Inspections conducted by the EDPS

Policy paper

Adopted in November 2013
1st revision October 2017
2nd revision November 2018

Contents

1. Introduction

Inspections are one of the tools used by the EDPS to ensure compliance with the Regulation (EU) 2018/1725 of the European Parliament and of the Councilof 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295/39 of 21.11.2018 (henceforth referred to as "Regulation (EU) 2018/1725") as well as 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[1]. The EDPS shall decide to carry out an inspection whenever on the spot verification is considered necessary for the performance of supervisory tasks or to comply with a legal obligation[2]. Inspections may also be conducted to monitor general compliance with official EDPS guidance on specific data protection issues.[3] They serve to underline the responsibilities of controllers[4] and are followed by appropriate feedback.[5] In some cases, they may result in the use of the powers of the EDPS in accordance with Article 58(1) of Regulation 45/2001 (for Europol: Article 43(3) of Regulation 2016/794), and Article 18 of the EDPS Rules of Procedure.

Although the overall goal of an inspection is to promote compliance with Regulation (EU) 2018/1725 and Regulation 2016/794 in terms of identifying specific shortcomings and solutions relating to a pre-defined scope, inspections may also serve to highlight other risk areas and increase awareness on data protection compliance in general.

This paper sets out the main elements of EDPS policy in this area, where relevant in order to give guidance to all involved and ensure transparency to stakeholders. Further details will be developed in internal procedures, and all sets of documents will be regularly updated where necessary.[6]

2. Scope of EDPS inspections

All EU institutions and bodies processing personal data in their activities and subject to the Regulation (hereinafter referred to as "the institutions"), could be inspected by the EDPS as set forth in Article 2(1) and Article 58(1)(b), (d) and (e) of Regulation (EU) 2018/1725[7], and further developed in Articles 15(3) and 36 of the Rules of Procedure.

---

[1] See Articles 53(3) and 58(1)(a) of Regulation (EU) 2018/1725, Articles 1, 17 and 36 of the EDPS Rules of Procedure and the EDPS Policy paper, "Monitoring and Ensuring Compliance with Regulation (EC) 45/2001", Brussels, 13 December 2010. For **Europol**, Article 43(4)(a) of Regulation (EU) 2016/794 stipulates that the EDPS has the power to "obtain from Europol access to all personal data and to all information necessary for his or her enquiries". Article 43(4)(b) of the Europol Regulation stipulates the EDPS power to "obtain access to any premises in which Europol carries on its activities when there are reasonable grounds for presuming that an activity covered by this Regulation is being carried out there". According to Article 46 of Regulation 2016/794, the processing of **administrative data** by **Europol is subject to Regulation (EU) 2018/1725**.

[2] Article 36(1) of the Rules of Procedure

[3] Article 17 of the Rules of Procedure

[4] Article 15(3) of the Rules of Procedure

[5] Article 36(6) of the Rules of Procedure

[6] Article 16 of the Rules of Procedure

[7] For **Europol**: Article 43(4) of Regulation 2016/794.

For Europol, under Article 44(2) of Regulation 2016/794, "The EDPS shall use the expertise and experience of the national supervisory authorities in carrying out his or her duties as set out in Article 43(2). In carrying out joint inspections together with the EDPS, members and staff of national supervisory authorities shall, taking due account of the principles of subsidiarity and proportionality, have powers equivalent to those laid down in Article 43(4) and be bound by an obligation equivalent to that laid down in Article 43(6). The EDPS and the national supervisory authorities shall, each acting within the scope of their respective competences, exchange relevant information and assist each other in carrying out audits and inspections."

Prior to the launch of an inspection, in principle, its scope will be announced in writing to the institution concerned.[8]

3. Types of inspections

3.1. Inspection classifications

Inspections typically cover the implementation of legal requirements and obligations (such as regarding the legal basis to collect and process data, conservation and deletion procedures, information notices for data subjects, security measures etc) for a number of identified processing operations.

