part of this survey, numerous DPOs designated in EU countries could be interviewed. This work could be helped by the survey launched in France in 2019 by the French Ministry of Labour (cf. Part III, Question 1 of this report), and could be a prerequisite for a potential revision of the Guidelines on Data Protection Officers (wp243rev.01), dated October 2017.

In France, a recent study (‘Saving Private DPO’) was published by a former DPO (Bruno Rasle) in May 2023. As part of this study, 26 DPO were interviewed. These DPOs were all in serious difficulty, sometimes isolated or dismissed. The objective of this work is to identify the reasons of these difficulties and understand if there are similarities, and to make proposals to prevent and manage these situations if they occur. The study is available at https://afcdp.net/media/documents/il-faut-sauver-le-soldat-dpo-bruno-rasle-5-mai-2023.pdf (an English version of this study is available on request).

It could be interesting for the EDPB to launch a study on the DPO (qualifications, scope of tasks, independence, training…) in all EU countries, in order to observe developments and trends. This study could be quite similar to the study launched in France (cf. Part III, Question 1). As a reminder, in 2019, the French Ministry of Labour decided to work alongside several organisations (including the National Agency for Vocational Training (or AFPA) and the CNIL) in order to launch an online research on the function of DPO. Three editions of this research took place in 2019, 2020 and 2021-2022. The 2021-2022 edition is based on a survey of 1811 DPOs designated by the CNIL, interviewed between September and October 2021. This research reveals in particular the diversification of profiles of DPOs (47% of DPOs come from fields of expertise other than legal and IT) and an important decrease in training (1/3 had not received any GDPR training since 2016).

3. Are there any leading practices of the organisations you have contacted that you would like to share?

In our investigations, we observed the following practices that seemed to prove beneficial for the DPO and his/her organization:

- 'Engagement letter': this document formalizes the tasks entrusted to the DPO and is usually given by the organization to the DPO when he/she takes up their post. It is important for Supervisory Authority to encourage DPO's tasks to be supported or highlighted. The CNIL published a template of 'engagement letter'; this template is available at https://www.cnil.fr/sites/cnil/files/atoms/files/cnil-gdpr_practical_guide_data-protection-officers.pdf (Appendix 2). This engagement letter can be communicated to the employees of the organizations to facilitate the involvement of the DPO in all matters relating to data protection.
- Using the document entitled 'The key questions to ask yourself when appointing a DPO', published by the CNIL in the reference guide on data protection officer in March 2022 (Appendix No.1 of the reference guide)[40]: this document helps the organization verifying that the GDPR requirements for a future DPO are met.
- An annual work plan presented by the DPO to the data controller in order to agree on the DPO's objectives and DPO's resources, and to prioritize DPO's tasks.
- An annual report of the DPO's activities provided to the highest management level and a presentation once per year of this report to the highest level of the organization.
- Establishment of an internal network of points of contact within the organisation, and organisation of regular meetings with the DPO and these contact points: these 'data protection intermediaries' report data protection issues to the DPO (such as projects, questions, or request to exercise rights), and provide operational support to the DPO.
- Implementation of internal procedure within the organization's governance, in order to ensure that the DPO is involved from the earliest stage possible in all issues relating to data protection (for instance, exercise of rights, data breaches…). This procedure should be communicated within the organization.
- Becoming a member of an association of Data Protection Officers is a leading practice for DPO, in order to prevent isolation and benefit from good practices.
- A training plan for the DPO should be scheduled, adapted to the profile of the DPO.

[40] Available at https://www.cnil.fr/en/cnil-publishes-guide-dpos.

- The use of the Supervisory Authority's online training (for instance the CNIL's MOOC[41] or webinars[42]) by DPO to train themselves, and also employees of the organization on the GDPR.

[41] Available at https://www.cnil.fr/fr/le-mooc-de-la-cnil-est-de-retour-dans-une-nouvelle-version-enrichie.
[42] Available at https://www.cnil.fr/fr/comprendre-le-rgpd/les-webinaires-de-la-cnil-le-programme-de-septembre-decembre-2023.

HR SA

Croatian Supervisory Authority – Croatian Personal Data Protection Agency (AZOP)

Part I - Statistics

Please see the consolidated figures in Appendix 1.1. The answers below may refer to the questions included in Appendix 1.1.

Part II – Substantive issues

1) Role of a DPO in the organisation (potential conflict of interest)

1. 113 DPOs when asked about the role in the organisation stated that they are directors/head of various departments, like HR department, Marketing department and other roles that could cause the conflict of interest. A significant number of DPOs come from the highest management within the organisations, there is a great possibility that such tasks and duties could result in a conflict of interests.
   7.46 % (226) of respondents stated that DPO comes from the highest management.
   13.39% (406) of DPOs didn't give answer to this question.
2. Article 38 (6) of the GDPR.
3. A significant number of DPOs come from the highest management within the organisations, there is a great possibility that such tasks and duties could result in a conflict of interests. 113 DPOs are performing at the same time roles as i.e. directors, heads of various departments where they determine means and purposes of processing of personal data.
4. There is a great difference between public authorities and private sector. In most cases, DPOs who might be in conflict of interest are coming from public authorities.
5. A comprehensive resolution to these issues involves enhancing educational initiatives for Data Protection Officers (DPOs) within the public sector. This should be coupled with increased involvement of the Data Protection Authority (AZOP) and, concurrently, heightened engagement from public authorities. It is imperative to allocate greater focus and resources to address data protection-related topics, fostering a collaborative approach to ensure robust safeguards and compliance.

2) Knowledge and experience of a DPO

1. A large number of DPOs do not have enough knowledge and experience in the field of personal data to carry out their duties and they don't invest enough time to gain necessary knowledge or to enhance existing one.
   29.03 % (880) of DPOs responded that they have no expert knowledge in the field of personal data and that they have nominated DPO because the nomination of a DPO was legal obligation.
   3.63 % (110) of DPOs doesn't know how many years of experience in the field of data protection DPOs has, and 5.05 % (153) of them didn't give any answer to this question.
   16.66 % (505) of DPOs answered that they invest 0 hours of time on yearly basis to enhance or gain knowledge in the field of personal data.
   31.18 % (945) of DPOs answered that they invest 1-8 hours of their time on yearly basis to enhance or gain knowledge in the field of personal data.

11.35 % (344) of DPOs said that they don't know how much time on yearly basis DPO spend to enhance or gain knowledge in the field of personal data.
4.98 % (151) didn't give any answer to this question

2. Article 37 (5) of the GDPR, Article 38 (2) of the GDPR.

3) Time allotted for the DPO to carry out their responsibilities and tasks

1. A large number of DPOs carry out other tasks, this is just an additional job for them. They don't dedicate enough time to carry out their duties and tasks as a DPO.
   83.47 % (2530) of DPOs responded that being a DPO is not their main task (role in the organisation), it is just and additional task, together with many other tasks.
   7.26 % (220) didn't respond to the question whether acting as a DPO is their main task (role) in the organisation.
   The largest number of respondents 30.55 % (926) of them can dedicate less than 5% of their working time for doing their task and duties of a DPO.
   14.02 % (425) of DPOs can dedicate 11 – 20 % of their working time for doing their tasks and duties of a DPO. 13.16 % (399) of DPOs didn't give any answer to this question.
   14.22 % (431) of DPOs is able to dedicate only 1 full working day (8 hours) on monthly basis in order to fulfil its duties and tasks as a DPO.
   17.98 % (545) of DPOs is able to dedicate 0 – 0,9 (less than one working day) on monthly basis in order to fulfil its duties and tasks as a DPO.
   18.15 % (550) of DPOs is able to dedicate 1,0 – 2,0 working days on monthly basis in order to fulfil its duties and tasks as a DPO.
2. Article 38 (2) of the GDPR.
3. The organisations don't provide enough time (working hours) to DPO to perform its tasks and duties. It could be concluded that they don't consider data protection as an important topic that deserves more time and investments.
4. Significant distinctions persist between the public and private sectors regarding GDPR compliance. The Act on Implementation of the GDPR stipulates that numerous public authorities are exempt from fines for GDPR infringements. Consequently, many allocate minimal time and effort to ensure compliance. Typically, these entities reach out AZOP only when a project, such as the development of a new IT solution, is in its final stages. At this juncture, they seek assistance in identifying a lawful basis for processing personal data and asking for 'confirmation' of overall GDPR compliance.
   Within the educational and health sectors, there exists a heightened awareness of GDPR compliance. However, DPOs in these fields often find themselves stretched thin, lacking sufficient time to fulfill their DPO duties adequately.
   In contrast, the private sector demonstrates a more pronounced interest in GDPR compliance. This heightened concern is primarily fuelled by the fear of substantial fines and potential damage to reputation resulting from GDPR violations. Consequently, DPOs in the private sector tend to possess a significantly higher level of knowledge, they invest more time in performing their DPO duties and responsibilities, reflecting the broader commitment to and understanding of GDPR requirements.
5. Raising awareness among organisations on the importance of the role of DPO. Recommendation sent to the organisations by AZOP. Intensive campaign among top management of organisations. More supervisory activities conducted by AZOP in relation to Article 38.

4) Obligations do not appoint a deputy DPO

1. 83.5 % (2531) of DPOs said that the deputy DPO has not been appointed.
2. Article 39 (a) (b) (c) (d) (e) of the GDPR.
3. Through our daily experiences, it has become evident that this poses a significant challenge for organizations. For instance, when the DPO takes sick leave or is absent for any reason, a gap is created, leaving no one to fulfill their responsibilities. This scenario presents a dual challenge for both the data controller/processor and the Data Protection Authority (AZOP) during supervisory activities. Specifically, organizations face issues providing explanations during audits, citing the unavailability of a replacement for the DPO, resulting in an inability to provide requested information promptly. This underscores the critical need for contingency plans and designated backups to ensure the continuity of data protection responsibilities and compliance even in the absence of DPO. This could be solved by appointing replacement for the DPO (deputy DPO).
4. No significant differences.
5. The organizational solution is to designate a Deputy Data Protection Officer with the requisite knowledge and skills to seamlessly assume the responsibilities of the DPO in their absence. The appointed deputy should possess a comprehensive understanding of all aspects of a DPO's role and functions.

5) Workload of a DPO and how often he is asked for advice from employees within the organisation

1. Many DPOs typically handle a modest volume of requests, with the majority receiving up to 10 inquiries per month from colleagues seeking guidance on data protection matters. A minority of DPOs consistently provide advice on data protection issues, demonstrating a proactive approach. Additionally, a small percentage of DPOs believe that they should be consulted on all matters related to data protection, emphasizing the importance they attribute to their role in safeguarding data across various contexts.
   86.24 % (2614) of DPOs receives only 0-10 requests from its co-workers related to data protection on monthly basis.
   Only 23.72 % (719) of DPOs participates and gives advice on data protection questions all the time (100%). 38.4 % (1164) of DPOs spend less 5% of their time to participate and give advice on data protection questions.
   38.01 % (1152) of DPOs thinks that consulting with a DPO is necessary only on some questions related to data protection. 12.54 % (380) of DPOs think that consulting with a DPO on data protection question is not necessary. 7.03 % (213) doesn't know answer to this question.
   87.2 %of DPOs receives only 0-10 requests from the data subject in relation to their data protection rights on yearly basis. – this is an indicator of low awareness on the role of data protection officer among Croatian citizens.
   In case when the organisation doesn't follow the advice of a DPO, only 31.18 % (945) of DPOs document the reasons why the DPO's advice has not been followed.
2. Article 38 (1) and Article 39 (1) (a) (b) (c) of the GDPR.
3. The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data. In large number of cases this is not the case, DPOs are not aware that it is their duty to be involved in all data protection issues, employees of the organisation are not aware that they should seek advice of the DPO. Engaging in high risk processing activities without consulting

DPO exposes an organization to the potential of GDPR infringements. Seeking the guidance of the DPO is crucial to mitigate risks and ensure compliance with GDPR.

4. The difference is again between private and public sectors, where in public sector the percentage of employees seeking advice of DPO is significantly lower.
5. Raising awareness of top management on the importance of seeking advice of DPO and respecting its advice in all data protection issues. Raising awareness of employees on the importance of seeking and respecting advice of DPO. More engagement of AZOP and organisations is needed in this matter.

6) Independence of a DPO and reporting to the highest management

1. A significant number of DPOs receive instruction on how to perform its duties and DPOs do not inform the highest management about their work and data protection issues in their organisation.
   35.3 % (1070) of DPOs receive instructions on how to do perform their tasks and duties**.**
   5.11 % (155) does not know the answer to this question and 6.6 % (200) did not give any answer.
   31.71 % (961) does not report about its work to the highest management not even once a year. (Čl. 38. st. 3. Opće uredbe o zaštiti podataka). 7.95 % (241) of respondents doesn't know the answer to this question.
   28.44 % (862) of DPOs does not report to the highest management at all.
2. Article 38 (3) of the GDPR, Article 38 (6) of the GDPR.
3. This is a big issue for organisations because they are not informed about data protection concerns and issues in their organisations, and they will be held responsible in case of GDPR infringements and data breaches. The reason can be that they simply do not care about it. Compounding this issue is the constrained autonomy of the DPO who, rather than operating independently, is subject to directives from top management, thereby limiting their effectiveness in fulfilling their responsibilities. It is imperative for organizations to foster a culture of awareness and commitment to data protection, ensuring that DPOs have the requisite autonomy to execute their duties effectively.
4. The same difference between public and private sector as stated before.
5. Raising awareness and education of all relevant stakeholders.

7) Guidance of the Supervisory Authority

1. 72.52 % of DPOs would like more FAQs from data protection authority.
   46.45 % (1408) of DPOs would like more online tools.
   49.06 % (1487) of DPOs would like additional guidelines.
   67.73 % (2053) of DPOs would like more training materials and documents to be distributed within the organisations.
   In free text box there were following comment:
   - There is a need for certification programme for DPOs (conducted by AZOP)
   - There is a need for more educational activities
   - There is a need for newsletter with information on various decisions of data protection authorities all over EEA
   - There is a need for clear and precise legal advice from AZOP
2. Article 39 of the GDPR (39.1.b) (39.1.c) (39.1.d) (39.1.e)
3. Croatian Act on Implementation of GDPR doesn't prescribe additional provisions concerning data protection officer.

4. When discussing the expectations of DPOs from the Croatian Personal Data Protection Agency (AZOP) in terms of providing support for their roles, a significant challenge for organizations arises from a lack of clarity regarding the distinct responsibilities of a DPO and those of a data protection authority (AZOP). Many organizations (DPOs) mistakenly believe that AZOP's primary function is to provide precise legal advice when they pose compliance inquiries. For instance, organizations often expect AZOP to take on tasks such as identifying legal bases, conducting Legitimate Interest Assessments (LIA), performing DPIA, and more.
   Frustrations emerge when organizations seek straightforward answers, such as, 'As a travel agency, do I have a legitimate interest in sending a client's personal data to a hotel?' Instead of giving precise response (which of course we can't do), we emphasize the need for the organization to conduct a balance test (LIA) if they wish to rely on legitimate interest and we give them a template with instructions on how to do it. DPOs very often perceive that AZOP duty is to do their job instead of them, leading to disappointment with our responses.
   There is a big difference between DPOs from public and private sector. According to Act on the implementation of GDPR: Exclusion of application of administrative fines to public authorities

   Article 47: Without prejudice to exercising the powers of the Agency laid down by the provision of Article 58 of the General Data Protection Regulation, in procedures conducted against public authorities, an administrative fine for a breach of this Act or the General Data Protection Regulation cannot be imposed on a public authority (state administration bodies and other state bodies, as well as local and regional self-administration units).

   Article 47 addresses the exclusion of administrative fines applied to public authorities in the context of procedures conducted against them for breaches of the GDPR or related legislation. While this provision protects public authorities from monetary penalties, it has led to a concerning trend where organizations in the public sector disregard GDPR compliance, citing immunity from fines.

   An observed challenge within the public sector, particularly concerning DPOs, is the delicate balance they must strike between two fundamental human rights: the right to data protection and the right to access information. Many DPOs in public entities express uncertainty regarding whether they are permitted to provide access to information containing personal data. Despite comprehensive guidelines provided by the Information Commissioner of the Republic of Croatia, it appears that some DPOs may be reluctant to independently carry out the required balance tests, perhaps expecting external entities to fulfill this responsibility on their behalf.

   Notably, there is a notable discrepancy in GDPR compliance across sectors. DPOs in the education and health sectors often face challenges with limited knowledge and insufficient organizational support. In contrast, organizations in the financial sector demonstrate a higher level of commitment to GDPR compliance, typically boasting dedicated privacy teams and substantial human and financial resources. Unfortunately, DPOs in the education and health sectors find themselves grappling with compliance hurdles without commensurate organizational backing.

   Another sector requiring attention is tourism, where substantial compliance issues have been identified alongside a lack of understanding of the DPO's role. Factors contributing to non-compliance include low awareness of the importance of personal data protection, a general disregard for data protection principles, and the perception of personal data as a lucrative source of income. In this sector, personalized offers for guests and the sharing of guest data

with other organizations are seen as revenue-generating strategies, overshadowing the imperative to adhere to data protection regulations.

Another problem is that performing his/her duties as a DPO in most cases is not the main job of a DPO but additional task, and DPOs are not paid for this additional work. Consequently, DPOs are not motived to do their job properly.

More support for DPOs from AZOP and organisations is needed and more fines for organisations who don't give enough time, budget and independency to their DPOs.

In conclusion, the observed challenges highlight the need for increased awareness, education, and support, particularly within the education, health, and tourism sectors, to ensure effective GDPR compliance and safeguard individuals' rights to data protection.

