EUROPEAN DATA PROTECTION SUPERVISOR

Position paper on the role of Data Protection Officers of the EU institutions and bodies

30 September 2018

Executive summary

In light of the revised Data Protection Regulation applicable to EU institutions, bodies, offices and agencies (EUIs), which introduces several novelties with an impact on the role of the Data Protection Officers (DPOs), this revised paper aims at providing guidance for DPOs, building on the principles and recommendations in the original version from 2005.

A DPO is expected to have expert knowledge of data protection law and practices, as well as adequate understanding of the organisation and functioning of the EUI.

The revised Regulation provides that a single DPO can be appointed for more than one EUI, depending on their size and organisational structure. The EDPS believes that a common designation should only be considered where these EUIs are closely connected, both geographically and in the nature of their functions. The conflicts of interest that could potentially arise in cases of a shared DPO should be duly taken into account.

Under the revised Regulation, the DPO function can either be entrusted to a staff member of the EUI or be outsourced to an external service provider. The EDPS is strongly in favour of appointing a member of staff as DPO, in order to ensure adequate knowledge of the functioning of the EUI.

The DPO should be involved early and systematically in all issues relating to data protection within the EUI. In order to enable the DPO to carry out the assigned tasks and responsibilities, the EUI should provide them with adequate support on a material, staff and managerial level. Part-time DPOs should have sufficient time to fulfil their duties, and it is therefore recommended to establish a sufficient percentage for the DPO function and to develop a work plan.

The Regulation emphasises the independence of the DPOs, which prevents them from receiving instructions regarding the exercise of their tasks. No DPO should suffer any prejudice in the workplace because of their function. The appointment of the DPO for a fixed term is also an important factor in ensuring their independence. The EDPS therefore recommends the EUI to appoint the DPO for the longest term possible.

The EDPS believes that assistant and acting DPOs should have same status as the DPO, and be offered the same guarantees in the exercise of their duties.

DPOs are allowed to have other functions, but depending on each case, the instances where conflict of interests could arise should be carefully considered. The evaluation of the performance of the DPO for their function should be clearly separated from the evaluation of other tasks.

The DPO is assigned with the tasks of informing data controllers of their obligations and data subjects of their rights, advising on data protection related issues, cooperating with the EDPS, ensuring internal application of the Regulation and handling queries and complaints.

The cooperation between the DPO and the EDPS is highly important. It helps ensuring compliance, as well as enforcement of the Regulation.

TABLE OF CONTENTS

Executive summary **1**

1. Background **3**

2. Introduction **3**

3. Designation of the DPO **5**

3.1. Designation of a single DPO for several EUIs 5

3.2. Expertise and skills of the DPO 6

3.3. Internal or external DPO 6

3.4. Publication of contact details 7

4. Position of the DPO **7**

4.1. Involvement of the DPO 7

4.2. Necessary resources 8

4.3. Independence of the DPO 9

4.4. Status of assistant DPOs and acting DPOs 10

4.5. Conflict of interests 11

4.6. Term of appointment 12

5. Tasks of the DPO **12**

5.1. Information and awareness-raising function 13

5.2. Advisory function 13

5.3. Organisational function 14

5.4. Cooperative function 14

5.5. Monitoring compliance 14

5.6. Handle queries or complaints 15

5.7. Enforcement 15

6. Relation DPO - EDPS **15**

6.1. Ensuring application 15

6.2. Enforcement 16

6.3. Measuring effectiveness 16

1. Background

Regulation (EC) No 45/2001 ('the Regulation')[1], was adopted in 2001 with two objectives in mind: to protect the fundamental right to data protection and to guarantee the free flow of personal data throughout the Union. On 28 November 2005, the European Data Protection Supervisor ('EDPS') adopted a position paper with the aim of examining the key role of Data Protection Officers ('DPOs') within the EU institutions, bodies, offices and agencies ('EUIs'), and the underlying synergies between the DPOs and the EDPS in ensuring effective compliance with data protection principles. The position paper also provided guidelines on the type of profile required by a DPO and the resources that needed to be allocated to the DPO to ensure the good performance of their duties.

On 27 April 2016, the European Parliament and the Council adopted the General Data Protection Regulation[2] ('GDPR'), which became fully applicable on 25 May 2018. The Regulation has been revised with the aim of adapting it to the principles and rules laid down in the GDPR in order to provide a strong and coherent data protection framework in the European Union and to enable both instruments to be applicable at the same time. In terms of adapting to their respective new legal framework, it must be emphasised though that the EUIs have a great advantage over the public authorities/bodies and private entities which must now appoint a DPO under the GDPR. Indeed, while having a DPO has merely been considered good practice for national entities prior to the GDPR, it has been a legal requirement for *all* EUIs - regardless of their size and core activities - for over fifteen years.