Example:
In early 2012, the EDPS selected a large European agency for general inspection based on a risk assessment exercise. The overall aim of the inspection was to verify facts and practices, particularly as a follow-up to specific complaints, and to check the full implementation of EDPS recommendations in a number of prior check opinions. Following a comprehensive examination of the evidence gathered during the inspection, the EDPS issued a number of further recommendations which were acted upon and implemented swiftly.

Where appropriate, more targeted inspections may also be launched to collect relevant information and gather pieces of evidence during the investigation phase of a complaint, in compliance with Article 33(2) of the Rules of Procedure.

Example:
In late 2009, the EDPS received two complaints about a European body's collection and further processing of personal data during an external investigation it had conducted. After analysing the details, the EDPS decided to carry out a targeted inspection at the body's premises. The purpose of the inspection was to clarify specific issues related to the proportionality of the collection of digital evidence. The information obtained during the visit was sought both in order to help finalise the EDPS decision on the above-mentioned complaints, and to check more general compliance with the Regulation in the specific area of digital and electronic data.

[8] Article 36(2)-(3) of the Rules of Procedure

The EDPS may choose to carry out thematically targeted on-the-spot inspections based on any areas or themes on which the EDPS has provided guidance, or that are considered relevant in the current data protection climate.

Next to, or instead of on-the-spot activites, various EU institutions or bodies may be approached and asked for their cooperation under each theme, to check whether the guidance has been correctly implemented and compliance has been achieved. The EDPS may subsequently complete a comprehensive report to outline the general findings of the data protection issue under examination.

Example:
In June and July 2012, thematic targeted inspections took place at thirteen Brussels-based EU institutions and bodies. This exercise formed part of the EDPS' annual inspection plan for 2012 and was designed to check, on the spot, the practical implementation of the recommendations contained in the EDPS Video-surveillance Guidelines published in March 2010. Following the inspection, the EDPS adopted a comprehensive report detailing relevant outcomes and findings.

3.2. It is important to distinguish inspections from on the spot compliance visits:

In accordance with Article 37 of the Rules of Procedure, compliance visits are conducted by EDPS management where there is an apparent lack of commitment to comply with the Regulation, a lack of communication, or a need to raise awareness. These visits are followed by a correspondence based exercise centred around a roadmap agreed between the EDPS and senior management of the EU institution or body visited. This roadmap is intended to commit the management of the institution to respect specific obligations under Regulation (EU) 2018/1725 within a set deadline.

Compliance visits differ from fact finding exercises as the former are carried out to broadly discuss what the EDPS expects in terms of adherence to Regulation (EU) 2018/1725 and Regulation 2016/794 in general terms. If the visit does not achieve positive results in terms of data protection compliance, the EDPS may decide to carry out an inspection or make use of powers granted under Article 58(1) of Regulation (EU) 2018/1725[9].

4. EDPS inspection powers

Articles 52(3) and 57(1)(a) and 58 of Regulation (EU) 2018/1725 provide broad powers for the EDPS to effectively perform the functions of a supervisory authority[10].

- Article 52(3) of Regulation (EU) 2018/1725 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 Union act relating to the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data by a Union institution or body, and for advising Union institutions and bodies and data subjects on all matters concerning the processing of personal data. To those ends the European Data Protection Supervisor shall fulfil the tasks provided for in Article 58 and exercise the powers granted in Article 59.";

[9] For **Europol** (operational data): see Article 43(3) of Regulation 2016/794.
[10] For **Europol**, see Article 43(4)(a) and (b) of Regulation 2016/794.

- Article 57(1)(a) of Regulation (EU) 2018/1725 provides that: "*Without prejudice to other tasks set out under this Regulation, the European Data Protection Supervisor shall: (a) monitor and enforce the application of this Regulation by a Union institution or body, with the exception of the processing of personal data by the Court of Justice of the European Union acting in its judicial capacity*";
- Article 58(1) provides: "The European Data Protection Supervisor shall have the following investigative powers: ...

(d) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;
(e) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law;
...".

