EDPS Inspection Guidelines (Adopted in November 2013, updated on 25 October 2017)

EDPS Inspection Guidelines

Definition

As the independent supervisory authority established by Article 41 of Regulation (EC) No. 45/2001[1] ("Regulation 45/2001"), the EDPS has the power to conduct on-the-spot inspections. The EDPS will carry out inspections as an investigative tool in order to verify reality and collect facts on actual situations within the EU institutions/bodies ("institutions"). Inspections can be conducted ex officio or may be triggered by a complaint, and in all cases are followed by appropriate feedback to the inspected institution.

Who can be submitted to an inspection?

Institutions processing personal data in their activities which fall fully or partly under the scope of EU law could be inspected by the EDPS as set forth in Articles 3(1) and 47(2) of Regulation 45/2001 and of Article 43(4) of Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) ("Regulation 2016/794") as regards the processing of operational data by Europol.[2]. These rules are further developed in Articles 15(3) and 36 of the EDPS Rules of Procedure.

Criteria to launch an inspection

The EDPS will perform inspections selectively in accordance with an Annual Inspection Plan (AIP) based on a risk analysis procedure, which will also reflect the means and resources available for inspections. Institutions identified for an inspection are selected on the basis of justifiable criteria, which may vary. For example, considerations include (but are not limited to) factors such as the categories of data processed as part of core business, number of complaints, data transfers, compliance with previous decisions, and general cooperation with the EDPS. In addition, specific legal provisions obligate the EDPS to conduct security audits of large scale IT systems and applications, which will also be reflected in the inspection planning accordingly.

---

[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.

[2] According to Article 46 of Regulation 2016/794, the processing of administrative data by Europol is subject to Regulation 45/2001.

Legal basis for EDPS inspections

Articles 41(2), 46(c) and 47(2) of Regulation 45/2001 and Article 43 of Regulation 2016/794 provide a legal basis for the EDPS to effectively perform his/her function as supervisory authority:

- Article 41(2) of Regulation 45/2001 stipulates that "*The European Data Protection Supervisor shall be responsible for monitoring and ensuring the application of the provisions of this Regulation and any other Community act relating to the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data by a Community institution or body, and for advising Community institutions and bodies and data subjects on all matters concerning the processing of personal data. To these ends he or she shall fulfil the duties provided for in Article 46 and exercise the powers granted in Article 47*";
- Article 46(c) of Regulation 45/2001 provides that: "*The European Data Protection Supervisor shall: (a) [...](c) monitor and ensure the application of the provisions of this Regulation and any other Community act relating to the protection of natural persons with regard to the processing of personal data by a Community institution or body with the exception of the Court of Justice of the European Communities acting in its judicial capacity*";
- Article 43 of Regulation 2016/794 states that:

  "*1. The EDPS shall be responsible for monitoring and ensuring the application of the provisions of this Regulation relating to the protection of fundamental rights and freedoms of natural persons with regard to the processing of personal data by Europol, and for advising Europol and data subjects on all matters concerning the processing of personal data. To that end, he or she shall fulfil the duties set out in paragraph 2 and exercise the powers laid down in paragraph 3, while closely cooperating with the national supervisory authorities in accordance with Article 44.*

  2. The EDPS shall have the following duties:

  (c) monitoring and ensuring the application of this Regulation and any other Union act relating to the protection of natural persons with regard to the processing of personal data by Europol".

Further information is contained in Article 36 of the EDPS Rules of Procedure. Finally, Article 46(a) and (b) of Regulation 45/2001, as well as Article 43(2)(a) and (b) of Regulation 2016/794, empower the EDPS to hear and investigate complaints, conduct enquiries and inform the data subject of the outcome within a reasonable period.

Powers of the EDPS

According to Article 30 of Regulation 45/2001, controllers are obliged to assist the EDPS in the performance of his or her duties upon request, particularly by providing the information referred to in Article 47(2)(a) of Regulation 45/2001 or Article 43(4)(a) of Regulation 2016/794 and by granting access as provided for in Article 47(2)(b) or Article 43(4)(b) of Regulation 2016/794. In executing his or her investigative powers, the EDPS has the power to:

(a) obtain from an institution access to all personal data and any other information necessary for his or her enquiries;

(b) obtain access to any institution's premises when there are reasonable grounds for presuming that an activity covered by the Regulation is being carried out there (Article 47(2) of Regulation).

The EDPS staff members who carry out the on-the-spot inspections are officers vested with public authority while performing their tasks. Due to the very nature of EDPS tasks, all members of staff are subject to strict confidentiality obligations, which are further enforced through internal rules and procedures.

