SQUIRE PATTON BOGGS

The Data (Use and Access) Act 2025 and the new right for individuals to complain to controllers

What organisations need to do before 19 June 2026

June 1, 2026

The UK's data protection framework continues to evolve following the enactment of the Data (Use and Access) Act 2025 (DUAA). One of the more operationally significant developments for organisations is the introduction of a new statutory right for individuals to complain to controllers regarding infringements of the UK General Data Protection Regulation (GDPR), as well as a framework governing how controllers must handle those complaints.

The relevant provisions will apply from 19 June 2026, pursuant to the Data (Use and Access) Act 2025 (Commencement No. 6) Regulations 2026. On or before that date, organisations subject to the UK GDPR will need to update their privacy notices, and introduce formal data protection complaint handling processes that meet specific legal requirements.

Although individuals will retain their right to complain directly to the Information Commissioner's Office (which will become the "Information Commission" under other changes introduced by the DUAA) (ICO), the reforms are designed to ease the ICO's related regulatory burden and therefore to encourage individuals to raise concerns with controllers in the first instance, with controllers now expected to provide accessible complaint channels, acknowledge complaints within prescribed timeframes, investigate concerns appropriately and communicate outcomes without undue delay.

These new obligations represent a significant formalisation and strengthening of regulatory expectations. In practice, complaints handling will become a more visible and auditable aspect of organisational accountability under UK data protection law.

What is changing?

The new right to complain and related complaints handling requirements are introduced through the new section 164A of the Data Protection Act 2018 (DPA 2018), as amended by the DUAA.

The new right allows individuals to make a complaint to a controller if they consider that the controller has infringed the UK GDPR when processing their personal data. Broadly, the reforms require controllers to:

- Provide at least one accessible way through which individuals can submit data protection complaints (for example, by providing an online complaint form which can be completed and submitted electronically)
- Acknowledge complaints within 30 days of receipt
- Take "appropriate steps" to investigate complaints (including making enquiries into their subject matter) without undue delay
- Keep complainants informed about the progress and outcome of complaints without undue delay
- Inform individuals of their right to complain in their privacy notices
- Maintain appropriate records relating to complaints and their resolution

The ICO has also published guidance explaining that organisations should treat complaints handling as part of their broader accountability obligations and ensure complaints can be identified, assessed, investigated and resolved consistently and transparently.

Importantly, the concept of a "data protection complaint" is broad. According to the ICO, complaints may arise in relation to any alleged infringement of the UK GDPR, including concerns relating to subject access requests, direct marketing, retention practices, transparency obligations, cookies and other tracking technologies (insofar as they involve the processing of personal data), as well as security incidents and the lawful basis relied upon for processing.

The reforms also introduce related changes to transparency and individual rights request response requirements under the UK GDPR.

In particular, Article 12(4) of the UK GDPR now requires controllers, where they do not take action on a request made by a data subject (such as a rectification, erasure or restriction request), to inform the individual not only of their right to complain to the ICO under section 165 of the DPA 2018, but also of their right to make a complaint to the controller under section 164A of the DPA 2018. Similarly,

Articles 15(1)(ea) and (f) of the UK GDPR require controllers, as part of the information provided in response to a subject access request, to inform individuals of both these rights.

These amendments are operationally significant because they require organisations not only to maintain a compliant complaints process, but also to ensure that complaints information and signposting are properly embedded into privacy notices, data subject access request (DSAR) response templates and broader data subject rights communications.

In addition, the new section 164B of the DPA 2018 gives the secretary of state the power to introduce regulations requiring controllers to provide the ICO with information about the number of complaints received over a certain period. Although no such reporting regime has yet been implemented, the provision indicates that complaints handling metrics and trends may become a more formal component of regulatory oversight in the future.

Why this matters

Many organisations already manage privacy-related complaints through existing customer service, legal or other compliance functions. However, the new regime introduces more prescriptive operational requirements and creates clearer regulatory expectations around how complaints are received, documented and resolved.

The ICO's guidance makes clear that organisations should have documented processes in place, train relevant staff and maintain records demonstrating how complaints were handled, and why specific decisions were reached.

