Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001[1]

14 October 2010

Network of Data Protection Officers of the EU institutions and bodies

[1] Regulation (EC) No 45/2001 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.1.2001, p. 1. Presently, some DPOs of EU bodies/agencies not falling under the scope of application of Regulation 45/2001 participate as observers in the network of DPOs of the EU institutions and bodies. The content of this document is also relevant to them insofar as their specific legal framework does not foresee different rules than the Regulation. For those DPOs, the references to the EDPS should be understood as references to their independent supervisory bodies.

TABLE OF CONTENTS

INTRODUCTION

Regulation 45/2001 provides that each Community institution/body is obliged to appoint at least one Data Protection Officer (DPO)(Art. 24.1). The duties, status and powers of the DPO are broadly established in the Regulation.

The DPO plays a fundamental role in ensuring respect of data protection requirements within the institution/body. The DPO is appointed by his institution to advise it on the application of the rules, but he/she is also required to ensure, in an independent manner, that the Regulation is applied internally. The DPO's dual responsibility is reflected in particular in the cooperation he has to develop with the EDPS.

The purpose of these standards is:

(1) To identify the profile of a person well qualified for appointment as DPO in an EU institution or body;

(2) To define minimum standards regarding the status of the DPO within the EU institutions and bodies, designed to ensure independence;

(3) To define best practices in performing DPO duties;

This document is designed to assist DPOs in performing their duties, and to clarify for EU institutions and bodies the profile of a qualified DPO, what they should expect from their DPO (and thus some criteria for evaluating the performance of their DPO), and the main aspects of their relations with their DPO.

This paper is future oriented and aims at describing criteria and best practices which should be taken into account by DPOs and the organisations for which they work in the future. It aims at improving the situation of the DPOs of the institutions, bodies and agencies, not at imposing new requirements to the DPOs already appointed.

In any case, it should be underlined that the performance of a DPO has to be assessed on a case-by-case basis and that, in that context, the data protection regime and system of the organisation as a whole has to be considered.

1. PROFILE OF A DPO

1.1. Selection criteria

Article 24.2 specifies that the DPO shall be selected on the basis of his or her personal and professional qualities, in particular, his or her expert knowledge of data protection.

Best practices: It is natural that more extensive knowledge and experience is required in institutions and bodies where data protection is related to the core business. Bearing in mind the duties which the DPO will be called upon to perform (discussed in section 4), the person appointed as DPO in an EU institution or body should ideally meet the following qualifications:

(1) Professional qualities and expert knowledge of data protection:

(a) Expertise in the area of EU privacy and data protection law, in particular Article 16 of the Treaty on the Functioning of the European Union, Article

8 of the Charter of Fundamental Rights of the European Union, Regulation (EC) 45/2001 and other relevant data protection legal instruments, and expertise in IT and IT Security; and

(b) A good understanding of the way the institution operates and of its personal data processing activities, and an ability to interpret relevant data protection rules in that context.

(2) Personal qualities which the DPO should possess:

(a) It is recommended that the DPO should have the following experience/maturity:

– at least 3 years of relevant experience[2] to serve as DPO in a body where data protection is not related to the core business[3] (and thus personal data processing activities are mainly administrative); and

– at least 7 years of relevant experience[2] to serve as DPO in an EU institution or in those EU bodies where data protection is related to the core business or which have an important volume of processing operations on personal data.

(b) Personal skills: integrity, initiative, organization, perseverance, discretion, ability to assert himself/herself in difficult circumstances, interest in data protection and motivation to be a DPO.

(c) Interpersonal skills: communication, negotiation, conflict resolution, ability to build working relationships.

.

1.2. Training after appointment

In order to ensure that the DPO maintains and updates his/her expert knowledge of data protection, the DPO should be given the opportunity to follow regular training, including that offered by:

- The EDPS and other institutions/bodies;
- External providers (universities, DP professional organisations);
- Participation in the EU DPO network;

---

[2] Relevant experience includes experience in implementing data protection requirements and experience within the appointing institution/organisation resulting in knowledge of how it functions. In the absence of the specified years of experience, the appointing institution/body should be prepared to make more time available to the DPO for training and for work on data protection tasks.