5. Addressing the challenge at hand requires a multi-faceted approach, focusing on enhanced support from AZOP for DPOs and imposing stricter penalties on organizations that appoint DPOs merely for formal reasons without providing them the necessary resources and time to fulfill their responsibilities.
   From 2018 to 2020, we implemented the EU-funded T4DATA project (https://azop.hr/eu-project-t4data/), designed to assist DPOs in the public sector in understanding GDPR provisions and integrating them into their business processes. Despite developing a comprehensive manual (https://azop.hr/wp-content/uploads/2021/01/the-dpo-_handbook_-t4data.pdf), a persistent issue arises wherein DPOs often lack the inclination or time to engage with the valuable resources available.
   Presently, we are actively working within the EDPB Support Pool of experts to create an extensive DPO training program specifically tailored for the health and educational sectors. The anticipated launch date for this program is February 2024.
   Our commitment to empowering DPOs is evident through various initiatives such as regular training sessions (https://azop.hr/edukativne-aktivnosti-azop-a/), workshops under the ARCII project for SMEs, free online training sessions on demand, and collaborations with the Public School for Administration. In addition, we respond to each question received from DPOs in written, and they can also contact AZOP by phone.
   Recognizing the value of technology in education, we are developing an online tool (https://olivia.foi.hr/hr) aimed at assisting SMEs, with the belief that it will be beneficial for a wide range of DPOs. Additionally, our dedicated webpage for DPOs (https://azop.hr/sluzbenik-za-zastitu-podataka-2/) provides a wealth of educational materials, and we have plans to establish a DPO network for the financial sector by the end of 2023.
   Given our current resource constraints, the efforts we are undertaking represent the best possible support. However, we emphasize that organizations must share the responsibility by appointing DPOs with the requisite knowledge and skills. We cannot be expected to compensate for gaps caused by insufficient investments on their part.
   Regarding DPOs in the public sector, we advocate for an amendment to the Act on the Implementation of GDPR. This amendment should empower AZOP to impose fines on public sector organizations found in violation of GDPR and the Act on the Implementation of GDPR. Such a regulatory change is essential to ensure accountability and compliance across all sectors. Also there is a high demand for certifications schemes and certified trainings conducted by AZOP.

Part III – Actions by the SA

1. **Have you already published general guidance (e.g. guides, guidelines, etc.) regarding DPOs (including before launching the coordinated action)?**
   If yes, please provide the date, link to the guidance, and a short description of the guidelines

Yes. We have developed a comprehensive manual for DPOs in public sector available at: https://azop.hr/wp-content/uploads/2023/09/DPO-prirucnik.pdf. The manual consists of 215 pages and describes in a detailed way all the tasks and duties that a DPO in public sector needs to perform, with practical examples and guidelines. Also, we have published a short brochure about the role and tasks of DPOs https://azop.hr/wp-content/uploads/2021/01/brosura-Zasto-je-vazno-imenovati-sluzbenika-za-zastitu-OP_2021_e_mail-version.pdf.

2. **Have you taken action (i.e., fact finding exercises, informal contact, prior consultation, investigation) towards any of the organisations concerning the designation, tasks and/or role of the DPO *prior to* launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**

Yes, in the period from 2018-2021 Croatian Personal Data Protection Agency sent to all the public authorities in Croatia letters (around 6000 letters) concerning the designation, tasks and/or role of the DPO with instructions to appoint a DPO.

3. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**

Based on the results of this coordinated action, we are planning to issue corrective measures such as orders, penalties and guidance/recommendations. We have 417 ongoing enforcement actions.

Part IV – Other

1. **What is your general impression of the levels of awareness and compliance of the organisations you consulted concerning the designation, tasks and/or role of the DPO?**

The general impression is that the level of awareness in some organisations is very low, especially in public sector (especially regional and local self-government units, state administration bodies, DPOs from health and educational sectors).

2. **Are there any other issues or topics that you would like to flag?**

NO (already described in previous questions).

3. **Are there any leading practices of the organisations you have contacted that you would like to share?**

No.

HU SA

Part I - Statistics

Please see the consolidated figures in Appendix 1.1. The answers below may refer to the questions included in Appendix 1.1.

Part II – Substantive issues

Main issues identified by the Hungarian SA:

- The designation, knowledge and experience of the DPO
- The tasks and resources of the DPO
- Training and resources of the DPO
- The role and position of the DPO
- Communication of the contact details of the DPO to the SA

Brief description of the issues: The Hungarian SA launched similar surveys three times in the past years, in connection to its Annual Conference for DPOs in 2019-2020-2021. These surveys focused on the position, independence and duties of DPOs, and their results show correlation at many points with the results of the survey within the CEF.

Although the number of DPOs notified to us under GDPR (or in case of LED under our national implementing act) have been increasing in recent years, it can also be concluded from the figures that not all data controllers with the obligation to have a DPO designated one, or if they have, they have not notified the contact details of the DPO to the Authority.

Year	No. of individual DPO addresses	No. of data controllers/processors notified
2019	1875	4200
2020	3075	7600
2021	3580	8600
2022	4057	11200

DPO notifications to HU SA Online Notification System

Previously and again this time, we found that only a part of the contact details were/are individual addresses. When digging into the details it turned out that 'professional external' DPOs who provide services for more than 1 data controller use the same email address for all of their clients, which does not allow them to provide answers in relation to all data controllers to whom they provide services. In many cases direct contact details of DPOs are not communicated, only the functional and/or central contact details of the data controller are available.

Regarding the communication of the contact details of the DPO to the Hungarian SA, it can be noted that although the data controllers usually notify us of the contact details of the DPOs, information is not kept up-to-date, and changes are not necessarily communicated to us, and in some cases even the privacy notice of the data controller contains outdated information.

Several data controllers in the public sector (public bodies) are still unaware that they are obliged to designate a DPO and are on the opinion that Article 37 of the GDPR does not apply to them. One reason for this is probably that some of the data controllers are not aware that they are performing public tasks and are therefore considered to be public authorities or bodies. (Although the survey did address this issue, it should be noted in this context, that it is also a common problem, that no DPO has been designated where it is mandatory according Article 37 (1) b) of the GDPR.)

Regarding this problem (i.e. the data controller is obliged to designate a DPO but has not done so, or has designated a DPO but has not published his or her contact details and/or no notification to us has been made) the Authority have launched 29 inquiries ex officio this year and based on the results and communication of the CEF report more public bodies are due to be involved.

We have experienced several times that the designated DPO holds a position within the organisation that includes the tasks relating to determining the goals and means of processing of personal data, or the DPO is a member of the highest management of the data controller. Some of the investigations mentioned above also cover the issue of conflict of interest.

Generally and unfortunately data controllers are not fully aware of the tasks and position of the DPO. We are also aware of cases where the data controller was/is convinced that the national act on data protection applicable prior to the GDPR is the governing law, hence the data controller was/is not aware of the additional requirements and enhanced role of the DPO, and therefore the data controller did/does not provide adequate and sufficient training, knowledge on particularly important issues (such as on data security, risk assessment practices, data breach management) and resources for the DPO.

A relatively high proportion of DPOs were/are not provided any trainings, materials to keep their knowledge up-to-date, and they would need much more resources for their tasks. Their knowledge is particularly lacking in the field of information security matters and information systems management and/or development, however the majority of respondents feel qualified in data protection and privacy matters, data protection processes and legislation on the processing and the protection of personal data.

It also can be considered as serious problem, that some DPOs are/were designated by a high number (even more than 100) of data controllers, and therefore these DPOs are most probably not able to perform their tasks and fulfil their duties as they should.

In terms of the officers' activities, the percentage results corresponded to last year's figures showing that a significant majority comply with their advisory tasks to be provided to controllers or processors and staff conducting processing work and the management of their entities typically request their professional opinion of the tasks specified under GDPR Article 39. However, similarly to the results experienced in recent years, the majority have not carried out any internal data protection compliance investigation or audit since their appointment, or if they have, they have not documented it and they have not prepared any plan for their activities, which could improve the prevalence of the principle of accountability, the level of awareness and transparency within the organisation.

A possible solution to these issues could be the annual DPO conference organised by the Hungarian SA at the end of each year. Topics and presentations of the conference may focus more on these topics, which might have a positive impact on the relationship between DPOs and the Hungarian SA.

Inquiries or administrative procedures in the forthcoming months may also cover these issues. Some colleagues of the Hungarian SA are guest lecturers of 5 Hungarian universities give lectures to LLM programs available on data protection. Spreading the knowledge on the requirements for the role of the DPO may be one of the key solutions to the main problems.

Part III – Actions by the SA

1. **Have you already published general guidance (e.g. guides, guidelines, etc.) regarding DPOs (including before launching the coordinated action)?**
   If yes, please provide the date, link to the guidance, and a short description of the guidelines

We published opinions on the position and designation of DPOs in 2018 in connection to requests for opinion in specific cases, but no general guidance has been issued.

WP29 Guidelines on Data Protection Officers (WP243) and a video-presentation on the tasks related to the appointment of the DPO prepared for the annual DPO Conference in 2019 are available on our website: https://naih.hu/dpo-konferencia-2019.html#vid3

2. **Have you taken action (i.e., fact finding exercises, informal contact, prior consultation, investigation) towards any of the organisations concerning the designation, tasks and/or role of the DPO *prior to* launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**

See Part II of this report.

3. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**

Annual DPO Conference that will take place at the end of the year (as usual).

Part IV – Other

1. **What is your general impression of the levels of awareness and compliance of the organisations you consulted concerning the designation, tasks and/or role of the DPO?**

Moderate knowledge due to lack of information available amongst colleagues responsible for this task.

2. **Are there any other issues or topics that you would like to flag?**

To be determined following the overall results of CEF.

3. **Are there any leading practices of the organisations you have contacted that you would like to share?**

N/A.

IE SA

Irish Supervisory Authority – Data Protection Commission (DPC)

Part I - Statistics

Please see the consolidated figures in Appendix 1.1. The answers below may refer to the questions included in Appendix 1.1.

Part II – Substantive issues

Substantive Issue 1: The Resources of the Data Protection Officer (Article 38(2) GDPR).

Data Protection Officers (DPOs) play an essential role, assisting organisations with their compliance obligations under the GDPR and Data Protection Act 2018. The DPO has numerous tasks as is laid out Article 39(1) GDPR. A DPO should be given the necessary resources to fulfil those tasks as stated in Article 38(2) GDPR. Organisations have an obligation to support DPOs when they perform their DPO tasks by providing DPOs with resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

The DPC noted the following findings from the questionnaire results:

- 33% of respondents replied that they do not have the resources sufficient to fulfil the role of a DPO. The high majority 86% of these respondents came from Public Sector, Voluntary or Not-for-Profit Bodies.
- Only 1 in 5 respondents answered that they can allocate all their time to performing the DPO's tasks and duties.
- 1 in 10 respondents stated that the role of the DPO is only a part-time resource in the organisation.
- Over 1 in 3 replied that the tasks of the DPO are in addition to other tasks performed by them in the organisation. Some of these tasks the DPC noted would not complement the role of a DPO, such as Health and Safety Officer, Human Resource Officer, Employee Engagement Manager, and Communications Officer.
- Almost half of respondent's do not have a designated deputy to assist them in their role.
- The high majority of respondents who stated they do not have adequate resources sufficient to fulfil the role of a DPO came from the Public and Not-for-Profit Sector. This supports the position that DPOs are better resourced in the Private Sector.

It is vital that DPOs have adequate and sufficient resources to carry out their tasks as DPOs in an organisation effectively and that the DPO can maintain their expert knowledge (Art 38.2 GDPR). It is concerning that one-third of DPOs state they do not have the adequate resources for the role, and also that some large organisations only have a part-time DPO in place. A part-time position may lead to a lack of clarity as to what is expected in the role and diminish the importance of the role. Such resources can only have a negative impact on the compliance levels of data protection within an organisation. The DPC appreciates that 'resources' is not defined under the GDPR; the DPC recommends organisations need to consider the EDPB Guidelines on Data Protection Officers

3.2 Necessary Resources which states the following should be considered by organisations.

- Active support of the DPO's function by senior management (such as at board level).
- Sufficient time for DPOs to fulfil their duties.
- Adequate support in terms of financial resources, infrastructure (premises, facilities, equipment) and staff where appropriate.
- Official communication of the designation of the DPO to all staff to ensure that their existence and function are known within the organisation.
- Necessary access to other services, such as Human Resources, legal, IT, security, etc., so that DPOs can receive essential support, input and information from those other services.
- Continuous training. DPOs must be given the opportunity to stay up to date with regard to developments within the field of data protection. The aim should be to constantly increase the level of expertise of DPOs and they should be encouraged to participate in training courses on data protection and other forms of professional development, such as participation in privacy fora, workshops, etc.

Whilst the DPC recognises there is no one-size-fits-all, the DPC considers further clarity on what could be regarded as providing adequate resources for DPOs in an organisation may be helpful to address this situation. It may be the case that organisations need a template for what is required to have adequate resources in place for the role of a DPO.

Substantive Issue 2: Conflicts of Interests (Article 38(6) GDPR).

Article 38(6) GDPR states: 'The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests'. The DPC noted in the submissions received that a number of DPOs alluded to performing other roles within the organisation. Some of these other roles may have the potential for a Conflict of Interests. Some of the roles noted included:

- General Manager
- Chief Financial Officer
- Chief Executive Officer
- Director of Corporate Services

Whilst the GDPR does not prevent a DPO from fulfilling other non-DPO tasks and duties an organisation must ensure the DPO does not carry out tasks that will not lead to a conflict of interests or the impact on the independence of the Role of Data Protection Officer. The CJEU has recently held 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. [43]

The DPC acknowledges in line with the CJEU decision that a conflict of interest must be evaluated on a case-by-case basis and will be specific to the each individual organisation and their structure. The DPC recommends that organisations consider the published EDPB guidance in this which states

Depending on the activities, size and structure of the organisation, it can be good practice for controllers or processors:

- to identify the positions which would be incompatible with the function of DPO
- to draw up internal rules to this effect in order to avoid conflicts of interests

[43] CJEU C-453/21 – X-Fab Dresden GmbH & Co. KG

• to include a more general explanation about conflicts of interests
• to declare that their DPO has no conflict of interests with regard to its function as a DPO, as a way of raising awareness of this requirement
• to include safeguards in the internal rules of the organisation and to ensure that the vacancy notice for the position of DPO or the service contract is sufficiently precise and detailed in order to avoid a conflict of interests.

Substantive Issue 3: Tasks of the DPO. Article 39 (1) (a to e) GDPR

Question 15 of the survey asks 'Have additional tasks been committed to the data protection officer compared to those envisaged in the GDPR?'.

The DPC noted that the following other tasks are carried out by the DPO.

- nearly 1/3 of DPOs are involved in the decision making on the processing of personal data
- Over half develop the organisation's data protection processes.
- Over half draft or carry out data protection impact assessments
- Over half fulfil the data subject requests on their data protection rights
- Almost half draft or negotiate contract such as data processing agreements.
- Over 25% are responsible for the lawfulness of the processing of personal data.

The DPC notes following responses received that in practice, DPOs carry out considerably more tasks with more responsibility than outlined in the GDPR. The DPC notes that some of these tasks are better served by the organisation, not an independent DPO. For example, over 50% of DPOs, as an additional task, state they draft or carry out DPIAs. Whilst the DPO can play a vital role in carrying out a DPIA by being consulted for advice before or during a DPIA project, it is the controller's task rather than the DPO's to carry a DPIA when necessary (Article 35(1) GDPR). The DPC believes that DPIAs should ideally come from the controller and, specifically, the Unit within the organisation with the best expertise in the area of the DPIA.

Positives.

Article 38(1) and 39 GDPR

The DPC welcomes that nearly all organisations have as a requirement that the DPO must be consulted on data protection issues, and for the most part, the DPO is involved or consulted in handling and solving problems related to the processing and protection of personal data in the organisation. (Q25/26). The DPC also sees as a positive that almost all DPOs stated that, in general, the DPO's opinions are being followed in the organisation and that the high majority, nearly 75% of DPOs, are documenting why their advice is not being pursued for example, why a DPIA was not deemed necessary prior to the undertaking of a project. The DPO's recording of why their advice is not followed and their decision-making process will assist an organisation in meeting its accountability obligations under Article 5(2) GDPR.

Part III – Actions by the SA

1. **Have you already published general guidance (e.g. guides, guidelines, etc.) regarding DPOs (including before launching the coordinated action)?**
   If yes, please provide the date, link to the guidance, and a short description of the guidelines

The DPC has published guidance on appropriate qualifications for a Data Protection Officer at the following link[44].

The guidance recommends that the appropriate level of qualification and expert knowledge should be determined according to the personal data processing operations carried out, the complexity and scale of data processing, the sensitivity of the data processed and the protection required for the data being processed.

The DPC has published guidance on Who Needs a DPO under Article 37(1) GDPR?[45].

The DPC has guidance published on how to notify the DPC of notifying the DPC of a DPO under Article 37 (7) GDPR[46].

The DPC also has an FAQ document on the DPC DPO notification/registration process[47].

2. **Have you taken action (i.e., fact finding exercises, informal contact, prior consultation, investigation) towards any of the organisations concerning the designation, tasks and/or role of the DPO *prior to* launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**

Pursuant to its tasks of a supervisory authority contained in Article 57 of the GDPR, in 2020, the DPC commenced a project to assess compliance by public bodies with the Article 37 (1) obligations. From a total of almost 250 public bodies, comprising Government Departments and agencies, as well as Local Authorities, 77 public bodies were identified as being potentially not compliant with the requirements. Engagement with each of these public bodies to bring themselves in to compliance with Article 37.7 of the GDPR by the end of 2020, raising the sector's compliance rate from 69% to 96%.

The DPC carried out an Own-Volition Inquiry into one of the public bodies as a result of the monitoring and enforcement exercise above[48]. Pursuant to the tasks of a supervisory authority contained in Article 57 of the GDPR following which the decision issued the body with a with a reprimand in respect of the infringements of Articles 31, 37(1), and 37(7) of the GDPR.

3. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**

[44] Available at https://www.dataprotection.ie/sites/default/files/uploads/2019-07/190708 Guidance on Appropriate Qualifications for a Data Protection Officer %28GDPR%29.pdf.
[45] Available at https://www.dataprotection.ie/en/dpos/who-needs-dpo.
[46] Available at https://www.dataprotection.ie/en/organisations/know-your-obligations/data-protection-officers.
[47] Available at https://www.dataprotection.ie/sites/default/files/uploads/2022-06/Data Protection Register FAQs Updated 010622_0.pdf.
[48] Available at https://www.dataprotection.ie/sites/default/files/uploads/2022-05/IN-22-2-1 PHECC Decision Final.pdf.

