INVESTIGATION · LAW, ETHICS AND REGULATION

Data Protection Authority Investigations and GDPR Enforcement

Data protection authorities investigate how organisations collect, use and protect personal data, and can impose large fines. This article explains how investigations under the EU General Data Protection Regulation and similar laws begin, the powers authorities use, how cross-border cases are handled, landmark decisions, and how organisations should prepare.

ModQu research article · 1,310 words · 15 references (APA 7th edition)

Personal data are now among the most valuable assets that organisations hold, and among the most frequently misused. Data protection authorities (DPAs) exist to enforce the laws that govern how personal data are collected, used, shared and protected. Since the European Union's General Data Protection Regulation (GDPR) took effect in May 2018, these authorities have had stronger powers and the ability to impose fines of up to 4 per cent of a company's worldwide annual turnover (Regulation (EU) 2016/679, 2016, art. 83). Their investigations now affect businesses of every size, and their decisions have reshaped how global technology companies handle data.

This article explains how DPA investigations begin, the powers and procedures involved, how cross-border cases work in the European Union, some landmark decisions, and practical lessons for organisations.

The legal framework

The GDPR sets out principles for processing personal data, including lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, and integrity and confidentiality (art. 5). It gives individuals rights, such as the right to access their data and to object to certain processing, and places obligations on organisations, including keeping records, assessing high-risk processing and protecting data securely. Hoofnagle et al. (2019) describe the GDPR as a comprehensive framework that combines individual rights with organisational accountability, and Lynskey (2015) traces its foundations in the fundamental right to data protection recognised in EU law.

Each EU member state has at least one independent supervisory authority. Outside the EU, similar authorities enforce national laws, such as the Information Commissioner's Office (ICO) under the United Kingdom's Data Protection Act 2018 and the Office of the Privacy Commissioner of Canada under the Personal Information Protection and Electronic Documents Act.

How investigations begin

DPA investigations usually start in one of four ways:

- **Complaints** from individuals, who have a right to complain to a supervisory authority if they believe their data have been processed unlawfully (art. 77). Complaints are the largest source of cases.
- **Breach notifications.** Organisations must notify the authority of a personal data breach within 72 hours of becoming aware of it, unless it is unlikely to result in a risk to people's rights and freedoms (art. 33). Guidelines from the European Data Protection Board explain how to assess and report breaches (European Data Protection Board [EDPB], 2023b).
- **Own-initiative inquiries**, in which the authority examines a sector, a practice or a company on its own initiative, often after media reports or research.
- **Referrals** from other authorities, including DPAs in other countries.

Powers and procedure

The GDPR gives authorities investigative powers, including to order organisations to provide information, to carry out audits, to obtain access to premises and equipment, and to review processing operations (art. 58). Corrective powers include warnings, reprimands, orders to bring processing into compliance or to stop it, orders to notify affected people, and administrative fines.

