VAN BAEL & BELLIS

28 August 2025

A New Era for UK Data Protection Law: Reform of the UK GDPR and Proposed renewal of EU Adequacy

The United Kingdom (***UK***) data protection legal framework has been reformed. The Data (Use and Access) Act 2025 (***DUAA***) received Royal Assent on 19 June 2025 and while some of its provisions came into force automatically, others will be commenced via regulations issued by the Secretary of State in four main stages, the first of which took effect on 20 August 2025.

The DUAA has introduced substantial reforms to UK data protection law, i.e., the UK General Data Protection Regulation (***UK GDPR***) (supplemented by the Data Protection Act 2018) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (***PECR***). Rather than replacing the existing legislation, the DUAA delivers a series of targeted adjustments aimed at increasing legal clarity and reducing administrative burden, particularly in artificial intelligence (***AI***)- driven and research-intensive sectors. In the words of the Information Commissioner's Office (***ICO***), the DUAA was introduced to promote "*innovation and economic growth*" whilst "*still protect[ing] people and their rights*".

Concurrently, as the UK charts its own regulatory path, the European Union (***EU***) intends to confirm the UK's adequacy status under both the GDPR and the Law Enforcement Directive (***LED***). On 22 July 2025, the European Commission (***EC***) published two draft decisions proposing a six-year renewal, under both the GDPR and the LED, of the UK's status as a country offering an adequate level of protection for the purposes of international transfers of personal data.

DUAA 2025: Strategic Pivot in UK Data Law

The DUAA introduces a broad set of reforms that recalibrate the UK's personal data protection rules. The most important reforms include:

- Section 80 DUAA: modernises **automated decision-making** (***ADM***) that has legal or similarly significant effects on individuals by allowing data controllers to use ADM more widely if data subjects are appropriately informed, can challenge outcomes and have access to human intervention. Nonetheless, restrictions on special categories of personal data – such as biometric data – remain but can be lifted by consent, contract, or a legal obligation.

- Sections 67-68: give **more flexibility for scientific research, including commercial scientific research** (e.g., a pharmaceutical company developing new medicinal products), subject to appropriate safeguards outlined in Section 86. It now explicitly recognises historical research (including genealogical research) and allows processing of personal data for technological development or demonstration, fundamental or applied research, or public health research. Processing for statistical purposes must produce aggregate, non-personal data. Researchers can also obtain broad consent for studies (or parts thereof) for which the full scope is not yet determined provided ethical standards are met.

- Section 70: introduces "**recognised legitimate interest" as a specific legal basis for processing personal data**. This covers a subset of pre-approved purposes – listed in the newly added Annex I to the UK GDPR which the Secretary of State may amend by regulation. The current list includes, among other purposes, national security, public security and defence, safeguarding vulnerable people and emergency response. Where a listed purpose applies, there is a presumption that the interest is legitimate and no assessment of whether it overrides individuals' data protection rights is required (i.e., the three-step balancing test will not be required for legitimate interests on this list). In addition, the DUAA contains a separate list of purposes that are presumed to constitute a "legitimate interest", but for which a balancing test will still be required. This second list includes processing activities for purposes of direct marketing, intra-group data transfers and cybersecurity. The DUAA provides that such processing operations "*may be processing that is necessary for the purposes of a legitimate interest*", thus facilitating step 1 of the three-step test.

- Section 71: sets out new **purpose limitation rules**, giving more operational leeway **for "further processing"**. It allows for data reuse for public security, responding to an emergency or vital interests of data subjects and others, as outlined in the new Annex 2 to the GDPR that can be updated over time.

- Section 85: **replaces the adequacy framework for international transfers of personal data with a new "data protection test"**, under which the Secretary of State may determine if a third country or an international organisation has a standard of data protection which is "*not materially lower*" than the standard in the UK. This departs from the EU "adequacy decisions" approach and sets an independent basis for the recognition of other jurisdictions.

- Sections 112-114: **expand the usage of cookies without consent in low-risk scenarios** such as functionality or basic analytics. It also allows the use of location-based cookies in emergencies, such as during natural disasters or urgent safety threats, and extends the soft opt-in rule to non-commercial entities such as charities, allowing them to send direct marketing without prior consent if the recipient previously interacted with them and can easily opt out.

- Sections 75-79: clarify **data subject access rights**, where the DUAA formalises the "*stop the clock*" mechanism for additional information requests and limits searches for the personal data requested to those that are "*reasonable and proportionate*". The existing threshold for refusing manifestly unfounded or excessive requests remains unchanged.

- Section 81: **strengthens protections for children's data online** by requiring child-focused design. Online services likely to be accessed by children – such as social networks, gaming platforms, and e-commerce sites – must take their needs into account when deciding how to use their personal data.

- Finally, the DUAA updates the rules on the use of personal data for **law enforcement purposes** and replaces the ICO with the **Information Commission**, providing it with stronger enforcement powers (Part 6 DUAA). Administrative fines for breaches of the PECR increase to GDPR levels, i.e., to a maximum of GBP 17.5 million or 4% of total global turnover, whichever is higher (Schedule 13).

EU Adequacy Decisions: Renewed Confidence Amid Cautious Divergence

After Brexit, the UK became a third country under EU data protection law and, as a result, transfers of personal data from the EU/EEA to the UK require a specific legal basis (i.e., adequacy, appropriate safeguards or derogations). To facilitate such transfers, in 2021, the EC issued two adequacy decisions allowing for the continued free flow of personal data from the EU/EEA to the UK, one under the GDPR and another under the LED. After a technical extension (for both the GDPR and for the LED) due to the (then pending) UK reform, these decisions are now set to expire on 27 December 2025.

The EC has now issued proposals to renew these adequacy findings for another six years. The draft documents, published shortly after the DUAA received Royal Assent, assessed UK data protection law and concluded that UK law continues to offer protections that are essentially equivalent to EU standards, despite certain reforms introduced by the DUAA.

The draft decisions await formal approval by EU Member States through the comitology procedure, in which national representatives vote on the EC's proposal, and a non-binding opinion from the European Data Protection Board (***EDPB***). While not final, the timing and the EC's positive assessment suggest likely adoption before the December 2025 expiry of the current adequacy decisions.

Consequences

For entities operating both in the UK and the EU, the diverging regulatory landscape presents a complex blend of opportunity and challenge. On the one hand, the DUAA introduces more permissive, innovation-focused and sector-aware data protection rules within the UK, aimed at offering increased flexibility, and reducing compliance burden. On the other, however, for such entities, continued alignment also with EU requirements remains critical. As a result, practices adopted under the reformed UK data protection law should be reviewed to ensure they do not compromise compliance with its EU counterparts.

With the UK's DUAA, compliance with data protection law is no longer 'one-size-fits-all': alignment exists, but uniformity is gone. And with the proposed EU renewal of the UK's adequacy status, signalling continued fundamental alignment despite regulatory divergence, personal data are likely to keep being transferred freely from the EU/EEA to the UK.

Thibaut D'hulst
Dariusz Kloza
Ajla Memic

Lawyers to contact

Thibaut D'Hulst
Counsel
tdhulst@vbb.com

Brussels office
Glaverbel Building
Chaussée de La Hulpe 166
B-1170 Brussels
Belgium

Phone:+32 (0)2 647 73 50

Geneva office
2, Chemin des Mines
CH-1205 Geneva
Switzerland

E-mail: geneva@vbb.com

London office
Holborn Gate
330 High Holborn
London
WC1V 7QH
United Kingdom

Phone: +44 (0)20 7406 1471

VAN BAEL & BELLIS

www.vbb.com