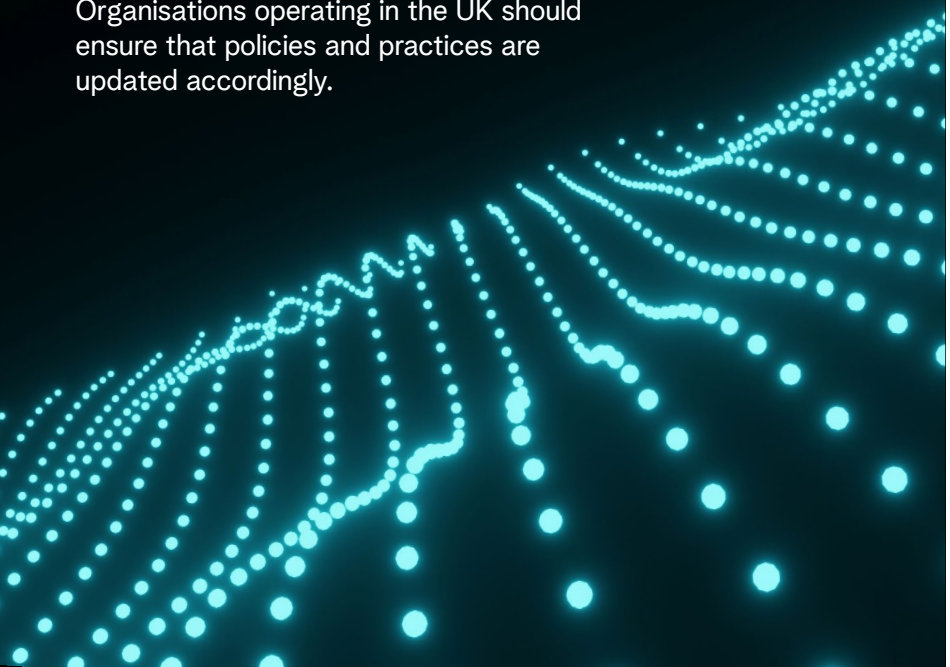
WALKER MORRIS

The Data (Use and Access) Act 2025

Key elements of the Data (Use and Access) Act 2025 (**DUAA**) came into force on 5 February 2026.

The DUAA amends the UK General Data Protection Regulation (**UK GDPR**), the Privacy and Electronic Communications (EC Directive) Regulations 2003 (**PECR**) and the Data Protection Act 2018 (**DPA**). The full list of provisions is available here.

Organisations operating in the UK should ensure that policies and practices are updated accordingly.



What's new?

Automated decisionmaking (ADM)

- The DUAA relaxes the previous restrictions on the use of personal data in ADM.
- The prohibition on ADM now applies only where significant ADM involves special category data, such as data revealing racial or ethnic origin, health information, religious beliefs or sexual orientation.
- Where significant ADM does not involve special category data, organisations may be able to rely on a wider range of lawful bases, including legitimate interests.
- In all cases, appropriate safeguards continue to apply, including UK GDPR transparency requirements and the right for individuals to challenge decisions made by ADM.