The review of the Regulation takes into account the results of inquiries and stakeholder consultations, as well as an evaluation study on its application over the last fifteen years. Information on the practical application of the Regulation was gathered from the EDPS and other EUIs, and a questionnaire was sent to the network of EUIs' DPOs. The DPOs from a number of EUIs participated in workshops on the reform of the Regulation at four occasions between July 2015 and March 2016. The evaluation showed that the governance system structured around DPOs and the EDPS is effective. It found that the sharing of powers between DPOs and the EDPS is clear and well balanced, and that both have an appropriate range of powers. However, it was highlighted that difficulties could arise from a lack of authority due to insufficient support for the DPOs from their management.

Since the revised Regulation includes several novelties that affect the role of the DPOs within the EUIs, the EDPS has reviewed its position paper on the role of the DPO. The revised paper intends to provide guidance for DPOs in their new role, building on the principles and recommendations contained in the original version.[3]

2. Introduction

The protection of natural persons in relation to the processing of their personal data is a fundamental right laid down in Article 8 of the Charter of Fundamental Rights of the European

[1] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000, on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.01.2001, p. 1).

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (OJ L 119, 4.5.2016, p. 1–88).

[3] Articles mentioned in the present paper refer to the text adopted by the European Parliament and the Council on 19 September 2018 (PE-CONS 31/18).

Union ('the Charter')[4], Article 16(1) of the Treaty on the Functioning of the EU ('TFEU')[5] and Article 8 of the European Convention on Human Rights[6]. As underlined by the Court of Justice of the European Union, the right to protection of personal data is not an absolute right, but must be considered in relation to its function in society. Data protection is also closely linked to respect for private and family life protected by Article 7 of the Charter[7].

The revised Regulation lays down rules on the protection of natural persons with regard to the processing of personal data by EUIs and the free movement of such data. It protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data. The EDPS shall monitor the application of the provisions of the Regulation to all processing operations carried out by an EUI[8]. The Regulation applies to the processing of personal data by all EUIs when the processing is carried out in the exercise of activities, which fall, wholly or partially, within the scope of Union law[9].

The data controller, defined in the Regulation as 'the Union institution, body, office or agency or the Directorate-General or any other organisational entity which, alone or jointly with others, determines the purposes and means of the processing of personal data'[10], is responsible for, and should be able to demonstrate compliance with the data protection principles (principle of accountability)[11]. The data controller often has insight into the processing operation itself and is an easy contact person for the data subject. To this effect, the data controller ensures that the data subject can exercise their rights and ensures respect of the principles established in the Regulation. It should be noted that although a person (e.g. Head of Unit or Director) or an organisational part of the institution (e.g. the HR Unit or the Security Unit) or body is *de facto* responsible for the processing operation, they, as officials, are acting on behalf of the EUI, which bears the legal responsibility for ensuring compliance with the Regulation.

[4] Article 8
Protection of personal data
1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

[5] Article 16
1. Everyone has the right to the protection of personal data concerning them.
(...)

[6] Article 8
Right to respect for private and family life
1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

[7] Article 7
Respect for private and family life
Everyone has the right to respect for his or her private and family life, home and communications.

[8] Article 1.

[9] Article 2(1).

[10] Article 3(8).

[11] Article 4.

The Regulation provides the obligation for each EUI to designate a DPO.[12] As will be examined below, the DPO is fundamental in ensuring the respect of data protection principles within EUIs.

The Regulation provides for an independent supervisory authority, the EDPS, in view of monitoring the processing of personal data by EUIs.[13] This notably implies providing support within the institutional framework to the work and role of the DPO.

DPOs have been in existence for over fifteen years and have proved to be a success not only in their work within the EUI, but also in the establishment of a DPO network. This network, which meets at regular intervals, has proved helpful in producing advice and exchanging views on common issues or problems.

3. Designation of the DPO

3.1. Designation of a single DPO for several EUIs

The revised Regulation provides that each EUI shall designate a DPO, but opens the possibility for several EUIs to designate a single DPO for several of them, taking into account their organisational structure and size[14]. The possibility of sharing a DPO, although previously not explicitly laid down in the Regulation, had already been envisaged in practice and such an arrangement has been put in place in at least one case. A common/shared DPO could indeed be a practical solution especially for smaller EUIs where the appointment of a full-time DPO is not feasible. However, the appointment of a shared DPO between EUIs must be made conditional upon the fact that they are closely connected in both their functioning and their geographical location or organisation. In addition, the EDPS underlines that all provisions of the Regulation apply to both institutions although the DPO function is shared between them.

In this regard, particular attention should be given to the provisions on conflict of interests[15], mandate[16] and necessary resources[17]. **Firstly**, it is important to consider the conflict of interests that could arise for a shared DPO, notably in the context of transfers of personal data between the EUIs in question, given that the DPO may be called upon to advise the controller as regards the necessity of such data transfers. In such cases, an alternative solution must be found.