[3] Organisations where data processing is related to the core business of the organisation include, for instance, OLAF, Eurojust and Europol, where the processing of personal data is inherent to the main operational activities of the organisation.

- Self study through documents provided to the DPO network on CIRCA, EDPS website, participation in conferences, etc.

1.3. Certification

The DPO should be given the opportunity to develop his/her skills. This could include the possibility to obtain certification as privacy professional. The most relevant certification at this stage would be the one provided by the International Association of Privacy Professionals (IAPP), which offers various privacy professional certifications, including Certified Information Privacy Professional (CIPP) and Certified Information Privacy Professional/Information Technology (CIPP/IT). An EU specific certification will be offered in the near future.

Other relevant certifications are:

- Certified Information Systems Security Professional (CISSP): developed for information security professionals;

- Certified Information Systems Auditor (CISA) certification: developed for information systems (IS) audit, control and security professionals;

- Certified Information Security Manager (CISM) certification: developed for persons who manage, design, oversee and/or assess an enterprise's information security.

The possession of such a certification should be considered as an asset by EU institutions/bodies when selecting their DPO.

2. DPO INDEPENDENCE AND STATUS

Regulation 45/2001 contains a number of provisions designed to guarantee the independence of the DPO, as follows:

- Obligation that the DPO ensure the internal application of the Regulation in an independent manner (Art. 24.1) and not receive any instructions with respect to the performance of his/her duties (Art. 24.7);

- Appointment and removal:

    - Appointed between 2 and 5 years, and eligible for reappointment up to a maximum of 10 years (Art. 24.4);

    - DPO's appointment shall be registered with the EDPS by the appointing institution/body (Art. 24.5);

    - DPO can be dismissed only if he/she no longer fulfils the conditions required for the performance of his/her duties, only with the consent of the EDPS (Art. 24.4);

- Staff and resources: The appointing institution/body must provide the DPO with the staff and resources necessary to carry out his/her duties (Art. 24.4);

- Relief from other duties: To the extent required, the appointing institution/body shall relieve the DPO of other activities (Annex to Regulation 45/2001, para. 5);

- Conflict of interest: The DPO should not have conflicts of interest between DPO duties and any other official duties, in particular in relation to the application of the provisions of the Regulation (Art. 24.3);

- Implementing rules: EU institutions/bodies must adopt further implementing rules (Art. 24(8) and Annex of Reg. 45/2001). These should emphasize the powers of the DPO to conduct investigations, the duty of all controllers to cooperate with the DPO, the right of the DPO to have access at all times to premises, offices, data processing operations and data carriers, and the protection of those who have brought to the DPO's attention an alleged breach of the Regulation.

In practice, however, it may be challenging for the DPO to exercise his/her duties in full independence. Needless to say, the individual situation and personality of the DPO will play a role but it can generally be assumed that certain elements may tend to weaken the position of a DPO:

- A part-time DPO faces a permanent conflict between allocating time and efforts to his/her DPO tasks versus other tasks. With respect to career development and performance review, management may place greater weight on the non-DPO activities. This creates pressure on the DPO to concentrate his/her efforts on the non-DPO tasks. A part-time DPO is also in danger of encountering conflicts of interest.

- The DPO with a limited contract would likely be in a weaker position to perform his/her DPO duties vigorously than one with a permanent contract (official or temporary agent with indefinite term contract). This is because he/she may be concerned about how his/her actions could negatively influence the renewal of his/her contract. A DPO who is very young and has only limited work experience may have difficulties standing up to controllers, and may be more focused on his/her own career development than on vigorous performance of DPO duties.

