Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001

Brussels, 28 November 2005

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 63
E-mail: edps@edps.eu.int - Web site: www.edps.eu.int
Tel.: 02-283 19 00 - Fax: 02-283 19 50

The role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001

I. Introduction

Regulation (EC) No 45/2001 of the European Parliament and of the Council (hereinafter Regulation 45/2001) provides a layered approach to guaranteeing data protection in the institutions and bodies: the institutions/bodies themselves, controllers, data protection officers (DPO) and the European Data Protection Supervisor (EDPS) all contribute to the application of the Regulation. This paper aims at examining the key role of DPOs and the underlying synergies between the DPOs and the EDPS in ensuring effective compliance with data protection principles. It will also provide guidelines on the type of profile required by a DPO and the resources that need to be allocated to the DPO so as to ensure the good performance of his/her duties.

It is up to the institutions and bodies to protect the fundamental rights and freedoms of natural persons and in particular their right to privacy with respect to the processing of personal data (Article 1.1 of Regulation No 45/2001)[1]. Thus the measures adopted in the Regulation are binding on the institutions and bodies.

In practice, due to their involvement in the actual processing operation, "controllers" are responsible for ensuring the respect of most data protection principles[2]. The controller often has insight into the processing operation itself and is an easy contact person for the data subject. To this effect, the controller ensures that the data subject can exercise his/her rights and ensures respect of the principles established in the Regulation. Article 2.d of the Regulation 45/2001 defines the controller as: "the Community institution or body, the Directorate-General, the unit or any other organisational entity which alone or jointly with others determines the purposes and means of processing of personal data". In some cases the controller is the institution or body itself or an organisational part of it. In practice, the controller is very often the specific person responsible for the implementation of the processing operations (Head of Unit/Department, for example). In any event this person, as an official of the institution, is acting on behalf of the institution/body which bears the responsibility for the respect of the Regulation.

Regulation 45/2001 provides the obligation for each Community institution / body to appoint a Data Protection Officer (Article 24.1)[3]. As will be examined below, the Data Protection Officer (DPO) is fundamental in insuring the respect of data protection principles within institutions/bodies.

An independent supervisory authority, the European Data Protection Supervisor is provided for in Regulation 45/2001 in view of monitoring the application of the Regulation in institutions and

[1] If the obligations provided for in the Regulation are not respected by the controller and the data subject suffers damage, Article 32(4) confirms that the Community is liable in damages for that loss.
[2] Notably data quality (Article 4), appropriate level of security (Article 22), notification to the DPO (Article 25).
[3] The idea of a DPO originates from article 18(2) of Directive (EC) 95/46 which allows Member States to exempt controllers from notification of a processing operation to the national data protection authorities where the controller appoints a data protection official. This alternative to notification provided by the Directive is currently implemented in five Member States: Germany, the Netherlands, Sweden, Luxembourg and France.

bodies and for advising these entities and data subjects on all matters concerning the processing of personal data (Article 41). This notably implies providing support within the institutional framework to the work and role of the DPOs.

II. Some experiences

Data protection officers have been in existence for over three years and have proved to be a success not only in their work within the institution/body, 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. Nevertheless, certain shortcomings in the institutions/bodies have to be underlined.

1. Appointment of a DPO

Regulation 45/2001 provides that at least one person should be appointed as data protection officer (Article 24.1). Even though the Regulation has entered into force in 2001, some Community bodies have still not appointed a DPO. The EDPS can only regret this and encourage such bodies to do so without further delay.

The Regulation leaves open the possibility of variations according to institutions (appointment of "at least" one person as data protection officer). Up to now institutions which have a DPO have nominated one person for the task. However, some institutions have coupled the DPO with an assistant or deputy DPO. The Commission has also 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. It has also appointed a specific DPO for OLAF.

The appointment of a DPO within an institution/body does not however automatically imply full compliance with the Regulation: a gap needs to be bridged between the requirements of the Regulation and the present situation. Measures must also be put into place for the Regulation to be fully implemented in practice. To name but one example, in the area of notification of processing operations (Article 25), despite efforts made by existing DPOs in this field, the EDPS would like to stress that institutions/bodies must also effectively contribute to ensuring that processing operations are notified to the DPO.

2. Independence

The Regulation provides that the DPO shall ensure "in an independent manner the internal application of the provisions of this Regulation" (Article 24.1.c). However, in those institutions and bodies that have appointed a DPO, certain elements have compromised this independent status within the Community institution/body.