If a shared DPO is asked to provide advice on the necessity of data transfers between their two EUIs, the assistant DPO or another staff member could be in charge of the assessment of the transfer. Alternatively, the opinion of the DPO of another EUI could be sought. Depending on the case and the available alternatives, the EDPS could also be consulted.

Secondly, since the DPO shall be designated for a term of three to five years (eligible for reappointment), EUIs that decide to appoint a shared DPO must ensure that the mandates are compatible with one another and with the time requirement of Article 44(8). This is particularly important in cases where the DPO's first mandate is a prerequisite for subsequently designating him or her as a DPO for a second EUI. **Thirdly**, both institutions must provide the DPO with necessary resources and training to carry out their duties. **Lastly**,

[12] Article 43(1).
[13] Article 52.
[14] Article 43(1)-(2).
[15] Article 44(6).
[16] Article 44(8).
[17] Article 44(2).

the shared DPO, with the help of a team if necessary, must be in a position to communicate efficiently with controllers, staff members, and other data subjects.

The availability of a DPO is essential to ensure that data subjects will be able to contact the DPO. Although a permanent physical presence on the same premises as staff members and controllers is not always necessary, a minimum physical presence should be provided in order to build the trust relation with the controllers and ensure availability for staff.

To sum up, this arrangement is not feasible for larger and medium-sized EUIs and the EDPS would not encourage this arrangement on a larger scale, since it could compromise the effectiveness of the DPO activity. The concept of a shared DPO should be limited to exceptional cases where it is duly justified. It is good practice to seek the EDPS' opinion before deciding to appoint a shared DPO.

3.2. Expertise and skills of the DPO

The DPO shall be designated on the basis of professional qualities, in particular, expert knowledge of data protection law and practices, and the abilities to fulfil their tasks[18]. The EDPS would like to emphasise two elements in this profile: an adequate knowledge of the organisation, structure and functioning of the EUI, and expertise in data protection[19]. This implies that it is in many cases preferable to recruit the DPO from within the EUI. However, if the required expertise is not available inside the organisation, it may be necessary to launch an external selection procedure. The required level of expertise is not defined, but it must be commensurate with the size of the EUI and the sensitivity, complexity and amount of data that they process.[20] Although expert knowledge of data protection law is a prerequisite to the function according to the Regulation, this may however not always be possible from the start. Providing the DPO with adequate resources includes continuous training and this can be ensured both at the time of entry into function and by regular up-dates in the course of the mandate.

Establishing a minimum term of appointment and a minimum percentage of time in order to carry out the function also helps to contribute to building expertise in the field. Professional qualities also include knowledge of IT, including security aspects, as well as organisational and communication skills. Ability to fulfil the tasks incumbent on the DPO should be interpreted as both referring to their personal qualities and knowledge, but also to their position within the organisation. Personal qualities should include integrity and high professional ethics.

3.3. Internal or external DPO[21]

Furthermore, the Regulation provides that the DPO may be a staff member of the EUI, or fulfil the tasks on the basis of a service contract.[22] This novelty abolishes the requirement of the DPO being a staff member of the EUI, which means that in practice the DPO function may be externalised to a law firm or a consultancy firm, etc. This is in line with the GDPR and the Guidelines on DPOs issued by the Working Party 29, which provide that the function of the

[18] Article 43(3).
[19] If possible, the DPO should also have knowledge of risk management/analysis to be in a position to give advice on data protection impact assessments ('DPIAs') and security measures.
[20] See recital 62.
[21] NB: Depending on the outcome of the legislation. The EDPS has repeatedly advised against the possibility of outsourcing the DPO function.
[22] Article 43(4).

DPO can also be exercised on the basis of a service contract concluded with an individual or an organisation outside the controller's organisation. However, the EDPS is of the opinion that in order to ensure adequate knowledge of the functioning of the EUI - its mandate, processing operations, staff and management - DPOs should, to the largest possible extent, be staff members. Outsourcing of the function should be limited to the strict minimum. The DPO function requires a high level of confidentiality that could be best maintained with an in-house DPO. In any event, the DPO function should always be attributed to a designated physical person that would serve as lead contact be in charge for the EUI. As in the case of a shared DPO, a minimum physical presence should be guaranteed to ensure the efficiency of day-to-day interaction.

Article 44(5) mentions the DPO 'and his or her staff' and the Regulation thus provides for the possibility to establish a DPO office with both assistant DPOs and administrative assistants where appropriate. According to the size of the EUI and the nature of the processing operations that they carry out, it might indeed be necessary for the DPO function to have assisting staff. In larger EUIs it could also be useful to spread the DPO function to all organisational parts, like in the European Commission, which has appointed a data protection coordinator ('DPC') in each Directorate-General ('DG') in order to co-ordinate all aspects of data protection in the DG. This has been justified by the size of the institution and the necessity to have relays in the different DGs. The Commission has also appointed a specific DPO for OLAF.

