



Complaint Handling Obligations in Data Protection Law: A Comparison of the EU GDPR, UK GDPR, and the DUAA

1. Introduction

The regulation of complaint handling in data protection law has undergone a significant transformation in the United Kingdom in 2025–2026. The Data (Use and Access) Act 2025 (hereinafter: DUAA) codifies a previously missing obligation that the EU General Data Protection Regulation (GDPR) never explicitly defined at the level of data controllers: the requirement to receive and handle complaints related to the processing of personal data within a formal, internal organizational procedure. This development also represents one of the most substantial substantive divergences between the EU GDPR and the UK GDPR.

2. The EU's GDPR framework – the supervisory authority-centered model

The backbone of the EU GDPR's complaint framework is Article 77. This provision ensures that every data subject, without prejudice to any other administrative or judicial remedy, has the right to lodge a complaint with a supervisory authority—particularly in the Member State of their habitual residence, place of work, or the place of the alleged infringement—if they consider that the processing of personal data relating to them infringes the Regulation.¹

Within the EU GDPR system, therefore, the direct and mandatory channel for lodging complaints is the independent supervisory authority (e.g., the national data protection authority). The GDPR does not impose an explicit requirement on data controllers to operate an internal complaint-handling mechanism; data subjects have a direct route to submit complaints to the supervisory authority.

Article 57(1)(f) sets out the obligations of supervisory authorities: they must handle complaints lodged by data subjects, investigate the subject matter of the complaint to the extent appropriate, and inform the complainant of the progress and outcome of the procedure within a reasonable timeframe.¹

In addition, Article 57(2) requires supervisory authorities to facilitate the submission of complaints by measures such as providing complaint forms that can also be completed electronically, without excluding other means of communication.¹

It is important to emphasize that the GDPR's concept of a complaint is broad in scope. The subject matter of a complaint is not limited to the data subject rights set out in Chapter III of the GDPR, but extends to any other data protection infringement caused by the controller or processor affecting the data subject.



The European Data Protection Board (EDPB), in its Internal Document No. 02/2021, confirmed that the supervisory authority's obligation to handle and investigate complaints under Article 57(1)(f) corresponds to the data subject's right to lodge a complaint under Article 77. The authority may not mechanically reject a complaint or leave it without substantive examination.⁶

3. The original UK GDPR framework – before and after Brexit

Since 1 January 2021, the United Kingdom has applied the text of the EU GDPR as incorporated into its domestic legal order under the UK GDPR. Prior to Brexit, the system set out in Article 77 of the EU GDPR was in force in the UK; in addition, Section 165 of the Data Protection Act 2018 (DPA 2018) established the complaint-handling obligations of the Information Commissioner's Office (ICO).³

Article 57(1)(f) of the UK GDPR essentially mirrored the corresponding provision of the EU GDPR: the ICO is responsible for handling complaints, conducting investigations, and informing the complainant of the progress and outcome of the procedure within a reasonable period.²

However, the original UK GDPR—like the EU GDPR—did not impose a mandatory internal complaint-handling procedure on data controllers; this obligation was introduced only with the DUAA.

4. DUAA's new obligation to handle complaints – Section 164A

4.1 Legal Basis

The DUAA entered into force in the United Kingdom on 19 June 2025. The obligation to handle complaints is introduced by Section 103 of the Act, which inserts a new Section 164A into the Data Protection Act 2018. From 19 June 2026—one year after Royal Assent—all data controllers subject to UK data protection law will be required by statute to implement a formal procedure for handling data protection complaints.^{4;3}

4.2 The scope of the new obligations

Data subjects must first submit their complaint directly to the data controller before bringing it before the ICO. This represents a fundamental change in the UK's complaint-handling system: it introduces an intermediate step between the data subject and regulatory intervention.³



The Act specifically requires:

- a) **Provision of an accessible complaint submission mechanism.** Data controllers must take steps to enable data subjects to lodge complaints regarding the processing of their personal data—for example, by providing an electronic complaint form. Organizations retain flexibility in how they implement this.³
- b) **30-day acknowledgment deadline.** The 30-day period begins on the day after the complaint is received, even if that day falls on a weekend or public holiday.³
- c) **Substantive response without undue delay.** Although the DUAA does not set a statutory maximum deadline for a substantive response, ICO draft guidance indicates that organizations should provide an outcome within three months, except in exceptional circumstances.^{3;5}
- d) **Appropriate investigation and ongoing communication.** The DUAA requires data controllers to conduct an appropriate investigation into the subject matter of the complaint and to keep the complainant informed of the progress and outcome of the procedure.³
- e) **Information on remedies.** Decisions must be communicated in clear and accessible language, and the data subject must be informed of the possibility of escalating the complaint to the ICO if they are dissatisfied with the outcome.³

