EUROPEAN DATA PROTECTION SUPERVISOR

Audits conducted by the EDPS

Policy paper

Adopted in November 2013
1st revision October 2017
2nd revision November 2018
3rd revision December 2021

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30 - B-1000 Brussels
E-mail: edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 32 2-283 19 00 - Fax : 32 2-283 19 50

Contents

Audits conducted by the EDPS - Policy paper

1. Introduction

Audits are one of the tools used by the EDPS to ensure compliance with Regulation (EU) 2018/1725[1] ("the Regulation"). The EDPS shall decide to carry out an audit whenever on-the-spot verification is considered necessary for the performance of supervisory tasks or to comply with a legal obligation. Audits may also be conducted to monitor general compliance with official EDPS guidance on specific data protection issues. They serve to underline the responsibilities of controllers and are followed by appropriate feedback. In some cases, they may result in the use of the enforcement powers of the EDPS in accordance with Article 58 of the Regulation.

Although the overall goal of an audit is to promote compliance with the Regulation in terms of identifying specific shortcomings and solutions relating to a pre-defined scope, audits 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.

2. Scope of EDPS audits

All EU institutions and bodies ("EUIs") processing personal data in their activities and subject to the Regulation, could be inspected by the EDPS as set forth in Articles 2(1) and 58(1)(b), (d) and (e) of the Regulation (as well as Articles 43 and 44 of the Europol Regulation[2]).

Prior to the launch of an audit, in principle, its scope will be announced in writing to the institution concerned (exceptions apply to remote audits that do not require fieldwork).

3. Types of audits

3.1. Audit classifications

EDPS audits are classified as:

a. General audit: to obtain a broad view of compliance with the Regulation, based on a number of identified data processing operations within an EUI.
b. Targeted audit: to focus on the specific requirements of only a small number of selected data processing operations within an EUI.

---

1 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 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

2 Regulation (EU) 2016/794 of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA

c. Thematic targeted audit: to focus on a specific theme across several EUIs.

3.1.1. General Audit

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

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

General audits 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 EU Agency for general audit based on a risk assessment exercise. The overall aim of the audit 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 audit, the EDPS issued a number of further recommendations which were acted upon and implemented swiftly.

3.1.2. Targeted Audit

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

As such, targeted audits will follow a lighter and simplified procedure. For example, less preparatory paperwork and administration will be required prior to the audit, and the fieldwork itself is likely to take less time than that of a general audit.

Where appropriate, targeted audits may also be launched to collect relevant information and gather pieces of evidence during the investigation phase of a complaint.

Example:
In late 2009, the EDPS received two complaints about a EUI´s collection and further processing of personal data during an external investigation it had conducted. After analyzing the details, the EDPS decided to carry out a targeted audit at the EUI's premises. The purpose of the audit 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 finalize 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 Audit

The EDPS may choose to carry out thematic targeted audits 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 EUIs 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 audits took place at thirteen Brussels-based EUIs. This exercise formed part of the EDPS' annual audit 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 audit, the EDPS adopted a comprehensive report detailing relevant outcomes and findings.

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

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 centered around a roadmap agreed between the EDPS and senior management of the EUI visited. This roadmap is intended to commit the management of the EUI to respect specific obligations under the Regulation within a set deadline.

Compliance visits (see Article 13 Rules of Procedure[3]) 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 make use of its powers granted under Article 58 of the Regulation.

4. EDPS audit powers

Articles 57 and 58 of the Regulation (Articles 43 and 44 of the Europol Regulation) of the Regulation provide broad powers for the EDPS to effectively perform the functions of a supervisory authority.

- Article 58(1)(b) of the Regulation states that the EDPS has the power to "carry out investigations in the form of data protection audits".
- Article 58(1)(d) lays down that the EDPS has the power to "to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks ".
- Article 58(1)(e) also gives the EDPS the power to "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 57(1)(e) and (f) of the Regulation empowers the EDPS to hear and investigate complaints, conduct enquiries and inform the data subject of the outcome within a reasonable period.

3 https://edps.europa.eu/sites/edp/files/publication/20-06-26_edps_rules_of_procedure_en.pdf.

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 audit. In any case, audits do not preclude the use of formal enforcement powers by the EDPS, especially in cases where the recommendations of an audit 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 32 of the Regulation provides that: "Union institutions and bodies shall cooperate, on request, with the European Data Protection Supervisor in the performance of his or her 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 audit, in compliance with Article 33 of the Regulation. Interviews and information obtained during an audit and the procedure followed will be recorded in minutes sent to the institution for comments. A list of evidence collected during the audit will be annexed to the minutes.

The EDPS staff members who carry out on-the-spot audits are officers vested with public authority while performing their duties, and will hold a mandate to perform the audits. 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 56 of the Regulation.

7. Criteria and planning

The EDPS will perform audits on the basis of a yearly plan providing for certain kinds of audits. The decision to choose specific EUIs for on-site audits will be based on a risk analysis using a selective approach that also reflects the means and resources available for audits. In principle, the EDPS will notify the relevant EUI of the audit plans in writing four weeks ahead of the planned audit date(exceptions apply to remote audits not requiring fieldwork). Furthermore, additional details on the audit process will be provided to the EUI before the audit is carried out.

Triggers for audits 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 audits can be triggered by a *combination of factors*, which when considered together, may indicate serious issues or failings within the EUI concerned. When deciding which EUIs to inspect, the EDPS will therefore need to consider all the information at its disposal.

The EDPS, as the supervisory authority of the EUIs IT systems and applications that process personal data, can also carry out audits 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 audit planning, and resources will be allocated accordingly.

8. Audit report and publicity

With the exception of complaints cases, the EDPS shall set forth in an audit report the findings made during an audit. 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 audit 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 audits and follow-up exercises carried out during the previous twelve months.

The EDPS website will contain general information about audits, such as the Audit Policy, Audit Guidelines (which supplement and expand on the Policy) and a corresponding data protection notice.

9. Appeal against EDPS decisions

Action against an EDPS enforcement decision taken as a result of an audit may be brought before the Court of Justice of the European Union in Luxembourg in accordance with Article 64(2) of the Regulation.