Any institution selected for inspection should therefore permit the authorised EDPS staff members to carry out their duties. For example, it should allow them to enter its premises during normal office hours and should produce any documents, electronic files, records, or other information related to its data processing operations, irrespective of the medium on which they are stored, as requested by the EDPS inspection team. It should permit EDPS staff members to examine any such information in situ and make copies. Staff of the inspected institution (or representatives) should immediately give on-the-spot oral explanations relating to the subject matter and purpose of the inspection as the EDPS staff members may require, and should allow that any such explanations be recorded, if necessary.

Main steps in an inspection procedure

- *Announcing an inspection*: An inspection is usually announced in advance (at least four weeks before the planned inspection date) to the concerned institution. The announcement letter contains the decision, defines the subject matter, starting date, time and place of the inspection, along with the purpose and powers of the EDPS. It also mentions potential recourse to the Court of Justice against the decision itself and contains the inspectors' mandates attesting their identity and capacity;

- *Preparatory phase:* In the preparatory phase of an inspection, the institution or the DPO may be asked to provide certain information and documents to the EDPS;
- *On-the-spot activities*: Inspectors rely on the cooperation of the staff members and managers of the inspected institution to provide them with the requested information, and to be granted any access to premises they might need. EDPS inspectors will only search premises and media actively themselves in exceptional circumstances; for example if there is a lack of adequate cooperation or in case competent staff are unavailable.
- *Documenting the procedure and facts*: The meetings, interviews, methodology and evidence collected are recorded in the EDPS inspection minutes in order to document the verification procedures applied, and to provide a record of any discussions that took place during the on-the-spot inspection.

  Draft minutes will be prepared at the EDPS premises following the closure of the on-the-spot activities and submitted - via e-mail or via other means if required by the rules on the protection of EU classified information and other applicable rules on sensitive non-classified information - to the DPO of the inspected institution for comments. A

list of documents obtained during the inspection is to be provided as an annex to the minutes.

Comments provided within the specified deadline are to be analysed and discussed amongst the inspection team to decide whether and to what extent they can be integrated into the minutes. In the absence of feedback within the set deadline, the content of the minutes will otherwise be considered as final.

The final text of the minutes is printed out in two copies and sent to the inspected institution top hierarchy via registered mail with another copy sent by email (with the DPO in copy) or via other means if required by the rules on the protection of EU classified information and other applicable rules on sensitive non-classified information. One of the two documents is to be signed by the top level hierarchy (or representative) of the inspected institution to acknowledge receipt, and returned to the EDPS within 15 days. If the representative of the inspected institution refuses to sign the minutes, this will be recorded in the document.

- *Inspection report:* The EDPS provides appropriate feedback to the inspected institution within a reasonable timeframe following the on-the-spot inspection.

- *Follow-up of an inspection:* The EDPS always monitors the implementation of any recommendations or decisions contained in the inspection report and may give the institution a deadline for feedback. In case of non-compliance, the EDPS can use the powers vested in him or her under Article 47 of Regulation 45/2001 and Article 43(3) of Regulation 2016/794.

Role of Data Protection Officers of the European institutions

In the preparatory phase of an inspection, Data Protection Officers are useful contact points for practical arrangements and to provide requested information to the EDPS. The extent of the DPO's participation during the on-the-spot activities will vary depending on the case in hand, and will be determined and communicated in advance. According to Article 24(b) of Regulation 45/2001 and Article 41(6)(e) of Regulation 2016/794, the DPO is expected to cooperate with the EDPS within the sphere of his or her competence, and to respond to any requests for information.

Appeal against EDPS decision

Actions against any EDPS decision relating to an inspection may be brought before the Court of Justice of the European Union in Luxembourg in accordance with Article 32(3) of Regulation 45/2001 and/or Article 48 of Regulation 2016/794.

Security measures

The EDPS implements appropriate technical and organisational measures to secure any documents against security risks in compliance with Article 22 of Regulation 45/2001.

Privacy policy

The information to be given to data subjects is attached to the announcement letter. The inspected institution is requested to circulate it to all concerned staff members.

Publicity

In principle, **general** information about EDPS inspections will be provided to the public. The two main *fora* for this publicity are the Annual Report and the EDPS website. Whenever the EDPS intends to publish or publicise details or summaries of his inspection actions, he will always inform the relevant institution beforehand to enable them to consider and prepare a public response if they feel this is appropriate