edgeGRC

Guide | United Kingdom

UK GDPR: practical guide

UK data protection after the Data (Use and Access) Act 2025: the responsibilities that stay the same as the EU GDPR, what changed in 2026, and what the ICO expects organisations to have in place.

Last reviewed: 27 November 2026

General information only. Not legal advice, a legal opinion or a certification of compliance.

1 At a glance

The UK's data protection framework is made up of four parts. The UK GDPR (the EU GDPR as retained in UK law after Brexit) sits alongside the Data Protection Act 2018 and the Privacy and Electronic Communications Regulations (PECR). The Data (Use and Access) Act 2025 (the DUAA) amends all three.

Date	Milestone
19 June 2025	The DUAA received Royal Assent. Its provisions were then brought into force in stages by commencement regulations.
5 February 2026	Most of the data protection changes to the UK GDPR, the Data Protection Act 2018 and PECR came into force.
19 June 2026	The new duty on controllers to handle data protection complaints came into force.

The regulator is the **Information Commissioner's Office (ICO)**. The DUAA also provides for the ICO to be restructured as the Information Commission, with its governance changes following on their own timetable.

2 What stays the same

The core of the UK GDPR remains closely aligned with the EU GDPR:

- the seven principles, including **accountability**: being able to demonstrate compliance;
- the six lawful bases for processing, and additional conditions for special category and criminal offence data (with the conditions in the Data Protection Act 2018);
- transparency information for individuals, and their rights of access, rectification, erasure, restriction, portability and objection;
- records of processing, data protection by design and by default, and data protection impact assessments for high-risk processing;
- security appropriate to the risk, and breach notification to the ICO **within 72 hours** where the breach is likely to result in a risk to individuals;
- contracts with processors, and Data Protection Officers where mandatory.

Organisations outside the UK that offer goods or services to, or monitor, individuals in the UK are generally in scope and may need a **UK representative**. Most UK organisations that process personal data must also pay the annual **data protection fee** to the ICO unless exempt.

3 What changed under the DUAA

Area	Change
Recognised legitimate interests	A new lawful basis for a defined list of purposes, such as crime prevention, safeguarding vulnerable individuals, emergencies and national security. For these purposes you do not need to carry out the usual legitimate interests balancing test.
Legitimate interests examples	The UK GDPR now gives examples of processing that may be carried out for legitimate interests, such as direct marketing, intra-group transmission for administrative purposes, and network and information security. The balancing test still applies to these.
Further processing	Clearer rules on when a new purpose is compatible with the original one, including listed compatible purposes.
Research	A clarified definition of scientific research, and more flexibility on consent to broad areas of research.
Automated decision-making	Articles 22A to 22D replace the old Article 22. Significant decisions based solely on automated processing are permitted more widely, but only with safeguards: information, the ability to make representations, human intervention, and the ability to contest. Stricter limits remain where special category data is involved.
Subject access requests	Organisations only need to make reasonable and proportionate searches. The time limit can be paused while they wait for information they reasonably need, for example to clarify the request.
Complaints	Controllers must have a process for data protection complaints. It must allow complaints to be made electronically, acknowledge them within 30 days, investigate without undue delay, and tell the complainant the outcome.
Children	Online services likely to be used by children must take account of children's higher protection needs when designing data protection measures.
International transfers	A new "data protection test" for UK adequacy-style decisions: protection in the destination must not be materially lower than in the UK.
Cookies and similar technologies (PECR)	New exemptions from consent for certain low-risk uses, such as some analytics, appearance and security purposes, provided users get clear information and a simple way to object.
PECR enforcement	Maximum fines for PECR breaches are aligned with UK GDPR levels.

Use the ICO's detailed guidance

Each change has conditions and limits that this summary cannot cover. The ICO has published a summary of the changes and topic-specific guidance; check it before relying on a new basis or exemption.

4 ICO expectations in practice

Accountability

The ICO expects organisations to show what they do. That means policies, records of processing, training, assessments and the evidence behind decisions, kept proportionate to the size of the organisation and the risk of its processing.

Rights handling

- Respond to requests within one month, extendable by up to two further months for complex or numerous requests.
- Use the "reasonable and proportionate search" standard deliberately, and record the reasons for the searches you made.
- Log the date you paused the clock and why, so the timeline is auditable.

Complaints handling

- Publish how to complain, with an electronic option such as an online form.
- Acknowledge within 30 days, investigate, keep the complainant informed and report the outcome.
- Individuals can still complain to the ICO. Your process does not replace that right.

Breaches

Report notifiable breaches to the ICO within 72 hours of becoming aware. Tell individuals without undue delay where there is a high risk to them, and record all breaches internally.

5 International transfers

Transfers outside the UK need one of the following:

- UK adequacy regulations ("data bridges") for the destination;
- appropriate safeguards, most commonly the UK **International Data Transfer Agreement (IDTA)** or the **UK Addendum** to the EU Standard Contractual Clauses, or Binding Corporate Rules;
- a limited exception for specific situations.

When using the IDTA or the Addendum, carry out and record a transfer risk assessment.

6 Enforcement

Tier	Maximum fine
Standard maximum	£8.7 million or 2% of total worldwide annual turnover, whichever is higher
Higher maximum (for example principles, lawful bases, rights and transfers)	£17.5 million or 4% of total worldwide annual turnover, whichever is higher

The ICO can also issue reprimands, enforcement notices and assessment notices. Individuals can seek compensation through the courts.

7 Programme checklist

Update for the DUAA

- [ ] Review lawful bases: identify any processing that may now rely on recognised legitimate interests, and record why.
- [ ] Review automated decision-making against Articles 22A to 22D, and put the required safeguards in place.
- [ ] Update the subject access procedure for reasonable and proportionate searches and the pause rule.
- [ ] Put a complaints process in place: electronic channel, 30-day acknowledgement, investigation and outcome.
- [ ] Review cookies and similar technologies against the new PECR exemptions, keeping clear information and an easy way to object.
- [ ] Update privacy information to reflect any changes in bases, rights handling or complaints.

Core programme

- [ ] Pay the data protection fee (unless exempt), and appoint a UK representative if required.
- [ ] Keep records of processing current, with lawful bases and retention for each activity.
- [ ] Screen new processing for DPIA requirements, and complete DPIAs before launch.
- [ ] Hold compliant processor contracts and track sub-processors.
- [ ] Map transfers and their mechanisms (data bridges, IDTA or Addendum), with transfer risk assessments.
- [ ] Test the breach response process against the 72-hour window.
- [ ] Keep evidence of policies, training and decisions, and review the programme at least annually.

8 Official sources

- Data (Use and Access) Act 2025: legislation.gov.uk/ukpga/2025/18
- The Data (Use and Access) Act 2025 (Commencement No. 6 and Transitional and Saving Provisions) Regulations 2026: legislation.gov.uk/uksi/2026/82
- GOV.UK, Data (Use and Access) Act 2025: plans for commencement: gov.uk
- ICO, the Data (Use and Access) Act 2025: summary of the changes: ico.org.uk
- ICO guidance on the UK GDPR, international transfers and the data protection fee: ico.org.uk

About this guide

This guide summarises publicly available legislation and regulator guidance in our own words, as of the review date above. Laws, rules and regulator guidance change; always check the current official text and obtain advice appropriate to your organisation's circumstances.

EdgeGRC and Cyber Intelligence Private Limited is an Indian technology company focused on developing software platforms for enterprise privacy management and AI governance. Questions about this guide: **info@edgegrc.com** · edgegrc.com