EDPS Audit Guidelines (Adopted in December 2021)

Definition

As the independent supervisory authority established by Article 56 of Regulation 2018/1725[1] ("the Regulation"), the EDPS has the power to conduct data protection audits. The EDPS will carry out audits as an investigative tool in order to verify reality and collect facts on actual situations within the EU institutions/bodies ("EUIs"). Audits can be conducted ex officio or may be triggered by a complaint, and in all cases are followed by appropriate feedback to the audited EUI.

Who can be submitted to an audit?

EUIs 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 2(1) and 58(1)(b), (d) and (e) of the Regulation (as well as Articles 43 and 44 of the Europol Regulation[2]).

Criteria to launch an audit

The EDPS will perform audits selectively in accordance with an Annual Audit Plan (AAP) based on a risk analysis procedure, which will also reflect the means and resources available for audits. EUIs identified for an audit 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 audit planning accordingly.

Legal basis for EDPS audits

Articles 57 and 58 of the Regulation (Articles 43 and 44 of the Europol Regulation) provide a legal basis for the EDPS to perform his/her function as 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;".

[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

Finally, 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.

Powers of the EDPS

According to Article 32 of the Regulation, controllers are obliged to cooperate with the EDPS in the performance of his or her tasks upon request, particularly by providing the information referred to in Article 58(1)(d) and by granting access as provided for in Article 58(1)(e). In executing his or her investigative powers, the EDPS has the power to:

(a) obtain from an EUI access to all personal data and all information necessary for the performance of his or her tasks (Article 58(1)(e) of the Regulation);

(b) obtain access to any EUI's premises (Article 58(1)(e) of the Regulation).

The EDPS staff members who carry out the audits 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 EUI selected for audit should therefore permit the authorized 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 audit team. It should permit EDPS staff members to examine any such information in situ and make copies. Staff of the audited EUI (or representatives) should immediately give on-the-spot oral explanations relating to the subject matter and purpose of the audit as the EDPS staff members may require, and should allow that any such explanations be recorded, if necessary.

Main steps in an audit procedure

- *Announcing an audit*: An audit is usually announced in advance (at least four weeks before the planned audit date) to the concerned institution (exceptions apply to remote audits that do not require fieldwork);
- *Preparatory phase:* In the preparatory phase of an audit, the institution or the DPO may be asked to provide certain information and documents to the EDPS;
- *Presentation of the decision and mandates*: The announcement letter contains the decision to conduct an audit, mandates EDPS staff members respectively, defines the subject matter, starting date, time and place of the audit, along with the purpose and powers of the EDPS. It also mentions potential recourse to the CJEU against the decision itself.
- *On-the-spot activities*: Auditors rely on the cooperation of the staff members and managers of the audited EUI to provide them with the requested information, and to be granted any access to premises they might need. EDPS auditors 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 audit 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 audit.

  Draft minutes will be prepared at the EDPS premises following the closure of the on-the-spot activities and submitted - via e-mail - to the DPO of the audited EUI for comments. A list of documents obtained during the audit is provided as an annex to the minutes.

Comments provided within the specified deadline are analysed and discussed amongst the audit 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 top hierarchy of the audited EUI via registered mail with another copy sent by email (with the DPO in copy). One of the two documents is to be signed by the top level hierarchy (or representative) of the audited EUI to acknowledge receipt, and returned to the EDPS within 15 days. If the representative of the audited EUI refuses to sign the minutes, this will be recorded in the document.

- *Audit report:* The EDPS provides appropriate feedback to the audited EUI within a reasonable timeframe following the on-the-spot audit.
- *Follow-up of an audit:* The EDPS always monitors the implementation of any recommendations or decisions contained in the audit report and may give the EUI a deadline for feedback. In case of non-compliance, the EDPS can use the powers vested in him or her under Article 58 of the Regulation.

Role of Data Protection Officers of the EUIs

In the preparatory phase of an audit, Data Protection Officers (DPOs) 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 45(1)(g) of Regulation, 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 audit may be brought before the Court of Justice of the European Union in Luxembourg in accordance with Article 64(2) of the Regulation.

Security measures

The EDPS implements appropriate technical and organizational measures to secure any documents against security risks in compliance with Article 33 of the Regulation.

Data protection notice

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

Publicity

In principle, general information about EDPS audits 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 audit 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.