- A DPO who reports to, and is reviewed by, a direct superior in the hierarchy (director or head of unit) may feel pressure to cooperate and get along smoothly with management and other colleagues, as vigorous performance of DPO duties may have a negative impact on career. The proper performance of DPO tasks often requires that the DPO take a firm and insisting attitude also with controllers who have a high position in the organisation, which may be perceived, at best, as bureaucratic or, at worst, unpleasant "trouble-making". Thus, the DPO must be able to withstand the pressures and difficulties which accompany this important position. To alleviate this pressure, the DPO should report to, and be reviewed by, the administrative head of the institution or body. This is particularly important for part-time DPOs, who should report directly to, and be reviewed by, the appointing authority for their DPO duties, and to/by the normal superior in the hierarchy for other duties.

- A DPO who must request staff and resources (IT resources, budget for business trips and training) from his/her direct superior could face difficulties if the latter is not fully committed to achieving data protection compliance. This can be avoided if the DPO has his own budget responsibility, and by having any requests for additional resources subject to approval by the appointing authority.

Best practices to help ensure the independence of the DPO are:

- The institution or body should establish the DPO post within the organisation as one of Adviser, Head of Unit or Director and in any event the DPO position should be officially recognized as management level, on the official organizational chart of the institution/body;

- The institution or body should appoint the DPO for the longest term possible, in light of the DPO's contract. Thus, a five year appointment should be the norm, unless it is not possible under the circumstances;

- The DPO should have a permanent/undetermined contract with the institution or body, should be sufficiently experienced (see section 2.1(2) above);

- The DPO should be able to dedicate his/her time fully to his/her DPO duties, especially for large institutions and bodies, and for smaller ones in the initial phase of establishing a data protection regime. Proper support in terms of resources and infrastructure should be provided. The non-DPO duties of a part-time DPO should not present a conflict of interest, or even the appearance of a conflict, with the DPO duties;

- DPOs in organisations where data processing activities are the core business of the organisation will normally require various staff members. Such staff capacity should be ensured;

- Rules should be in place within the organisation ensuring the obligation of all staff members to cooperate with the DPO without having to wait for an order or permission of their superior;

- The DPO should report to the head of the institution or body, who should be responsible for review of the DPO's performance of his/her duties, as established by the Regulation. The person responsible for the DPO's performance review should be sensitive to the need for the DPO to take strong positions which others in the organization may not appreciate. The DPO should not suffer any prejudice on account of the performance of his/her duties. The appointing authority should ensure that during the DPO's term of office, he/she has at least a "normal" career advancement. When reviewing the DPO's performance, the evaluator should be careful neither to reprimand the DPO for taking unpopular positions nor to consider data protection requirements as an administrative burden. For a part-time DPO, performance on the DPO duties should be given equal weighting to performance on the non-DPO duties. If provided in the implementing rules of the institution/body, the EDPS should be given the opportunity to provide input on the DPO's performance;

- The DPO should have his/her own budget line, set up in compliance with the relevant rules and procedures of the respective institution/body; his/her requests for any further resources should be subject to approval by the administrative head. Other arrangements are acceptable if they provide the DPO with the resources he/she needs to perform his/her mission in an independent manner;

- The DPO should have signing power for DP related correspondence.

3. DUTIES AND FUNCTIONS OF THE DPO

Article 24, paragraph 1 and the Annex of the Regulation specify the tasks of the DPO. This section will review each of the tasks and provide guidance on how they should be achieved.

3.1. Duty to inform

The DPO is responsible to ensure that controllers and data subjects are informed of their rights and obligations under the Regulation (Art. 24(1)(a)).

