Implementing rules concerning the tasks, duties and powers of the Data Protection Officer (Article 24.8)

Introduction and scope

Article 24.8 of Regulation 45/2001 (hereinafter "the Regulation") stipulates that further implementing rules concerning the Data Protection Officer should be adopted by each Community institution or body in accordance with the provisions in the Annex of the Regulation. The rules concern the implementation of the function of the DPO and, in particular his/her duties and powers[1].

The role of the controller and the rules pursuant to which a data subject may exercise his/her rights may be integrated in the document. This inclusive approach is recommended by the EDPS.

Further to Article 28.1 of the Regulation, Community institutions and bodies shall inform the EDPS when drawing up administrative measures relating to the processing of personal data. Therefore, **draft implementing rules and revision of implementing rules should be submitted for consultation to the EDPS.** The present guidelines are based on this consultation practice and designed to facilitate the drafting of implementing rules where these have not yet been adopted.

In general, the instrument should at least contain the principles established in Articles 24, 25, 26 and in the Annex of the Regulation. To the extent required, the document will adapt these principles to the institution/body concerned (size, administrative practices, hierarchy, etc). The document should be adopted in a long term perspective[2]. Ideally, the document will also include best practices, some of which are

[1] The role of the DPO has been analysed in the EDPS document "Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) No 45/2001. The DPOs are preparing a document on "Professional standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001". When adopted, the document will be published on the EDPS website. Both documents provide useful information for drafting data protection implementing rules.

[2] The document will also be subject to revision in due course. Revision should not be conducted annually but rather every five or ten years or whenever the institution/body considers it necessary (change in mandate, change in the core activities of the institution, etc.). The revision is subject to consultation under Article 28.1.

described in the present document. However, depending on the characteristics of the institution/body concerned and its necessities *vis-à-vis* the processing activities, other best practises could be envisaged.

Content

---

1) Preamble and definitions

The preamble should at least make reference to:

- Article 16 of the Treaty on the functioning of the European Union;
- Regulation (EC) No 45/2001 and in particular Article 24.8. and the Annex thereof.

If definitions are included in the document, the EDPS recommends not adapting the definitions already provided in the Regulation. Indeed, this may introduce confusion as to data protection terms and change their meaning[3].

2) Appointment and status of the Data Protection Officer (Article **24.1. a**)

> **"1.** Each Community institution and Community body shall appoint at least one person as data protection officer."

The implementing rules shall contain information on:

- the term of office of the DPO and in which circumstances he/she can be dismissed (Article 24.4);
- the registration of his/her appointment with the EDPS (Article 24.5);
- his/her professional qualities and specific knowledge of data protection (Article 24.2); the document may also specify that the DPO should have a sound knowledge of the institution/body services if appropriate;
- resources shall be provided to him/her to carry out his/her duties (Article 24.6). In some cases a deputy DPO may be necessary. Every DPO should benefit from the possibility to be appropriately trained and have the opportunity to update his/her knowledge, mainly on data protection law and technical aspects;
- the fact that his/her selection shall not result in a conflict of interest between his/her duties of DPO and any other official duties (Article 24.3), to the extent required, the Data Protection Officer shall be relieved of other activities (Annex);
- the fact that he/she should act in an independent manner while ensuring the internal application of the provisions of the Regulation (Article 24.1.c) and may not receive instructions with respect to the performance of his/her duties (Article 24.7). In the case of a Deputy DPO, the same guarantees of independence must be enshrined in the document.

[3] This is particularly true for the notions of controller/processor. The EDPS also recommends avoiding any mention of "processors within the agency". Implementing rules should preferably treat the processor's issue by focusing on external outsourcing.

3) Tasks, duties and powers of the DPO

Article 24 also includes a general principle which states that the DPO shall ensure that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations. In what follows, the EDPS develops the tasks and the duties of the DPO to ensure that processing operations are compliant with the Regulation, as well as the powers of the DPO to exercise his or her data protection function.

> "**(a)** ensuring that controllers and data subjects are **informed** of their rights and obligations pursuant to this Regulation;"

The DPO shall **raise awareness** on data protection issues and encourage a **culture** of protection of personal data within his/her institution/body. Controllers shall be informed of their obligations (see below point 6) and data subjects shall be made aware of their rights (see below point 7). This can take different forms:

- Training of staff members and controllers;
- Making the register accessible also in electronic form as a tool to ensure transparency as regards the processing operations in place in the institution/body (see below);
- Assistance given by the DPO to the controllers in notifying processing operations, which may also be formalised in the rules (see below);
- Contribution of the DPO to the **Annual Activity Report** of the institution/body, as this is a good tool to raise awareness on data protection issues internally but also externally.

