7 Reforms To Note Under New UK Data Protection Law

By **James Castro-Edwards** (July 11, 2025)

James Castro-Edwards

The Data (Use and Access) Bill received Royal Assent on June 19, taking effect as the Data (Use and Access) Act 2025, or DUAA.

The act introduces a range of legislative measures around the use of data in the U.K., with the underlying aims of growing the economy, improving public services, creating a digital identity verification framework and reforming data protection law.

Most of the DUAA's provisions will take effect either two or six months from the date of royal assent, although some may take up to 12 months.

This article briefly discusses the evolution of the DUAA, provides an overview of its provisions with a particular focus on data protection and provides practical suggestions for practitioners responsible for data protection compliance.

Background

The DUAA is the culmination of a series of attempts to reform U.K. data protection legislation by the current and previous governments. The Data Protection and Digital Information Bill, or DPDI, was introduced in July 2022, and would have made significant changes to the U.K. General Data Protection Regulation and the Data Protection Act 2018.

The then Conservative government announced the DPDI as a Brexit dividend, demonstrating a benefit of the U.K. no longer being bound to follow European legislation. However, the DPDI was controversial, and risked the European Commission's adequacy finding that enabled the free flow of personal data to continue from the European Union to the U.K., post-Brexit.

A revised Data Protection and Digital Information (No.2) Bill was introduced in March 2023, which failed to complete the parliamentary so-called wash-up, following the Conservative government's defeat in the general election last year.

Following the general election, the Labour government introduced the Data (Use and Access) Bill to the House of Lords on Oct. 23, 2024. The bill retained many of the changes proposed by the DPDI, absent the more controversial provisions.

Overview of the DUAA

The changes the DUAA introduces extend further than data protection reform alone, and include the following.

Smart Data Schemes

Part 1 of the DUAA gives the science and technology secretary and HM Treasury the power to introduce so-called smart data schemes. New regulations will specify the scope of a scheme, including who is required to provide data and what data they must provide and how, as well as security and access controls.

For instance, open banking allows people to aggregate account information from different banks in order to see all their money in one place. Smart data schemes envisaged by the DUAA would extend the concept to other sectors, such as energy, giving consumers a better deal and boosting competition.

Digital Verification Services

Part 2 of the DUAA legislates digital verification services, by requiring the secretary of state to set out rules around trusted digital verification tools. These tools are intended to enable people to prove their identity online more easily, which will simplify important tasks, such as renting a flat or starting work.

The National Underground Asset Register

Part 3 of the DUAA introduces the National Underground Asset Register, a government scheme intended to provide instant access to a U.K.-wide map of underground pipes and cables for authorized users.

This will improve the installation, maintenance, operation and repair of buried infrastructure, providing a comprehensive view and enabling work to be conducted safely and efficiently, avoiding accidental strikes to underground cables and pipes during construction and repair.

Registers of Births and Deaths

Part 4 of the DUAA moves national registers of births and deaths from paper to digital format.

Bereaved Parents

Part 7 of the DUAA includes provisions intended to help bereaved parents obtain information in cases where social media is linked to the death of their child.

New laws will establish a data preservation process that will require the Office of Communications, known as Ofcom, when notified by a coroner, to issue a data preservation notice to social media companies supporting their investigations into the child's death.

Data Protection Reform Under DUAA

The DUAA reforms rather than replaces existing regulation. Part 5 amends the U.K. GDPR, the Data Protection Act and the Privacy and Electronic Communications (EC Directive) Regulations 2003, or PECR. It is a refinement of existing legislation rather than a radical overhaul.

The changes include the following.

1. Definition of Scientific Research and Changes to Rules on Consent to Scientific Research

The DUAA defines "scientific research" to encompass any research reasonably described as scientific, whether commercial or noncommercial. This includes technological development, fundamental or applied research and public health studies conducted in the public interest.

It also explicitly includes genealogical research as historical research and clarifies what qualifies as statistical processing, emphasizing that such processing must produce aggregate, nonpersonal data, without being used to make decisions about individuals.

Consent under the U.K. GDPR is expanded to include cases where full research purposes cannot be specified at the time consent was obtained, but where ethical standards are met and partial consent can be given.

2. Changes to Lawful Basis for Processing — Legitimate Interest

The DUAA introduces a new lawful basis for processing personal data. Processing necessary for a so-called recognized legitimate interest permits processing for a number of specified purposes, including direct marketing, internal group transmission and cybersecurity.

This change is likely to be welcomed by data protection advisers since it provides clarity by aligning the operative provisions of the U.K. GDPR with its recitals. The secretary of state may amend the list of recognized legitimate interests from time to time.

3. Clarification of Purpose Limitation Principle — And Exemption to Associated Transparency Requirements

The DUAA refines the so-called purpose limitation principle, emphasizing that data processing must be strictly for the purpose originally collected, unless the new purpose is compatible with the original purpose.

The DUAA provides a number of situations where further processing is compatible with the original purpose for which personal data were collected.