The DPC participated in the 2023 CEF as a fact-finding exercise to feed into the wider EDPB CEF. The answers received will assist the DPC in gaining greater insights into the designation and position of the Data Protection Officer and assist the DPC in supporting DPOs in their role. The answers received will not lead to any formal actions or investigations by the DPC.

Part IV – Other

1. **What is your general impression of the levels of awareness and compliance of the organisations you consulted concerning the designation, tasks and/or role of the DPO?**

The DPC's general impression of the levels of awareness and compliance of the organisations concerning the designation, tasks and role of the DPO in general is quite high. In the large majority, almost 80% of DPOs replied they have at least 3 + years of experience working on the application and the interpretation of data protection requirements (Art 37.5 GDPR). This level of expertise broadly matched the DPO's relevant experience working in the organisation's particular industry with over 50% stating they have 8+ years in organisations industry or field.

The DPC is concerned, however, that the DPO role in some organisations is considered part-time and as previously noted, this may have an impact on the effectiveness of the role. It was noted that this situation arose more in the voluntary and not-for-profit sectors, which may indicate budgetary constraints in those sectors as opposed to organisations in the private sector. In some cases, the DPO could allocate as little as 10% or 20 % of their working hours to performing their tasks and duties, likely impacting effective data protection compliance in an organisation.

2. **Are there any other issues or topics that you would like to flag?**

N/A.

3. **Are there any leading practices of the organisations you have contacted that you would like to share?**

N/A.

IT SA

Italian Supervisory Authority – Garante per la protezione dei dati personali

Part I - Statistics

Please see the consolidated figures in Appendix 1.1. The answers below may refer to the questions included in Appendix 1.1.

Part II – Substantive issues

1) Designation of the DPO

1. As regards the public sector, it has been declared that the DPO sometimes belongs to the top management and this circumstance must be assessed on a case-by-case basis to verify the existence of possible conflicts of interest. In the private sector, it emerged that in some cases one DPO was designated for the entire business group, made up of numerous subsidiaries (e.g.: in one case, 53 subsidiaries designated the same DPO). Furthermore, it was found that in one case the DPO's contact details were communicated to the Authority only by the holding company and not by the subsidiary company, which is established in Italy and acts as data controller.
2. Article 38 (6), Article 37 (2), (7), Article 39 GDPR.
3. These are conducts that may give rise to a violation of the provisions on the protection of personal data set out in the GDPR. With particular reference to the designation of a single DPO by several controllers, it should be pointed out that the designated DPO should be able nevertheless to provide the necessary support to all the controllers (also in terms of time and resources) and perform the tasks under Article 39 adequately. Furthermore, with reference to the case reported above, it is to be highlighted that the communication of the DPO's contact details to the SA as well as their publication are necessary in order to enable both the SA and data subjects to contact the DPO in an easy and direct way. Indeed, although Article 37 (7) allows designating a single DPO on behalf of several controllers/companies, this does not do away with the obligation for every controller to communicate the DPO's contact details to the SA and to publish them.
4. There are many differences between organisations and this is a limited problem and only detected in specific cases.
5. General guidance, implementation of training and updating processes, revising the Guidelines on data protection officers (WP 29 n. 243 Rev. 01), possible initiation of individual proceedings and imposition of corrective measures, exchanges with and suggestions to data controllers.

2) Knowledge and experience of the DPO

1. In some cases, in the public sector, DPOs have declared that they do not have specialized expertise in data protection matters, however they have sometimes stated they were familiar with the relevant legislation. In the recruitment procedures, specific skills or experience were sometimes not required. In some cases, no training periods were foreseen for DPOs. On the contrary, widespread specialist knowledge has emerged in the private sector and DPOs follow several training courses of several hours' duration throughout the year.
2. Article 37 (5) GDPR.

3. It may give rise to a violation of the GDPR. In particular, appointing a DPO without professional qualities and specific expertise nullifies the rationale of the appointment and the contribution the DPO can give to the controller's organization.
4. With respect to this specific issue, there is a certain difference between DPOs operating in the public sector and those operating in the private sector.
5. General guidance, implementation of training and updating processes, revising the Guidelines on data protection officers (WP 29 n. 243 Rev. 01), possible initiation of individual proceedings and imposition of corrective measures, exchanges with and suggestions to data controllers.

3) Tasks and resources of the DPO

1. Sometimes, in the public sector, the controller's management has not clearly defined and provided a written description of the DPO's duties. Sometimes the DPO discharges additional tasks and the DPO-related activities are not the main task of the designated person who devotes less than 5% of their time to discharging the relevant duties. In some cases, the staff is not enough and in almost all cases, no deputy has been appointed, whilst the available resources are considered insufficient. In the private sector, on several occasions DPOs have declared that they do carry out other tasks and have insufficient resources and time to discharge their tasks as DPOs (less than half responded that they manage to dedicate 50% of their time to their DPO function due to additional tasks). In terms of resources, while on the one hand the staff available to the DPO is considered adequate and a budget is allocated, only half of the DPOs in the private sector responded that they could manage the budget independently. Finally, it should be noted that a minority of DPOs indicated that the controller had appointed a deputy.
2. Articles 38 (2), (6), 39 GDPR.
3. It may give rise to a violation of the GDPR. In particular, if the DPO carries out several other tasks, poor efficiency or incompatibility or conflicts of interests may arise as the performance of further tasks could prevent them from usefully fulfilling their duties as DPOs (especially if their additional tasks entail a workload that ultimately hampers the performance of the DPO's duties). In other cases, such multiple tasks might prevent the DPOs from acting independently (for example where the other roles covered by the DPO within the organization entail the determination of the purposes or means of the processing of personal data).
4. There are many differences between organisations and this is a limited problem and only detected in specific cases.
5. General guidance, implementation of training and updating processes, revising the Guidelines on data protection officers (WP 29 n. 243 Rev. 01), possible initiation of individual proceedings and imposition of corrective measures, exchanges with and suggestions to data controllers.

4) Role and position of the DPO

1. In the public sector, there remain cases where the DPO is not consulted on issues relating to the protection of personal data and does not receive sufficient information on the relevant issues. The DPO is generally not expected to report regularly to the highest level of management in the organization. Sometimes the DPO's contact details are published on the website, but not in the privacy policy. In the private sector, conversely, the involvement of DPOs in data protection issues was found to be thorough. Also in the private sector, it was found that the DPO does not report directly to the top management in most cases as they rather report to other functions in the organization's structure. Cases were found in both the

public and private sectors in which the controller did not document the reasons why the DPO's opinion was disregarded.
2. Articles 13 (1); 38 (1), (3); 39 (1) GDPR.
3. It may give rise to a violation of the GDPR. In particular, where there is little involvement of the DPO, this voids the relevant appointment of any significance and therefore trumps the privacy by design and by default approach promoted by the GDPR - which may entail consequences for the controller in terms of accountability and non-compliance with the GDPR. As to the situations where the DPO does not report directly to the top management, this may jeopardise the independent discharge of the relevant tasks.
4. Some differences were found between DPOs operating in the public sector and those operating in the private sector with regard to the involvement of the DPO on issues relating to the protection of personal data. However, in both the private and the public sector, the DPO is not expected to report regularly to the organisation's top management in the majority of cases.
5. General guidance, implementation of training and updating processes, revising the Guidelines on data protection officers (WP 29 n. 243 Rev. 01), possible initiation of individual proceedings and imposition of corrective measures, exchanges with and suggestions to data controllers.

5) Guidance of the Supervisory Authority

1. In many cases it was stated by the DPOs that they would like to be able to take advantage of further guidance from the Supervisory Authority such as FAQs, online tools, guidelines, materials for the training of the DPO, materials for use by the DPO for the internal training of the personnel, and that publication of the contact details of the DPOs by the SA would be helpful as well. In the public sector, in one case the request was made to develop 'Templates to draft a comprehensive regulatory instrument addressing the structure and legal positioning of the DPO and the respective Staff Office by having regard to the tasks and size of the public authority/ related Organisation'.
2. None.
3. It would be useful to provide DPOs with tools to better perform their tasks.
4. N/A.
5. Identifying ways to disseminate what has already been developed by the individual European SAs over time in a more structured manner, also in light of the Final CEF Report published by the EDPB; developing common tools and decisions at European level, taking into account in any case that there is no ultimate best practice, much less so a 'one-size-fits-all' best practice at EU level, and that it is up to controllers to identify the best and most effective solution by having regard to the context in which they operate – in line with the accountability principle.

Part III – Actions by the SA

1. Have you already published general guidance (e.g. guides, guidelines, etc.) regarding DPOs (including before launching the coordinated action)?
If yes, please provide the date, link to the guidance, and a short description of the guidelines

1) FAQ concerning DPOs in the private sector on 26/03/2018

Faq sul Responsabile della Protezione dei Dati (RPD) in ambito privato - Garante Privacy[49]

2) FAQ concerning DPOs in the public sector on 15/12/2017
Faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico... - Garante Privacy[50]

3) Documento di indirizzo su designazione, posizione e requisiti del Responsabile della protezione dei dati (RPD) in ambito pubblico on 29/04/2021 [Guidelines on appointment, position and qualifications of DPOs in the public sector]
Documento di indirizzo su designazione, posizione e compiti del... - Garante Privacy[51]

These Guidelines were adopted following investigations into complaints, alerts and questions submitted to the SA as well as on the basis of specific inspections concerning companies that provide DPO services to public bodies and in connection with a comparative analysis carried out with the SAs of other EU countries in the form of voluntary mutual assistance requests. The Guidelines provide clarifications on several issues concerning the role, position and tasks of the DPO in the public sector and suggest measures to strengthen the DPO's role in public administrations. Reference can be made in particular to the following: enhancing the role of the DPO as a contact point for the SA at the organisation; issues relating to the obligation to appoint a DPO; issues concerning the choice of an external DPO; publication and communication of the DPO's contact details; involvement of the controller, performance of the DPO's tasks and setting up a team of collaborators; incompatibility with other roles and conflicts of interests concerning both internal and external DPOs.

2. **Have you taken action (i.e., fact finding exercises, informal contact, prior consultation, investigation) towards any of the organisations concerning the designation, tasks and/or role of the DPO *prior to* launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**

The Garante has taken action with several decisions addressed at various data controllers in the public sector (including entities other than those involved in circulation of the CEF questionnaire). Examples are listed below:

- Provv. 11 February 2021, n. 54, doc. web n. 9556625[52],
- Provv. 13 May 2021, n. 193, doc. web n. 9687954[53],
- Provv. 16 September 2021, n. 318, doc. web n. 9718134[54],
- Provv. 7 April 2022, n. 119, doc. web n. 9773950[55],
- Provv. 28 April 2022, n. 163, doc. web n. 9777996[56],
- Provv. 12 May 2022, n. 174, doc. web n. 9781242[57],

[49] Available at https://www.garanteprivacy.it/faq-sul-responsabile-della-protezione-dei-dati-rpd-in-ambito-privato.
[50] Available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7322110.
[51] Available at https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9589104.
[52] Available at https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9556625.
[53] Available at https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9687954.
[54] Available at https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9718134.
[55] Available at https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9773950.
[56] Available at https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9777996.
[57] Available at https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9781242.

- Provv. 9 June 2022, n. 214, doc. web n. 9794895[58],
- Provv. 10 November 2022, n. 365, doc. web n. 9834477[59],
- Provv. 10 November 2022, n. 367, doc. web n. 9835095[60],
- Provv. 10 novembre 2022, n. 372, doc. web n. 9843603[61],
- Provv. 15 December 2022, n. 423, doc. web n. 9852800[62].

Furthermore, it should be taken into account that non-enforcement related activities were also carried out, such as public meetings promoted by the Authority, among other things, with the DPOs from Ministries, the financial administration, research organisations and the University, and banks aimed at fostering 'networking' actions with a view to strengthening their position vis-à-vis the respective controllers. Additionally, campaigns were carried out over the years aimed at urging local authorities, in particular, to communicate the contact details of their DPOs. The IT SA has already implemented several initiatives relating to the DPO's role and mission (most recently, a national conference called 'The DPO in focus', which took place on 23 June 2023 in Bologna: https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9901692), within which ideas and proposals emerged which are currently being evaluated. These contributions could be matched with the results of the questionnaire and could ultimately lead to initiatives of different nature - including regulatory, institutional, awareness-raising or training ones.

3. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**

If criticalities are detected, ad-hoc investigations will be opened to evaluate whether to adopt specific corrective measures against the data controllers, and possibly also general decisions by the Authority if common issues are found in different sectors so as to provide guidance, recommendations or suggestions.

Part IV – Other

1. **What is your general impression of the levels of awareness and compliance of the organisations you consulted concerning the designation, tasks and/or role of the DPO?**

Good, although some shortcomings have been found which point to the need for raising awareness among controllers regarding designation, role, professional preparation and involvement of the DPO in matters relating to the protection of personal data.

2. **Are there any other issues or topics that you would like to flag?**

In any case, it would be necessary to promote awareness of data protection issues within organizations so as to ensure that the DPO is perceived as a resource rather than an obstacle/cost or a mere bureaucratic requirement for the controller.

[58] Available at https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9794895.
[59] Available at https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9834477.
[60] Available at https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9835095.
[61] Available at https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9843603.
[62] Available at https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9852800.

3. Are there any leading practices of the organisations you have contacted that you would like to share?

For the time being, we are unable to indicate any.

LI SA

Liechtenstein Supervisory Authority – Datenschutzstelle Fürstentum Liechtenstein

Part I - Statistics

Please see the consolidated figures in Appendix 1.1. The answers below may refer to the questions included in Appendix 1.1.

Part II – Substantive issues

Issue 1 (the designation, knowledge and experience of the DPO / tasks and resources of the DPO): Conflict of interests

1. A number of DPOs seem to hold positions in their organisation which could give rise to a conflict of interest. In fact, some answers given in the survey highlight that some DPOs hold positions or have duties related to the (highest) management level of their organisation, where they have to make final and binding decisions on data processing activities. This may lead to conflicts with their tasks as DPOs when they have to evaluate, scrutinize and possibly criticise data processing activities in a free and independent manner.
2. Art. 38 (6) GDPR.
3. If a member of the (highest) management level acts simultaneously as a DPO, the organisation might be induced to engage in riskier data processing activities than if an independent DPO advised them. This might lead to higher risks for the data subjects concerned but also for the organisation itself.
4. Most organisations are aware of this issue and have appointed a DPO who is not part of the (highest) management. This ensures that the DPO can perform his/her tasks completely independently with no conflicts of interest.
5. Organisations with a DPO that might not be free of conflicts of interest should appoint another person as DPO and even are bound to do so in accordance with Article 38 (6) GDPR. The LI SA will raise awareness about this issue in its upcoming communication to the DPOs in LI. In particular, the LI SA will draw attention to the obligation resulting from Article 38 (6) GDPR.

Issue 2 (the designation, knowledge and experience of the DPO): Insufficient training

1. One third of the DPOs answering the questionnaire have only a maximum of 8 hours (one day) of training available to them per year in order to maintain, train and further their professional qualification and expert knowledge on data protection law and practices. In view of the LI SA, the scarce time allocated to them per year is not enough to deepen their knowledge in the required areas given that data protection is a very dynamic and complex legal area.
2. Art. 38 (2) GDPR.
3. Most DPOs answering the questionnaire are not performing their task as DPO on a full-time basis. In order to be able to truly monitor the organisation's compliance with data protection law, it is essential that DPOs are afforded enough time to maintain and develop and expand their professional expertise and knowledge. Especially in the dynamic area of data protection law, where case law continually influences the interpretation of the GDPR and national data protection law as well as the corresponding practices in organisations, DPOs require enough

time for training made available to them. This is the only way for DPOs to keep up with legal developments and to correctly advise their organisations.

4. The other two thirds of DPOs answering the questionnaire are afforded more than one day of training per year in order to maintain or train their professional qualification and expert knowledge on data protection law and practices.
5. In the view of the LI SA, all organisations should afford their DPOs a minimum of two days of training per year in order to maintain and develop and expand their professional qualities and expert knowledge on data protection law and practices. The LI SA will raise awareness about this issue in its upcoming communication to the DPOs in LI.

Issue 3 (the tasks and resources of the DPO): Lack of written description of tasks

1. Some DPOs answering the questionnaire have indicated that their management has not clearly defined the tasks incumbent on DPOs and has not provided them with a written description of the their tasks.
2. Art. 38 GDPR (However, there is no specific legal requirement to have a written description of the DPOs' tasks.)
3. None of the DPOs answering the questionnaire has indicated a specific problem arising from this issue. Nevertheless, if the tasks of the DPO are not clearly defined and no written description is given to the DPO at the beginning of his/her appointment (besides the tasks written down in the GDPR and national data protection legislation), there might arise conflicts between the DPO and the management: If it is not clear what exactly the DPO is expected to do and what not, or in which way he or she is expected to support the management in data protection matters, then he or she – acting independently – will define this himself/herself, irrespective of whether it corresponds with the expectations of the management or not. It shall be noted that a conflict between the DPO and the management about the competences and tasks of the DPO will always be to the detriment of data protection and the data subjects concerned.
4. Almost 75% of the DPOs answering the questionnaire have indicated that their management has clearly defined their role as DPO and provided them with a written description of their tasks.
5. Organisations that have not done so yet should clearly define the tasks and provide their DPOs with a written description of their tasks as soon as possible. This will help to avoid potential conflicts between the DPO and the management. The LI SA will raise awareness about this issue in its upcoming communication to the DPOs in LI.

Issue 4 (the tasks and resources of the DPO): Responsibility beyond legal duties

1. Most of the DPOs answering the questionnaire have indicated that additional tasks have been committed to them compared to those strictly envisaged by the GDPR and national data protection law. Many of these tasks are not problematic and it seems logical that the DPOs are entrusted with them, e.g. developing the organisation's data protection processes or drafting and negotiating data processing agreements. However, other tasks can become an issue, when responsibility for compliance with data protection law is shifted from the management towards the DPO. This can happen, for example, when a DPO is not only advising on data protection issues but has to decide himself/herself on data processing activities in an organisation. Furthermore, DPOs run the risk of not having enough time for their actual legal duties if they are committed with too many additional tasks and responsibilities.
2. Art. 38 (6) GDPR, Art. 39 (1) GDPR.

