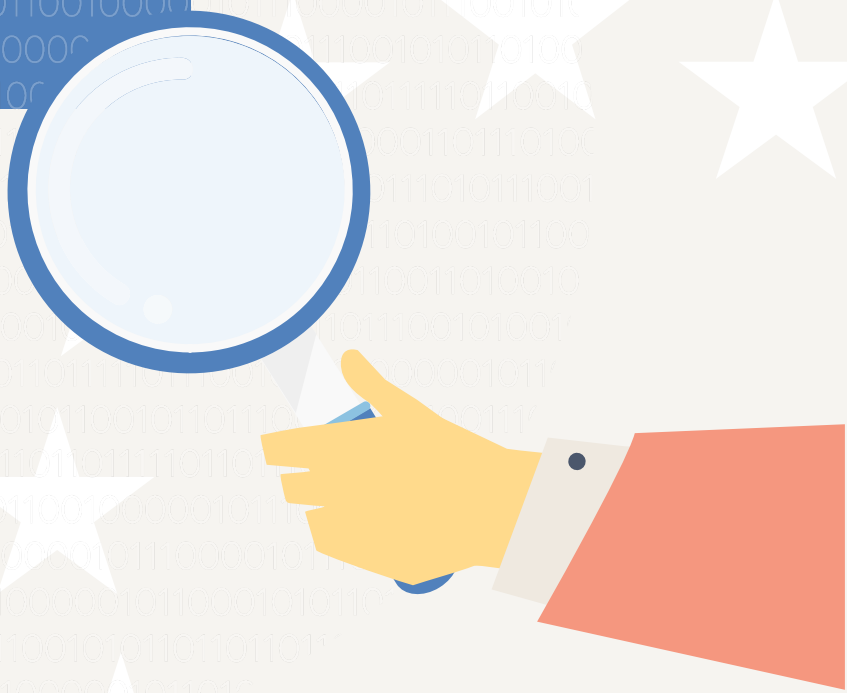
EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

WHAT TO EXPECT WHEN WE INSPECT

Data protection audits explained



WHO ARE WE?

The European Data Protection Supervisor (EDPS) is the EU's independent data protection authority responsible for monitoring and ensuring that the EU institutions and bodies (EUIs) comply with **EU data protection rules**, set out in Regulation (EU) 2018/1725, when they process personal information, i.e. personal data.

Data protection is a fundamental right, protected by European law and enshrined in Article 8 of the Charter of Fundamental Rights of the European Union. The EU administration is not only obliged to comply with Regulation (EU) 2018/1725, but to also demonstrate its compliance with these rules. The EDPS verifies this compliance and holds EUIs accountable according to the EDPS Rules of Procedure. The EDPS also encourages EUI staff, especially those responsible for the processing of persona data, to promote a data protection culture within their respective institutions.

Audits are one of the tools used by the EDPS to ensure that EUIs comply with data protection rules. During an audit, we are able to verify compliance on the spot, and make recommendations if we identify areas for improvement. The EDPS' powers in relation to audits can be found under Articles 52(3), 57(1)(b) and 58(1)(b), (d) and (e) of Regulation (EU) 2018/1725.

WHEN, WHY AND WHICH EUIs ARE AUDITED?

We carry out audits according to our Annual Inspection Plan. To establish this plan, we conduct a risk analysis and take into account the resources that are available for carrying out audits. Security audits of large scale IT systems and applications take place according to the laws governing their supervision.

Although we reserve the right to carry out audits on a random basis, we consider a variety of factors when deciding which EUI to audit, such as:

- the categories of data they process (e.g. health data are particularly sensitive);
- the number of complaints we receive about a particular EUI;
- whether the EUI regularly transfers data and to whom this data is transferred;
- compliance of the EUI with previous EDPS decisions;
- the EUI's overall history of cooperation with the EDPS.

With COVID-19 preventing the EDPS from conducting fieldwork, we adapted our audit planning and moved to remote audits by inspecting, for example, EUIs' public registers and their procedures when managing newsletter subscriptions. The format of remote audits is likely to be continued post-COVID-19 in a selection of circumstances.