These include where the data subject has given fresh consent to the new purpose, where the processing is for scientific or historical research, where archiving is in the public interest, or where the processing is for any of the purposes specified in Annex 2.

Purposes specified in Annex 2 include where the processing is necessary for disclosure to a person carrying out a public interest task; public security; responding to an emergency; the detection, investigation or prevention of crime; protecting a data subject's vital interests; and safeguarding vulnerable individuals. The secretary of state may add, vary or omit provisions to Annex 2.

4. Data Subjects' Rights

The DUAA aligns the subject access provisions of the U.K. GDPR with existing Information Commissioner's Office, or ICO, guidance. For instance, stopping the clock where the controller cannot proceed with the response without further information from the data subject or proof of the data subject's identity.

The act also clarifies that controllers need only conduct a reasonable and proportionate search for information and personal data in response to a subject access request, which reflects current case law, although it does not provide further information on what constitutes a reasonable and proportionate search.

However, the proposal from the DPDI for controllers to be able to refuse a subject access request on the grounds that it is vexatious has been dropped. Accordingly, controllers will

still have to demonstrate that a request is manifestly unfounded or excessive in order to refuse to comply with a request.

5. Automated Decision-Making

The DUAA clarifies that a decision based on automated decision-making is one with no meaningful human involvement. It relaxes some of the current restrictions on the use of personal data, but not the use of special categories of personal data, such as health data, for the purposes of automated decision-making.

Controllers must consider the extent to which a decision has been made on the basis of profiling when establishing whether or not human involvement has been meaningful. A significant decision is one that results in legal or comparably significant effects on a data subject.

A significant decision based wholly or partially on the use of any of the special categories of personal data is prohibited unless the data subject has given their consent, the activity is necessary for the purpose of entering into or performing a contract, or is required by law.

6. Data Transfers

The DUAA introduces a more flexible, risk-based approach to data transfers, which aligns with the U.K.'s broader strategy to diverge from the EU, although not so far as to jeopardize the U.K. adequacy finding made by the commission.

The DUAA replaces Chapter V of the U.K. GDPR and requires the secretary of state, when assessing adequacy, to consider whether the standard of data protection in the country under consideration is materially lower than that of the U.K., and apply a data protection test, which must be considered in relation to the appropriate safeguards.

7. Changes to the PECR

The DUAA makes a number of changes to the PECR. In particular:

- New exemptions are provided to the requirement for consent to set cookies for collecting statistical information to improve the service: functional purposes, i.e., how an information society service is displayed; personalization cookies, which automatically authenticate a repeat user of digital services or repeat visitor to a website and maintain a record of settings or preferences; or where the sole purpose is to enable the geographical position of a user to be ascertained in response to an emergency communication.

- Charities are now permitted to rely on the soft opt-in.

- The ICO's enforcement powers are aligned with those available under the U.K. GDPR, i.e., maximum fines of the greater of £17.5 million ($23.8 million) or 4% of the previous year's worldwide annual turnover, compared to the previous maximum penalty of £500,000.

Likely Impact on U.K. Adequacy Decision

The DUAA includes many of the reforms proposed by the DPDI bill, although not the more radical changes, such as the DPDI's proposals to replace data protection officers, change the definition of personal data, amend the provisions relating to data protection impact assessments, extend the requirement to maintain a record of processing activities, or abolish the requirement to appoint a U.K. representative.

The DUAA diverges less from the GDPR than the DPDI would have done, reflecting the current government's desire for a reset and strengthening relationship with Europe.

The DPDI's more controversial changes threatened the U.K.'s adequacy decision made by the commission in 2021, which, following Brexit, enables the continued free flow of personal data from the EU to the U.K. and was set to expire on June 27. The commission has extended the U.K. adequacy decision by a period of six months to expire on Dec. 27, to allow the commission to assess the adequacy of the protection of personal data under the U.K. data protection regime, as amended by the DUAA.

The DUAA does not appear to be a significant departure from the standards of the GDPR. However, the renewal of the U.K. adequacy decision should not be treated as a foregone conclusion, albeit that it seems more likely than not.

Practical Considerations for Lawyers

The changes the DUAA makes to the U.K. GDPR, the Data Protection Act and the PECR are subtle, and should not necessitate substantial revision to organizations' data protection compliance programs.

The DUAA relaxes a number of requirements and many of the changes reflect the U.K. GDPR's recitals and ICO guidance.

Nonetheless, organizations would be prudent to review their data protection policies and procedures, to ensure that they reflect the new law. This is advised particularly around electronic direct marketing, in light of the increased maximum fines for breaches of the PECR.

A substantial proportion of the ICO's enforcement activity relates to noncompliant direct marketing activities, so penalties for the PECR breaches are a real possibility.

Organizations must also monitor the status of the U.K. adequacy decision: In the seemingly unlikely event that this is not renewed by the commission, businesses would need to move quickly to develop a data transfer solution, such as the standard contractual clauses or binding corporate rules, and a transfer risk assessment.

James Castro-Edwards is counsel at Arnold & Porter Kaye Scholer LLP.