3. The responsibility for the processing of personal data always lies with the controller or the processor according to the GDPR and never with the DPO of an organisation. The latter is only supposed to monitor compliance with the GDPR and to inform and advise the organisation and its members on data protection. Accordingly, a DPO can never be responsible or liable for infringements of data protection law, if he or she has adhered to the tasks committed to him/her by the GDPR and national data protection law.
4. Most DPOs answering the questionnaire have additional tasks to fulfil compared to the ones foreseen by the GDPR. However, these additional tasks – most of them not problematic – vary widely between DPOs.
5. Organisations should refrain from shifting responsibility for compliance with data protection law from the management towards the DPO. In cases where DPOs have to assume personal responsibility for decisions or the lawfulness of data processing activities, such decision-making tasks and according responsibilities have to be shifted back to the management of an organisation. Furthermore, organisations should refrain from burdening the DPO with too many tasks and responsibilities that go beyond his/her actual legal duties. The LI SA will raise awareness about this issue in its upcoming communication to the DPOs in LI.

Issue 5 (the tasks and resources of the DPO): Lack of deputy

1. Only half of the DPOs answering the questionnaire have a designated deputy. The LI SA strongly recommends that organisations designate a deputy for the DPO in order to always be in a position to fulfil his/her tasks foreseen by the GDPR and national data protection law, e.g. to act as the contact point for the SA.
2. Art. 38 (4) GDPR, Art. 39 GDPR.
3. If no deputy is designated for the DPO, an organisation can face difficulties fulfilling all of the tasks of a DPO foreseen by the GDPR, if the actual DPO is absent due to vacation, illness, etc.
4. Half of the DPOs answering the questionnaire have a designated deputy.
5. If not done yet, the LI SA strongly recommends all organisations to designate a deputy for their DPO. The SA will raise awareness about this issue in its upcoming communication to the DPOs in LI.

Issue 6 (the role and position of the DPO): Insufficient involvement in data processing / data protection matters

1. Only about half of the DPOs answering the questionnaire indicate that they are usually (at least 75% of the time) getting involved and/or are consulted in handling and solving issues relating to the processing and protection of personal data in their respective organisation. The other DPOs are frequently not consulted to the extent foreseen by the GDPR or – in the worst case – are simply ignored.
2. Art. 38 (1) GDPR.
3. According to Article 38 (1) GDPR an organisation has to ensure that the DPO 'is involved, properly and in a timely manner, in all issues which relate to the protection of personal data'. If a DPO is not properly consulted or - worse - is not consulted at all, such practice does not comply with Article 38 (1) GDPR. Furthermore, it increases the likelihood of non-compliant data protection processes and/or data processing activities in an organisation, which might lead to significant risks for the data subjects concerned but also for the organisation itself.
4. The degree to which a DPO is involved in handling and solving issues relating to the processing and protection of personal data strongly varies from organisation to organisation.

5. As Article 38 (1) GDPR states, DPOs have to be involved in all issues which relate to the protection of personal data in their respective organisations. The LI SA will raise awareness on this issue in its upcoming communication to the DPOs in LI.

Part III – Actions by the SA

1. **Have you already published general guidance (e.g. guides, guidelines, etc.) regarding DPOs (including before launching the coordinated action)?**
   If yes, please provide the date, link to the guidance, and a short description of the guidelines

We have published guidance for DPOs on our website: https://www.datenschutzstelle.li/datenschutz/themen-z/datenschutzbeauftragter. In this guidance information is provided on the following topics: necessity to designate a DPO in an organisation, tasks of the DPO, cooperation of the DPO within the organisation and with the SA, liability of the DPO, communication of the contact details of the DPO, guidelines of the WP29 regarding DPOs. Additionally, an online form for communicating the DPO to the LI SA is available.

Furthermore, we organise an annual meeting (training) for all DPOs in LI. In these annual meetings for DPOs the LI SA provides information about its work, recent jurisdiction, legal developments and also presents a varying topic deemed to be of importance for and of interest to the DPOs.

2. **Have you taken action (i.e., fact finding exercises, informal contact, prior consultation, investigation) towards any of the organisations concerning the designation, tasks and/or role of the DPO *prior to* launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**

We have not taken any such action yet.

3. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**

We will inform the DPOs in LI at the next annual meeting in November 2023 about the outcome of the survey and about the main issues identified. Furthermore, we will remind the DPOs of the services offered by the LI SA to support them. Whether there will be any additional action beyond this has yet to be decided by the LI SA.

Part IV – Other

1. **What is your general impression of the levels of awareness and compliance of the organisations you consulted concerning the designation, tasks and/or role of the DPO?**

Based on the survey, our general impression is that the levels of awareness and compliance of organisations regarding their DPOs are satisfactory. In addition, most organisations appear to be compliant with respect to Articles 37 to 39 GDPR. Furthermore, most DPOs seem to be competent and

sufficiently equipped with resources to fulfil their tasks. Notwithstanding this generally satisfying impression some answers nonetheless gave room for some concern. However, given that the survey was conducted on an anonymous basis we are not able to detect those organisations which would require special attention by the LI SA. Therefore, as mentioned above, we plan to address these issues generally at our next annual meeting with all DPOs in LI and will invite them to seek support with the LI SA in case of need.

2. **Are there any other issues or topics that you would like to flag?**

No.

3. **Are there any leading practices of the organisations you have contacted that you would like to share?**

No.

LT SA

Lithuanian Supervisory Authority – State Data Protection Inspectorate

Part I - Statistics

Please see the consolidated figures in Appendix 1.1. The answers below may refer to the questions included in Appendix 1.1.

Part II – Substantive issues

1) Conflict of interests due to conflicting roles or tasks.

Some organisations have additional tasks assigned to DPOs, which include tasks relating to determining the goals and means of processing of personal data (e.g. decision-making on the processing of personal data and developing the organisation's data protection processes).

A possible conflict of interests will be investigated and guidance provided if necessary.

2) Further guidance from SAs.

All of the respondents are eager to receive further guidance from SAs and would like to be provided with Q&As / FAQs, or training materials or documents for data protection officers.

Part III – Actions by the SA

1. **Have you already published general guidance (e.g. guides, guidelines, etc.) regarding DPOs (including before launching the coordinated action)?**
   If yes, please provide the date, link to the guidance, and a short description of the guidelines

First, the Public consultation on the obligation to appoint a data protection officer[63]. A consultation on the assignment of DPOs in the private sector, which discusses the criteria, which is established in GPR Article 37 (1) (b) and (c).

Second, the 2019-06-11 Recommendation on the appointment of data protection officers in the public sector and the peculiarities of their activity regulation[64]. The purpose of the recommendation is to draw the attention of authorities or institutions to the practice observed shortcomings related to the appointment of a DPO, ensuring his independence and regulating activities in government institutions or institutions.

2. **Have you taken action (i.e., fact finding exercises, informal contact, prior consultation, investigation) towards any of the organisations concerning the designation, tasks and/or role of the DPO *prior to* launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**

[63] Available at https://vdai.lrv.lt/uploads/vdai/documents/files/Viesoji%20-%20dap_2017.pdf.
[64] Available at https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomendacija-del-DAP-viesajame-sektroiuje-2019-06-13.pdf.

No.

3. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**

The questionnaires are part of a formal investigation and the answers are being evaluated. The decision will be made by the end of the year. If the violations are identified, the State Data Protection Inspectorate will issue an order to organize the documents so that they comply with the legislation.

Part IV – Other

1. **What is your general impression of the levels of awareness and compliance of the organisations you consulted concerning the designation, tasks and/or role of the DPO?**

We did not notice any major shortcomings, and most of the organisations cooperated willingly.

2. **Are there any other issues or topics that you would like to flag?**

There are no issues.

3. **Are there any leading practices of the organisations you have contacted that you would like to share?**

None.

LV SA

Latvian Supervisory Authority – Data State Inspectorate (DVI)

Part I - Statistics

Please see the consolidated figures in Appendix 1.1. The answers below may refer to the questions included in Appendix 1.1.

Part II – Substantive issues

Analysing the responses provided during the preventive inspection, it is evident that the Institutions have appointed data protection officers who hold pivotal roles within their organizational structures. In many instances, the requirement to appoint a data protection officer is derived from the standard obligations of the GDPR, while in some cases, it is stipulated by alternative regulatory measures. This suggests that the legislator, when enacting these additional regulatory measures, has taken into consideration the escalating risks associated with data protection. As digitalization continues to expand across virtually all sectors, accompanied by heightened demands for data security, the obligation to designate data protection officers has been duly established.

The relationship between institutions that engage external service providers for the services of a data protection officer is akin to those that appoint specialists from their internal resources. This implies that institutions adopt varied measures to fulfil their data protection obligations.

Despite being a relatively new profession, with more than 50% of practitioners having 6 or more years of experience in data protection, and nearly 35% possessing over 8 years of experience in the field.

In general, the advice and recommendations of data protection officers are heeded in the course of the institution's subsequent activities in 94% of cases.

While the overall survey results suggest that institutions generally understand and value the role of the data protection officer, it is evident that there is room for improvement in this regard. For instance, it is concerning that only 30% of respondents have designated a substitute for the data protection officer, which can be crucial when the specialist is on vacation or unavailable.

Another concerning aspect is that more than 30% of institutions provide instructions to the data protection officer regarding their tasks and duties. This raises concerns about the specialist's independence when they receive instructions from management.

In general, the survey reveals positive trends regarding the data protection officer's role in organizations. However, there are inconsistencies in some areas, possibly due to a lack of full understanding of the role. This underscores the need to continue efforts to strengthen the role of the data protection officer, enhance recognition, and emphasize its importance in the context of data protection.

MT SA

Maltese Supervisory Authority – Office of the Information and Data Protection Commissioner (IDPC)

Part I - Statistics

Please see the consolidated figures in Appendix 1.1. The answers below may refer to the questions included in Appendix 1.1.

Part II – Substantive issues

Issues identified during investigations

1) Lack of resources and time afforded to the DPO

During the investigations, the most emerging issue related to the notion of resources, which includes time afforded to the DPOs. From the responses received, it can be concluded that the majority of the DPOs do not solely focus on the role of the DPO in their work. In fact, only 22.02% can allocate between 91% to 100% of their time to the DPO's tasks and duties, with 73.39% saying that they do not have a designated deputy. This must be considered jointly with the fact that an aggregate amount of (65.12%) organisations have appointed a DPO due to Article 37(1) of the DPO – in other words, a DPO was appointed due to a requirement set by the GDPR.

This issue relating to the time DPOs can allocate to their duties has also emerged in a separate but highly similar investigation conducted by this Office in early 2023, the results of which shall also be briefly considered in this Report due to their relevance. Over 80% of DPOs for public organisations have other roles and/or work responsibilities in addition to those of DPO. When asked for further comments, the lack of adequate time some DPOs have to dedicate to the tasks and duties related to the DPO was repeatedly stressed, with a significant portion of respondents stressing that their principal role prevents them from fulfilling their duties diligently. Particularly, in relation to the public sector, some DPOs have argued that the role should be a full-time one, and/or given adequate compensation for their role.

Simultaneously, a general lack of resources was registered in the public sector. Contrastingly, however, 77.06% of respondents in the private sector have said that there are sufficient resources in order to fulfil the tasks of the DPO. This is despite of the fact that the majority of respondents (52.29%) have said that there is no allocated budget to the office of the DPO. Out of the 30% who answered yes, only 15% maintained that the DPO can manage the budget independently.

Given this data, there seems to be a lack of clarity with regard to the time and resources allowed to DPOs. There seems to be a dissonance when contrasting the fact that the majority of the DPOs were appointed due to Article 37(1)(b) of the GDPR, and on the other hand the fact that most DPOs have other roles to fulfil.

Imperatively, the chief solution to this issue is strengthening communication between DPOs and C-suite level management in order to enforce awareness and importance of GDPR compliance. The independent nature of the DPO is also somewhat alack based on the responses received, due to the fact that most of the DPOs in the private sector either do not have an allocated budget, or else they cannot manage the budget independently.

2) Inadequate hours of training

It is this Office's view that another emerging issue as evidenced in the results relates to the training provided to DPOs. Question 12 asked the respondents how many hours of training the DPO is allocated in order to develop and/or maintain their professional qualities, on a yearly basis. Training, which falls

under the GDPR's Article 39(2), imposes the obligation on the controller to 'support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge'. It is concerning that the prevailing answer was between 1 to 8 hours a year (34.86% of the respondents marked this option), whilst an aggregate amount of circa 12% either said 0 hours a year, or 'I do not know or wish to answer'.

This issue is two-fold:

On one hand, it is the obligation of the controllers and processors to support the DPOs and ensuring they are able to maintain their expert knowledge. Therefore, this is a scenario wherein controllers and processors are potentially in breach of their obligations at law. On the other hand, it is vital for DPOs to progress and strengthen their training due to the ever-evolving nature of data protection legislation. It is beneficial for DPOs to not only participate in internal/external training, data protection conferences and similar event, but also have the opportunity to network with other DPOs in order to share experiences and practices.

Having a majority where the DPOs are only provided with the minimum amount of yearly training is not sufficient for DPOs to maintain their expert knowledge and keeping abreast with latest technologies and practices impacting data protection, and emerging rules or norms emanating from the Courts. An ideal solution to this would be the creation of a holistic and educative framework for DPOs, which would include a yearly continuing professional development process of accredited courses, conferences, workshops and the like. Creating a minimum threshold of mandatory training for DPOs would not only ensure the maintenance of DPO's expert knowledge on data protection but also a way for supervisory authorities to remain aware of issues DPOs encounter when fulfilling their duties as per the GDPR.

Part III – Actions by the SA

1. **Have you taken action (i.e., fact finding exercises, informal contact, prior consultation, investigation) towards any of the organisations concerning the designation, tasks and/or role of the DPO *prior to* launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**

During the months prior to the launching of the coordinated action, the IDPC was investigating a data protection complaint with a local organisation operating in the insurance and travelling sectors. During the course of the investigation the DPO who was engaging with the office occupied the position of a Chief Executive Officer. Although this issue did not relate to the subject matter of the complaint, the IDPC took immediate ex-officio action to formally raise this serious matter with the controller. An order to bring the processing operations in compliance with the provisions of the GDPR was issued. The controller fully cooperated and complied with such order within the prescribed timeframe.

2. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**

Presently, this Office is not planning to undertake any action specifically based on the results of this report, due to other already planned and ongoing activities. Having said that, we are internally considering to provide more information targeted to DPOs both on our portal and also by making use of other communication methods.

Part IV – Other

1. **What is your general impression of the levels of awareness and compliance of the organisations you consulted concerning the designation, tasks and/or role of the DPO?**

The overall general impression is encouraging. This conclusion could be drawn from the replies provided by DPOs who stated that their advice and opinions are well received and followed by the controller. Furthermore, the DPOs' expertise, gathered through questions 9 and 10, is broad and adequate, with significant numbers showing that their knowledge corresponds with the requirements of Articles 37 – 39 of the GDPR. This is indeed important as DPOs play an important role within the data protection eco-system and therefore it is positive to observe that they have the necessary skills and expertise in this area.

2. **Are there any other issues or topics that you would like to flag?**

An interesting and adjacent point to investigate may relate to DPOs' qualifications and possible certifications, since this questionnaire does not explore how DPOs obtain their expert knowledge. Although the GDPR does not impose an obligation for particular accreditations/qualifications, in practice a myriad of standardized certifications are being recognised more and more.

3. **Are there any leading practices of the organisations you have contacted that you would like to share?**

No.

NL SA

Dutch Supervisory Authority – Autoriteit Persoonsgegevens

Part I - Statistics

Please see the consolidated figures in Appendix 1.1. The answers below may refer to the questions included in Appendix 1.1.

Part II – Substantive issues

Introduction

The Dutch SA approached only DPOs that are registered with the Dutch SA. As a consequence, a 100% score is reflected on the DPO appointment rate of the approached organisations. Over 12.000 organisations in the Netherlands have registered their DPO with the Dutch SA. 946 DPOs that were contacted completed the questionnaire. Of all responding DPOs, 370 respondents are active in public administrative organisations. 576 DPOs work in the private sector.

Access to resources

28,95% of the DPOs responded that, in their opinion, they have insufficient access to resources to carry out their tasks as mandated in article 38 paragraph 2 of the GDPR.

If DPOs have insufficient resources available to carry out their tasks, it is likely that their supervision is less effective than it should be. This will not improve GDPR compliance in general. This is particularly a problem in cases where appointing a DPO is required by law.

61,94% of DPOs responded that in their opinion, they have sufficient access to resources to fulfil their tasks.

A solution could be to provide more guidance by the SA's on the interpretation of the open standard of sufficient resources. The new guidance would allow for the DPO to explicitly report on their need for resources to the highest management level. Ultimately, enforcement by the SA could also be a possible solution to stress the priority as set out by the SA's.

Conflict of interests

18,92% of DPOs responded that they are designated as DPO while also performing management tasks. The combination of both tasks could prove to be a challenge considering article 38 paragraph 6 GDPR (conflicting tasks and/or duties).

In case of a conflict of interest, the DPOs cannot perform their duties independently. As a consequence, the supervision cannot be considered independent, resulting in a dangerous decline of the DPO's oversight.

37,63% of DPOs responded that they do not have other duties and/or tasks besides those of DPO.

A possible solution to prevent DPOs from having conflicting duties and/or tasks is to provide a list of roles and/or tasks that indicate a high risk and are deemed as incompatible (by the SA) with the independent performance of the DPO's tasks.

Instructing the DPO

11,94% of DPOs responded that they received instructions by the organisation regarding their tasks and duties, despite this being a violation of article 38 paragraph 3 and 6 GDPR.

The DPOs cannot act independently when an organisation provides its DPO with instructions regarding their tasks and/or duties. Consequently, it becomes increasingly difficult for the DPO to voice the necessary concerns when these arise.

Additionally, any clear guidance by the SA could increase awareness among the organisations and DPOs on this subject. Enforcement on this subject should also be considered an option.

Reporting to the highest management

20,5% of DPOs responded that they do not report to the highest management as required by article 38 paragraph 3 GDPR.

When a DPO does not report to the highest level of management, it is questionable whether the highest management is sufficiently aware of the compliance level and the risks arising therefrom. Consequently, essential decisions made at the highest management level may be in violation of GDPR requirements.