WHAT ARE THE 3 STAGES OF AN EDPS AUDIT?

1.

Before an EDPS inspection occurs, the EUI is usually informed at least four weeks in advance. At this stage, the EUI concerned or its Data Protection Officer (DPO) may be asked to provide information and documents to the EDPS.

2.

During an on-the-spot audit, the EDPS meets the EUI's staff members responsible for the processing of personal data at their institution. The EDPS also requests information on and demonstrations of how the EUI processes individuals' personal data in its day-to-day work. The results of these meetings, interviews and demonstrations, as well as any evidence collected are recorded by the EDPS and are then submitted to the audited EUI for comments. Ensuring compliance means that we need to make sure that all recorded facts are correct. Consulting the EUI concerned is an opportunity for all actors involved in the audit to flag any misunderstandings about what has actually happened.

3.

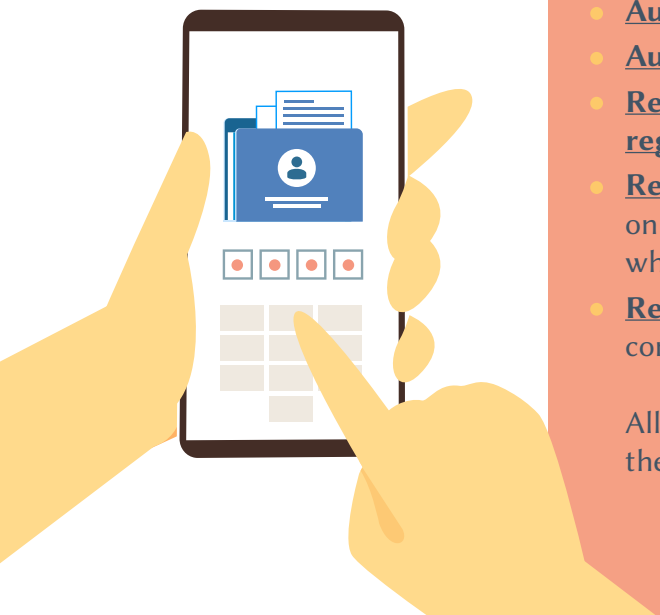
After an audit, the EDPS always provides appropriate feedback to the institution concerned in an audit report which contains a roadmap of recommendations to put in place where necessary. While the EDPS does not publish details of its audit reports, we regularly provide information on our audit activities in our Annual Reports and other publications. The EDPS always follows up on whether our recommendations included in the roadmap have been implemented.

AS A MEMBER OF STAFF, HOW MIGHT YOU BE INVOLVED IN AN EDPS AUDIT?

The EDPS tries to combine audits with information sessions on data protection, organised in cooperation with your institution's DPO. If you receive an invitation to attend a data protection training, we encourage you to join us!

If you are a staff member responsible for one of the data processing operations audited by the EDPS, we might ask you to meet us for an interview or for an on-the-spot demonstration. You will usually receive this request via your DPO, who will also provide you with a data protection statement, containing further information. All members of EDPS staff, including our auditors, are subject to strict confidentiality obligations.