3.1.1. Controllers

Best practices for informing controllers of their duties are:

- Offer training to controllers and their staff, which is specifically targeted to the practical steps they should take in order to comply with data protection requirements in the performance of their duties in the context of the respective institution or body. Training should be repeated on a regular basis, to refresh and update and to ensure that all newcomers receive training; specific training/info sessions also should be organised for the different groups of staff with similar data processing activities and on specific occasions with DP relevance such as DP day, previous to inspections etc.;

- Develop, where appropriate, together with controllers, data protection guidelines, if a substantial number of people within the organization must process the personal data, to ensure that it is being done consistently and in compliance with all DP requirements;

- Use best efforts to attend meetings of senior and middle management on a regular basis or to meet, at least twice a year, with management in order to provide updates on the status of implementation and compliance within the organisation are provided. It is an obligation of the institution's management to include the DPO in such meetings, which can be followed by bilateral meetings with the relevant controllers during which the specific situation of their unit/service is reviewed and necessary updates to the existing notifications are discussed;

- Create an intranet page for data protection in the institution/body, which includes the Register, privacy statements, DP guidelines/instructions of the institution/body, opinions of the EDPS on the prior checks of the institution/body, DP quality assurance reports, DPO periodic reports, and any other elements which may be helpful to the controllers and the staff of the institution/body;

- Publish short articles and regular reports in any existing internal newsletter, publication etc.;

- Prepare short information booklets, folders etc.;

- Participate in European Data Protection Day activities, such as information sessions, a booth with leaflets and other information, DP quizzes, posters, etc.;

- If the size of the institution/body justifies it, the DPO should encourage the creation of a network of local DPO correspondents/coordinators.

The DPO should also provide his/her institution/body with periodic reports as to the status of implementation.

The DPO should not only inform the controllers but also build a stable professional relationship with them, providing advice where necessary and investing time and efforts in showing the benefits of DP compliance to them. It is imperative to "sell the product" to the management of the organisation and ensure that DP compliance is reflected in the relevant management plans and considered as a relevant objective of the organisation.

3.1.2. Data subjects

The DPO is responsible to ensure that data subjects are informed of their rights under the Regulation (Art. 24(1)(a)). Best practices for informing data subjects are:

- To create an Internet DP page containing most of the content of the above mentioned intranet page, excluding only items that are internal to the institution/body, such as quality assurance reports, DPO reports, and internal instructions to staff concerning data protection;

- A leaflet could be used to supplement the information to the data subject.

The requirements for information to data subject are set out in Articles 11 and 12 of the Regulation. It is the responsibility of the controller to ensure that this requirement is satisfied. The DPO should ensure that the controller has taken the necessary steps to satisfy this requirement, as follows:

- Privacy statements should be prepared for each processing operation, and appropriate means should be developed to ensure that the privacy statement is provided to the data subjects, for instance, by assisting controllers in drafting such statements;

- If forms are used for communicating with data subjects, an abbreviated privacy statement should be added to the form;

3.2. Duty to cooperate with the EDPS

The DPO is responsible for responding directly to requests from the EDPS addressed to him/her and for ensuring that requests from the EDPS addressed to controllers are acknowledged by them. The DPO also has a duty to cooperate with the EDPS (Art. 24(1)(b)). In general, the EDPS sends requests to the DPO for the following purposes:

- To supplement information that was provided in a notification for prior checking;

- With respect to a complaint concerning the DPO's institution or body;

- To monitor progress on implementation of EDPS recommendations;

- To gather information for a survey being conducted by the EDPS on an issue which he is examining.

The DPO should respond to all requests within a reasonable period. This should normally occur within two weeks of receipt of the request. He/she should also ensure that requests from the EDPS addressed to controllers are answered within a reasonable period. If more time is needed, a note should be sent to the EDPS indicating when a substantive reply

will be sent. This would be consistent with Article 14 of the European Code of Good Administrative Behaviour.

In general, strong collaboration of the DPO and the EDPS will aid both in meeting their responsibilities to ensure the application of DP requirements.

3.3. Duty to maintain a register of processing operations

The DPO is responsible to keep a register of the processing operations carried out by the controller, containing the items of information referred to in Article 25(2). (Art. 24(1)(d)).

To meet this requirement, the DPO will normally begin by making an inventory of all DP operations within his/her institution/body. This may be done by sending a note or approaching directly all middle and senior managers asking them what personal data processing operations occur within their unit/directorate. A form requesting the basic information about the processing operation (name of controller and delegated controller, name of processing operation, description, and purpose) should accompany the note. The replies with completed forms would constitute an inventory.