3.4. Publication of contact details

Article 43(5) requires the EUIs to publish the contact details of the DPO and communicate them to the EDPS. The Regulation does not require that the published contact details include the name of the DPO. Whilst it may be a good practice to do so, it is for the EUI and the DPO to decide whether this is necessary or helpful in the particular circumstances. However, communication of the name of the DPO to the EDPS is naturally essential in order for the DPO to serve as contact point between the EUI and the EDPS. It is equally essential to inform staff members of the name and contact details of the DPO, by publishing them internally on the EUI's intranet, internal telephone directory, and organisational charts. It is also important to mention that the DPO's contact details should be included in the information to be given to data subjects when their data are collected[23]. For practical purposes, the EDPS recommends the EUI to set up a functional mailbox for the DPO, which should be indicated in data protection notices, on the internet and other public communications.

4. Position of the DPO

4.1. Involvement of the DPO

The Regulation obliges the data controller to ensure that the DPO is involved, properly and in a timely manner, in all issues which relate to data protection[24]. This provision reflects one of the aspects of creating a data protection culture within the organisation. Ensuring that the DPO is informed and consulted at the outset will facilitate compliance with the Regulation and promote a privacy by design approach. Involving the DPO early and systematically whenever decisions with data protection implications are taken should therefore be standard procedure

[23] Articles 15(1)(b) and 16(1)(b).
[24] Article 44(1).

within the EUI. This will help ensuring compliance with the principles of data protection by design and by default[25].

It is good practice to consult the DPO in the planning phase of an IT system before it is launched. Involving the DPO early can help identifying and evaluating issues, such as whether personal information will be processed, the exact categories of data that will be collected, the purpose of the processing operation, etc.

In addition, the DPO should be seen as a discussion partner within the EUI and they should be part of the relevant working groups, steering committees, etc., dealing with data processing activities. The EDPS also recommends that the DPO be invited to participate regularly in management meetings and that their opinion always be given due weight. To involve the DPO in a timely manner requires that they are visible within the organisation and receive relevant information in time to allow them to provide adequate advice. The position of the DPO in the organisation chart is an important element of visibility that can be further improved via newsletters and the intranet.

Article 39(2) provides that the controller must seek advice of the DPO when carrying out a data protection impact assessment, and in accordance with Article 34(5), the controller must inform the DPO about personal data breaches. Besides these specific cases, the controller could develop, where appropriate, data protection guidelines or programmes that set out when the DPO must be consulted. The implementing rules are also a starting point and a useful tool to help reinforce the involvement of the DPO.

4.2. Necessary resources

The EUI shall support the DPO in performing their tasks by providing resources necessary to carry out those tasks.[26] This implies that the DPO should be provided not only with adequate support in terms of financial resources, infrastructure (premises, facilities, equipment) and staff where appropriate, but also that the senior management actively supports the DPO function. Such support includes that the designation of the DPO is communicated officially to all staff to ensure that their existence and function are known within the EUI. If needed, DPOs should be given support from other services, such as the legal service or the communication team. The necessary resources also include giving access to personal data, processing operations and premises. Furthermore, the need for continuous training is clearly set out in the above provision. 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, meetings of the DPO network, and other forms of professional development, such as participation in privacy fora, workshops, etc.

However, the most important element for a part-time DPO is to have sufficient time to fulfil their duties. Otherwise, conflicting priorities could result in the DPO duties being neglected. It is a good practice to establish a percentage of time for the DPO function where it is not performed on a full-time basis. For the calculation of this percentage, the working days, including travel time and preparation, for the DPO meetings should be taken into consideration. It is often not easy to determine a specific percentage of time to perform the duty of DPO. Indeed, the time needed to carry out the duties of the DPO is not necessarily linked to the size of the EUI: even a small institution could have many or sensitive processing

[25] Article 27.
[26] Article 44(2).

operations involving personal data. Moreover, a new DPO post (e.g. in a newly established agency) requires a lot of investment at the start in order to raise the awareness of staff and to monitor compliance. If the post is not new, the function is also time-consuming for a newly appointed DPO who has to get to grips with the subject. The EDPS therefore recommends the appointment of a full-time DPO at least at the start of the function. In any event, the EUI should not underestimate the workload of the DPO when determining the percentage to be devoted to the function.

Assuming that there are 200 working days per year, 10% for the DPO function means that the DPO should work 20 days/year on data protection issues. Given that there are two DPO meetings each year and that these in some cases account for 4 days for each (2 meeting days and 2 travel days), there are only 12 days left for the DPO to work on data protection issues throughout the year. Controllers must evaluate whether this allocation of time for the DPO function is proportionate to the workload in order to ensure application of the revised Regulation.

A preferable measure to determine the time needed to carry out the function and to determine appropriate level of priority for DPO duties for part time DPOs is to encourage DPOs (or the institution) to draw up a work plan. This work plan could also be a useful instrument in the evaluation of the DPO.