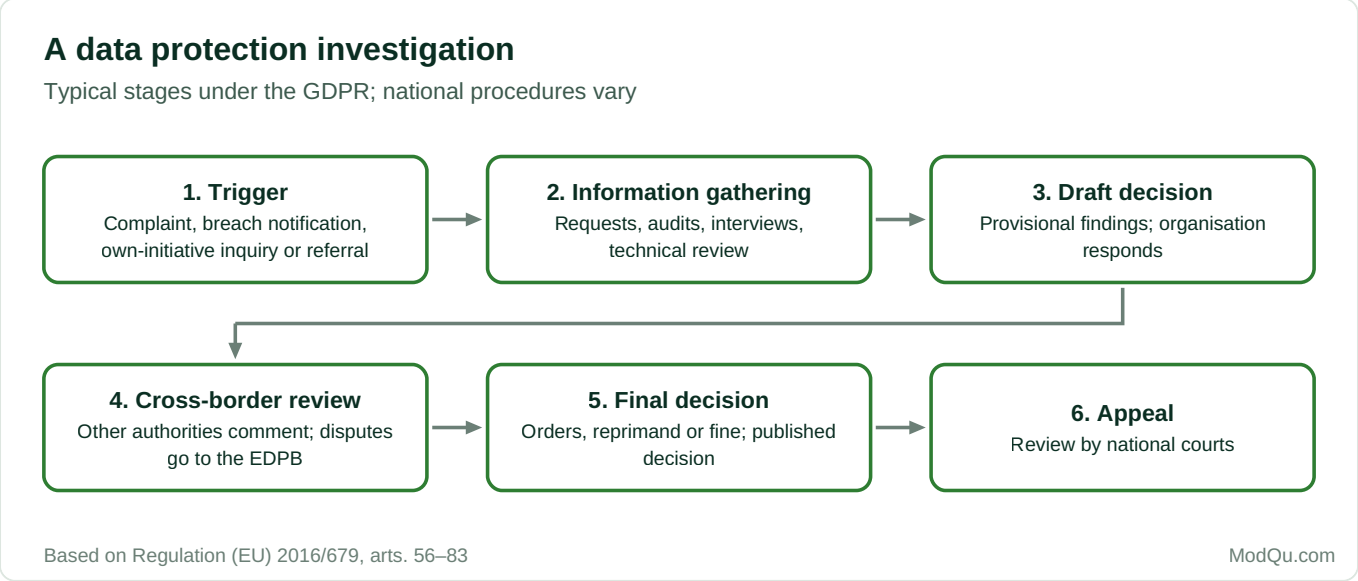


Figure 1. The main stages of a data protection investigation. In cross-border cases, the lead authority's draft decision is shared with other concerned authorities, and unresolved objections are settled by the European Data Protection Board. Diagram by ModQu.

The authority gathers information through formal requests, documents such as data protection impact assessments and records of processing, technical examination of systems and websites, and interviews. It then prepares a draft decision, which the organisation can respond to before a final decision is made.

Cross-border cases and the one-stop shop

When a company processes data across several EU countries, the GDPR's "one-stop shop" mechanism makes the authority of the country where the company has its main European establishment the lead supervisory authority (art. 56). Because many large technology companies have their European headquarters in Ireland, the Irish Data Protection Commission leads many of the most significant cases. Other authorities whose residents are affected can object to the lead authority's draft decision, and if they cannot agree, the European Data Protection Board makes a binding decision (art. 65).

The mechanism has been criticised. Gentile and Lynskey (2022) argue that it has concentrated enforcement in a few authorities with limited resources, leading to long delays in major cases, and that differences in national procedures have made cross-border enforcement inconsistent. The EU has since adopted additional procedural rules to address some of these problems.

Landmark decisions

Several decisions illustrate the scale and scope of enforcement. In 2019, the French authority, the CNIL, fined Google €50 million for failing to provide clear information to users and for not obtaining valid consent for personalised advertising (Commission Nationale de l'Informatique et des Libertés [CNIL], 2019). In 2020, the ICO fined British Airways £20 million and Marriott International £18.4 million after investigations into security failures that allowed attackers to obtain personal data of millions of customers (Information Commissioner's Office [ICO], 2020a, 2020b).

The largest fine to date arose from a cross-border case. In 2023, following a binding decision by the European Data Protection Board, the Irish Data Protection Commission fined Meta Platforms Ireland €1.2 billion and ordered it to suspend transfers of European users' Facebook data to the United States (EDPB, 2023a; Data Protection Commission, 2023). The case followed the Court of Justice's ruling in *Data Protection Commissioner v. Facebook Ireland and Schrems* (2020), which invalidated the EU–US Privacy Shield arrangement because United States surveillance law did not give EU citizens adequate protection.

Court rulings also shape what authorities investigate. In *Google Spain SL v. Agencia Española de Protección de Datos* (2014), the Court of Justice held that search engines must, in some circumstances, remove links to information about a person on request, establishing what became known as the "right to be forgotten" and generating many complaints and investigations.

