EUROPEAN DATA PROTECTION SUPERVISOR

Monitoring and enforcing compliance with Regulation (EU) 2018/1725

8 May 2020

TABLE OF CONTENTS

1 Introduction

The EDPS' role is to ensure effective protection of people's fundamental rights and freedoms against the (mis)use of technologies, in particular in relation to the processing of personal data by the EU institutions, bodies, offices and agencies (collectively 'EUIs').

More specifically, under Article 57 of Regulation (EU) 2018/1725[1] ('the Regulation') on data protection for the EUIs, one of our main tasks is to 'monitor and enforce the application of this Regulation'.

This paper explains how we will act in that role[2], explaining both to individuals whose data EUIs process (the data subjects) and the EUIs themselves what they can expect from us as the supervisory authority for EUI's processing of personal data and what we expect EUIs to do.

EUIs are responsible for complying with the Regulation and for showing how they did it (accountability). It is their responsibility to apply the Regulation properly. The first line of defence is the responsibility of staff in the EUIs when they handle personal data for their activities. The second line are the EUI's own internal control mechanisms. As the supervisory authority for how EUIs process personal data, we are further line of defence for protecting data subjects here.

The Regulation performed a shift compared to the old Regulation (EC) 45/2001[3] – fewer ex-ante authorisations and less red tape, more accountability and ex-post verification, with a focus on the risks for people caused by the processing of their data. We mirror this shift in our supervisory work, adapting our tools with a bigger focus on proactive activities, such as surveys, investigations and audits. We also put individuals in the centre. We ask what risks planned processing operations pose for them, how personal data breaches have affected them, how to prevent repetition of harm, etc.

As public institutions bound by the Charter, compliance is also in the EUIs' own interest as it contributes to trust in their work. In this spirit, we monitor their compliance and provide support, for example in the form of guidelines and training sessions, to improve it. However, when EUIs step over the line, we do not hesitate to use our enforcement powers.

2 Accountability – what do we expect EUIs to do?

The Regulation stresses the controllers' accountability – as organisations processing personal data, the responsibility for compliance with the Regulation is in the first place on them.

This means that they need to develop their processing activities from the start with data protection by design and by default in mind, implement the relevant technical and organisational safeguards to mitigate any risks to an acceptable level, document their processing operations, including data protection impact assessments where required, respond to data subjects' inquiries and so on. All of this needs to be done in a reproducible way, documenting the choices made. This documentation both enables EUIS to learn and the EDPS to provide reassurance that EUIs have handled personal data responsibly.

In order to do so, the EUI need to establish internal procedures for governing their processing operations. This includes consulting their data protection officers (DPOs) on relevant

[1] OJ L 295, 21.11.2018, p. 39–98

[2] That is, excluding our other roles, e.g. as regards technology monitoring, as an adviser to EU institutions on policy and legislation and as member of the EDPB.

[3] OJ L 8, 12.1.2001, p. 1–22

developments. Having a strong DPO with appropriate resources is an important component of accountability. DPOs also are the main contact point between EUIs and the EDPS.

3 What are our main activities as a supervisory authority?

As supervisory authority for the processing of personal data by EUIs[4], our activities mirror those of our fellow DPAs on the national level, albeit in a specific international public sector environment. We ensure that EUIs are guided by the utmost respect for the protection of the fundamental rights and freedoms of individuals in relation to the processing of personal data. We also promote awareness and understanding inside the EUIs of the risks to people's rights and freedoms as well as to society. The EDPS' staff has the different areas of expertise required for this task – technical, legal, and institutional.

3.1 Complaints

We handle complaints from individuals who allege that EUIs have handled their personal data in breach of the Regulation (see Articles 57(1)(e) and 63of the Regulation). We cannot handle complaints against companies or national public authorities; for those, complainants should contact the national data protection authorities in the EU Member States.

Before turning to the EDPS, we advise prospective complainants to contact the EUI whose conduct they take objection to – many issues can be resolved at this level already. Complainants need to be personally affected by the alleged breach to have standing. However, we may decide to launch own-initiative-investigations based on allegations made by persons who formally do not have standing.

There is an exception to the requirement of being personally affected. Under Article 68 of the Regulation, persons *employed by* EUIs can lodge complaints without being personally affected. The same Article includes protection against retaliation. This is in effect a whistleblowing provision

The complaint mechanism serves first to ensure that EUIs treat data subjects right. Apart from how to remedy a breach in the individual case, our decisions on complaints usually also show a way forward to structural improvements.

We also use insights gained from handling complaints for better targeting our other activities, e.g. on which topics to issue guidelines or conduct investigations. Complaints are a valuable tool for the EDPS to obtain an overview of the problems people face with EUIs' processing of personal data.