As outlined above, a common/shared DPO could be a solution for smaller institutions where the appointment of a full-time DPO is not feasible.

As mentioned above, the Commission has also appointed a DPC in each DG in order to co-ordinate all aspects of data protection in the DG. The DPC should also be chosen at an appropriate hierarchical level and according to his knowledge of the functioning of the Commission in general and particularly the DG where they are appointed. A number of principles applicable to the DPOs also apply to a large extent to the DPCs so as to enable them to carry out their work efficiently (evaluation, independence, time allocated to the duty, etc.).

4.3. Independence of the DPO

DPOs are placed in a difficult position: they are a part of the EUI and yet must remain independent from it in the performance of their duties. As part of the institution they are ideally placed to monitor compliance from the inside and to advise or to intervene at an early stage, thereby avoiding possible intervention from the EDPS. A number of guarantees, which aim at ensuring that the DPOs fulfil their duties in an independent manner, have been provided for in the Regulation

The Regulation provides that the EUIs shall ensure that the DPO does not receive any instructions regarding the exercise of their tasks.[27] This provision is paramount in ensuring independence of DPOs. It refers not only to direct instructions from a superior, but also implies that a DPO must not be in a position to be inclined to accept certain compromises when dealing with controllers in high positions. This could be an issue for 'contractual' DPOs, including temporary agents, who feel that their position in a certain context could influence the extension or renewal of their contract. Certain elements can thus compromise this independent status within the EUI. Experience has shown that part-time DPOs have found themselves in a permanent conflict between allocating time and efforts to their regular tasks as opposed to investing in their DPO duties. Moreover, since DPOs are often evaluated based on their

[27] Article 44(3).

regular tasks rather than their work as DPO, they have often felt pressured to invest more in these other tasks. Even though the idea of a full-time DPO is preferred, the EDPS acknowledges that smaller EU bodies will not find it practical, or even possible, to appoint a full-time DPO. The issue of a shared DPO, as explained above, could be envisaged in certain exceptional cases.

Independence is also an issue related to the hierarchal position of the DPO and the person to which they should report. Some DPOs have found that they are confronted with authority problems vis-à-vis high-ranking controllers when providing advice or recommendations or during investigations. In this regard, the revised Regulation clearly sets out that the DPO shall report to the highest management level of the controller or the processor.[28] This is a clear improvement, but does not necessarily solve all problems related to the hierarchical position of the DPO, since they might very well have another reporting line in their other role. Distinguishing between such different reporting lines might entail difficulties for both the DPO, the management and other staff members.

Moreover, in order to guarantee independence, the DPO shall not be dismissed or penalised by the controller or processor for performing their tasks.[29]

Such penalties include denial of benefits that other employees receive, delay of promotion, and any other type of discriminatory measures imposed on the DPO solely for performing their duties.

DPOs should thus not suffer prejudice in their career development from the mere fact of having been a DPO. It goes without saying that dismissal or disciplinary sanctions for other legitimate reasons, such as gross misconduct, remain possible at any time.

The fact that the Regulation clearly spells out that the DPO and their staff shall be bound by secrecy or confidentiality concerning the performance of their tasks, further reinforces their independence and their position within the EUI[30].

The EDPS encourages DPOs to develop their own common principles of good supervision (requirements, annual work programme, annual report, etc.), which will serve to measure the performance of their work.

4.4. Status of assistant DPOs and acting DPOs

In practice, assistant DPOs not only assist the DPO, but also ensure the continuity of the function in the event of absence of the DPO. Despite the fact that the Regulation does not address the issue of the status of assistant DPOs, the EDPS believes that assistant DPOs should be offered the same guarantees as those provided for in the Regulation as concerns DPOs themselves[31]. The same rules apply also to acting DPOs. The latter shall ensure in an independent manner the internal application of the Regulation, they may not receive any instructions in the performance of their duties, and their selection as acting DPO shall not be liable to result in a conflict of interests between his/her duty as acting DPO and any other official duties.

[28] Article 44(3).
[29] Article 44(3).
[30] Article 44(5).
[31] This is valid also for Data Protection Coordinators and other staff members of the DPO office.

4.5. Conflict of interests

According to Article 44(6), the DPO may fulfil other tasks and duties. It requires, however, that the controller ensures that 'any such tasks and duties do not result in a conflict of interests'. 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. This entails in particular that the DPO cannot hold a position within the EUI that leads them to determine the purposes and the means of the processing of personal data, i.e. the part-time DPO should not act as a controller in his initial activity. Due to the specific organisational structure in each EUI, this has to be considered case by case and the different duties must be evaluated separately. In some cases, functions lower down in the organisational structure can be concerned if such positions lead to the determination of purposes and means of processing.

Functions that would in principle be incompatible with the DPO function include **high level** positions within management, human resources, IT services, medical services, security services, internal audit, etc. A conflict of interests may typically also arise (even for lower level positions), when a part-time DPO who belongs to the IT service must assess processing operations that they have designed; or when a DPO who is also part of the compliance team must assess compliance checks and related data processing that they have designed.