Outside the EU, the Privacy Commissioner of Canada and the British Columbia commissioner jointly investigated Facebook after the Cambridge Analytica revelations and found that it had failed to obtain meaningful consent and to safeguard users' information (Office of the Privacy Commissioner of Canada, 2019).

Preparing for an investigation

Organisations can reduce both the risk and the impact of an investigation. They should keep records of what personal data they process and why, carry out impact assessments for high-risk processing, have a tested breach response plan that allows notification within 72 hours, respond promptly and fully to individuals' requests, and document decisions about lawful bases and security measures. When an investigation begins, they should preserve relevant records, appoint a single point of contact, provide accurate and complete information, and correct problems quickly. Authorities consider cooperation, mitigation and previous conduct when deciding on fines (art. 83).

A short example

The following hypothetical case illustrates a typical investigation. A survey company discovers that a misconfigured storage folder has exposed the names, email addresses and answers of 20,000 respondents online for three weeks. It closes the folder, investigates, finds no evidence that anyone other than a security researcher accessed it, and notifies the authority within 72 hours. Because some answers concerned health, it also informs the respondents.

The authority opens an investigation, requests the company's security policies and access logs, and interviews its staff. It finds that the company had no procedure for checking storage settings and had kept the survey answers for longer than its own policy allowed. Taking into account the prompt notification, the lack of evidence of misuse and the company's cooperation, the authority issues a reprimand and orders the company to introduce configuration checks and delete data it no longer needs, rather than imposing a fine.

Conclusion

Data protection authority investigations are triggered by complaints, breach reports, own-initiative inquiries and referrals, and use powers to obtain information, audit systems and impose corrective measures and fines. In the European Union, the one-stop-shop mechanism channels cross-border cases through a lead authority, with disputes resolved by the European Data Protection Board. Landmark decisions against major companies show the reach of these powers, but most investigations concern ordinary organisations. Good records, a tested breach plan, honest cooperation and prompt correction of problems are the best preparation.

References

Commission Nationale de l'Informatique et des Libertés. (2019). *Délibération n° SAN-2019-001 du 21 janvier 2019 prononçant une sanction pécuniaire à l'encontre de la société GOOGLE LLC*.

Data Protection Act 2018, c. 12 (UK).

Data Protection Commission. (2023). *Decision in the matter of Meta Platforms Ireland Limited* (Inquiry IN-20-8-1).

Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems, Case C-311/18, EU:C:2020:559.

European Data Protection Board. (2023a). *Binding decision 1/2023 on the dispute submitted by the Irish SA on data transfers by Meta Platforms Ireland Limited for its Facebook service (Art. 65 GDPR)*.

European Data Protection Board. (2023b). *Guidelines 9/2022 on personal data breach notification under GDPR* (Version 2.0).

Gentile, G., & Lynskey, O. (2022). Deficient by design? The transnational enforcement of the GDPR. *International and Comparative Law Quarterly, 71*(4), 799–830. https://doi.org/10.1017/S0020589322000355

Google Spain SL v. Agencia Española de Protección de Datos, Case C-131/12, EU:C:2014:317.

Hoofnagle, C. J., van der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: What it is and what it means. *Information & Communications Technology Law, 28*(1), 65–98. https://doi.org/10.1080/13600834.2019.1573501

Information Commissioner's Office. (2020a, October 16). *Penalty notice: British Airways plc*.

Information Commissioner's Office. (2020b, October 30). *Penalty notice: Marriott International Inc*.

Lynskey, O. (2015). *The foundations of EU data protection law*. Oxford University Press.

Office of the Privacy Commissioner of Canada. (2019). *Joint investigation of Facebook, Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia* (PIPEDA Findings #2019-002).

Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 (Canada).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). (2016). *Official Journal of the European Union, L 119*, 1–88.