3.2 Personal data breach notifications

When EUIs suffer a personal data breach, they have to notify the EDPS about this (Article 34 of the Regulation) and, under certain conditions, also communicate the breach to the data subject (Article 35 of the Regulation). We keep an internal register of breaches notified to us.

We use the notifications received for verifying compliance with the Regulation's provisions on personal data breaches and for checking EUIs' follow-up to the breach. Where necessary, we use our enforcement powers to ensure proper follow-up, such as ordering an EUI to inform data subjects about a breach.

[4] This document refers to the Regulation as the main framework for data protection in the EUIs. Some EUIs are subject to special rules for some parts of their activities, e.g. Europol and EPPO.

These notifications also give us an overview of recurrent issues and may help us identify areas for guidance documents, stock-taking exercises etc.

For more information, see the EDPS Guidelines on Personal Data Breach Notification.

3.3 Voluntary consultations

The EDPS provides advice to EUIs on specific (planned) processing operations and any other question related to data protection (Article 57(1)(g)). Depending on the needs of the requesting EUI and the complexity of the case, this advice can take different forms – from calls to our DPO hotline, through informal advice on staff level, to formal letters signed by the Supervisor.

These consultations help both the EUIs, by providing advice on how to apply the Regulation, and us, by providing an overview of recurrent issues. In line with the principle of accountability, consulting the EDPS does not mean that we will do the controller's work for them. We point EUIs in the right direction and give recommendations, but final responsibility for the processing remains with the controller.

For more information on this and the following point, see our Policy on Consultations and Authorisations in the Field of Supervision and Enforcement.

3.4 Mandatory consultations and authorisations

In some cases, the Regulation obliges EUIs to consult the EDPS on planned processing operations or documents governing them and in some cases obtain authorisation.

Prior consultations following a data protection impact assessment (Article 40) and consultations on internal rules for restricting data subjects' rights (Article 41(2)) are mandatory. Ad-hoc contractual clauses and provisions in administrative arrangements for adducing appropriate safeguards for extra-EU transfers of personal data require prior authorisation (Article 48(3)).

In our replies to such consultations and authorisation requests, we provide input on any necessary improvements.

3.5 Stocktaking exercises

Many data protection questions are horizontal and will affect all, or at least a large number of, EUIs. To obtain an overview of practices and to address issues here, we conduct stocktaking exercises with questionnaires sent to the EUIs. They can cover any topic – from how EUIs verify that the person requesting access to their own personal data is actually the data subject to the arrangements used for third-country transfers.

These exercises are a further development of the biennial surveys we carried out under the old Regulation. They will be more frequent, more targeted, and can also lead to enforcement actions.

3.6 Data protection audits

We choose the targets of our data protection audits in a risk-based annual plan. On top of this, there are some large-scale information systems whose establishing acts oblige us to conduct inspections / audits in a regular cycle.

These audits offer a valuable opportunity to check actual practices and in most cases include an on-site part. Some audits may however be carried out remotely, e.g. when assessing EUIs' websites. Following the on-site part, we prepare minutes and a report with recommendations that we will follow-up on.

For more information, see 'what to expect when we inspect'.

3.7 Own-initiative-investigations

We also conduct own-initiative investigations into topics of interest. The triggers for such investigations can be different: recurring complaints that suggest structural problems, press reports about newly discovered vulnerabilities in IT systems, etc.

These investigations may also include on-site checks, where required without prior announcement.

3.8 Guidance and training

We distil our decisions and opinions into Guidelines and Papers covering both specific questions such as how to conduct administrative inquiries and disciplinary procedures in a compliant way as well as horizontal questions such as how to document processing operations. We also have the task to issue certain standard contractual clauses for hiring processors.

In addition to the guidelines, we also provide training sessions for the EUIs on these and other topics.

4 What are our powers and how we will use them?

Article 58 of the Regulation gives the EDPS has a wide array of powers to use to fulfil our tasks. We choose the approach that we deem to be the most likely to yield positive results for the persons affected by EUIs' processing of personal data. Depending on the context, we choose from a scale ranging from providing informal advice to formally using our enforcement powers, including our corrective powers. There are many cases in which a cooperative approach is fruitful, but we back this up with enforcement where necessary.

The most important powers are listed below:

In terms of **investigatory powers** which are listed in Article 58(1), we have the right to order controllers and processors to provide any information required for our tasks, to obtain access to all personal data necessary for our tasks and to obtain access to any premises of the controller and the processor, including to any data processing equipment and means.

Example: when announcing a data protection audit, we request information – documentation, statistics etc. – from the controller. During the on-site part, we may collect evidence, e.g. copies of log files, additional documents, or screenshots and take minutes of interviews.