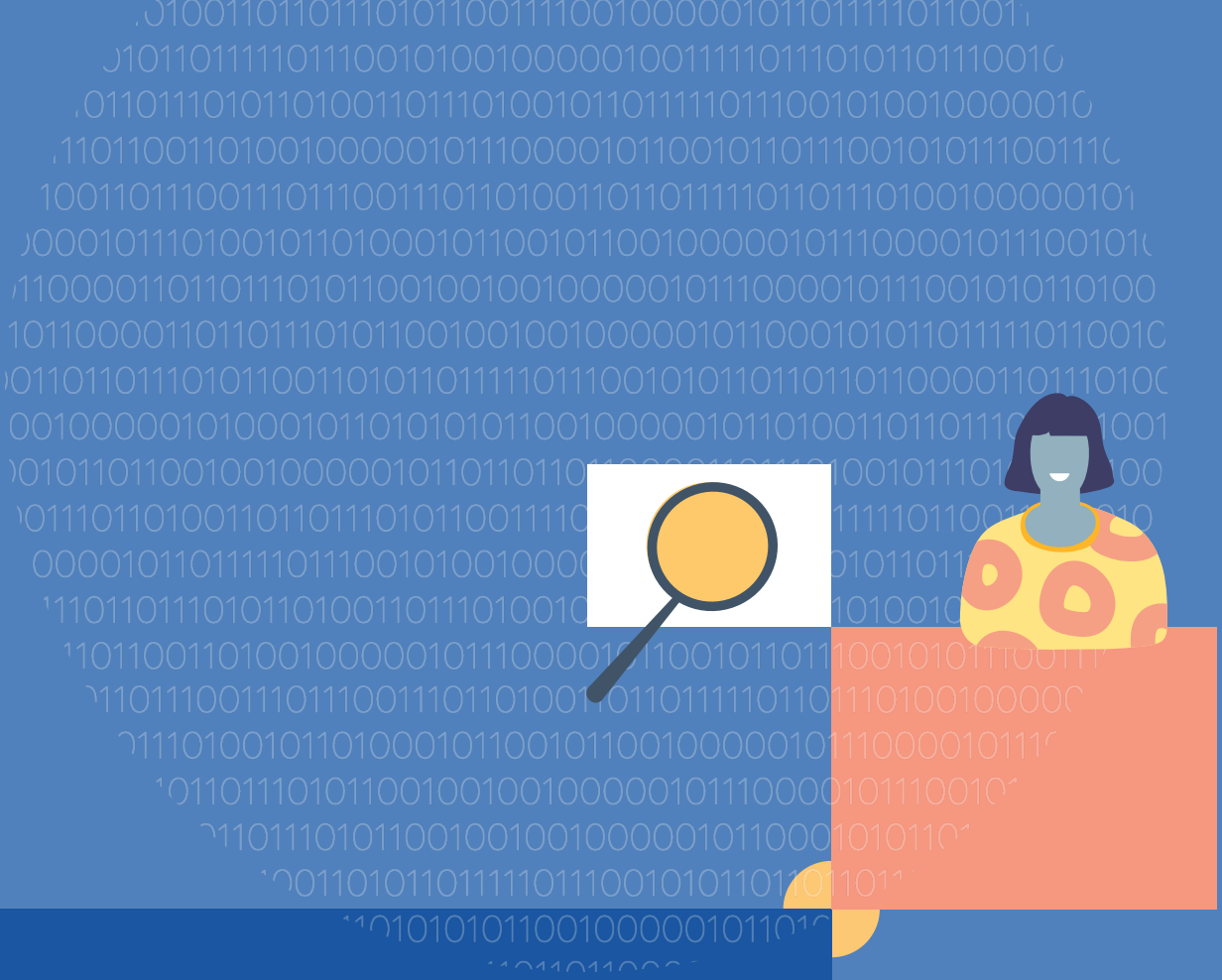
All EUIs are obliged to assist EDPS auditors upon request under Article 32 of Regulation (EU) 2018/1725. The obligation to assist us also applies to you as a staff member. We might therefore ask you to provide us with information on the data processing activities you carry out in your day-to-day work, to grant us access to personal data and to your premises, as well as allowing us to collect the necessary evidence for the audit. We know that assisting us in this way will increase your workload, so we try to minimise the disruptive impact we have on staff members as much as possible. EDPS auditors will search the premises and for evidence themselves only in exceptional circumstances, for example when there is a lack of adequate cooperation from staff or from the EUI or because the competent members of staff are unavailable.



FURTHER READING

- **Audit Policy**
- **Audit Guidelines**
- **Report on remote inspection of publicly accessible registers under Article 31(5) of the Regulation**
- **Regulation (EU) 2018/1725**: Articles 58(1)(b), (d) and (e) on Powers of the European Data Protection Supervisor when carrying out audits
- **Regulation (EU) 2018/1725**: Article 32 on Obligation of controllers to assist the EDPS

All EDPS documents listed in this section are available on the EDPS website.



edps.europa.eu

@EU_EDPS

EDPS

European Data Protection Supervisor

QT-02-21-642-EN-N ISBN: 978-92-9242-695-8 DOI: 10.2804/36732