The next step is for the responsible controller to prepare a full notification for each of the processing operations in the inventory. The DPO should provide whatever advice is needed to complete the notification. The DPO has the right to refuse a notification if he/she considers that the processing operation breaches a provision of Regulation 45/2001.

The Regulation requires that the Register may be inspected by any person directly or indirectly through the EDPS. If the size of the institution/body and the volume of processing operations justify it, the DPO should ensure that the register is accessible on line.

An IT application to create the inventory and register, and to manage notifications, is an efficient way to accomplish these tasks. A mere webpage could be considered as an alternative tool.

3.4. Duty to notify the EDPS of risky processing operations

The DPO is responsible to notify the EDPS of the processing operations likely to present specific risks within the meaning of Article 27 (Art. 24(1)(e)).

It is the responsibility of the DPO to determine initially whether the processing operation presents specific risks, and is thus subject to prior checking. In case of disagreement with the controller on the necessity to submit a processing operation to a prior check, the opinion of the DPO shall prevail. In applying the criteria listed in Article 27(2) for making this determination, the DPO should consult with the responsible controller. In case of doubt as to whether prior checking is required, the DPO must consult the EDPS.

The DPO should also update any notifications made to the EDPS, where necessary.

As noted in the previous section, the DPO is also responsible to ensure that any follow-up questions submitted by the EDPS during the course of a prior check receive a timely reply.

The EDPS' opinion on the prior check will normally contain a list of recommendations. It is the responsibility of the controller to implement the recommendations. The DPO should follow implementation activities, as part of the duty to ensure the internal application of the regulation. The DPO should ensure that the controller keeps the EDPS informed of the status of implementation of such recommendations.

3.5. Duty to provide the appointing institution/body with recommendations and advice

The DPO may be consulted by his/her institution/body, a controller, the Staff Committee, or any individual on any matter concerning the interpretation or application of the Regulation. The DPO may advise, on request or on his/her own initiative, the institution and the controllers on the application of data protection provisions. The DPO may also make recommendations for the practical improvement of data protection at his/her institution and advise it on matters concerning the application of data protection provisions. (Annex to Regulation 45/2001, paras. 1, 2).

3.5.1. Advice on application of DP provisions

The DPO may be asked to provide advice, or may spontaneously provide advice, in various contexts. The most common instances where the DPO will give advice are when the institution/body:

- Considers any new information systems or processing operations;
- Prepares notifications;
- Prepares replies to requests from data subjects for access, rectification, blocking, or erasure;
- Prepares replies to complaints from data subjects and to requests from staff within the meaning of Article 90 of the Staff regulations if they are linked to DP issues;
- Prepares any rules having impact on DP;
- Discusses any legal, practical or technical issues having impact on DP;
- Implements recommendations from the EDPS;
- Prepares replies to requests for information from the EDPS;

Advice may be given orally or in writing, as appropriate. Any written advice that could have significance beyond the context of the specific case in which it is given should be published on the intranet DP page.

Whenever the DPO has doubts about the advice to be given, he/she may consult the EDPS on the matter or suggest that the controller submit a request for advice to the EDPS.

The DPO should ensure that his/her institution informs the EDPS when drawing up administrative measures relating to the processing of personal data, in accordance with Article 28(1) of Regulation 45/2001.

3.5.2. Recommendations for practical improvement

In the course of performing DPO duties, it may become apparent that improvements can be made in the manner in which data protection requirements are being implemented in the institution/body. Possible systemic improvements may, for instance, be revealed by audits of data processing operations conducted by the DPO or internal auditor. The DPO can make recommendations to the institution/body for practical improvements at his/her own initiative, or at the request of the institution/body.

3.6. Duty to ensure compliance

The DPO is charged with ensuring in an independent manner the internal application of the Regulation (Art. 24(1)(c)), and that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operation (Art. 24(1)). The Regulation requires controllers to assist the DPO in performing his or her duties and to give information in reply to questions, and states that the DPO shall have access at all times to the data forming the subject matter of processing operations and to all offices, data processing installations and data carriers.