Note: the questionnaire did not cover cases where a DPO provides information to the highest management level without being in an actual two-way conversation. In addition, if the DPO does not report to the highest management, then it is not known how many levels below the DPO actually reports.

72,41 % of DPOs confirmed that they report to the highest management at least once a year.

Resolving this matter should be done along two lines.

1. If access to top management is deliberately prevented, an enforcement measure by the SA may be most efficient.

2. DPOs should be stimulated to take the initiative to report to the highest management only.

Documenting when the DPO's advice is not followed

28,85% of DPOs replied that their advice is followed poorly or very poorly by their organisations.

12,89% of DPOs confirmed that when advice is not followed by the organisation, the reasons for this deviation are rarely or never documented. When organisations do not document reasons to not follow a DPO's advice, it is in breach of article 5 paragraph 2 GDPR as it is not able to demonstrate compliance. The EDPB guidelines on DPOs confirm it is good practice to document arguments for deviating from a DPO's advice.

The lack of the abovementioned documentation is an indication of poor overall GDPR compliance. If an organisation prioritises GDPR compliance, then it is inevitable to explicitly justify the reasons for deviating from the DPO's advice. This justification can provide valuable insights to the data subjects, the DPO and the SA as required by the transparency principle.

A possible solution is to provide more guidance on this so that these cases of a lack of awareness are reduced. In cases where deviation from the DPO's advice is intentional and undocumented, only the use of enforcement resources by the SA may be the appropriate solution.

Conclusion

The common solution in the abovementioned matters is to provide clear and concise guidance by the SA on the open standards regarding the role and positioning of a DPO. Preferably, this would be done based on updated EDPB guidelines. The issuing of clear and concise guidelines will allow all organisations to comply. Subsequently, if organisations fail to comply, a follow-up by enforcing the law seems like the logical next step.

Part III – Actions by the SA

1. **Have you taken action (i.e., fact finding exercises, informal contact, prior consultation, investigation) towards any of the organisations concerning the designation, tasks and/or role of the DPO *prior to* launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**

The Dutch SA has undertaken the following actions concerning the designation, tasks and/or role of the DPO.

1. The Dutch SA has held meetings with the highest level of management of controllers to convey the required standards regarding the independent role and position of the DPO. The Dutch SA followed up on their meetings to verify if progress was being made.

2. The Dutch DPO has asked written questions to various organisations about the combination of the DPO role and other tasks not related to the DPO role.

3. The Dutch DPO has held meetings with the highest level of management of controllers regarding the termination of a service agreement of a DPO within the terms of that service agreement and asked written questions about the non-renewal of a service agreement. In both situations, the DPOs indicated to the Dutch SA that they felt they were punished for their responsibilities as a DPO.

4. The Dutch SA also had meetings with DPOs who contact the Dutch SA. Said DPOs believe that they are constrained in fulfilling their duties. The Dutch SA discussed possible solutions and appropriate actions with the DPOs. In some cases, these discussions led to an intervention by the Dutch SA and/or the DPO.

5. The Dutch SA has a phone number and an e-mail address that are exclusively available for DPOs. DPOs can contact the Dutch SA about their questions relating to the role and position of the DPO and for guidance on GDPR related matters.

6. A newsletter for DPOs is published every quarter and the Dutch SA organises a national conference for DPOs on a regular basis.

7. A position paper on the designation, tasks and/or role of the DPO is available on the SA's website.

8. The Dutch SA has profiled companies in the Netherlands that may be required to have a DPO but have not provided a DPO's contact details to the Dutch SA. 300 of said companies have received a written request to explain why they have not provided contact details of their DPO or substantiate why a DPO is not required for their organisation.

2. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**

The Dutch SA will make an in depth analysis of the results before deciding on the actions. Nevertheless, it is clear to the Dutch SA that the aforementioned analysis will provide valuable insights for the purpose of prioritising actions and allocating the limited available resources.

Part IV – Other

1. **What is your general impression of the levels of awareness and compliance of the organisations you consulted concerning the designation, tasks and/or role of the DPO?**

The Dutch SA has the impression that the level of awareness amongst respondents is far above average. This is hardly surprising since only registered DPOs were invited to complete the questionnaire.

2. **Are there any other issues or topics that you would like to flag?**

The Dutch SA found that in many meetings with controllers regarding the position and role of the DPO, awareness at the highest management level required additional training. In addition, open standards were often the point of discussion. Controllers oftentimes do not meet the requirement for DPOs to report to the highest management.

3. **Are there any leading practices of the organisations you have contacted that you would like to share?**

N/A.

PL SA

Polish Supervisory Authority – UODO

Part I - Statistics

The Polish Supervisory Authority - UODO, while participating in the CEF DPO action, decided not to send the form developed as part of the CEF DPO. This decision was due to the fact that, prior to the launch of the CEF DPO, the Polish SA had already sent 27 questions prepared by this authority to national controllers and processors (both from the public and private sector), which addressed the main obligations of controllers to ensure the proper performance of the DPO's tasks (Articles 37-39 GDPR). More information on the Polish SA's action, as well as the questions sent by the authority, can be found on the website: https://archiwum.uodo.gov.pl/en/553/1325.

The entities to which questions were addressed by the Polish SA, exercising their powers under Article 58(1)(a) and (e) GDPR, were requested to provide detailed explanations of the arrangements adopted for each of their obligations under Articles 37-39 GDPR and to demonstrate this accordingly, in accordance with the principle of accountability. Proceedings initiated following responses received in this regard are still pending.

Therefore, in order not to mislead the entities as to the purpose of the previous action, Polish SA did not participate in the distribution of the form developed under the CEF DPO action, due to its own questions sent regarding the function of the DPO in the organisation and the national investigations conducted as a result.

Therefore, Appendix 1.1 does not include the PL SA's figures.

Part II – Substantive issues

In several entities, we have identified the problem where companies, which provided DPOs services (outsourcing), provided at the same time the services consisting in performing on behalf of the controller the so-called "implementation of GDPR" as well as other services related to risk analysis and assessment, handling requests and claims of data subjects, broadly understood information security.

Thus, the same person decided on the rules for the processing of personal data, how to perform the duties of the controller, identifying and assessing the risks associated with the processing and safeguarding of personal data, and then – in the performance of the position of the DPO – assessed the correctness of the decisions and solutions taken by the DPO, which led to situations where the DPO monitored its own activities, i.e. a conflict of interests, which is expressly prohibited by Article 38(6) GDPR.

In accordance with Article 38 (6) GDPR, the DPO may carry out other tasks and responsibilities, provided that the controller or processor ensures that those tasks and responsibilities do not result in a conflict of interests. Due to the nature of the tasks of the DPO focusing on advising and monitoring the activities of the controller in terms of the compliance of personal data processing operations with the data protection legislation and the requirement to perform this function independently, the controller should not impose on the DPO tasks which, in accordance with the provisions GDPR, belong to the controller. Adopting a different assumption, where the DPO would be responsible for carrying out a specific task of the controller, e.g. breach notification, while monitoring the compliance of this task with the provisions on the protection of personal data, as required by the provisions of Article 39

(1)(b) GDPR, as a result, would lead to a situation where the DPO would de facto supervise its own activities, i.e. a conflict of interests.

A conflict of interest occurs, inter alia, where the proper performance of the tasks of the DPO, indicated in Article 38(4) GDPR and Article 39 GDPR, with the implementation of other tasks, because there is a contradiction between the tasks, which prevents them from being properly carried out. In the case of a DPO, such a contradiction may result from the DPO acting simultaneously in two roles or taking actions or decisions, which must then be assessed in accordance with Article 39(1)(b) GDPR.

A DPO with a special status in the area of ensuring proper compliance with data protection legislation must be guaranteed for this purpose appropriate conditions of operation, i.e. those which enable DPO to effectively, independently and correctly fulfil its obligations under the law, as is apparent from Article 38(1)-(3) GDPR. Imposing obligations on DPOs leading to a conflict of interests puts into question not only the ability of the DPO to perform effectively the tasks to which it is required by Article 39 GDPR, but undermines the very of the DPO institution, based primarily on the independence of the functioning of the DPO.

In addition, the following problems were identified in several proceedings: the absence of procedures to ensure that conflict of interests are avoided, the conclusion of a data processing agreement with third-party DPOs at the same time, that runs counter to the provisions of Article 38(3) GDPR - the duty of the controller to ensure that the DPO does not receive instructions concerning its tasks, the representation of controllers by the DPO as proxies, the failure of the DPO to be subject to the highest management of the controller, the failure to ensure that recommendations to the DPO regarding the sphere of data protection are addressed to the DPO, failure to demonstrate that the controller provides the DPO with adequate resources, including raising the level of expertise.

Part III – Actions by the SA

1. **Have you already published general guidance (e.g. guides, guidelines, etc.) regarding DPOs (including before launching the coordinated action)?**
   If yes, please provide the date, link to the guidance, and a short description of the guidelines

These guidelines and answers were published by the Polish SA both before and after the entry into application GDPR. Before the entry into application of GDPR, the Polish SA maintained an information website dedicated for Information Security Administrators (ABI) - the predecessors of the Data Protection Officers - where, in addition to explaining the functioning and status of the ABI, the Polish SA also provided guidance and answers to questions addressed the authority regarding the Data Protection Officers and the GDPR. Since 25 May 2018, the Data Protection Officers' tab has been kept on the website of the Polish SA, divided into the following sections:

- Designation and status of DPO (present UODO website - https://uodo.gov.pl/pl/495, https://www.uodo.gov.pl/en/p/for-dpos, previous UODO website - https://archiwum.uodo.gov.pl/p/wyznaczenie-i-status-iod).
- Notifications by the President of the UODO related to DPO – (previous UODO website - https://archiwum.uodo.gov.pl/pl/p/zawiadomienia-prezesa-uodo-zwiazane-z-iod)
- Tasks of DPO – (previous UODO website - https://archiwum.uodo.gov.pl/pl/p/zadania-iod).

In the tab called the Data Protection Officer, answers to questions raised by officers and controllers in this regard were published. The guidance provided was intended to facilitate their compliance with the obligations and tasks imposed by GDPR and to develop appropriate solutions tailored to their organisation. It addresses issues relating to the designation and status of the DPO (including, inter alia, detailed guidance on the DPO's qualifications, conflict of interests, the assessment of the admissibility of combining position of the DPO with various other roles, clarifications regarding the exclusion of the

possibility to conclude a data processing agreement with an external DPO and providing the DPO with periodic resources) and the tasks of the DPOs (in particular which tasks are assigned to the DPO and which tasks are to be carried out by the controller and should not be transferred to the DPO). The tab also contains detailed instructions on the correct notification of the Designation of a data protection officer to the supervisory authority and the publication of the DPO's contact details (https://www.uodo.gov.pl/en/679/1543) by the controller or processor on their website for the sake of data subjects. The DPO tasks section provided guidance on how to resolve the specific problems encountered by the controller in their practice in relation to the reasons for processing personal data, the concepts of 'controller', 'joint controller', 'processor', 'controller', obligations and answers to questions concerning the making available of personal data.

The authority stressed in its communications that the decision to select the appropriate person to act as a DPO must be taken in full knowledge of the controller's responsibility for the compliance with the law. The controller must assess a number of factors before appointing a specific person to act as DPO. The controller's assessment should take into account the effective availability of the DPO, the ability of the DPO to acquire detailed knowledge of the functioning of the organisation, the DPO's availability of sufficient time for the scope of the tasks and the specificities of the data processing operations, the size and organisational structure of the controller and the need to avoid conflict of interests. It was our intention to provide such guidance as it was important to ensure that the DPO has the right status which translates into the proper performance of the DPO's tasks.

The Polish supervisory authority has repeatedly addressed the issue of conflict of interests and allows the position of DPO to be discharged with various other positions, e.g. a classified information protection officer, the head of the organisational unit, the IT system administrator, a barrister or legal advisor. In each of its recommendations on the status of DPO, the Authority stressed that the assessment of whether there is a conflict of interests should be assessed on a case-by-case basis, taking into account the specific circumstances. This means that the possibility of a conflict should be continuously monitored, as the causes of such conflict may also arise at a later stage after the DPO has taken up the position. In doing so, the controller should take into account, inter alia, the following criteria: organisational (the DPO should be directly accountable to the top management of the establishment), substantive (other duties should not adversely affect the independent performance of DPO tasks), temporary (the DPO should have sufficient time to perform its tasks, taking into account, inter alia, the number of duties or the complexity of the duties).

In response to questions from DPOs, the Polish supervisory authority referred to the issue of the obligation of the controller by providing resources necessary for the DPO in Article 38 (2) GDPR. This controller's obligation is closely linked to the DPO's planning of work and the presentation of this plan to the controller (processor). The establishment of an action plan by the DPO facilitates the best and real use of the resources at his/her disposal as a DPO. The establishment of the plan helps to determine whether these resources are sufficient and whether, in all monitored areas, the DPO is provided by the controller with the cooperation of those who process personal data and have knowledge of the processing of personal data. It is important that the controller's internal procedures are adequately regulated in this regard. Such a plan should take into account a multitude of factors depending on the specific characteristics of the controller and its processing procedure (activities). It needs to be aligned with the risk assessment carried out in the organisation and giving higher priority to areas that are of particular relevance to the data protection regime of a specific controller (https://archiwum.uodo.gov.pl/pl/225/1870). The provision of adequate resources and the work plan of the DPO should be reflected in the internal rules of the controller (processor).

In addition, a lot of information on this issue, as well as the proper performance of DPO tasks, can be found in the Data Protection Officers' Newsletter, which has been issued cyclically since 2019. The 'Newsletter UODO for Data Protection Supervisors' archives for the period April 2019 – November 2022 is available at the following link: https://archiwum.uodo.gov.pl/p/archiwum-newslettera-dla-iod/. Further numbers of the 'Newsletter UODO for Data Protection Supervisors' (since March 'UODO Bulletin') can be found at https://uodo.gov.pl/pl/p/archiwum-biuletynu-dla-iod.

From 2016 to 2019, the Polish supervisory authority provided a cycle of free training for DPOs for data protection officers (DPOs) from selected sectors (e.g. education, medical, judiciary, foundations and associations, and social assistance centres). Sectoral training focused on new EU data protection rules and national legislation applicable to data processing in a specific field of activity. This training not only raised the level of knowledge of the DPO serving the industry, but also provided an opportunity to exchange experiences, solutions and good practices between participants in these meetings. We also delivered a training cycle on selected principles and obligations stemming from personal data protection provisions, e.g. transparency and compliance with information obligations (Articles 13, 14 GDPR), transfers of personal data to third countries (Articles 44 to 49 GDPR), personal data breach notifications (Article 33 GDPR), carrying out a data protection impact assessment (Article 35 GDPR). Separate training for DPOs was devoted to the provisions adopted in Poland on the basis GDPR.

Since February 2019, the Polish supervisory authority launched a helpline for the DPO, which in March 2020 was turned into a helpline for all stakeholders, including DPOs.

2. **Have you taken action (i.e., fact finding exercises, informal contact, prior consultation, investigation) towards any of the organisations concerning the designation, tasks and/or role of the DPO *prior to* launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**

Since the beginning of the application of GDPR, both in the framework of ongoing investigations and in response to cases of non-compliance with DPO's tasks reported to us, we have taken action under our powers, as set out in Article 58 of GDPR. Compliance with the provisions relating to the proper designation and functioning of the DPO was checked during the basic control activities. The control covered, inter alia, the obligation to designate an DPO, the notification to the supervisory authority of the designation or dismissal of an DPO, the provision of the first and last name of the DPO on the controller's website, the position of the DPO in the organisation, the involvement of the DPO data protection issues, and the possible existence of a conflict of interests.

In most cases, this verification was positive and did not give rise to corrective powers. It was only in a few cases that the UODO found irregularities in relation to the existence of the conflict of interests, e.g. the performance of the position of DPO by the municipal secretary, or the failure to consult the DPO of the personal data processing operations undertaken.

Several infringements related to the performance of the position of DPO required corrective action by the supervisory authority as set out in Article 58(2) GDPR, including an order to designate a data protection officer in a housing cooperative and to impose an administrative fine for the DPO's performance of his/her tasks without taking due account of the risks associated with processing operations and of not involving the DPO in the processing operations carried out.

As far as irregularities reported by data protection officers (and sometimes by other entities) are concerned, so far there have not been many such signals and they have mainly concerned the following:

- failure to publish the DPO's first and last name on the controller's website
  failure to update the DPO's contact details on the controller's website
- the adoption of procedures imposing on the DPO duties resulting in a conflict of interests
- providing in the organisational rules that the DPO can be dismissed at any time
- the reasons for the DPO's dismissal
- the positioning of the DPO in the organisational structure of the controller was incorrect: the DPO did not report directly to the highest management
- failure to provide the DPO with sufficient time and other resources necessary to carry out his/her tasks
- failure to provide the DPO with the financial and infrastructural support as well as the possibility to update knowledge
- omission of the DPO in cases concerning the processing of personal data (including those in which the controllers asked for the opinion of the Polish SA without asking the DPO first)

In each situation reported by the DPOs pursuant to Article 58(1) GDPR. Points (a) and (e) of GDPR, the Polish supervisory authority called on controllers to explain the solutions they had adopted in relation to a specific obligation under personal data protection law, together with detailed and evidence-based information on the regulations and practices adopted to properly comply with that obligation. In all these cases, controllers indicated that they had taken steps to bring their activities in line with the DPO's tasks by providing revised, detailed organisational arrangements for this purpose. Only one case was the subject of a decision in which the supervisory authority issued a reprimand finding that one hospital had infringed Article 38(6) GDPR, in so far as the hospital imposed on the DPO an obligation to grant authorizations to process personal data for the staff.

3. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**

In view of the identified GDPR infringements, it is envisaged to initiate administrative proceedings and to issue decisions requiring the DPO's operating conditions to be brought into line with the requirements of GDPR and the imposition of fines in cases where there are grounds for such a sanction.

Part IV – Other

1. **What is your general impression of the levels of awareness and compliance of the organisations you consulted concerning the designation, tasks and/or role of the DPO?**

It has been observed that, in some cases, the level of awareness is insufficient, whereby, as a general rule, controllers are aware and comply with key standards stemming from the rules on the performance of DPO's tasks.

