muckle LLP

Data (Use and Access) Act 2025

Frequently Asked Questions (FAQs)

The Data (Use and Access) Act 2025, or DUAA, makes important changes to UK data protection laws. It also includes some of the publicly available guidance to help organisations better understand complicated areas and improve their overall knowledge of what they need to do to comply with the law.

What is the Data (Use and Access) Act 2025 (DUAA)?

The DUAA is the latest development in updating the UK data protection legislation, which consists of the Data Protection Act 2018, the UK GDPR, and the Privacy and Electronic Communications Regulations (PECR) 2003.

When will the Data (Use and Access) Act 2025 (DUAA) come into effect?

The DUAA will come into effect in phases. It is anticipated that this will happen within two, six, and 12 months after the DUAA came into force (19 June 2025). It is advised organisations should follow the old data protection regime in the meantime.

What is classed as a 'recognised legitimate interest' under the Data (Use and Access) Act 2025 (DUAA)?

- When controller one requests personal data from controller two to carry out a public interest task, the DUAA permits sharing.
- When the processing is necessary for national security, public safety, or defence.
- In response to emergencies under the Civil Contingencies Act 2004, such as threats to human welfare, the environment, or national security (e.g. war or terrorism).
- For detecting, investigating, preventing crime, or prosecuting offenders.
- To safeguard a child or vulnerable adult.

Do organisations have to carry out a Legitimate Interests Assessment (LIA) under the new Data (Use and Access) Act 2025 (DUAA)?

If you're relying on recognised legitimate interests for your processing, then no. Unlike the previous regime, the recognised legitimate interests do not require an organisation to undertake an LIA.

Can charities use soft opt-ins under the Data (Use and Access) Act 2025 (DUAA)?

Charities can send marketing emails directly to people who have supported them before or shown interest in their work, without needing explicit consent, using a rule known as the "soft opt-in."

However, this can only be done on the basis that the nature of the direct marketing is to further the charity's charitable purposes, and the individual has been given a simple means of refusing to have their contact details used for direct marketing at all times.

Can organisations reuse personal data under the Data (Use and Access) Act 2025 (DUAA)?

The DUAA lets organisations reuse personal data for a new purpose, as long as it's similar to the original one, without needing to carry out a full compatibility check. However, this only applies if your organisation is confident that the new purpose is genuinely compatible with the original one.

If your organisation is unsure whether the new purpose is compatible with the original purpose, it must complete a compatibility test before processing personal data for the new purpose.

What fines can the Information Commission (ICO) now issue under Privacy and Electronic Communications Regulations (PECR) for breaches to data protection legislation?

The ICO can issue fines of up to £17.5 million or 4% of the global annual turnover under PECR (which, under the previous data protection regime, only enabled the ICO to impose fines of up to £500,000).

How can people make complaints about their data rights?

Before contacting the ICO, individuals must first complain directly to the organisation. Under the previous rules, people could go straight to the ICO if they were unhappy with how their data rights request was handled. That's no longer the case — they must now give the organisation a chance to respond first.

How long do organisations have before responding to complaints about their data rights?

Organisations must set up a complaints process to handle these issues and respond within 30 days. To make things easier, the ICO recommends offering an online complaint form to help individuals submit their concerns.

How does the Data (Use and Access) Act 2025 (DUAA) classify automated decision making?

Automated decision-making is the process of making a decision by automated means without any human involvement. These decisions can be based on factual data, as well as on digitally created profiles or inferred data. Examples of this include:

- An online decision to award a loan.
- An aptitude test used for recruitment which uses pre-programmed algorithms and criteria.

When can organisations use automated decision-making?

The DUAA opens up the lawful bases (for example, legitimate interests), on which an organisation may rely to make significant automated decisions about individuals. However, they must have proper safeguards in place and meet extra requirements if they are using special category data.

Do organisations need consent to use website cookies to collect individual's data?

The DUAA will allow organisations to use some website cookies to collect an individual's technical and usage data without having to obtain their consent, for example, to collect personal data for statistical purposes and to improve the overall functioning of the website.

In relation to cookies that are used for marketing purposes (for example, targeting cookies), organisations must still comply with the requirements set out in PECR and obtain consent from the website user via a cookie pop-up before using their technical and usage data for marketing purposes.

For further information, call or email Rhiannon on:

Rhiannon Hastings
Paralegal
Commercial

T: 0191 211 7891
rhiannon.hastings@muckle-llp.com