Depending on the activities, size and structure of the EUI, it can be good practice for controllers 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, 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. In this context, it should also be borne in mind that conflicts of interests may take various forms depending on whether the DPO is recruited internally or externally.

In cases where the DPO is also a data subject and has reason to believe that their data have been unlawfully processed by their EUI, a conflict of interests would be unavoidable. The DPO should then involve the EDPS if the matter cannot be resolved directly with the controller.

Moreover, the EDPS has considered that the DPO cannot represent the EUI before the Courts of the European Union in relation to any data protection case against the EUI. This task would be incompatible with the statutory independence of the DPO, even in the event that they have not been previously involved in the case at any stage. Litigating for and acting on behalf of the institution before a Court in data protection related cases would jeopardise independence and impartiality of the DPO, not only in the present case, but also in general. This could potentially damage the perception of the DPO as independent within the EUI and would inevitably give rise to a conflict of interests. This should be borne in mind, if, as is rather common, the EUI designates a member of the legal service as DPO. [32] The same applies to other instances where the application of data protection rules might be at stake, such as the European Ombudsman's inquiries into alleged maladministration or appeals under Article 90(2) of the Staff Regulations. The DPO should in principle not be involved as a representative of the Appointing Authority

[32] If the DPO is also a member of the legal team, organisational measures should be put in place to allow the DPO and his staff to clearly distinguish their activities, e.g. by having a separate functional mailbox for DPO matters (so that the rest of the organisation can see whether the advice comes from the DPO function or legal advisory function).

in such cases. There is therefore a need to ensure that internal policies reflect this and that procedures are in place to ensure that the DPO is not called upon to represent the EUI in data protection related cases.

Furthermore, evaluation of a DPO in the performance of their duties as DPO must not be related in any way to the performance of other tasks. Furthermore, the DPO should not be prevented from exercising his duties due to lack of time as a result of other official duties. As mentioned above, in practice the percentage of time granted to the DPO in order to perform their duty as DPO has been problematic in many EUIs.

4.6. Term of appointment

Article 44(8) stipulates that the DPO shall be appointed for a term of between three and five years. They may be eligible for reappointment. Moreover, they may only be dismissed from the post if two cumulative conditions are met: if they no longer fulfil the conditions required to perform their duties, and with the consent of the EDPS.

The appointment of the DPO for a fixed term and the conditional dismissal before the end of the mandate, are important factors in ensuring the independence of the DPO. The longer the mandate, the more this contributes to providing the guarantee to the DPO that they can carry out their function in an independent manner. The EDPS therefore supports the appointment for a term of five years. The fact that the EDPS must consent to the dismissal of the DPO if they no longer fulfil the conditions required for the performance of their duties also contributes to ensuring independence.

Certain implementing rules concerning the tasks, duties and powers of the DPOs adopted by the EUIs according to Article 45(3), provide that the EDPS take part in the evaluation the work of the DPOs on a regular basis. The EDPS welcomes the idea of a formal consultation by which the EDPS could provide general comments as an element to be taken into consideration in the staff evaluation of the DPO since this can be seen as additional support to the work of the DPOs and a further guarantee of their independence. Needless to say, the EDPS is not in a position of evaluating the day-to-day work of the DPO and his input would be only cover areas where there is direct cooperation with the EDPS (e.g. working groups, inspections, accountability/compliance visits).

5. Tasks of the DPO

The DPO has a central role within the EUI: DPOs are familiar with problems of the organisation and, given their status, have a crucial role to play in giving advice and helping solve data protection issues. The DPOs are unique since they will simultaneously act as advisor, educator and point of contact for competent authorities and data subjects. The revised Regulation reinforces this role of the DPO in requiring that data controllers involve them, properly and in a timely manner, in all issues, which relate to the protection of personal data.

To this effect, the Regulation grants the DPO a number of tasks, duties and powers. These are further detailed in the implementing rules concerning the DPO to be adopted by each EUI[33].

DPOs are expected to fulfil the tasks described below and those in relation to the EDPS as described under section 6. However, it should be borne in mind that the responsibility of

[33] Article 45(3); it is considered good practice for institutions and bodies to submit their implementing rules to the EDPS for advice.

carrying out all processing operations in compliance with the revised Regulation remains with the controllers.

5.1. Information and awareness-raising function[34]

This implies both informing data controllers and processors of their obligations and responsibilities, and ensuring that data subjects are informed of their rights and obligations pursuant to the Regulation. Awareness-raising can take the form of staff information notes, training sessions, setting up of a web site, data protection notices, etc.