Indeed, part-time DPOs have found themselves in a permanent conflict between allocating time and efforts to his/her regular tasks as opposed to investing in his/her DPO duties. Moreover since DPOs are often evaluated on the basis of their 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 bodies will not find it practical, or even possible, to appoint a full-time DPO. The issue of a

"shared" DPO has been envisaged in practice. The EDPS will give some guidance on the issue of part/full-time DPOs and "shared" DPOs in this document.

Independence is also an issue related to the hierarchal position of the DPO and the person he/she should report to. Some DPOs have found that they are confronted with "authority" problems vis-à-vis high-ranking controllers when providing advice/recommendations or during investigations. Furthermore, reporting to a direct superior may create a risk of interference by the superior in DPO duties. Institutions and bodies must be aware of these possible challenges to the independence of the DPO.

3. Adequate staff and resources

The Community institution or body should provide the DPO with the staff and resources necessary to carry out his/her duties (Article 24.6). The issue of sufficient resources whether they be IT resources, HR resources or financial resources has also been an important element to enable the DPO to carry out his/her duties in practice. By reaffirming the crucial role of the DPO the EDPS aims to contribute to the commitment by the institutions and bodies to providing means for the DPO to carry out his/her duties.

III. Role of Data Protection Officers: Ensuring in an independent manner the internal application of Regulation 45/2001

The DPO has a central role within the institution/body: DPOs are familiar with problems of the entity where they work (idea of proximity) and, given their status, have a crucial role to play in giving advice and help in solving data protection issues.

To this effect, Regulation 45/2001 grants in its Articles 24-26 and its Annex, a number of tasks, duties and powers of the DPO. These are further detailed in "Implementing rules" to be adopted by each Community institution or body (Article 24.8)[1].

III.1. Functions of the DPO within the institution:

- **Information** and **raising awareness** function (article 24.1.a): This implies, on the one hand informing staff members of their rights and, on the other hand, informing controllers and the institution/body of their obligations and responsibilities. Raising awareness can take the form of staff information notes, training sessions, setting up of a web site, privacy statements.

- **Advisory** function (recital 32 and Annex §1 & 2): DPOs must ensure that the Regulation is respected and advise controllers on fulfilling their obligations. The DPO may make recommendations for the practical improvement of data protection to the institution/body and advise it, or the controller concerned, on matters concerning the application of data protection provisions. The DPO may also be consulted by the institution/body, by the controller, by the Staff Committee and by any individual on any matter concerning the interpretation or application of the Regulation.

[1] Some institutions have submitted their implementing rules to the EDPS for advice, this has given the EDPS the occasion to stress some important points which will be highlighted in this document.

- **Organisational function** (Articles 25 and 26): As mentioned above, data processing operations must be notified to the DPO. This requires the drafting of a notification form to be filled in by controllers containing at least information as mentioned in Article 25. The DPO must organise a register of processing operations. The register must be made accessible to any person. The EDPS believes that it would be most appropriate to have an on-line access to this register, but non electronic access cannot be refused to a person who asks for it. Once the DPO has received the notification she/he must identify cases falling within the scope of Article 27 and notify the EDPS for prior checking taking into account the two-month delay within which the EDPS must render his opinion. The EDPS has developed a notification form to this effect to be filled in by the controller and/or DPO. In case of doubt as to the need for prior checking, the DPO may consult the EDPS.

- **Cooperative function** (Article 24.1.b): The DPO has the task of responding to requests from the EDPS and, within the sphere of his competence, cooperate with the EDPS at the latter's request or on his/her own initiative. This task emphasises the fact that the DPO facilitates cooperation between the EDPS and the institution notably in the frame of investigations, complaint handling or prior checks. The DPO not only has inside knowledge of the institution, but is also likely to know who the best person to contact within the institution is. The DPO may also be aware, and duly inform the EDPS, of recent developments likely to impact the protection of personal data. The cooperation and possible synergies between the DPO and the EDPS will be examined in this document (part IV).

- **Monitoring of compliance** (Article 24.1.c & Annex § 1 and 4): the DPO is to ensure the application of the Regulation within the institution. The DPO may, on his own initiative or at the request of the institution or body, the controller, the staff committee or any individual investigate matters and occurrences directly relating to his/her tasks and report back to the person who commissioned the investigation or to the controller. This function is supported by the fact 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.

- **Handle queries or complaints:** Although not explicitly mentioned in the Regulation, this function can be deduced from the fact that the DPO is granted with investigation functions: "Furthermore he or she may, on his own initiative or at the request of the Community institution or body which appointed him or her, the controller, the Staff Committee concerned or any individual, investigate matters and occurrences directly relating to his tasks and which come to his or her notice, and report back to the person who commissioned the investigation or to the controller" (Annex §1). Furthermore the Regulation provides that "No one shall suffer prejudice on account of a matter brought to attention of the competent Data Protection Officer" (Annex §3). The EDPS, as the principal complaint handling instance in the field of data protection, encourages the investigation and handling of complaints by DPOs (see point IV. 3). The fact that the DPO acts from within the institution and is close to the data subject places him/her in an ideal situation to receive and handle queries or complaints at a local level. This does not however prevent the data subject from addressing him/herself directly to the EDPS under Article 33.

