Data (Use and Access) Act Policy

Key provisions of the Data (Use and Access) Act 2025 (DUA Act) came into effect on 5 February 2026 under The Data (Use and Access) Act 2025 (Commencement No. 6 and Transitional and Saving Provisions) Regulations 2026.

The Data (Use and Access) Act (DUAA) amends, but does not replace, the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA) and the Privacy and Electronic Communications Regulations (PECR).

Businesses that are subject to the UK GDPR and/or The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) should ensure that policies and practices reflect this tranche of amendments to UK data protection law.

Key changes that took effect on 5 February 2026

Automated decision-making

The DUA Act narrows the general prohibition on the use of personal data for solely automated decision-making (ADM) for significant decisions affecting data subjects.
In other words, if you are processing 'special category' data e.g. health data, you are prohibited to use this in any automated decision-making system or platform, where significant decisions could affect data subjects.

(A data subject is any living individual who can be identified, directly or indirectly, by personal data, such as a name, ID number, location data, or online identifier. They are the human beings whose personal information is collected, stored, or processed by organisations).

Automated decision-making that is based on special category data must continue to rely on specific legal bases for processing under UK GDPR (for example, explicit consent). This would be where the individual has been provided with knowledge about the activity which involves automated decision-making, understands why their personal data is being used and gives explicit consent in writing to go ahead.

Safeguards (such as transparency and contestability requirements) will apply to all significant automated decision-making based on personal data.

Cookie consent

Cookies are small text files placed on a user's device by websites to remember information, such as login status, shopping cart items, or browsing preferences.
The DUA Act clarifies and expands the circumstances in which consent for cookies will not be required under the Privacy and Electronic Communications Regulations (PECR).

It will no longer be necessary to obtain cookie consent for:

- Statistical cookies – cookies that solely collect information for statistical purposes about the use of the service;
- Appearance cookies – cookies that adapt appearance of the service according to the user's preferences (e.g. displaying the website in a different language);
- Emergency assistance cookies – cookies that are used to find the geolocation of the user of a device in order to provide emergency assistance after a request from the user.

The DUA Act specifies that for 'statistical and appearance cookies', controllers and processor must still provide an informed and simple opt-out mechanism shown on their website.

It will remain the case that cookie consent is not required for 'strictly necessary' cookies (for example, those that an online service could not operate without). The DUA Act also provides examples of cookies falling under the 'strictly

necessary' exemption, such as cookies that automatically authenticate users, that prevent or detect technical faults when providing a service, and that prevent or detect fraud when providing a service.

The DUA Act also amends PECR to state that references to 'storing information, or gaining access to information stored, in the terminal equipment of a subscriber or user' (cookies and similar technologies) includes "instigating" the storage or access.

Recognised legitimate interests

The DUA Act introduces a new legal basis for data processing – 'recognised legitimate interests'. The following processing activities are considered recognised legitimate interests under the DUA Act:

- processing necessary for national security, public security and defence purposes;
- processing necessary for the detection, investigation or prevention of crime;
- responding to requests made by bodies acting in the public interest, for processing by those bodies for purposes laid down in law (for example, to help a government agency discharge its duties and functions); or
- processing necessary for the safeguarding of vulnerable individuals.

Processing personal data based on 'recognised legitimate interests' under the UK GDPR will not require a further 'balancing test' to be carried out (that is, balancing Amazon's legitimate interests against the privacy rights of data subjects).

Research and statistical purposes

The DUA Act defines "research and statistical purposes" to include "any research that can reasonably be described as scientific, whether publicly or privately funded and whether carried out as a commercial or non-commercial activity". This aligns the substantive provisions of the UK GDPR with existing recitals and regulatory guidance to encourage a broad interpretation of the concept of scientific research, such that the UK GDPR's purpose limitation principle, and its restrictions on the processing of special category data, are less likely to restrict processing for such purposes provided certain safeguards are met. The DUA Act also clarifies that data subjects can give "broad consent" for processing of their data for an area of scientific research in certain circumstances.

Purpose limitation and further processing

The DUA Act clarifies the circumstances under which personal data may be re-used for purposes different to the purposes for which the personal data was originally collected. Depending on the original legal basis relied on, purposes deemed to be compatible for further processing may include:

- research, archiving or statistical purposes
- detecting, investigating or preventing crime.

The DUA Act also sets out factors that controllers should consider when determining "purpose compatibility" for data re-use in other circumstances (for example, possible consequences for data subjects of the proposed processing, and the existence of appropriate safeguards).

PECR fines increased

Previously fines for breaches of PECR were limited to £500,000. DUA Act now brings maximum fines under PECR to UK GDPR levels (that is, £17.5 million or 4% of global annual turnover). PECR is the instrument that implements the EU's ePrivacy Directive into UK law, regulating cookies and email marketing, among other things. These changes raise the stakes for non-compliance with PECR requirements.

The ICO's enforcement toolkit expanded

The ICO is newly empowered to:

- require the preparation of a report at the expense of the controller or processor being investigated (by way of illustration, this might be a report setting out findings from an internal investigation into how unauthorised access to a restricted database occurred);
- compel a witness (e.g. a manager or employee) to attend interview, where giving a false statement in response to an interview question would be an offence; and

- by way of issuing an information notice, require not only the provision of general information but the production of specific documents (for example, a data protection impact assessment or transfer risk assessment).