5.2. Advisory function[35]

DPOs shall ensure in an independent manner the internal application of the Regulation and advise data controllers on fulfilling their obligations. In addition to this general advisory role, the DPO should provide advice in a number of specific situations. **Firstly**, the DPO should advise, where requested, on the necessity for a notification or a communication of a personal data breach pursuant to Article 34 and 35 of the Regulation. **Secondly**, the DPO should provide advice, where requested, on data protection impact assessments ('DPIAs') and monitor their performance pursuant to Article 39 of the Regulation. It is the responsibility and task of the data controller, not of the DPO, to carry out DPIAs. However, the DPO can play a very important and useful role in assisting the data controller in advising whether to carry out a DPIA, what methodology to use, what safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the data subjects, whether or not the DPIA has been correctly carried out, and whether its conclusions are in compliance with the Regulation. **Thirdly**, the DPO should provide advice, where requested, on the need for prior consultation of the EDPS in accordance with Article 40 of the Regulation. Similarly, as for DPIAs, the DPO can play an essential role in this regard, given their expertise and experience in assessing sensitive processing operations in the framework of the former prior checking system. Furthermore, the Regulation explicitly lays down that the DPO may consult the EDPS as to the need for DPIA and prior consultation.

The DPO may make recommendations for the practical improvement of data protection to the EUIs and advise them, or the controller or processor concerned, on matters concerning the application of data protection provisions. The DPO may also be consulted by the controller and processor, by the staff committee and by any individual, without going through the official channels, on any matter concerning the interpretation or application of the Regulation. No one shall suffer prejudice on account of a matter brought to the attention of the competent DPO alleging that a breach of the Regulation has occurred. Furthermore, data subjects may contact the DPO with regard to all issues related to the processing of their personal data and to the exercise of their rights.

It is good practice to provide a secure channel for communication with the DPO. This could entail the use of an encrypted email address or a dedicated internal communication/chat system. DPOs should be free to choose which communication options they would like to provide, they should be encouraged to be as open as possible to any inquiries and whistleblowing efforts, and they should be able to provide at least a minimum level of confidentiality on a technical level. Furthermore, the DPOs should demonstrate their commitment to protect the identity of complainants vis-à-vis the EUI if needed, to encourage data subjects to exercise their rights without fear of repercussions.

[34] Article 45(1)(a), (b) and (c).
[35] Article 45(1)(a), (d), (e) and (f), Article 45(2), Article 44(4) and (7).

5.3. Organisational function[36]

Under Article 31 of the Regulation, it is the data controller and/or the processor, not the DPO, who is required to 'maintain a record of processing operations under its responsibility' or 'maintain a record of all categories of processing activities carried out on behalf of a controller'. In practice, DPOs often create inventories and hold a register of processing operations based on information provided to them by the entities responsible for the processing of personal data. Under the former Regulation, keeping such a register was the responsibility of the DPOs and it enabled them to have an overview of all processing operations carried out within the EUI. Under the revised Regulation, the EDPS strongly recommends that EUIs centralise their records in a public register kept by the DPO[37]. Such a record helps the DPOs to perform their tasks of monitoring compliance, informing and advising the controller or the processor. In any event, the record required under Article 31 should also be seen as a tool allowing the data controller and the EDPS, upon request, to have an overview of all the personal data processing activities carried out. It is thus a prerequisite for compliance, and as such, an effective accountability measure. However, it should be noted, that it is the controller's task to keep appropriate records, and that accountability for generating records and for their content remains with the controller. While the DPO can help generating the records and supporting documentation, this is the duty of the controller.

5.4. Cooperative function[38]

The DPO has the task of responding to requests from the EDPS and, within the sphere of their competence, cooperate and consult with the EDPS at the latter's request or on their own initiative. This task emphasises the fact that the DPO facilitates cooperation between the EDPS and the institution, notably in the framework of investigations, complaint handling, DPIAs and prior consultations. The DPO not only has inside knowledge of the institution, but is also likely to know whom to contact within the institution. The DPO may also be aware, and duly inform the EDPS, of recent developments likely to impact the protection of personal data.

5.5. Monitoring compliance[39]

The DPO is to ensure in an independent manner the internal application of the Regulation and to monitor compliance with the Regulation, with other applicable EU law containing data protection provisions, and with the policies of the data controller or processor in relation to data protection, including the assignment of responsibilities, the raising of awareness and training of staff involved in processing operations, and the related audits. In order to monitor compliance, DPOs can prepare templates for the data controllers to fill in, on the basis of which they can monitor compliance with the Regulation and make recommendations. DPOs can also assist controllers by developing internal policies and FAQs on thematic topics to provide guidance to data controllers.

Furthermore, the DPOs may, on their own initiative or at the request of the data controller or the processor, the staff committee, or any individual, investigate matters and occurrences directly relating to their tasks and which come to their notice, and report back to the person who commissioned the investigation, or to the data controller or processor. It is important that

[36] Article 31.
[37] https://edps.europa.eu/sites/edp/files/publication/18-02-06_accountability_on_the_ground_part_1_en_0.pdf
[38] Article 45(1)(g).
[39] Articles 45(1)(b) and 45(2).

the staff committee and all services of the EUI cooperate closely with the DPO in cases of an alleged breach of data protection rules and ensure that they are duly informed and consulted.