- **Enforcement:** Despite having competence to monitor compliance with the Regulation and to handle complaints, the DPO has limited powers of enforcement: the DPO has 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 possible application of Article 49 of the Regulation.

III.2. Guaranteeing independence

The DPO is placed in a difficult position: he/she is a part of the institution and yet must remain independent from this institution in the performance of his/her duties. As already mentioned, the fact of being a part of the institution (idea of proximity) puts him/her 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 body. A number of guarantees have been provided for in the Regulation which aim at ensuring that the DPO fulfils his duties in an independent manner.

1. No conflict of interest between duties (24.3)

Ensuring full application of the provisions of the Regulation should not be jeopardised by an overlap in his/her functions resulting in conflicting interests. For example, a part-time DPO should not act as data controller in his initial activity.

So as to avoid conflicts of interests and to guarantee independence, if the DPO has several duties, these duties must be evaluated separately. Evaluation of a DPO in the performance of his/her duties as DPO must not be related in any way to the performance of other tasks.

Article 24.3 also implies that 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 his/her duty as DPO has been problematic in many institutions.

It is not easy *a priori* 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 institution: even a small institution could have many processing operations involving personal data.

Moreover, a new post of DPO requires a lot of investment at the start in order to raise the awareness of staff and to ensure compliance in the field of notifications. 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.

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.

A common/shared DPO could be a solution especially for small institutions where the appointment of a full-time DPO is not feasible. However the appointment of a "shared" DPO

between institutions must be made conditional upon the fact that the institutions are closely connected both in their functioning and their geographical location or organisation.

2. Institution or body must provide staff and resources to carry out duties (24.6)

Certain institutions have seconded the DPO with an assistant/deputy DPO whose role is to assist the DPO (particularly in large institutions) and to ensure continuity of the DPO function. Quite apart from the question of independence (see above), the institution/body must also address issues such as those of temporary replacement of the DPO by the assistant/deputy DPO in the event of absence (sick leave, mission, retirement).

As mentioned above the Commission has also appointed a "Data protection coordinator" (DPC) in each DG in order to co-ordinate all aspects of data protection in the DG[1]. 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 Directorate General where he is appointed. A number of principles applicable to the DPOs also apply to a large extent to the DPCs so as to enable him/her to carry out his/her work efficiently (evaluation, independence, time allocated to the duty...).

Article 24.6 also implies that the DPO is provided with sufficient financial resources to carry out his/her duties. It could also imply that the DPO receives adequate support if needed from other services (the legal service, for example) and access to training facilities.

3. May not receive instructions from anyone in performance of duties (article 24.7)

According to Article 24.7, with respect to the performance of his/her duties, the DPO may not receive any instructions. This article 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. There is also a risk that junior DPOs are confronted with "authority" problems vis-à-vis high ranking controllers. Furthermore, DPOs should not suffer prejudice in their career development from the mere fact of having been a DPO. Finally, the DPO should only report to his/her appointing authority and not to a direct superior.

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

4. DPO shall have access to information and to offices and data-processing installations (Annex §4)

According to the Annex §4, the DPO "shall have access at all times to the data forming the subject-matter of the processing operations and to all offices, data-processing installations and data-carriers". This provision gives the DPO investigative powers in the performance of his/her duties. This is supported by the fact that the same provision provides that the controller shall be

[1] Seeing the size of an institution like the Commission, the idea of proximity is therefore pushed a step further here.

required to assist the DPO in the performance of his/her duties and to give information in reply to questions.

5. Term of appointment

Article 24.4 stipulates that the DPO shall be appointed for a term of between two and five years. He/she may be eligible for reappointment up to a maximum of ten years. He/she may only be dismissed if two conditions are met: if he/she no longer fulfils the conditions required to perform his/her 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, contribute to ensuring the independence of the DPO. The longer the mandate, the more this contributes to providing the guarantee to the DPO that he/she can carry out his/her function in an independent manner. The EDPS therefore supports the appointment for a term of 5 years. The fact that the EDPS must consent to the dismissal of the DPO if he/she no longer fulfils the conditions required for the performance of his/her duties also contributes to ensuring independence.