2. **Are there any other issues or topics that you would like to flag?**

As part of our activities of verifying compliance with the DPO tasks in several organisations, we have identified the problem of the controller imposing on the DPO the task of maintaining a record of processing activities, resulting in a conflict of interests referred to in Article 38(6) GDPR. The DPO cannot take actions or decisions that must then be subject to his/her assessment in accordance with Article 39 (1) (b) GDPR. From the wording of Article 30 (1) GDPR it follows that maintaining a register of processing activities is the responsibility of the controller.

In our view, the current wording of the Guidelines on Data Protection Officers WP 243 rev.01, allowing the DPO to carry out the controller's task of maintaining a record of processing activities, leads to a conflict of interests prohibited by Article 38 (6) GDPR.

In para 4.5. on page 19 of the abovementioned Guidelines the Article 29 Working Party indicated that: "In practice, DPOs often create inventories and hold a register of processing operations based on information provided to them by the various departments in their organization responsible for the processing of personal data. This practice has been established under many current national laws and under the data protection rules applicable to the EU institutions and bodies."

In a footnote, the Article 29 Working Party referred to Article 24 (1) (d) of Regulation (EC) 45/2001, which defined the designation and tasks of the DPO. In accordance with Article 24(1d), which is no longer in force, it was the responsibility of the Data Protection Officer to maintain a record of the processing operations carried out by the controller. Nevertheless, Regulation (EC) 45/2001 was repealed by 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.

The current Regulation 2018/1725, as well as the GDPR indicates in Article 30 GDPR that each controller shall maintain a record of processing activities under its responsibility. Furthermore, Article 44(6) of Regulation 2018/1725 relating to the status of DPOs indicates (similarly to the GDPR) that the Data Protection Officer may perform other tasks and responsibilities. The controller or processor shall ensure that such tasks and responsibilities do not give rise to a conflict of interest.

In addition, it should be pointed out that the practice of maintaining a register of processing activities referred to in the Guidelines has not been developed as a result of the application of the provisions of Regulation 2016/679, but of acts which were in force before the entry into force of that regulation.

What is more, the Guidelines state that: "Article 39(1) provides for a list of tasks that the DPO must have as a minimum. Therefore, nothing prevents the controller or the processor from assigning the DPO with the task of maintaining the record of processing operations under the responsibility of the controller or the processor."

Indeed, the list of the tasks of the DPO is not exhaustive, but Article 38(6) GDPR should always be taken into account when imposing other tasks on the DPO, i.e. that the tasks imposed by the controller on the DPO cannot cause a conflict of interest.

It is worth mentioning that such recommendations as to the admissibility of maintaining a record of processing activities by the DPO by the Polish SA and published on its website (https://archiwum.uodo.gov.pl/pl/225/659). In that case, Polish SA explained that it was in accordance with Article 30 (1 – 2) GDPR, it is for the controller to maintain a record of the personal data processing activities for which it is responsible and for the processor to maintain a record of the categories of

processing activities carried out on behalf of the controller. Those entities are responsible for the effective implementation of that obligation and be ready to demonstrate this at the request of the data protection authorities. On the other hand, the Data Protection Officer, as a professional, can only assist the controller in establishing and maintaining records by, for example, advising it on matters relating to the implementation of that obligation.

Another problem identified was the issue of giving the DPO a mandate to act on behalf of the controller (representation of the controller) before a supervisory authority and a court in personal data protection cases. Although the Polish proceedings before both the court and the supervisory authority do not expressly provide for the data protection officer to be excluded from the circle of persons who may be legal representatives in data protection matters, the granting of such a power of attorney is contrary to the prohibition of entrusting DPOs with tasks giving rise to a conflict of interest (Article 38(6) GDPR) and the prohibition of giving instructions to the DPO in the performance of his or her tasks (Article 38(3) GDPR). The task of the trustee is to protect the principal's interests, act in accordance with the instructions and suggestions of the principal, which is contrary to the independence of the Data Protection Officer as guaranteed by GDPR. On the other hand, the DPO's main objective is not to act solely in the interest of the controller, as demonstrated both by the scope of the DPO's tasks and by the guarantees of its independence. The DPO's main task is, inter alia, to monitor and advise the controller's compliance with the rules on the protection of personal data. Therefore, the DPO's role as representative in matters relating to the protection of personal data is in conflict with the prohibition on entrusting DPOs with tasks giving rise to a conflict of interest. The DPO, acting as the controller's representative for the protection of personal data before a supervisory authority or a court, shall, on behalf of the principal, clarify the processing of personal data by the controller. Acting with the will and interest of the principal in these explanations, it could be forced to overlook its own observations and recommendations that it had developed as DPO. In addition to the above arguments, the Polish SA should point out that the DPO, in view of its role as an advisor and monitoring body independently of compliance with the rules on the protection of personal data, should, for its part, identify and alert the controller in good time to the risk of such a conflict. This makes it possible to prevent any potential conflict of interests in a timely manner. In such a case, the DPO should refrain from acting on behalf of the controller or terminate the power of attorney granted to him or her.

Another important problem raised by the Polish SA is the incorrect practice of concluding a data processing agreement between a controller and a DPO who is not an employee of the DPO. The Polish SA referred to this problem by publishing on its website answers to DPOs' questions on this issue (https://archiwum.uodo.gov.pl/pl/223/2050, https://archiwum.uodo.gov.pl/pl/223/2092). The Polish SA pointed out that the conclusion of an entrustment agreement between the controller and the DPO was in conflict with the prohibition on instructing the DPO to perform the tasks and to avoid any conflict of interest. According to the GDPR, the processor is obliged to follow the instructions given by the controller. On the other hand, with regard to the Data Protection Officer, the controller and processor are, inter alia, required to ensure that the DPO is not instructed to carry out his or her tasks (Article 38 (4) GDPR). In addition, the possibility for a person with whom a service contract is concluded to carry out tasks other than those laid down in the GDPR is limited by the prohibition of a conflict of interest in this respect (Article 38(6) GDPR).

The essence of the above position is that the existence of a DPO as a processor who is to carry out data processing tasks in the name and on behalf of the controller and is required to comply strictly with the instructions given to him in that regard by the controller, undermines the DPO's independence. On the other hand, in the controller-processor relationship, there is no space for the processor to act independently, in any way inconsistent with the controller's instructions. For this reason, the DPO cannot act as a processor (be a party to the entrustment agreement) and act on the instructions of the

controller, as this is contrary to the independence of the DPO guaranteed by the GDPR. This independence is necessary in order for the DPO to be able to properly carry out his or her tasks listed in Article 39 (1) GDPR.

The controller and the external DPO designated by the controller shall combine the service contract referred to in Article 37 (6) GDPR. The purpose of this service agreement should be the tasks referred to in Article 39 (1) GDPR, implemented in compliance with the conditions laid down in the provisions of GDPR, in such a way as to guarantee the independence of the DPO.

Access to the personal data necessary to carry out the DPO's tasks shall be provided by law. Article 38 (2) GDPR provides that the controller and processor shall support the DPO in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge. This also applies to the external data protection officer performing his or her tasks under a service contract.

3. Are there any leading practices of the organisations you have contacted that you would like to share?

Our investigations and audits have shown that the least problematic to reliably demonstrate compliance with the obligations under Articles 37-39 of GDPR had organisations that had carefully considered and subsequently implemented in their internal regulations specific rules and procedures adapted to their activities.

This accountability-based approach of controllers and processors was already emphasised by the Polish supervisory authority in its educational material. This approach was also guided by the drafting of 27 questions created to verify compliance with the provisions regarding the DPO. In questions concerning, for example, the involvement of the DPO in cases of protection of personal data or conflict of interest, the authority indicated that information should be provided on the appropriate mechanisms (solutions, procedures) to ensure compliance with a given provision of GDPR.

PT SA

Portuguese Supervisory Authority – Comissão Nacional de Proteção de Dados (CNPD)

Part I - Statistics

Please see the consolidated figures in Appendix 1.1. The answers below may refer to the questions included in Appendix 1.1.

Part II – Substantive issues

Introduction

The PT SA decided to address the questionnaire only to DPOs and to do it directly. For that purpose, the PT SA used the contact details of the DPO, which were notified to the authority. The objective was to get the most accurate picture of their position, role and activities, without any kind of constraints. To reinforce this action, the PT SA decided to make the survey anonymous.

The PT SA contacted the full universe of DPOs notified, even if they were representing more than one organisation. In such case, they would have to ask for an additional token to be able to reply to the questionnaire for each organisations where they are DPOs.

Therefore, in total, the questionnaire was addressed to 2,671 DPOs of 2,671 organisations, and we received 625 replies, which represents about 23.40 % of the target.

The questionnaire was available for the DPOs to answer during six weeks, between first of April until 15th of May 2023.

Since the questionnaire was anonymous and there was no possibility to identify the organisations, the PT SA has also collected some additional information regarding the nature of the organisation, sector and dimension, in order to obtain an overview of the organisations concerned and get a better reading of the results.

It is interesting to highlight that 60.64% of the respondents were DPOs of private sector, while 39.36% were of public sector.

Within the private sector, the majority of respondents (58.6%) were SMEs. In the public sector, the majority (64.22%) were DPOs from regional or local administrations.

Based on the replies received, the PT SA identified the main following issues of concern:

1) Potential conflict of interests

One of the findings concern the potential conflict of interests between the tasks of the DPO and other tasks performed by the DPO within the same organisation, in particular related to highest management duties.

This would be in breach of Article 38(6) of GDPR.

Assessing the replies to Question 8 of this report, related to the department the DPO belongs, whenever the DPO is a staff member of the organisation, it is noticed that almost 18% of the DPO perform functions at the highest level of management. When crosschecking Question 8 with Question 25, we can confirm that the replies are consistent, since in Question 25 also about 18% of the respondents have as Management as an additional task/role in the organisation.

This means that they are decision-makers as well, what most likely has consequence at the level of data processing, what constitute a conflict of interest with the DPO tasks.

This situation does occur in an uneven way: about 2/3 for the private sector and 1/3 for the public administration.

2) Lack of training

Another relevant finding relates to the lack of training made available to DPOs to develop or maintain their professional qualities and expert knowledge.

This would be in breach of Article 38(2) of GDPR.

When assessing the replies to Question 12 of this report, it is evident that there is a significant lack of training. It is observed, notably, that the majority of the DPOs (53.14 %) who have some kind of training does have less than 32 hours per year in training, what is less than a working week.

In this question, the PT SA added a question to the common questionnaire, asking how many DPOs had no training (zero hours). Surprisingly, about 11.5 % of the respondents said they received no training at all. In addition, it should be noted that almost 10% of the respondents did not know or wish to answer. Finally, only 25% of the DPO answered they had training for more than 32 hours per year.

When comparing public and private sectors, one can detect that the situation in the private organisations is slightly better than in the public bodies, especially when it comes to training of more than 32 hours per year.

This issue raises much concern, since in Portugal the DPOs have little experience as data protection officers, because before GDPR such role did not exist in the national legislation. When crosschecking with the replies given to Question 7, on the average duration of the DPO appointment, it is eminent that 65% of the respondents state they have less than 2 years in the job and, if extended that period for less than 4 years, we got a 94% of DPOs.

Therefore, in a scenario where DPOs do not have much experience in performing DPOs tasks, the lack of training becomes even more significant as a problem to be tackled.

3) Tasks unduly allocated to DPOs

Another issue identified concerns the tasks assigned to the DPO by the organisation which are legally entrusted to the controller/processor and not to the DPO.

This would be in breach of Article 39(1) of GDPR.

When analysing the replies to Question 17, about the additional tasks committed to the DPO, it should be underlined firstly that almost 20 % of the respondents did not know or wish to answer, with split results for both public and private sectors. In our opinion, this high percentage is an indicator of wrongdoing by the organisations.

When looking into the tasks description, it is clear that DPOs are performing tasks, which are incorrectly allocated to them. Instead of providing advice on DPIAs, internal policies and procedures and data processing agreements, for instance, the DPOs are drafting themselves the documents, which is a responsibility of the organisation.

Considering the statistics, it is obvious that this deviation of tasks is much more notorious in the private sector than in the public, with much fewer cases.

The replies to Question 16.b already flag a problem in this regard when around 77.30% of the respondents state that the DPOs are committed to the drafting and maintaining of the policies of the organisation in relation to the protection of personal data.

It may also be pointed out that in Question 15 on whether the written description of the DPO tasks cover the actual tasks of the DPO in the organisation, a high number of DPOs (more than 20%) did not know or wish to answer. This may indicate that there are tasks unduly assigned to the DPO, which, for that reason, are not formally described.

4) Lack of independence

A significant finding concerns the lack of independence of the DPO when acknowledging that receives instructions from the organisation regarding the exercise of his or her tasks and duties.

This would be in breach of Article 38(3), first sentence, of GDPR.

When assessing Question 32 of this report, it is noted that 28 % of the respondents answered that they receive instructions, which is a very high percentage for such a key-issue. Additionally, if we take into consideration the number of DPOs who stated they do not wish to answer (7.5%), the issue of lack of independence is likely to affect more than 35 % of the respondents.

When comparing the public and private sectors, one find out that this situation is more problematic in the private sector (with a split of 2/3 for the private organisations and 1/3 for the public ones).

The issue raised above, under C. on the tasks unduly allocated to DPOs and that are direct responsibility of the controller or processor, may also be linked to this issue, as they potentially lead to giving instructions to the DPO.

This is a very serious matter requiring to be addressed by data protection supervisory authorities.

5) Lack of reporting

Another important finding relates to the deficiencies in the reporting of the DPOs, reflected in the high numbers of DPOs stating that they do not report or they do not report to the highest management level of the controller or processor, even when such reporting is expected. Depending on how the questions were interpreted by the respondents, the answers may reveal that reporting is done to lower levels of management inside the organisation.

This would be in breach of Article 38(3), last sentence, of GDPR.

When analysing the replies to Question 34, it is observed that 36.8% of the respondents say no reporting is done, among those 178 DPOs state that no reporting is expected. It is also meaningful that almost 14% of the DPOs chose not to answer whether they report and how often, since they picked the option do not know or wish to answer, which might be an indicator that the legal requirement is not met. In this question, the lack of reporting is more evident in the private sector than in the public sector.

These results are somehow confirmed by the replies to Q35, about the ways used for the data protection officer's to report. In this question, where the PT SA introduced a new possibility: no reporting at all, 21.6% of the DPOs selected this option. On the other hand, in Question 35, also 13.3% of DPOs picked the option do not know or wish to answer.

Also relevant to retain that 17% of the respondents expressed to report in other way. This could mean that the reports are not made in a written form or that they do not report to the boards or management group of the organisation but to a lower level.

The answers related to the DPO reporting demonstrate, on the other hand, that the data protection officers may not be involved by the organisations in matters on which they should be consulted, in spite of the answers provided in Question 27 and Question 28 that show a high level of involvement on data protection issues. Furthermore, the lack of reporting may also be a hint that some DPOs may not be proactive enough in the exercise of their tasks.

This is a matter that surely needs to be clarified as to the extension of lack of reporting and may benefit from guidance of data protection authorities on the interpretation of this legal requirement.

6) Lack of resources

The majority of the respondents consider they do not have sufficient resources in order to fulfil the tasks of DPO.

This would be in breach of Article 38(2) of GDPR.

In fact, 346 respondents out of 625 flag this problem of lack of resources, what represents around 55%.The situation has more impact in the public sector, where around 70% of the DPOs answered not having enough resources to perform their legal tasks. In the private sector, though still with a high percentage, when compared with the public bodies, the statistics is lower, achieving 47%.

The replies to Question 23 on the allocation of a dedicated budget to the DPO function (only happens in 16% of the cases and mostly in the private sector) may be a plain signal that the allocation of resources to the DPO is not a given fact or a standard resolution of the organisations.

This is a very concerned issue, since it means that the DPOs acknowledge not being able to fulfil their tasks due to the lack of resources. The kind of resources is not determined in the questionnaire; however they could be linked not only with financial resources but also with human resources, including the time to allocate to the exercise of the DPO duties, in view of the performance of cumulative tasks (as stemming from Question 25 replies).

Part III – Actions by the SA

1. **Have you already published general guidance (e.g. guides, guidelines, etc.) regarding DPOs (including before launching the coordinated action)?**
   If yes, please provide the date, link to the guidance, and a short description of the guidelines

The PT Supervisory Authority provided guidance on two issues regarding DPOs in the public sector:

- Guidelines on incompatibility between the exercise of cumulative functions as data protection officer and as officer responsible for Access to Documents, of 11 April 2023[65].
- Draft Guidelines on the performance evaluation of staff when being also DPO, of 18 April 2023, and submitted to public consultation until June 2023[66]. The final text has not been adopted yet. This guidance intends to safeguard the independence of the DPO when cumulating those tasks with other kind of work as staff member, while ensuring that the staff is not affected in his or her career for being a DPO.

2. **Have you taken action (i.e., fact finding exercises, informal contact, prior consultation, investigation) towards any of the organisations concerning the designation, tasks and/or role of the DPO *prior to* launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**

The PT SA has opened several infringement procedures against local governments and other public bodies related to the lack of designation of DPO, lack of publication of the DPO contact details and/or lack of communication of such contacts to the data protection supervisory authority. The SA has been applying fines in this regard.

[65] 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.
[66] Available at https://www.cnpd.pt/media/vy3h045x/projeto-de-orienta%C3%A7%C3%A3o_avalia%C3%A7%C3%A3o-epd.pdf.

3. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**

This coordinated action was developed only as a fact-finding exercise. Therefore, the mainly objective is to get an overview of the situation of DPOs and to identify potential problems regarding the position and role of the data protection officer.

The result will most probably lead to the issuance of recommendations and/or guidance to clarify the interpretation and application of the legal provisions, and thus, to contribute to reinforce the DPOs role within the organisations, as well as generally improve compliance with the GDPR.

Part IV – Other

1. **What is your general impression of the levels of awareness and compliance of the organisations you consulted concerning the designation, tasks and/or role of the DPO?**

The replies to the questionnaire made available by the PT SA were only addressed to DPOs. Accordingly, their perception of the situation is relevant and might be more accurate as to the factual situation of the organisations. Based on that, our general impression is that there is a reasonable level of awareness but a significant deficit of compliance.