The international data transfer test reformulated

The DUA Act reformulated the test for assessing a third country's adequacy in connection with international data transfer. The newly introduced "data protection test" requires the Secretary of State to assess whether the standard of protection in a third country in respect of a transfer is "not materially lower" than the standard in the UK. The data protection test is also to be applied by controllers and processors before they may transfer personal data to a third country in reliance on "appropriate safeguards" (such as standard contractual clauses). It remains to be seen whether this proves to be a meaningful distinction compared with the "essential equivalence" test referred to in the EDPB's guidance and in judgments of European Union courts. The UK Government is also empowered to approve new clauses which are capable of securing that the data protection test is met.

On 15 January 2026, the ICO updated its guidance on international transfers, including by replacing the EU's "essentially equivalent" adequacy test with the new "not materially lower" data protection test.

Complaints from data subjects

Creates a right for data subjects to complain directly to controllers in relation to infringements of data protection law (to exist alongside the existing ability to lodge complaints with the ICO). Controllers must facilitate the making of such complaints, for example by providing a complaint form "which can be completed electronically and by other means", and must acknowledge complaints within 30 days, take appropriate steps to resolve the complaint without undue delay, and inform the data subject of both progress and the outcome. Businesses that use the EU GDPR as their high-water mark for data protection obligations should take special note, as these provisions now exist in the UK GDPR but do not exist in the EU GDPR.

Are you ready?

Businesses should consider the increased PECR fines when assessing their compliance with cookies and direct marketing practices. The expanded ICO enforcement powers raise the stakes for engagement for regulatory engagement. Businesses should also review their data protection policies and practices to ensure that DUA Act amendments are now reflected. For example, where processing activities are based on recognised legitimate interests, you will need to update records of processing and privacy notices, and may wish to deprecate historical legitimate interest assessments.

Background

Since Brexit, the UK has sought to modernise its data protection laws to maintain high standards while easing administrative burdens on businesses. Previous efforts with the DPDI Bill failed, but the Labour Government has revived a more modest set of reforms under the DUA Bill. The goal is to modernise data laws while safeguarding the UK's "adequacy" status, which is essential for seamless data flows between the EU and the UK.

Key updates to UK GDPR and DPA 2018

The DUA Bill introduces several significant changes:

- **Legitimate Interests**: the Bill defines different types of processing that automatically qualify as "legitimate interest", such as processing for "direct marketing" (widely defined), intra-group transfers and for network security.
- **Recognised legitimate interest**: a new ground for lawful processing allows processing necessary for purposes like national security, public safety or emergency response, outlined in a new annex to UK GDPR.
- **Data Subject Access Requests (DSARs)**: A change that will be welcomed by many businesses on the wrong end of DSARs from a disgruntled or ex-employee is that a controller will only need to conduct searches that are "reasonable and proportionate." However, an express exemption for "vexatious" requests—proposed in the

DPDI Bill—has been omitted. It also confirms a procedure enabling the courts to inspect withheld material to determine whether it is exempt from disclosure.

- **Purpose Limitation**: clarifies when personal data can be used for purposes beyond the original intent, with certain scenarios like public interest research or statistical analysis) deemed compatible.
- **Cookies**: The Bill simplifies pop-ups by removing the need for consent for low-risk cookies, such as those used for statistical purposes or to improve websites. It also defines when a cookie is "strictly necessary" (e.g., for fraud prevention, user safety, or maintaining user preferences). Transparency requirements remain, but consent will often no longer be needed. On the other hand, GDPR-level fines (up to 4% of global turnover) will now apply to breaches of cookie rules, replacing the current £0.5m cap.
- **Automated Decision-Making (ADM)**: The Bill allows ADM with To facilitate increased use of AI for ADM (where there is "no meaningful human involvement in the taking of the decision"), the Bill provides that, apart from cases using "special categories" of data, ADM resulting in a legal or similarly significant effect will no longer be prohibited with exceptions. Instead, ADM will be possible regardless of the lawful basis, as long as suitable safeguards are in place. This includes reliance on legitimate interests as a lawful basis, except for cases involving "special categories" of data.
- **Scientific Research**: provides a clearer definition of "scientific research" and guidance on when consent is needed.
- **Complaints Process**: requires controllers to take "appropriate steps" to facilitate data subject complaints, such as by providing a complaints policy or online form. It also paves the way for regulations requiring controllers to notify the Information Commissioner of the number of complaints received.
- **International Data Transfers**: Introduces a less stringent adequacy test for third countries, requiring protection to be "not materially lower" than the UK's. This could allow more countries to achieve UK adequacy but may complicate the EU's adequacy review of the UK in 2025.

What's Missing?

The Bill excludes some of the more controversial proposals from the DPDI Bill, such as removing the requirement for Data Protection Officers (DPOs), redefining "personal data," and relaxing Data Protection Impact Assessment (DPIA) obligations. These omissions likely aim to preserve the UK's adequacy status with the EU.

Beyond Data Protection

At over 260 pages, the Bill covers more than data protection. As the title of the Bill indicates, it includes sections related to the use of and access to data more generally, including:

- use of "smart data" (supporting open banking and the development of new smart data schemes such as in respect of utilities);
- establishing a "trust mark" for approved digital verification services;
- simplifying data use for law enforcement and the NHS, including enabling easier patient data transfers;
- creating a national map of the UK's underground infrastructure (pipes and cables).

This broader approach reflects aspirations similar to the EU's Data Act, treating data as a shared asset for businesses and consumers alike.

The Government aims to "put technology and data protection at the heart of the economy" by simplifying rules to make data laws more business-friendly while maintaining high standards. Supported by the ICO (soon to be known as the Information Commission), the Bill seeks to modernise the UK's data framework without jeopardising EU adequacy status, which comes up for review in June 2025.

The expectation is that the Bill will be finalised before this review. However, amendments may still arise, so watch this space for further updates.