Inspections conducted by the EDPS

Policy paper

Adopted in November 2013

Contents

1. Introduction

2. Scope of EDPS inspections

3. Types of inspections

3.1. Inspection classifications
3.1.1. General Inspection
3.1.2. Targeted Inspection
3.1.3. Thematic Targeted Inspection

3.2. Compliance visits

4. EDPS inspection powers

5. Obligation to cooperate

6. Confidentiality and security

7. Criteria and planning

8. Inspection report and publicity

9. Appeal against EDPS decisions

Inspections conducted by the EDPS - Policy paper

1. Introduction

Inspections are one of the tools used by the EDPS to ensure compliance with Regulation (EC) 45/2001 (henceforth referred to as "the Regulation")[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 enforcement powers of the EDPS in accordance with Article 47(1) of the Regulation and Article 18 of the EDPS Rules of Procedure.

Although the overall goal of an inspection is to promote compliance with the Regulation 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. It updates and replaces the EDPS Inspection Policy of July 2009, presenting new and revised issues for consideration. 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 3(1) and Article 47(2) of the Regulation, and further developed in Articles 15(3) and 36 of the Rules of Procedure.

Prior to the launch of an inspection, in principle, its scope will be announced in writing to the institution concerned.[7]

[1] See Articles 41(2) and 46(c) of the Regulation, 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.
[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] Article 36(2)-(3) of the Rules of Procedure

3. Types of inspections

3.1. Inspection classifications

EDPS inspections are classified as:

a. General inspection: to obtain a broad view of compliance with the Regulation, based on a number of identified data processing operations within an EU institution.
b. Targeted inspection: to focus on the specific requirements of only a small number of selected data processing operations within an EU institution.
c. Thematic targeted inspection: to focus on a specific theme across several EU institutions.

3.1.1. General Inspection

A general inspection is carried out when the EDPS has concerns relating to compliance with the Regulation. In certain instances, such inspections are deemed necessary in order to investigate and ensure compliance with previous EDPS decisions (such as the outcome of prior check opinions or complaints), and to make sure that EDPS recommendations have been fully implemented.

In some cases, institutions that have previously undergone targeted or thematic inspections may later be subject to a general inspection if wider data protection concerns come to light. However, other reasons for this type of inspection could include a lack of cooperation with the EDPS or the length of time taken to make the recommended changes, for example.

General 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.

3.1.2. Targeted Inspection

A targeted inspection is carried out on the same basis as a general inspection but on a smaller scale. In the course of a targeted inspection, the EDPS will focus on checking compliance with the specific legal requirements of only a few predefined data protection processing operations.

As such, targeted inspections will follow a lighter and simplified procedure. For example, less preparatory paperwork and administration will be required prior to the inspection, and the visit itself is likely to be shorter than that of a general inspection.

Where appropriate, 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.

3.1.3. Thematic Targeted Inspection

The EDPS may choose to carry out thematic targeted 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. 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 will 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 <u>compliance visits</u>:

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 the Regulation 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 the Regulation 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 enforcement powers granted under Article 47(1) of the Regulation.

4. EDPS inspection powers

Articles 41(2), 46(c) and 47(2) of the Regulation provide broad powers for the EDPS to effectively perform the functions of a supervisory authority.

- Article 41(2) stipulates: "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) provides: "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 47(2) provides: "The European Data Protection Supervisor shall have the power:
  (a) to obtain from a controller or Community institution or body access to all personal data and to all information necessary for his or her enquiries;
  (b) to obtain access to any premises in which a controller or Community institution or body carries on its activities when there are reasonable grounds for presuming that an activity covered by this Regulation is being carried out there".

Article 47(1) outlines the EDPS' enforcement powers, which include (amongst other things) ordering compliance with data subjects' requests to exercise their rights, warning or admonishing the controller, and imposing a temporary or definitive ban on processing.

It is important to note that the EDPS can have recourse to formal enforcement 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 enforcement 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, the Regulation places on obligation on controllers to provide their cooperation and assistance during any such tasks.

Article 30 of the Regulation provides that: "At his or her request, controllers shall assist the European Data Protection Supervisor in the performance of his or her duties, in particular by providing the information referred to in Article 47(2)(a) and by granting access as provided in Article 47(2)(b)."

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 22 of the Regulation 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 obligations, which are further enforced through internal rules and procedures, in line with Article 45 of the Regulation.

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. 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 obligate 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.

In principle, a summary of the inspection reports will also be published on the EDPS website, and press releases will be issued where appropriate. 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 32(3) of the Regulation and Article 40 of the Rules of Procedure.