When assessing the replies and crosschecking the answers, having into consideration that most of the respondents are from SME in the private sector or from local governments in the public sector, it seems that the position and role of the DPOs face major challenges within the organisations, in particular the ones of smaller dimension and resources.

Apart from the main concerns already raised in Part II of this Report, it could be noted in general terms that the organisations that have designated a DPO chose a member of its staff; which in the great majority of the organisations do not perform their tasks in full time, but cumulate with additional duties.

Besides, the majority of the respondents do not have any supporting staff (FTE) to assist them in the fulfilment of DPOs tasks, and only a few percentage have deputy DPOs. Moreover, it is evident that the DPOs perform duties related to data processing activities, which go beyond their strict legal functions and are responsibility of the controllers or processors.

It should be also emphasised that, in spite of the positive trend to consult the DPO and follow their advice, in a significant number of cases it is reported that DPOs do not have enough information to fulfil their tasks.

In conclusion, there are many visible shortcomings in the compliance of the GDPR related to Articles 37 to 39. Even when having designated a DPO, then a very high percentage of organisations do not provide the DPOs with proper conditions for the fulfilment of their tasks, such as insufficient resources, lack of training, not ensuring the DPO's independent position.

2. **Are there any other issues or topics that you would like to flag?**

No.

3. Are there any leading practices of the organisations you have contacted that you would like to share?

Not applicable.

SE SA

Swedish Supervisory Authority – Swedish Authority for Privacy Protection's (IMY)

Part I - Statistics

Please see the consolidated figures in Appendix 1.1. The answers below may refer to the questions included in Appendix 1.1.

Part II – Substantive issues

1) Other tasks or roles in addition to the tasks of the DPO - when is there a risk of conflict of interest?

1. Main issue: The SE SA has noted that several DPO's have other tasks/ roles outside of their role as DPO which in some situations potentially could result in a conflict of interest with the assignment as DPO.
2. Provision: Article 38(6) GDPR.
3. Development of the issue: The responses show a wide variety of other roles/tasks assigned to the DPO. There are examples of operating responsibilities, follow-up responsibilities, management responsibilities or administrator roles etc. within several different areas i.e. information security, compliance, administrative law and data protection.
4. Possible solutions: One solution could be to clarify the term 'conflict of interests' further than what is presented in the guidelines from the article 29 group regarding data protections officers, e.g. through more examples of what other tasks are normally acceptable and not. It may be possible to make this assessment easier for the data controller by developing a checklist of questions that the data controller should ask about what the proposed other tasks involve in terms of decision-making etc. to make it easier to determine whether or not there may be a conflict of interest.

2) Differences concerning how many hours of training the DPO have in order to develop and/or maintain their professional qualities and expert knowledge on data protection law and practices annually

1. Main issue: The SE SA has noticed that there are differences concerning how many hours of training per year the DPO have to develop and/or maintain their qualifications and expertise in data protection law, which may pose a problem for some DPO's in maintaining expertise.
2. Provision: Article 38(2) GDPR.
3. Development of the issue: The answers show a wide variation regarding how many hours of training the DPO have in order to develop and/or maintain their professional qualities and expert knowledge on data protection law and practices annually. Some estimate the range is between 5-10 hours per year and others to 150 hours per year.
4. Possible solutions: The responses indicate that data controllers need guidance on this issue. This specifically since the SE SA performed a survey during 2022 where the data protections officers expressed that they did not receive enough hours for further education.

3) Differences regarding the resources of the DPO

1. Main issue: The SE SA has noticed that there are differences regarding the amount of resources the DPO have in order to fulfill their tasks, indicating difficulties in assessing the required resources.
2. Provision: Article 38(2) GDPR.
3. Development of the issue: The responses show a great variety when it comes to how much resources are at hand to the data protection officers to perform their tasks. Some have stated that the DPO has 0-0.9 full time equivalents at their disposal while others have stated that the DPO has 6 full time equivalents or more and the rest has stated to lie within that range. The resources differ heavily despite that all organisations asked handle large amounts of personal data. Some have also stated that the allocated resources need to be reviewed. This can be compared to a survey made by the SE SA in 2022 where it was found that several DPOs stated that they do not have enough resources to perform their task.
4. Possible solution: It can possibly be concluded that it is difficult for data controllers to assess how much resource the DPO needs at his/her disposal to perform the task. A guidance document, as suggested in the next point 4, that further clarifies the tasks of the DPO would probably help data controllers to determine how much resources the DPO needs to fulfil its tasks.

4) Different views on what should be included in the role of the DPO

1. Main issue: The SE SA has noticed that there are different views on what tasks are considered to be part of the DPO's role.
2. Provision: Article 39(1) GDPR.
3. Development of the issue: The answers show that the respondents to some part have different views on what tasks are included in the role of the DPO. For example, several of the organisations believe that the DPO should take part when managing a personal data breach, and only 2/3 of organisations believe that the DPO should take part in the planning of new procedures including processing of personal data.
4. Possible solution: The variation may be due to the fact that the data controller considers it difficult to determine what tasks should be included in the role of the DPO. The SE SA has received requests outside of this review of further guidelines regarding the role of the DPO including examples of what should be included and what should not be included as well as methodical support. Such guidelines would facilitate the work of the DPO while at the same time create a greater insight for the data controllers regarding the scope of the role.

Part III – Actions by the SA

1. **Have you already published general guidance (e.g. guides, guidelines, etc.) regarding DPOs (including before launching the coordinated action)?**
   If yes, please provide the date, link to the guidance, and a short description of the guidelines

No.

2. **Have you taken action (i.e., fact finding exercises, informal contact, prior consultation, investigation) towards any of the organisations concerning the designation, tasks and/or role of the DPO *prior to* launching the coordinated action? Please describe the action you have taken**

and the outcome of this action (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).

No.

3. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**

Formal investigations are still ongoing. It is still unclear whether any investigation will lead to an action.

Part IV – Other

1. **What is your general impression of the levels of awareness and compliance of the organisations you consulted concerning the designation, tasks and/or role of the DPO?**

The perception is that the level of awareness and compliance varies.

2. **Are there any other issues or topics that you would like to flag?**

No.

3. **Are there any leading practices of the organisations you have contacted that you would like to share?**

No.

SI SA

Slovenian Supervisory Authority – Information Commissioner of the Republic of Slovenia (Informacijski pooblaščenec)

Part I - Statistics

Please see the consolidated figures in Appendix 1.1. The answers below may refer to the questions included in Appendix 1.1.

Part II – Substantive issues

1) Lack of consulting with the DPOs.

Brief description: The survey showed a notable variance in how frequently DPOs are consulted within organizations. Some DPOs are consistently involved in organizational processes, while others are consulted less than 5% of the time (181 out of 895 respondents). This suggests a possible gap in the recognition of the DPOs expertise and/or their integration within the organizational structure.

Legal framework: This issue primarily concerns Articles 37 to 39 of the GDPR and Articles 44, 45 and 48 of the Slovenian Data Protection Act (ZVOP-2), where both outline the designation, position, and tasks of a DPO. The provisions emphasize the necessity for DPOs to be involved in all issues relating to the protection of personal data, which implicitly necessitates their consultation.

GDPR:

- Article 37 specifies the conditions under which the designation of a DPO is mandatory. It lays out that public authorities and bodies shall designate a DPO, as well as organizations that carry out large-scale processing of special categories of data.
- Article 38 emphasizes the DPOs accessibility within the organization. It states that the DPO 'shall be involved, properly and in a timely manner, in all issues which relate to the protection of personal data.' The article also calls for the DPO to be provided with the necessary resources to carry out their tasks and maintain their expert knowledge.
- Article 39 lists the tasks of the DPO, which are essentially advisory, supervisory, and cooperative in nature. The DPO serves as the point of contact for the supervisory authority and also plays a role in awareness-raising and training of staff.

Slovenia's national Data Protection Act (ZVOP-2):

- Article 44 complements Article 39 of the GDPR, specifying that the DPOs advisory role aims to ensure compliance with not only the GDPR but also the national laws, enriching the scope and responsibilities of the DPO.
- Article 45 aligns with GDPR's Article 37 by providing details on who needs to designate a DPO. It adds a national layer to the obligation, such as the eight-day timeframe for publicizing the DPOs contact information and sending a notice of their designation to the supevisory authority.
- Article 48 delves into the operational aspects of the DPOs role. It talks about the DPOs responsibility to conduct risk assessments concerning data security. This independent duty harmonizes with the GDPR's Article 39, amplifying the importance of involving the DPO in pertinent activities on data protection.

Issues: The issue of inconsistent consultations with the DPOs, as revealed in the survey, could prove to have implications for compliance at multiple levels. It could contradict the aim of both GDPR and ZVOP-2, which both regulate the DPOs role as an integral part of the data protection framework, envisaging their proactive involvement in all relevant data protection issues at the controller. The survey results (in some segments of respondents) indicate a minimal involvement of the DPOs in organizational processes therefore exposing a systemic gap in the practical application of the regulations. The results are consistent with results from our own survey from 2019, showing late or incomplete inclusion of DPOs in data processing decision-making. Given these provisions, the lack of consultations with the DPOs not only indicates a deviation from best practices but potentially a direct contravention of GDPR's requirements, particularly those set in Article 38 GDPR concerning the timely and proper involvement of the DPO in (all) data protection issues.

This gap could lead to a failure in achieving the fundamental goals of data protection, thereby exposing the organization to legal risks such as non-compliance fines, enforcement actions, and reputational damages. In the absence of regular and meaningful consultation with DPOs, there is an elevated risk that data protection impact assessments may be inadequately performed, staff could be poorly trained in data protection issues, and data breaches may not be managed effectively. This inconsistency also compromises the DPOs ability to serve as a liaison between the controller and the supervisory authority, thereby weakening the overall data protection ecosystem.

Differences: Some organizations seem to integrate DPOs thoroughly into all relevant data processing activities, while others only engage them in specific circumstances. This split indicates that there is no uniform approach to leveraging the expertise of DPOs, which could potentially affect the efficacy of data protection measures in these organizations.

Additionally, the data show that while most organizations appear to be attentive to the advice given by their DPOs, there is a significant discrepancy when it comes to documenting instances where this advice isn't followed. This lack of documentation could undermine accountability and transparency in data protection practices. Moreover, the responses about how often DPOs are provided sufficient information to perform their duties reveal that access to necessary information is not consistent across organizations. This could impact the ability of DPOs to carry out their roles effectively, thereby affecting the overall compliance of the organization.

Solutions: One viable solution to improve the integration of DPOs in organizational processes is to establish a mandatory consultation mechanism. Alongside this, it could be beneficial to institute a formal process for documenting instances when the DPO's advice is not followed. By doing so, organizations can maintain a transparent record, providing accountability and facilitating any future audits or inspections in this matter. By revising internal protocols to ensure that DPOs are involved at key stages of any data processing activities, their role would be better institutionalized. Instituting mandatory checkpoints could then bridge the gap between organizations where DPOs are already actively involved and those where they are consulted less frequently.

Another approach to ensure a more active role of DPOs could be to invest in regular training and awareness-raising campaigns for both the DPOs and other key personnel within the organizations. The consultation and its documentation requirements could be emphasized in these training sessions. For DPOs to be truly effective, it is crucial that their peers and superiors also understand the importance and legal imperatives of data protection. This educational initiative could serve as a forum for clarifying the circumstances under which the DPO should be consulted and how their recommendations should be documented, thereby fostering a culture of data protection compliance throughout the whole organization.

Data controllers are regularly reminded by the supervisory authority in their opinions on received DPIAs to consult DPOs when conducting DPIs and document their involvement.

2) Lack of resources (time & expert knowledge) of the DPOs.

Brief description: There seems to be a clear desire by respondents for additional guidance and resources on data protection issues, such as templates for various documents and more practical, issue-specific advice from the SA. This suggests that DPOs may be under-resourced in terms of both (i) time that they can allocate to exercise the role as the DPO and (ii) expert knowledge needed to perform the role, making it challenging for them to execute their tasks effectively.

Legal framework: Article 38(2) of the GDPR explicitly stipulates that the controller and processor 'shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.' Meanwhile, the first paragraph of Article 46 of ZVOP-2 states that one of the qualifications for a DPO is the 'possession of knowledge or practical experience in the field of data protection'. Both legal frameworks are thus not merely suggestive but explicit about the essential resources and qualifications needed for DPOs to execute their roles effectively.

Issues: The issue of DPOs being under-resourced presents a significant challenge for organizations in fulfilling their data protection obligations. Based on the survey, respondents expressed a desire for additional resources like templates and issue-specific advice from supervisory authorities. This suggests that DPOs are often stretched thin, lacking both the time and the specialized knowledge required to perform their duties effectively. This resonates with the legal stipulations in both GDPR and ZVOP-2, which explicitly mention the necessity of providing adequate resources for DPOs to maintain their expert knowledge and perform their roles while also echoing the results of our national survey done in 2019.

Under-resourcing not only undermines the effectiveness of DPOs but also poses a risk for organizations in terms of compliance. When DPOs are under-resourced, there is a higher likelihood of lapses in data protection measures, which could potentially result in legal ramifications for the organizations involved. Therefore, the lack of adequate resources is not just an internal organizational issue but one that has broader compliance and legal implications.

A particular issue also arises when an external DPO is tasked with serving a large number of clients, posing challenges both in resource allocation and specialized expertise. The extensive client list raises concerns about the DPO's ability to adequately manage the diverse and complex data protection needs of each organization. This dilution of focus can compromise the effectiveness and compliance of various data protection programs under the DPO's supervision. Furthermore, the GDPR mandates that DPOs be involved in all issues related to the protection of personal data, necessitating an in-depth understanding of each client's specific internal processes, data flows, and their concrete data protection risks. Given these requirements, an external DPO responsible for multiple clients may struggle to maintain the specialized expertise required for each client's unique data protection landscape, which can lead to the DPO being inadequately informed and less effective.

Differences: The survey results show several differences and inconsistencies among DPOs in their experience and resources. For example, most DPOs have experience in data protection and privacy (803 out of 895), but far fewer are skilled in information systems management or development (113 out of 895). This suggests an uneven spread of skills that could impact how well data protection is

carried out. Likewise, while most respondents view expert knowledge of data protection rules and GDPR tasks as essential (742 and 726 respectively), a notable number (56 respondents) report that they were designated as DPOs simply because it was required, not because they had specific expertise. When it comes to time allocation, only a small number (40 respondents) can devote 91-100% of their working hours to DPO tasks, and 146 can give less than 5% of their time. Among the 895 respondents, approximately 34.2% of DPOs (306 out of 895) stated that they receive 8 or fewer allocated hours per year for professional development in data protection law and practices. Notably, within this group, 121 DPOs reported having zero allocated hours, indicating a concerning lack of resources for enhancing their expertise in data protection. In contrast, 228 DPOs (approximately 25.5%) reported having more than 32 hours allocated annually for such development. This significant variance in allocated hours for professional development underscores the need for more consistent and substantial opportunities for DPOs to enhance their expertise in data protection matters, while the differences point to a challenging situation where DPOs may not have the support or resources they need to do their jobs effectively.

Solutions: One potential solution to address the lack of resources for DPOs is for supervisory authorities to provide a more comprehensive set of guidelines, tools, and training materials, tailored to the specific needs identified in the surveys. For instance, 100 respondents expressed a desire for Q&As/FAQs, while 73 indicated that they would benefit from specialized training materials. These resources could help DPOs navigate complex issues and save time, thus allowing them to focus on critical aspects of data protection. Adding to this, supervisory authorities could create a user-friendly, transparent, centralized online database of their opinions and decisions, similar to the existing databases from the Slovenian SA[67] and the EDPB[68]. Such a database would serve as an invaluable resource for enhancing the DPO's expert knowledge.

It is also important to raise awareness among the management that there are clear obligations for them to provide adequate resources and training for their DPOs. Given that the SA was unable to issue fines until January 2023 this may have resulted in data controllers neglecting their DPO obligations therefore increased enforcement by the SA could improve management's attitudes towards providing sufficient resources for DPOs thus also respecting their legal obligations

Another viable solution is for organizations themselves to reassess and realign the resources allocated to the DPO role, as mandated by paragraph 2 of Article 38 of the GDPR. Providing DPOs with adequate time, staffing, and budget can ensure that they effectively carry out their tasks. Organizations can develop a system to document instances where the advice of DPOs is not followed, thus highlighting areas where additional resources or training may be required. This would not only empower DPOs but also foster a data protection culture within the organization, contributing to GDPR compliance.

Regarding the challenges of external DPOs not being able to be fully informed and focused to the individual controller's data protection needs, all organizations employing external DPOs should exercise due diligence in evaluating whether their DPO has both the resources and expertise to effectively manage their specific data protection needs.

3) Independence of the DPOs.

Brief description: There appears to be a lack of comprehensive understanding regarding the DPO's role as an independent advisor. A segment of respondents indicated that their organizations give

[67] Register of issued SI SA opinions: https://www.ip-rs.si/vop

[68] Register of Final One Stop Shop Decisions: https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-article-60-final-decisions_en

instructions to the DPOs, which could compromise the independence essential for the role of the DPO. Also, only 255 out of 316 DPOs who have an allocated budget, manage it independently, raising questions about the DPO's operational independence.

Legal framework: Under the GDPR, the independence of the DPO is specifically highlighted in Article 38, paragraph 3, which states that the DPO should not receive any instructions regarding the exercise of their tasks and should report directly to the highest management level.

Separately, in Slovenia's ZVOP-2, the independence of the DPO is outlined in the first paragraph of Article 48. This provision stipulates that the DPO performs its tasks in an independent manner, particularly when advising on risk assessments related to data security for all processing activities carried out by the controller or processor.

Issues: One significant concern that arises when a DPO lacks independence is the erosion of regulatory compliance and internal oversight mechanisms. Without the freedom to act impartially, a DPO may be inclined to prioritize organizational goals over regulatory obligations, which in turn, can compromise the effectiveness of performed DPIAs, data protection rights requests, and internal audits on data protection issues at the controller. The result could be overlooked vulnerabilities, gaps in compliance, and ultimately, a heightened risk of personal data violations. A compromised DPO undermines the entire foundation of data protection within the organization, opening the door to scrutiny and increased regulatory action.