Cookies and the PECR

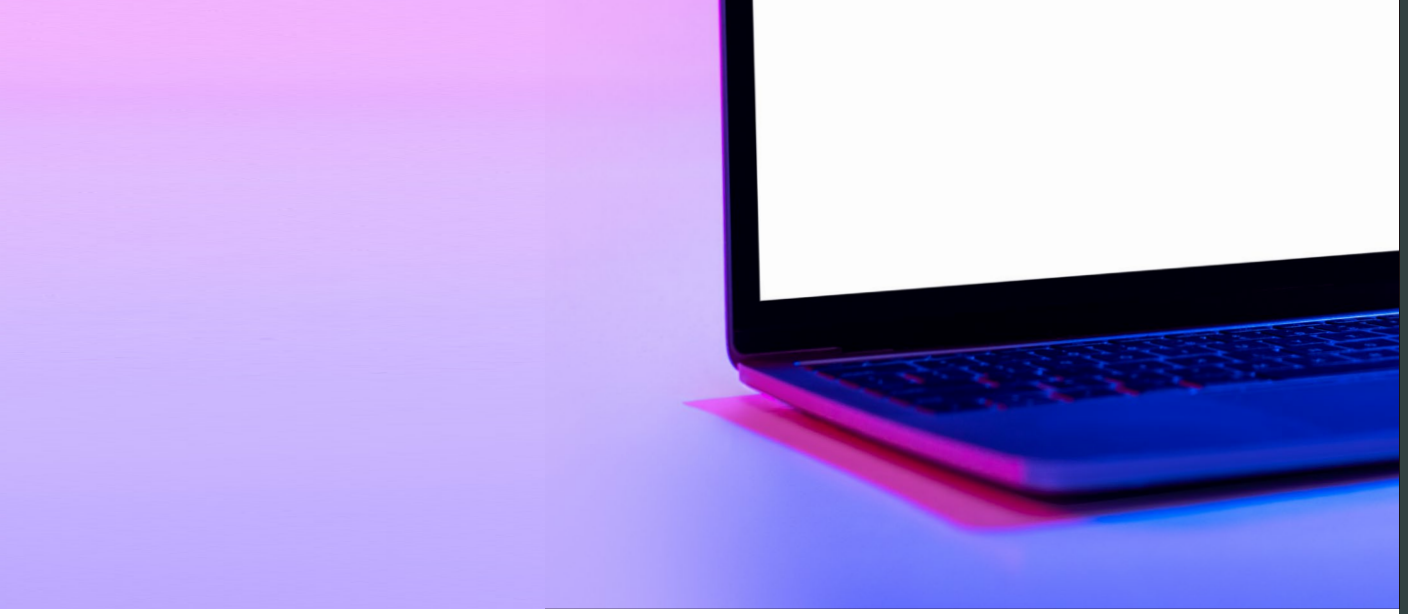
- The DUAA widens when website cookies can be used without consent. Consent is no longer required for:
  - » statistical cookies used solely for analytics;
  - » appearance cookies (for example, those managing language or display preferences); and
  - » emergency assistance cookies used for identifying geolocation on user request.
- For statistical and appearance cookies, organisations must still offer users a clear and accessible way to opt-out.
- Consent is still not required for "strictly necessary" cookies, which now explicitly includes cookies used for authentication, fraud prevention and technical fault detection.
- At the same time, maximum fines under the PECR have increased from £500,000 to align with UK GDPR thresholds (£17.5 million or 4% of global annual turnover), meaning that noncompliance with cookie and direct marketing rules now carries significantly greater regulatory risk.

Recognised legitimate interests

- The DUAA introduces a new lawful basis for processing personal data, known as "recognised legitimate interests". This applies to certain types of processing that are considered necessary, including activity relating to:
  - » national security, public security and defence;
  - » the detection, investigation and prevention of crime,
  - » responding to requests from public bodies acting in the public interest; and
  - » safeguarding vulnerable individuals.
- Where processing falls within these recognised legitimate interests, organisations are not required to carry out a separate legitimate interests balancing test.

International data transfers

- The DUAA updates the approach to international data transfers by replacing the EU's "essential equivalence" test with a UK-specific standard based on whether data protection is "not materially lower" than in the UK.
- The Information Commissioner's Office (**ICO**) updated its international transfers guidance earlier this year to reflect this change, which can be viewed here.



What's next?

Data protection complaints

The DUAA is set to introduce a new right for individuals to raise data protection complaints directly with organisations. In preparation, organisations will need to have appropriate arrangements in place, including:

- clear and accessible complaints processes;
- arrangements to ensure complaints are acknowledged within 30 days of receipt;
- procedures to investigate complaints and respond without undue delay; and
- procedures to keep complainants informed of progress and outcomes.

The ICO has already published new complaints guidance here. Organisations should review and update complaints procedures ahead of the provisions coming into force on 19 June 2026.

The final tranche of DUAA reforms relating to ICO governance and a transition to a new "Information Commission" structure is expected later in 2026, with further ICO guidance to follow.

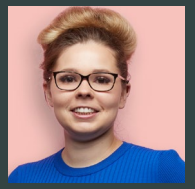
How we can help

The Walker Morris Regulatory & Compliance team deals with all aspects of data protection compliance, privacy and cybercrime. We monitor the legal landscape to provide you with timely updates.

We can help you with the preparation and updating of policies and procedures and with the provision of staff training, to ensure you stay on the right side of data protection laws including the UK GDPR, the PECR, the DPA 2018 and now, the DUAA.

We can also deal urgently and effectively with data subject requests and data breaches and advise on appropriate strategic responses. For more information, you can try our interactive cybersecurity and DSAR risk assessment tool here.

ANDREW NORTHAGE
Partner
+44 (0)771 170 4434
andrew.northage@walkermorris.co.uk



GRACE PARKIN
Senior Associate
+44 (0)770 309 9849
grace.parkin@walkermorris.co.uk

JOCELYNE GIRGIS
Associate
+44 (0)758 588 3144
jocelyne.girgis@walkermorris.co.uk