> "**(b)** responding to requests from the European Data Protection Supervisor and, within the sphere of his or her competence, **cooperating** with the European Data Protection Supervisor at the latter's request or on his or her own initiative;"

- The obligation to cooperate with the EDPS should be formalised in the document. The cooperation may be described further: provision of additional information about a notification for prior checking, cooperation in the frame of a complaint, implementation of EDPS recommendations and responding to request from the EDPS, etc.;

> "**(d)** keeping a register of the processing operations carried out by the controller, containing the items of information referred to in Article 25(2);"

- The register may be kept in electronic and paper format (see above);
- The DPO could maintain an inventory of all processing operations on personal data of the institution/body to better identify processing operations to be notified. An inventory of processing operations has proved to be an useful tool to ensure compliance with Article 25 of the Regulation and to provide a basis for further implementation of the Regulation;
- The assistance given by the DPO to the Controllers in notifying processing operations may also be formalised in the document;

> **"(e)** notifying the European Data Protection Supervisor of the processing operations likely to present specific risks within the meaning of Article 27"

- The DPO shall determine whether the processing operation presents specific risks in the sense of Article 27 and is thus subject to prior checking. The DPO should consult the responsible controller if necessary. The possibility to consult the EDPS in case of doubt as to the need for prior checking may also be mentioned with reference to Article 27.3.

> "The Data Protection Officer may be consulted by the Community institution or body which appointed him or her, by the controller concerned, by the Staff Committee concerned and by any individual, without going through the official channels, on any matter concerning the interpretation or application of this Regulation. **Annex"**

- The advisory role is of importance and should be formalised in the instrument following the administrative practices of the institution/body;

> "on his or her 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 or her tasks and which come to his or her notice, and report back to the person who commissioned the investigation or to the controller, **Annex."**

- The DPO has the duty to investigate matters and occurrences directly relating to his or her tasks and therefore "investigative powers" should be elaborated in the document (see point below);

> "Other good practices to enhance compliance with the Regulation that can usefully be mentioned in the document:"

- The DPO may keep an anonymous inventory of the written requests from data subjects for the exercise of the rights referred to in Articles 13, 14, 15, 16 and

18 of the Regulation. This documentation could then be used to conduct an analysis to measure compliance with the Regulation and to allow the DPO to identify weaknesses of the systems;

- An **annual work programme** and an **annual report** may be submitted by the DPO on his/her activities. A work programme of the DPO should define its priorities and show which results the DPO wants to achieve in terms of raising awareness, inventory, notifications, prior checking and register, etc;

> "In performing his or her duties, the Data Protection Officer 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 not explicitly mentioned in the Regulation, the EDPS encourages the handling of queries or complaints by the DPO, where appropriate. Indeed, the handling of queries and complaints at a local level can help in most cases to solve problems.

- It is good practice to elaborate on the investigation powers of the DPO. The procedural aspects should be defined: delay for the DPO to respond to the person who commissioned the investigations (written reply), obligation and deadline for the controller in charge of the processing operation at stake to respond to the DPO (written reply), obligation of confidentiality, obligation to conduct the enquiry in full independence, etc;

> "The Data Protection Officer may make recommendations for the practical improvement of data protection to the Community institution or body which appointed him or her and advise it and the controller concerned on matters concerning the application of data protection provisions, **Annex**"

- The DPO should be involved whenever his/her institution/body elaborates internal rules related to the protection of personal data; the DPO should be an actor of the institutional framework (see below).

4) Sources of information of the DPO

Implementing rules are also a tool to formalise the cooperation with the DPO within the institution/body, notably with:

- Internal Auditor, IT services, Local Information Security Officer (LISO) may request DPO's observations and conversely;
- The DPO should be informed whenever the institution/body consults the EDPS under Article 28.1, 28.2 or 46.d. (and more widely, be informed of any correspondence with the EDPS), he/she should be informed of direct interactions between the controllers of the institution/body and the EDPS;

- The DPO should be informed / consulted before any opinion, document or internal decision on matters related to data protection provisions is adopted by his/her institution or body.
- The DPO should be informed when the controller receives a request for access, rectification, deletion, etc., as well as of any complaint related to data protection matters.

5) Role and duties of the Controllers

> "Every controller concerned shall be required to assist the Data Protection Officer in performing his or her duties and to give information in reply to questions **(Annex)"**

- Controllers should give prior notice to the DPO of any processing operation. Information to be given is detailed in Article 25.2. Processing operations should be notified sufficiently well in advance to allow for prior checking by the EDPS (at least two months) because the operation cannot be implemented before the EDPS's opinion is issued;
- Any change in the processing implying personal data should be notified promptly to the DPO;
- Controllers should cooperate with the DPO to establish the inventory of processing operations referred to in Article 4(2) hereof;
- Where appropriate, controllers should consult the DPO on the conformity of processing operations, in particular in the event of doubt as to conformity;
- Controllers should prepare notifications to the DPO for all existing processing operations which have not yet been notified;
- In case the controller outsources part(s) of the processing operations to a processor, this should be done in compliance with Article 23. Ideally, relevant parts of the article should be quoted.

6) Rights of the data subject

- Data subjects should be properly informed of the processing of their personal data in compliance with Articles 11 and 12 of the Regulation;
- The document may also explain how the data subjects may exercise their rights pursuant to Article 13 to 19 of the Regulation (whom to address, request in writing, deadlines, etc.).

Concluding remarks

Regulation (EC) No 45/2001 provides for a prescriptive and detailed frame for the implementing rules concerning the tasks, duties and powers of the DPO. However, the

EDPS recommends that other parts of the Regulation are also further developed in the instrument adopted by every institution/body, taking into account its own characteristics.

The scope of the instrument should be extended to the role and the duties of the controller and to the rights of the data subject as developed above. The instrument should also be the occasion to better integrate the role of the DPO into the institutional framework of each institution/body.