Another issue pertains to the integrity of communications about data protection to both internal and external stakeholders. A DPO without independence might be pressured to present the state of data protection within the organization in an overly favorable light. This can create a distorted picture that misleads the management, the workforce, and external partners. Such misrepresentation not only jeopardizes compliance but also poses substantial reputational risks. In the event of a data breach or audit, stakeholders will question the reliability of past and future communications from the DPO, leading to a loss of trust that can have long-lasting repercussions.

Another issue that arises also seems to be related to the operational independence of the DPOs, particularly when a DPO lacks control over its own budget. Without this financial autonomy, the DPO's ability to prioritize critical activities, such as specialized training, is significantly hindered. This can lead to insufficient or delayed responses to urgent data protection issues, thereby undermining compliance efforts. When a DPO lacks control over its budget, managed instead by the organization, the lack of financial autonomy could make the DPO hesitant to critique the organization's data protection practices, fearing budget cuts or resource limitations as a form of ‘retaliation’.

Differences: The survey results highlight two distinct aspects of DPOs independence that warrant attention. First, although 635 respondents believe they have sufficient resources to fulfill their roles, only 316 report having an allocated budget, while only 255 manage it independently. This discrepancy suggests that the operational independence of numerous DPOs could be compromised.

Second, the survey shows that 58 respondents indicated their organizations give instructions concerning the DPO's tasks and duties. Given the DPO's role as an independent advisor, such directives could undermine the integrity of the DPO function and thus, data protection compliance. Further, while the survey shows that only one DPO has been dismissed or penalized for performing their duties, the fact that it has occurred at all could have a chilling effect, hindering DPOs from executing their roles with full independence.

Solutions: One effective measure to enhance the independence of the DPO could be for supervisory authorities to develop clear and stringent guidelines on DPO's independence, beyond what is already articulated in GDPR and national laws like ZVOP-2. These could detail the impermissibility of organizational interference in the DPO's tasks, specifically outlining the autonomy over budget management. An additional measure could be requiring DPOs to complete an annual declaration of conflicts of interest, similar to what is often required for board members and executives. This can help in the early identification of potential issues that may compromise a DPO's independence.

Moreover, organizations themselves can take proactive steps to safeguard the independence of their DPOs. For instance, mandatory, periodic training sessions can be conducted to educate executives and decision-makers about the critical importance of DPO's independence. Internal policies could be introduced, ensuring that DPOs are not given other roles that could create a conflict of interest, as indicated by the survey where DPOs also serve in multiple roles, such as in high management capacities. Another constructive solution could be the establishment of a performance review process for DPOs carried out by an external, independent body, thereby eliminating internal biases and promoting accountability.

4) Inconsistency in compliance reporting.

Brief description: The issue highlights a lack of uniformity in the DPOs reporting mechanisms for data protection activities and compliance measures to the top management. Such inconsistencies can compromise the DPO's efficacy, risking the oversight of critical data protection issues and thereby influencing the organization's overall compliance.

Legal framework: The reporting obligations of DPOs are explicitly stated in Article 38(3) of the GDPR, which mandates that the 'data protection officer shall directly report to the highest management level of the controller or the processor.'

Issues: The issue of infrequent or irregular reporting by DPOs to the highest management level raises significant concerns about effective oversight and governance. While GDPR's Article 38(3) stipulates that the DPO should report directly to the highest management level, it does not specify the frequency of these reports or their format, be it oral or written. This lack of concretization can lead to inconsistent practices across organizations. A written report, for instance, offers greater accountability and traceability than an oral briefing, thereby serving as a stronger instrument for data protection compliance.

Moreover, the absence of guidelines on what the reports should include leaves room for discrepancy in the comprehensiveness and usefulness of these communications. Ideally, these reports should provide an unambiguous overview of the organization's data protection posture, including risk assessments, potential violations, and recommendations for improvements.

Differences: The survey results reveal notable differences in the frequency and method of DPO's reporting to the highest management level. While a majority of 568 respondents indicated that their DPO reports 1–2 times a year, 144 respondents stated that no reporting is expected at all. Additionally, the methods of reporting also vary considerably: 385 instances involved a written report submitted to the board, 68 were submitted to other management groups, and 394 were mostly oral reports. This lack of uniformity in the reporting format—whether written or oral—further complicates matters, as written reports usually offer better traceability and accountability.

Solutions: To address the inconsistency in reporting frequency, organizations should establish a standardized reporting schedule that aligns with both operational needs and compliance requirements. This schedule should be formalized in the organization's data protection policy or governance framework to ensure regularity and accountability. Such a step would ensure that DPOs are aligned with management expectations and are regularly auditing, updating, and informing the highest management level about the organization's data protection posture.

As for the reporting format, a hybrid approach could be beneficial. DPOs should provide written reports for formal board meetings to ensure traceability and support accountability. These reports should comprehensively outline compliance status, risk assessments, and any data breaches or complaints received. For more frequent updates or less formal settings, oral reports or presentations can be considered sufficient. By employing both written and oral methods, organizations can maintain flexibility while upholding accountability standards.

Supervisory authority has issued DPO recommendations for organizations that cover also the relationship and reporting to the management[69].

5) Accountability and Responsibility of External DPOs.

Brief description: This issue pertains to the complexities arising when an external DPO serves and acts as a DPO for multiple controllers. Questions arise concerning who bears ultimate responsibility for data protection violations, and how a controller ensures that the external DPO is adequately monitoring compliance and focusing on them as a client. This situation can create ambiguities around accountability and potentially dilute the effectiveness of the DPO's role.

Legal framework: GDPR mandates the appointment of DPOs under Article 37, while delineating the tasks and responsibilities of a DPO in Article 39. However, the GDPR does not explicitly address the issue of responsibility when an external DPO serves multiple organizations, leaving a gap in the legal framework concerning accountability and the division of responsibilities between the controller and an externally appointed DPO.

In the context of Slovenia, ZVOP-2 provides additional clarity on the issue of external DPOs serving multiple organizations. Specifically, Article 47 of ZVOP-2 allows multiple controllers or processors to appoint a single, shared DPO, given considerations of their organizational structure, size, or diversity of data processing activities. The same article also contains provisions for special categories of organizations, like law firms, notaries, and trade unions, to appoint a shared DPO in consultation with their respective professional bodies.

Issues: One significant issue with external DPOs serving multiple organizations lies in the distribution of responsibility and accountability for data protection violations. Given that these DPOs oversee multiple organizations, there is a risk that their attention could be divided and level of provided services inadequate, potentially leading to lapses in compliance or oversight. In turn, this raises questions about who bears the responsibility in case of data protection breaches—whether it's solely the controller or (also) the external DPO (also in terms of civil liability between them). This is particularly relevant when the DPO's role includes providing advice, monitoring compliance, and liaising with supervisory authorities, among other responsibilities.

[69] Available in Slovenian: https://www.ip-rs.si/fileadmin/user_upload/Pdf/novice/Priporocila_IP_glede_delovanja_DPO_koncno.pdf

Given that the SA was unable to issue fines until January 2023 this may have resulted in data controllers neglecting their DPO obligations. This is also particularly relevant where the management has appointed an external DPO merely to fulfill their legal obligations, but in practice do not require external DPOs to perform their duties properly. The latter appears to be especially the case in smaller organizations in the public sector (mandated by the GDPR to nominate a DPO) that lack appropriate in-house data protection personnel and resort to external DPOs that however lack stimulus to provide DPOs services comprehensively and proactively. Feedback from the field shows that some external DPOs cater hundred plus clients (often small organizations required to nominate DPOs by law), provide only a basic-level service to their clients, which on the other hand also do not ask them to provide service levels that would be appropriate. Of concern in such situations could also be potential conflict of interest where external DPOs not only provide DPO-related services to their clients (e.g., awareness raising, monitoring compliance), but also act as advisors providing other data protection services (e.g., drafting contracts, records of data processing, consent forms etc.).

Another concern is the mechanism for performance assessment and quality control. There are challenges in establishing standardized protocols to evaluate how well the external DPO is managing data protection compliance across the organization. There is also the question of how these organizations ensure that the DPO is effectively focused on them as clients and is not prioritizing one organization over another. Both the DPO and the controllers need to have transparent lines of communication and clear expectations to manage these challenges effectively. Additional issues could stem from managing sensitive information across multiple organizations, which increases the risk of confidentiality breaches while also facing a challenge to ensure that the DPO is adequately trained and updated on the specific needs and nuances of each organization they serve, which seems like an immense operational challenge.

Differences: The survey findings reveal a wide spectrum of roles that DPOs occupy within organizations. While 379 DPOs of the 895 participants in the survey primarily serve as internal staff members, 135 extend their responsibilities to cover multiple authorities or a group of undertakings. Appointment durations for DPOs also vary considerably, with the most common term being one to three years, often with the possibility of extension. This flexibility in appointment terms raises questions about the continuity of data protection efforts, as longer-term appointments can foster institutional knowledge and in-depth expertise, while shorter terms may introduce fresh perspectives but disrupt ongoing initiatives. These variations emphasize the importance of tailoring DPO roles and appointments to suit the specific needs and structures of each organization.

Solutions: Addressing the issue of accountability and responsibility for external DPOs necessitates a multi-faced approach. First, organizations employing external DPOs should establish robust contractual agreements that clearly outline the DPO's roles, responsibilities, and reporting mechanisms. These contracts should specify the scope of their duties, communication protocols, and compliance expectations. Additionally, they should include provisions for regular performance assessments and feedback mechanisms to ensure that the DPOs remain aligned with the organization's data protection objectives.

Secondly, we as supervisory authorities can play a pivotal role by providing guidelines and recommendations for organizations employing external DPOs. These guidelines could offer best practices for DPOs designations, emphasizing the importance of independence, expertise, and allocated resources. Supervisory authorities could also facilitate knowledge sharing and collaboration among external DPOs through industry-specific forums/networks/trainings, enabling them to stay updated on evolving data protection issues and regulatory challenges.

Thirdly, implementing regular internal audits/inspections of external DPOs also seems as a proactive approach to ensure accountability and adherence to data protection regulations. These audits/inspections should be conducted both by the organizations employing external DPOs and by supervisory authorities. They could serve as a means to assess the DPO's performance, independence, and compliance with contractual obligations. By subjecting external DPOs to periodic scrutiny, organizations can maintain confidence in their data protection practices and swiftly address any issues that may arise, ultimately raising the effectiveness of data protection measures.

Lastly, increased enforcement by the supervisory authority, including when necessary, resulting in fines, could improve management's attitudes towards providing sufficient resources for DPOs thus also respecting their legal obligations.

Transparency also seems as a key element to ensure that external DPOs remain accountable. Legislators should foresee a need of implementing higher transparency obligations for external DPOs, to require them to provide transparent reports on their activities, including the number of organizations they serve, the types of issues they handle, and the outcomes of their interventions. This in respect could enhance visibility into their work and ensure better accountability.

Part III – Actions by the SA

1. **Have you already published general guidance (e.g. guides, guidelines, etc.) regarding DPOs (including before launching the coordinated action)?**
   If yes, please provide the date, link to the guidance, and a short description of the guidelines

We refer to Working Party Article 29/EDPB Guidelines on DPOs. However, we have a dedicate sub-site with information on DPOs[70] and have published a report based on our survey among DPOs in the public sector conducted in 2019 that covered similar issues as this survey. The report was released on January 28, 2020, and is accessible via the following link: DPO Survey 2020 Report[71].

We have also issued recommendation and best practices for organizations with DPOs[72].

2. **Have you taken action (i.e., fact finding exercises, informal contact, prior consultation, investigation) towards any of the organisations concerning the designation, tasks and/or role of the DPO *prior to* launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**

In late 2019 we have conducted a survey among DPOs in the public sector in order to establish what is the situation regarding their designation, position and tasks in practice. We also wanted to find out the perceived obstacles and key success factors according to the opinion of DPOs themselves to fulfil their goals successfully. We have received 100 replies (responding was not mandatory). The results were then analysed and presented on the occasion of European Data Protection Day 2020.

[70] Available at https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/ključna-področja-uredbe/pooblaščena-oseba-za-varstvo-podatkov
[71] Available at https://www.ip-rs.si/fileadmin/user_upload/Pdf/Porocila_IP/Dan varstva OP 2020 - rezultati DPO ankete.pdf.
[72] Available in Slovenian at https://www.ip-rs.si/fileadmin/user_upload/Pdf/novice/Priporocila_IP_glede_delovanja_DPO_koncno.pdf.

The results of the survey indicated that there were no substantial problems arising from the lack of management support, however in general DPOs reported not having enough time to fulfil their tasks and responsibilities to assure compliance with data protection legislation. DPOs reported, that the most important key success factors are: management support (4.64 out of 5), management's trust (4.61), timely inclusion of the DPOs in decision-making processes (4.54) and sufficient training and education for DPOs to maintain their knowledge and expertise (4.52).

We have also carried out two waves of privacy sweeps in 2022 in the public sector aimed towards organisations that have not yet designated a DPO. We discovered roughly 520 public bodies that have not yet informed us of their DPO's designation to our SA (but are in the public sector register) and contacted them via e-mail encouraging them to fulfil their DPO designation and information obligations using the web form at our website within a one-month deadline. In the privacy sweep conducted, we have also included a link to all information about the designation, position and tasks of DPOs including DPO's guidelines and DPO's recommendations that we had posted on our website. Within first two weeks we had received 150 new notices on the DPOs designation; 226 in the first round and around 400 new notices in both rounds of privacy sweep[73]. All in all, the sweep was very successful. The results guided primarily our awareness raising activities and insofar, given that our national data protection law was adopted in January 2023, have not resulted in enforcement or sanctioning procedures.

3. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (e.g. letter, recommendations to the organisation, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**

The results of the 2023 CEF will be used in our awareness raising and enforcement strategies, most likely resulting in increased co-operation between the supervisory authority and respective DPOs organisations in particular sectors (e.g., in education, health and other sectors). DPO networking also seems as an important platform to share knowledge and best practices among DPOs and where the supervisory authority can play an important role in empowering DPOs, while assisting them in forming networks and alliances. Responses from DPOs will therefore guide our awareness raising and training activities - we will continue providing guidance materials (mostly guidelines, opinions and infographics which had received very positive responses from the DPOs) and try to publish them in form(at) that is most usable for DPOs to carry out their data protection training and awareness raising in their organisations.

Dedicated and targeted enforcement actions are not foreseen as this was a 'fact finding and determining follow-up action based on the results' type action. However, given the fact that our national data protection law was adopted in 2023, which (finally) allows us to issue fines regarding the DPO-related obligations of data controllers/processors, the results of the action will be taken into account in our future enforcement activities. Several DPO related issues be a direct consequence of the (legal) inability of the supervisory authority to issue fines, resulting in data controllers neglecting their DPO-related obligations.

[73] As the time from the privacy sweep passes on by, it is hard to determine whether a concrete new notice of designation of the DPO is a direct result of conducting the sweep or not.

Part IV – Other

1. What is your general impression of the levels of awareness and compliance of the organisations you consulted concerning the designation, tasks and/or role of the DPO?

Based on survey results, there is a keen interest in compliance with data protection obligations, particularly regarding the roles and responsibilities of DPOs. Controllers are generally keen to align their operations with data protection regulations but often find themselves in need of additional guidance, especially when encountering challenges that existing SA guidance (opinions, guidelines…) don't cover comprehensively and specific to the concrete data processing. It may be observed in general that particularly smaller organizations have lower awareness and resources in terms of DPOs. Often, they resort to external DPOs for their services, which are however only basic-level both from the aspect of the organizations in terms of their demands and form the aspect of providers. Lack of enforcement and fines has undoubtedly had a negative impact on the level of compliance.

The survey reveals inconsistent DPO involvement in data protection activities within organizations, contributing to uncertainty for controllers. While some organizations consult their DPO almost continuously (129 respondents), a noteworthy number involve their DPO less than 5% of the time (181 respondents). This variability not only signals a need for further guidance on this matter but also highlights that a more structured form of interaction between controllers and DPOs may be beneficial. Significantly, 100 respondents called for Q&As or FAQs from the SA and 126 for DPOs and internal employees training materials. This high demand for additional guidance suggests that practical, scenario-based advice from the SA would be particularly beneficial in enhancing both compliance levels and confidence among controllers.

A concerning aspect seems to be varying degree to which advice from DPOs is acted upon. While a considerable number of respondents (476) indicated that the DPOs advice is generally well-followed, there remains a segment where advice of the DPOs might not always be followed. The absence of documented reasons for this non-compliance seems as a point of concern.

Additionally, there is seems to be a lack of clarity regarding the DPOs role within organizations. Specifically, 58 respondents stated that their organization instructs the DPO in the execution of tasks, indicating a potential misunderstanding of the DPOs role as an independent advisor rather than an extension of the management. Further adding complexity is the inconsistent frequency with which DPOs report to the highest level of management, revealing varying perceptions of the DPO's importance within different organizations.

In summary, while there seems to be a base level of awareness and an aspiration for compliance, gaps in understanding both the role of the DPO and SA are evident. These gaps are pronounced in areas such as the inconsistent involvement of DPOs in data protection activities, the extent to which their advice is disregarded, misunderstandings about their role as independent advisors and the misunderstanding of the SA’s role, whereas our tasks are to supervise compliance and not be individual consultants in concrete matters.

2. Are there any other issues or topics that you would like to flag?

We would like to flag several key issues based on the responses received in the survey. First and foremost, a recurring theme is the lack of specialized training and expertise of DPOs in the area of data protection. Respondents consistently mention that they face resource constraints both in terms of time and human capacity.

In light of this, it is apparent that there is a strong desire among respondents to fulfil their obligations under data protection laws; however, they often find themselves in need of additional support. Specifically, they are looking for expert knowledge, more comprehensive guidance, document templates, and tailored assistance for confronting practical challenges they encounter. According to the survey, a large number of respondents indicated the need for further guidance in the form of Q&As/FAQs. This could be indicative of a broader need for easily accessible information that can be referred to in real-time as challenges arise.

In summary, there is an evident need for more targeted resources and guidance to help organizations (and the DPOs) meet their data protection responsibilities effectively.

3. Are there any leading practices of the organisations you have contacted that you would like to share?

No specific practices were identified that exceed the existing legal obligations concerning the role and tasks of DPOs within organizations.