Certain implementing rules concerning the tasks, duties and powers of the DPOs adopted by the institutions/bodies according to Article 24.8 provide that the EDPS takes part in the evaluation the work of the DPOs on a regular basis. The EDPS welcomes the idea of a formal consultation 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 to their independence.

6. Independence of Deputy DPOs

In practice, Deputy 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 independence of deputy DPOs, the EDPS believes that Deputy DPOs should be offered the same guarantees as those provided for in the Regulation as concerns DPOs themselves.

III. 3. Guaranteeing Expertise

"The Data Protection Officer shall be selected on the basis of his or her personal and professional qualities and, in particular, his or her expert knowledge of data protection" (Article 24.2). Without entering into the debate of the types of personal qualities required, the EDPS would like to emphasise two elements in this profile: an adequate knowledge of the organisation and structure of the institution/body and, where possible, expertise in data protection.

The EDPS believes that in order to carry out his/her duty in an efficient way it is recommended to have adequate knowledge of organisation, structure and functioning of institution/body. This implies that, in principle the DPO should be recruited from within the institution.

Good working knowledge of Community data protection law, in particular Regulation 45/2001, 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 as mentioned above could include training sessions on the subject both at the time of entry into function and regular up-dates in the course of his/her career.

"Personal and professional qualities" also preferably include knowledge of information technologies (IT) including security aspects, and organisational and communication skills.

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.

IV. Relation DPO - EDPS

Ensuring compliance with the Regulation will be influenced by the working relationship between the DPO and the EDPS. The DPO must not be seen as an agent of the EDPS, but as a part of the institution/body in which he/she works. As already mentioned, this idea of proximity puts him/her 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 body. 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 developing possible synergies between DPOs and the EDPS which would contribute to achieving the overall aim of effective protection of personal data within the institutions.

IV. 1. Ensuring compliance

Ensuring compliance notably starts by raising awareness. As mentioned above, DPOs play an important role in developing knowledge on data protection issues inside the institution/body. The EDPS welcomes this and its consequence in terms of stimulating an efficient preventive approach rather than repressive data protection supervision.

The DPO also provides advice to the institution/body on practical recommendations for improvement of data protection within the institution/body or concerning the interpretation or application of the Regulation (Annex §1 and 2). This advisory function is shared with the EDPS who shall advise all Community institutions/bodies on matters concerning the processing of personal data (Article 46 sub d)). In this field the EDPS has often been called upon to advise DPOs on specific issues related to data protection (case by case approach). The EDPS also intends to produce position papers on certain themes so as to afford guidance to the institutions/bodies on certain more general topics.

IV.2 Prior checks

Opinions delivered in the framework of an Article 27 prior check, are also the occasion for the EDPS to monitor and ensure compliance with the Regulation 45/2001. Prior checks should in principle be completed prior to the start of a processing operation ("proper prior checks"). This enables controllers to fully take into account the recommendations made by the EDPS prior to the processing of personal data. However the time gap between the entry into force of the Regulation and the appointment of the EDPS has created a large backlog of cases which are now being prior checked on an "ex post" basis. In this respect the EDPS would like to see the full implementation of the data protection requirements of the Regulation as concerns notification and prior checks by Spring 2007. The DPO and the EDPS are to be seen as strategic partners in this field.

The EDPS largely relies on the DPOs to give him a full picture of the situation concerning ex-post cases. The DPO should also update the EDPS on any developments leading to new prior checks. Furthermore, before the final adoption of a prior check opinion, the EDPS sends a provisional draft to the DPO with information on intended recommendations thereby opening up room for discussion on efficiency and consequences of intended recommendations. The EDPS intends to be attentive to the concerns of the institution as expressed by the DPO so as to work towards practicable recommendations.

IV. 3. 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 checks and of complaints and other inquiries. Measures are effective if well targeted and feasible: the DPO can also be seen as a strategic partner in determining the well targeted application of a measure.

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 at a local level before referring to the EDPS. The DPO should also be invited to consult the EDPS whenever he/she has doubts on the procedure or content of complaints. This does not however prevent the data subject from addressing him/herself directly to the EDPS under Article 33. The limited powers of enforcement of the DPO also imply that in some cases, the complaint or query must be escalated to the EDPS. The EDPS therefore provides for valuable support in the field of enforcement. In turn, the DPO can be relied on to provide information to the EDPS and to provide follow-up on the measures adopted.

IV.4. Measuring effectiveness

As concerns measuring the effectiveness of the implementation of the data protection requirements, the DPO must be seen as a useful 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...). These criteria will in turn enable the EDPS, where invited to do so, to evaluate the work of the DPO, but will also serve to enable him to measure the state of implementation of the Regulation within the institution/body.