Although the DPO has no enforcement power vis-à-vis controllers, he/she is empowered to monitor compliance by collecting all relevant data, which the appointing institution/body and its controllers are obliged to make available.

IT tools may be developed to assist the DPO in performing regular monitoring. Administrative arrangements can also be made, such as ensuring that the DPO receives a copy of all mail raising data protection issues, and requiring that the DPO be consulted on documents raising data protection issues. Careful, regular monitoring of compliance and reporting of results can create a strong pressure on controllers to ensure that their processing operations are compliant. Regular monitoring and reporting are thus the DPO's strongest tools for ensuring compliance. To this end, an annual survey/report issued to the management and made available to the EDPS, either by publication or by sending it directly to him/her, is a best practice (see later under 4.1).

It is also important that a procedure exists in case of non-compliance. In such case, it is important that the DPO can directly report non-compliance to the highest hierarchical level within the organisation[4] and that, when the DPO is not satisfied with the measures taken, or none are taken, he/she can directly report the issue to the EDPS.

3.7. Duty and power to investigate

The DPO may investigate matters and occurrences directly relating to his/her tasks and report back to the person who requested the investigation and/or the controller. An investigation may be requested by the DPO's institution/body, the Staff Committee, or any individual.

Upon receipt of the request for an investigation, the DPO should ask the controller to provide all relevant information and documentation. As stated in the previous section, the

[4] See, e.g., Article 28.4 Council Decision establishing the European Police Office (Europol), OJ L 121, 15.5.2009, p. 37; Article 17.4 of the Council Decision 2009/426/JHA on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crim, OJ L 138, 4.6.2009, p. 14.

institution/body and its controllers are obliged to provide the DPO with any information and access to any data that he/she requests. The DPO should analyse these materials, and provide the person who requested the investigation with a written reply, with copy to the controller and the head of the institution/body. The reply should state that it is possible to raise the matter with the EDPS.

It is important that the procedure for filing and dealing with complaints is well defined in the institution's implementing rules adopted pursuant to Art. 24(8) of the Regulation, in order to avoid having procedural questions impede an appropriate resolution of the complaint.

4. BEST PRACTICES

In view of the differing situation of the various EU institutions and bodies, the following best practices should be used for reference purposes. However, the best practices for each DPO will have to be commensurate to the available staff and resources allocated by his/her institution/body.

4.1. Periodic DPO Report

The DPO should prepare a report, normally once or twice a year, to inform his/her institution, and in particular the controllers, of the status of data protection compliance. The reports should be published on the institution/body's intranet site. A copy of these reports should be available to the EDPS, either by publication or by sending it to him/her directly. These reports could, for instance, include:

- A status report on notifications, prior checks, and the state of the institution/body's Register;
- A summary of any supervision activities of the EDPS with respect to the institution/body over the relevant period;
- Information on any training activities that were provided over the relevant period, and any training planned for the future;
- A status report on efforts undertaken to satisfy the recommendations made by the EDPS in prior checking opinions;
- Report on requests and complaints received from data subjects, and their status; and
- The results of checks and audits carried out by the DPO in selected parts of the organisation using a rotation system, including conclusions as to the state of compliance and where necessary recommendations to solve situations of non (or non full) compliance;
- Report of activities in the EU DPO Network;
- Report of activities of internal correspondents' network, if applicable.

Such report should be presented to the highest management level of the organisation, highlighting best practices and examples of good compliance but also areas which require further attention or specific actions.

4.2. Work Programme

In order to help focus his/her efforts, the DPO should prepare a work programme at the beginning of each year for the upcoming year for the attention of the senior management of the institution/body. The Work Programme should specify what the DPO hopes to achieve over the course of the year. This could include work to be done on:

- Actions being taken regarding awareness such as info sessions etc.;
- notifications, prior checks and the Register;
- implementation of data protection requirements and EDPS recommendations;
- systemic projects to be undertaken (e.g., creation of an electronic register);
- efforts to be undertaken with respect to requests and complaints from data subjects;
- Areas which require special attention within the organisation.