5.6. Handle queries or complaints

The DPO is granted with investigatory powers as laid out above and can as a result handle queries or complaints submitted by members of staff or the public. In this context, the EDPS regrets that the Regulation no longer explicitly grants DPO access to all personal data and to information necessary for the performance of their tasks.[40] This change of wording should not entail any change in practice and should not hinder the DPO in the exercise of their tasks, in particular, investigations and complaint handling.

Furthermore, the Regulation provides that no one shall suffer prejudice on account of a matter brought to the attention of the competent DPO alleging that a breach of the Regulation has occurred. The EDPS, as the principal complaint handling instance in the field of data protection, encourages the investigation and handling of complaints by DPOs and, as a general rule, advises complainants to first contact the DPO. The fact that the DPO acts from within the institution and is close to the data subject places them in an ideal situation to receive and handle queries or complaints at a local level. This does not however prevent data subjects from directly addressing the EDPS under Article 63.

5.7. Enforcement

Despite having competence to monitor compliance with the Regulation and to handle complaints, the DPO has limited powers of enforcement. However, they have the possibility to bring to the attention of the Appointing Authority any failure to comply with the obligations under the Regulation with a view to a possible application of Article 69 of the Regulation.

6. Relation DPO - EDPS

In order to ensure effective internal application of the Regulation, the working relationship between the DPO and the EDPS is of high importance. The DPO must not be seen as an 'agent' of the EDPS, but as a part of the EUI where they work. As already mentioned, this idea of proximity puts them in an ideal situation to ensure compliance from the inside and to advise or to intervene at an early stage, thereby avoiding possible intervention from the supervisory authority. At the same time the EDPS can offer valuable support to DPOs in the performance of their function.

The EDPS therefore supports the idea of further developing collaboration between DPOs and the EDPS, which contribute to achieving the overall aim of effective protection of personal data within the EUIs.

6.1. Ensuring application

Ensuring application notably starts by raising awareness. As mentioned above, the DPO plays an important role in developing knowledge on data protection issues inside the EUI. The EDPS welcomes this and the consequence in terms of stimulating an efficient preventive approach rather than repressive data protection supervision.

[40] C.f. the Annex to Regulation (EC) 45/2001.

The DPO also provides advice to the EUI on practical recommendations for improvement of data protection within the EUI, or concerning the interpretation or application of the Regulation. This advisory function is shared with the EDPS who shall advise all EUIs on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to the processing of personal data[41]. In this field, the EDPS has often been called upon to advise DPOs on specific issues related to data protection (informal consultations). The EDPS also intends to revise existing positions papers and guidelines and issue new ones where required in order to continue providing guidance to the EUIs on a wide range of topics.

6.2. Enforcement

In the area of implementation of particular data protection measures, synergy potentials between the DPOs and EDPS emerge as regards the adoption of sanctions and handling of complaints and queries. As already mentioned, the DPOs have limited powers of enforcement. The EDPS will contribute to ensuring compliance with the Regulation by taking effective measures in the field of prior consultations, complaints and other inquiries. Measures are effective if they are well-targeted and feasible and the DPO can also be seen as a strategic partner in determining the well-targeted application of a measure.

As mentioned above, the handling of complaints and queries by the DPO at a local level is to be encouraged, at least as concerns a first phase of investigation and resolution. The EDPS therefore believes that DPOs should try to investigate and resolve complaints within the EUI before referring to the EDPS. The DPO should also be invited to consult the EDPS whenever they have doubts on the procedure or substance of complaints. The limited powers of enforcement of the DPO may also lead them to escalate certain matters to the EDPS for support. Such consultations can naturally be made without involving the EUI. In certain sensitive cases where the DPO might fear repercussions from their EUI if they act upon a complaint, it may be preferable for the EDPS to handle the complaint or open an own-initiative inquiry.

This does not, however, prevent the data subject from lodging a complaint directly with the EDPS under Article 57(1)(e). The EDPS therefore provides valuable support in the field of enforcement. In turn, the DPO can be relied upon to provide information to the EDPS and to provide follow-up on the measures adopted. The DPO is in copy of all communication with the EUI in the framework of complaints and is thus kept informed of the investigation and its outcome.

6.3. Measuring effectiveness

As concerns measuring the effectiveness of the implementation of the data protection requirements, the DPO should be seen as a valuable partner to evaluate progress in this area. For example, when it comes to measuring performance of internal data protection supervision, the EDPS encourages DPOs to develop their own criteria of good supervision (professional standards, specific plans for the institution, annual work programme, etc.). These criteria will in turn enable the EDPS, where invited to do so, to evaluate the work of the DPO, but will also allow them to measure the state of implementation of the Regulation within the EUI.

[41] Article57(1)(g).