4.3 The ICO's “must / should / could” framework

On 12 February 2026, the ICO published its guidance entitled “*How to deal with data protection complaints*”, which follows its standard structure by distinguishing between what organizations **must**, **should**, and **could** do.⁵

Among the ICO's expectations is that organizations should not unduly restrict the channels through which complaints can be submitted, and should ensure that complaints received via non-designated channels—such as customer service—are properly identified and handled. (ICO guidance, “must” requirements)

In the spirit of transparency and accountability, the ICO also recommends that organizations consider publishing anonymized complaint statistics and integrating complaint oversight into existing governance structures—for example, within the reporting lines of the Data Protection Officer (DPO).⁵



5. A Comparison of the EU GDPR and the UK GDPR/DUAA

Below, we summarize the main features of the two systems:

EU GDPR:

- **Legal basis:** Article 77, Article 57(1)(f) and (2)
- **Primary recipient of the complaint:** Supervisory authority (e.g., NAIH, BfDI, CNIL)
- **Internal obligations of the data controller:** There is no specific legal obligation
- **Deadline for acknowledgment:** Not recorded at the data controller level
- **Deadline for a substantive response:** Reasonable time (at the administrative level)
- **Electronic complaint form:** Article 57(2): The authority is required to ensure
- **Right to contact the ICO:** N/A
- **Supervisory role:** DPA (e.g., NAIH) direct recipient

UK GDPR + DUAA:

- **Legal basis:** UK GDPR Article 77 + DPA 2018, new Section 164A
- **Primary recipient of the complaint:** Data Controller (mandatory internal step)
- **Internal obligations of the data controller:** Yes – a legal requirement effective June 19, 2026
- **Deadline for acknowledgment:** 30 days (at the data controller level)
- **Deadline for a substantive response:** Without undue delay; ICO proposal: 3 months
- **Electronic complaint form:** Section 164A: The data controller is required to ensure
- **Right to contact the ICO:** Prerequisite: You must first file a complaint with the data controller
- **Supervisory role:** ICO secondary level; preceded by an internal procedure

6. The significance and consequences of the discrepancy

The UK system departs from the EU GDPR by imposing a statutory obligation on data controllers to investigate and respond to complaints. No such explicit requirement exists under the EU GDPR; there, data subjects have a direct route to the supervisory authority.^{1;3}

This structural difference is relevant in several respects:

From a compliance perspective, organizations operating in the United Kingdom must formalize their internal complaint-handling processes by 19 June 2026, regardless of whether such procedures previously existed. Data controllers are required to develop a written complaints policy, align complaint handling with the management of data subject rights (e.g., access



requests), and produce regular reports on the volume and outcomes of complaints for senior management or audit committees.^{4;5}

For organizations operating in the EU, internal complaint handling at the controller level remains a matter of best practice rather than a mandatory legal requirement—the data subject may at any time обратиться directly to the supervisory authority.¹

From the perspective of adequacy: the European Commission has recently renewed its adequacy decision for the United Kingdom. The Commission concluded that the UK GDPR and the Data Protection Act 2018 ensure a level of protection that is essentially equivalent to that of the EU GDPR, and the new decision is valid for six years. At the same time, the changes introduced by the DUAA—particularly the obligation for controller-level complaint handling—indicate a growing divergence between the two regimes. (European Commission adequacy decision, 2025)

7. Summary

Section 164A, inserted into the Data Protection Act 2018 by Section 103 of the DUAA, establishes a statutory complaint-handling obligation for data controllers in the United Kingdom that is entirely absent from the EU GDPR framework. While the EU GDPR, under Article 77, is built on a direct relationship between the data subject and the supervisory authority, the UK model introduces a preliminary, organizational-level step: the data subject must first contact the data controller, and may escalate the matter to the ICO only if the internal complaint process proves unsuccessful.

This change represents a significant compliance burden for organizations operating in the United Kingdom: by 19 June 2026, they must implement a functional, documented internal complaint-handling system aligned with ICO expectations—otherwise they may face the ICO's expanded enforcement powers, including fines of up to 4% of global turnover or £17.5 million.

Sources:

1. *Article 57(1)(f) and (2) and Article 77 of the EU GDPR;*
2. *Article 57 of the UK GDPR;*
3. *Data Protection Act 2018, Section 165 and new Section 164A;*
4. *Data (Use and Access) Act 2025, Section 103;*
5. *ICO, “How to Handle Data Protection Complaints” (February 12, 2026);*
6. *EDPB Internal Document 02/2021 European Commission Decision on the Adequacy of the UK (2025).*