4.3. Involvement in relevant discussion groups

It is important that the DPO is seen as a discussion partner within the organisation and that he/she is part of the relevant groups (team, working groups and so forth) dealing with data processing activities of the organisation; the independence of the DPO should however also be respected in this context as well. For instance, the DPO should be involved in the work of the security committee, if existing, or of any teams responsible for negotiation of agreements/arrangements covering exchange of personal data with any third party/country or international organisation. The opinion of the DPO should always be considered as to the adequacy of the level of protection offered by such partners.

In the cases where the DPO is aware that he/she has not been invited to participate, he/she should openly address the management and inquire about the reasons for being excluded from such discussions. Any problems in this regard should be reported to the EDPS.

4.4. Network of DP coordinators

In large EU institutions and bodies, it may be appropriate to institute a network of coordinators to improve the penetration of data protection information and to enhance the DPO's awareness of developments in the institution/body.

5. ETHICAL STANDARDS FOR DPOS

5.1. Duty of loyalty

The DPO owes a duty of loyalty to the protection of personal data in the institution or body that appointed him/her. Accordingly:

- The DPO shall take all steps necessary to ensure the application of data protection requirements within his/her institution, as elaborated in the Regulation, the institution/body's implementing rules, and these standards.

- The DPO shall exercise independent professional judgment in performing his/her duties and render candid advice to his/her institution, its controllers, and data subjects on data protection matters;
- In handling a complaint of a data subject, the DPO shall act with diligence and promptness to impartially analyze the issues raised in order to determine whether there has been a violation of the requirements of the Regulation. If so, he/she should attempt to resolve the matter with his/her institution and thereafter report to the complainant on the solution found. A DPO shall not counsel or assist his/her institution to alter, destroy or conceal a document or other material relevant to the complaint.

5.2. Need to know

The DPO shall utilize his/her power of access to the data forming the subject-matter of processing operations and all offices, data processing installations and data carriers strictly on a need-to-know basis, in order to perform his/her duties as delineated in the Regulation.

5.3. Duty of confidentiality

The DPO and related staff shall not divulge information or documents which they obtain in the course of their duties, and are subject to the requirements of professional secrecy, as specified in Article 339 of the Treaty on the functioning of the EU.

5.4. Conflict of interest

As stated in section 2 above, the DPO should not have conflicts of interest between DPO duties and any other official duties, in particular in relation to the application of the provisions of the Regulation (Art. 24.3). A conflict of interest is present when the other duties which a DPO is asked to perform may have directly adverse interests to that of protection of personal data within his/her institution. If necessary, the DPO should raise this matter with his/her appointing authority.

6. RELATION BETWEEN THE DPO AND THE EDPS

It is crucial that the DPO is perceived as part of the organisation and not as an “agent” of the EDPS. However, in order for the DPO to be successful in ensuring compliance within the organisation, the support of and good cooperation with the EDPS is of vital importance, in particular:

- Regular exchanges of views and information should take place between the DPO and the EDPS;

- The DPO should be informed by the EDPS about any intended inspections, being properly involved during the process and in the follow-up to such inspections;

- The DPO and the EDPS should as a rule inform each other about any complaints they have received concerning the DPO's appointing institution/body.

Good and regular cooperation with the EDPS will enhance the DPO's ability to achieve compliance within his/her institution/body.

7. CONCLUSION

Regulation 45/2001 establishes an institutional framework for implementation of data protection requirements. Within this framework, the DPO plays a fundamental but difficult role: to ensure respect of data protection requirements within the institution/body. Because the DPO works inside the appointing institution/body, he/she is best placed to guarantee the internal application of data protection requirements. This document has attempted to give further precision to the profile, status, and duties of the DPO in order to help DPOs understand what is expected of them, and to help the EU institutions/bodies to understand the role of their DPO.