Article 58(1) and (2) of the Regulation (EU) 2018/1725 outlines the EDPS' investigative and corrective powers[11], which include (amongst other things) ordering compliance with data subjects' requests to exercise their rights, warning the controller, impose an administrative fine and imposing a temporary or definitive ban on processing.

It is important to note that the EDPS can have recourse to formal corrective powers, should serious concerns be raised about any data processing operation during or following an inspection. In any case, inspections do not preclude the use of formal corrective powers by the EDPS, especially in cases where the recommendations of an inspection are not respected.

5. Obligation to cooperate

In order to ensure that the EDPS can carry out supervisory functions in an effective and productive manner, Regulation (EU) 2018/1725 places on obligation on controllers to provide their cooperation and assistance during any such tasks.

Article 32 of Regulation (EU) 2018/1725 provides that: "Union institutions and bodies shall cooperate, on request, with the European Data Protection Supervisor in the performance of its tasks.."

6. Confidentiality and security

The EDPS implements appropriate technical and organisational measures to secure any documents obtained or used in the course of an inspection, in compliance with Article 33(1) of Regulation (EU) 2018/1725 and Article 36(4) of the EDPS Rules of Procedure. Article 36(5) of the Rules of Procedure further stipulates that interviews and information obtained during an inspection and the procedure followed, shall be recorded in minutes sent to the institution for comments. A list of evidence collected during the inspection shall be annexed to the minutes.

The EDPS staff members who carry out on the spot inspections are officers vested with public authority while performing their duties, and will hold a mandate to perform the inspections. Due to the very nature of EDPS tasks, all members of staff are subject to strict confidentiality

[11] For **Europol**, see Article 43(3) of Regulation 2016/794.

obligations, which are further enforced through internal rules and procedures, in line with Article 56 of Regulation (EU) 2018/1725[12].

7. Criteria and planning

The EDPS will perform inspections on the basis of a yearly plan providing for certain kinds of inspections. The decision to choose specific EU institutions/bodies for on-site inspections will be based on a risk analysis using a selective approach that also reflects the means and resources available for inspections. In principle, the EDPS will notify the relevant institution or body of the inspection plans in writing four weeks ahead of the planned inspection date in accordance with Article 36 of the Rules of Procedure. Furthermore, additional details on the inspection process will be provided to the institution before the inspection is carried out.

Triggers for inspections can be identified during the various internal activities of supervision and consultation within the EDPS, but they can also come from external sources such as the media. It is important to note that inspections can be triggered by a **combination of factors,** which when considered together, may indicate serious issues or failings within the institution or body concerned - but do not necessarily have to be indicative of those (a fraction of targeted institutions is determined by the drawing of lots). When deciding which institutions to inspect, the EDPS will therefore need to consider all the information at his disposal.

The EDPS, as the supervisory authority of the European Commission's IT systems and applications that process personal data, can also carry out inspections of its large scale IT networks (such as the Eurodac database and Visa Information System). Where specific legal provisions oblige the EDPS to perform such security audits, these will be reflected in the EDPS inspection planning, and resources will be allocated accordingly.

8. Inspection report and publicity

With the exception of complaints cases, the EDPS shall set forth in an inspection report the findings made during an inspection. The report shall include any actions to be undertaken by the institution inspected, and shall be subject to follow up by the EDPS.

Each year, the EDPS publishes an annual report, which also contains information relating to any inspections and follow-up exercises carried out during the previous twelve months.

The EDPS website will contain general information about inspections, such as the Inspection Policy, Inspection Guidelines (which supplement and expand on the Policy) and a corresponding Privacy Policy.

9. Appeal against EDPS decisions

Action against an EDPS enforcement decision taken as a result of an inspection may be brought before the Court of Justice of the European Union in Luxembourg in accordance with Article 64(2) of Regulation (EU) 2018/1725[13] and Article 40 of the Rules of Procedure.

[12] For **Europol**, see Articles 43(6), 44(2) and 67 of Regulation 2016/794.

[13] For **Europol**, see Article 48 of Regulation 2016/794.