Before taking formal enforcement action, we can provide recommendations to controllers and refer the matter back to them. We can also refer matters to the political level in Parliament, Council and Commission, where necessary.

Concerning **corrective powers** (listed in Article 58(2)), apart from issuing **warnings** and **reprimands**, we can order controllers and processors to **comply with data subjects' requests** to exercise their rights under the Regulation; to **bring processing operations into compliance** with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period; to **notify** personal data breaches to data subjects.

Example: an EUI asks us for advice on a planned processing operation. In our reply, we provide recommendations on possible steps to minimise the impact on data subjects. Formally this is a referral to the controller. In the follow-up to the consultation, it becomes clear that the institution failed to take any steps to remediate the shortcomings. This is a situation where the EDPS would issue an order to bring processing operations into compliance with the Regulation by obliging the EUI to change specific aspects of the processing operation.

One of our strongest tools is the power to **impose temporary or definitive limitations on processing** operations, up to a complete **ban**. This also includes the **suspension of data flows**.

When deciding whether and how to use our corrective powers, we take into account the circumstances of each case, the gravity of the infringement and the risks to the rights and freedoms of the persons concerned.

Furthermore, under Article 66, the EDPS can also issue **administrative fines** against the other EUIs. We will usually use this power as a last resort. When imposing an administrative fine on a EUI, the EDPS will consider the proportionality of amount of the fine[5]. The administrative procedure for the imposition of administrative fines on EUI's will respect the general principles of Union law as interpreted by the Court of Justice.

Example: a person complains that an EUI unlawfully withheld personal data it held about her when replying to a request for access to one's own personal data under Article 17 of the Regulation. Following an on-site check, the EDPS decision establishes that the EUI indeed unlawfully withheld the data and orders it to provide a complete reply to the complainant by a specified deadline. The EUI fails to comply with the order by that deadline. This is a situation in which the EDPS may decide to impose a fine.

Fines collected feed into the general budget of the Union; the EDPS does not retain any money from them.

Our corrective powers are always exercised against EUIs, not members of their staff. Should a breach of the Regulation be due to individual wrongdoing, we cannot take disciplinary action against staff members of other EUIs – that power is reserved to their employer. We can however suggest that the employer do so.

We also have certain authorisation powers (Article 58(3)) - e.g. for the use of specific tools for data transfers (see 3.4 above).

Decisions of the EDPS can be appealed against before the Court of Justice (Article 64(2) of the Regulation).

5 Cooperation with other stakeholders

We do not conduct our work in isolation, but stay in contact with other stakeholders.

The network of the EUI's DPOs is our main interlocutor – we met with them on a regular basis, exchange on priorities and cooperate in working groups on specific topics.

Example: before issuing guidelines, we consult the DPO network to see whether the scope matches DPOs' need for guidance and whether the proposed solutions are feasible for EUIs.

We also exchange with fellow data protection authorities in the EU Member States and beyond in fora such as the European Data Protection Board and regular case handling workshops.

Example: in our audits at Europol, we involve experts from national DPAs as part of the audit team. We may also conduct joint investigations with our peers from national DPAs, where the topics are of common concern.

[5] This will take into account all relevant circumstances of the specific situation, with due regard to the nature, gravity and duration of the infringement, its consequences and the measures taken to ensure compliance with the obligations under the Regulation and to prevent or mitigate the consequences of the infringement in the specific situation (see also recital 81).

6 Transparency and publicity

We strive to be as transparent to the public as possible in our work and usually issue press releases or similar announcements on our activities to the public. However, there may be some limitations on what we can publicly say about for example complaint cases or vulnerabilities discovered in data protection audits.

Example: we publish replies to consultations that are also relevant for other EUIs or the public, for example because they refer to a horizontal issue that affects also other EUIs or because they have caused public interest. We inform the EUI that consulted us about our intention to publish before doing so. On the other hand, while as a rule we do not publish audit reports in full, where they may reveal specific vulnerabilities, we may publish summaries of such reports. Similarly, we may decide not to publish complaints decisions, as they may contain confidential information, e.g. for complaints requesting rectification of data. Where complaints raise issues of broader significance beyond the individual case, we may publish the key outcomes in an anonymised way, also to provide guidance to other EUIs, which may face the same or similar issues.

We clearly communicate whether we intend to make replies to EUIs and data subjects public. Where appropriate, we may consider publication in a redacted form. Where we re-use non-published content for guidelines, training sessions and similar content, we anonymise it where required. This is without prejudice to Regulation (EC) 1049/2001[6] on public access to documents, which applies also to the EDPS.

[6] OJ L 145, 31.5.2001, p. 43–48