The reforms are therefore likely to require organisations to move away from informal or fragmented approaches to complaints handling. Complaints processes will need to be sufficiently structured and auditable to withstand regulatory scrutiny, if challenged.

What should organisations do now?

With the commencement date approaching, organisations should assess whether their existing privacy governance frameworks are capable of supporting the new requirements.

In particular, organisations that are subject to the UK GDPR and processing personal data as controllers should consider the following steps:

1. Review and update privacy notices

Privacy notices should be updated to explain:

- The individual's right to raise a data protection complaint with the organisation
- How complaints can be submitted
- The channels available for complaints
- The individual's continuing right to complain to the ICO

Organisations should also put together, or review existing templates used in response to data subject rights requests to ensure that appropriate complaint signposting is included, where required.

2. Establish a formal complaints handling process

Organisations should implement a documented process for managing data protection complaints from intake through to resolution.

This should include:

- Mechanisms for receiving complaints through appropriate channels
- Procedures for identifying and classifying complaints
- Escalation pathways for high-risk or complex matters
- Investigation and response procedures
- Record-keeping requirements
- Oversight and governance arrangements

The ICO recommends ensuring that complaints are easy to submit, and that organisations can recognise complaints even where individuals do not use formal terminology or expressly refer to "data protection" concerns. Controllers should also recognise that, as with other requests from individuals to exercise their rights under the UK GDPR, complaints may be received through any channel (including in person, by phone, in writing or via social media) and do not need to be labelled explicitly as "data protection complaints" in order to fall within scope.

Examples provided by the ICO include:

- Providing a complaint form that individuals can submit to the controller either electronically or in writing (e.g., by email or post)
- Providing an email address to which individuals can submit complaints
- Allowing people to make complaints over the phone
- Providing an online complaints portal
- Having a live chat function with the option to escalate to a human if needed
- Giving individuals a way to make complaints in person (e.g. if you don't have an online presence)

3. Implement tracking and audit capabilities

Organisations should ensure that complaints can be logged, monitored and evidenced appropriately.

This is particularly important given the statutory requirement to acknowledge complaints within 30 days of receipt, and to take appropriate steps to respond without undue delay.

Organisations should therefore consider whether their existing systems, processes and procedures can sufficiently:

- Record receipt dates, key milestones and other pertinent information
- Distinguish complaints from DSARs and other rights requests
- Maintain investigation records and details of the rationale for the outcome
- Identify repeat or systemic issues
- Support management reporting and governance oversight

4. Train relevant teams

Frontline personnel, customer service teams, HR teams, legal functions, compliance personnel and data protection officers (DPOs) should understand:

- What constitutes a data protection complaint
- How complaints should be escalated internally
- Applicable timelines and obligations
- How complaints interact with other regulatory processes, such as personal data breach management and rights request handling.

Given that a data protection complaint could be made to any member of staff, the ICO also specifically recommends ensuring staff understand how to recognise and route complaints appropriately.

5. Review processor and group arrangements

Organisations should also assess whether existing contractual arrangements with processors (including, where relevant, other group entities) adequately cover support in complaint handling obligations or in responding to data subject rights requests, more broadly.

Although the statutory obligations apply primarily to controllers, controllers may still require support from processors when investigating complaints relating to outsourced processing activities.

International organisations should also consider whether UK-specific complaints handling requirements need to be incorporated into broader global privacy governance frameworks.

Looking ahead

The new complaints handling regime reflects a broader regulatory trend towards demonstrable accountability in data protection compliance.

From 19 June 2026, organisations will not only need to comply with substantive data protection obligations under the UK GDPR and DPA 2018, but also demonstrate that they can receive, manage and resolve complaints in a structured, transparent and timely manner.

Organisations that have not yet reviewed their complaints handling arrangements should begin readiness assessments now. Updating privacy notices, implementing documented complaint handling procedures and ensuring appropriate governance and audit mechanisms are in place should be treated as key priorities ahead of commencement.

For an overview of other changes introduced by the DUAA, please visit our article, "The Data (Use and Access) Act 2025: A New Chapter in the UK's Data Protection Framework."

71304/06/26