

June 23, 2025

# The UK's Data Protection Reforms Finally Arrive: What You Should Know About the Data (Use and Access) Act

On June 19, 2025, the UK's Data (Use and Access) Act 2025 (the "Act")<sup>1</sup> came into force, following an extended period of Parliamentary 'ping pong' between the House of Commons and the House of Lords. The Act seeks to modernise the UK's data protection regime and provide a boost to business and innovation, while still upholding the principles of the UK GDPR<sup>2</sup>. Significantly, the Act marks the UK's first express divergence from the EU GDPR<sup>3</sup>, with eyes now turning to Brussels' reaction. This alert summarises the key changes to UK data protection legislation adopted through the Act and identifies key practical takeaways for data controllers.

## Key Takeaways

- Divergence from EU GDPR.** In most cases, the UK's divergence from the EU GDPR is to decrease the burden on UK businesses (e.g., fewer obligations relating to automated decision making, legitimate interests, data subject access requests and cookies), although the UK has also taken steps to increase enforcement power in relation to direct marketing activities (a step that has been stuck in EU legislative process for many years). The result is that businesses that operate in both the UK and EU will need to consider how to comply with divergent legislation (using lowest common denominator vs different compliance model in each jurisdiction).
- UK Adequacy.** With the UK's adequacy decision from the EU expiring at the end of 2025, there will be speculation whether these changes (albeit not individually significant) could affect renewal. If not renewed, there could be additional administrative burdens on EU businesses transferring personal data to the UK (e.g., via implementation of additional standard contractual clauses).
- Watch this space.** Most of the Act's provisions do not come into force until secondary legislation is implemented (for which no clear timeframe has been provided). Additionally, the Act creates a number of governance changes for the UK regulator and the ability for the Government to add to the Act, which will require careful monitoring. Finally, after significant and heated debate, the Government ultimately did not accept any provisions regarding transparency for use of proprietary data in AI tools. The Government has promised to finalise a review within nine months, but it is uncertain whether the end result will match the EU's text and data mining exceptions or take another approach.

<sup>1</sup> Available here: <https://www.legislation.gov.uk/ukpga/2025/18/enacted>

<sup>2</sup> Available here: <https://www.legislation.gov.uk/eur/2016/679/contents>

<sup>3</sup> Available here: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>

### Summary of Legislation

In addition to specific provision regarding digital verification services, scientific research, data on national infrastructure apparatus, the UK birth and death register, law enforcement processing, children's data in online services, national security and the role of the UK regulator, the Act introduced the following key provisions:

- **Automated Decision-Making.** The Act narrows the range of situations in which the UK GDPR's requirements around automated decision making ("ADM") apply, now only requiring additional safeguards for "significant decisions" that entirely or partly use ADM (i.e., decisions producing an adverse legal or similarly significant effect on the data subject) and for situations where special category personal data is not involved. Crucially, the Act removes data subject rights to object to ADM in any other circumstances, providing a significant boost to business' freedom to deploy ADM (in particular, through the use of AI tools).
- **Legitimate Interests.** Certain recognised legitimate interests have been inserted into the UK GDPR, allowing organizations to rely on them without conducting a legitimate interests assessment (with the power for the Government to expand this list). These recognised legitimate interests comprise processing under public interest criteria, for national security or defence, for responding to emergencies, if necessary for detecting, investigating or preventing crime, or for safeguarding a vulnerable individual. The Act also amends the UK GDPR to make clear that processing of personal data for direct marketing, intra-group administration and security of IT systems are all types of processing that may be considered necessary for the purposes of the existing legitimate interests test in Article 6(1)(f) UK GDPR. This will be welcome news for reducing the administrative burden on internal data protection compliance functions in the UK.
- **Purpose Limitation.** The Act updates the UK GDPR to formalise UK Information Commissioner's Office's ("ICO") guidance on when processing by a controller for a new purpose will be considered compatible with the original purpose. The core tenets are that: (i) there must be consideration of the links between the purposes, the context of original collection, the types of personal data, the consequences for the data subjects and the existence of appropriate safeguards; (ii) processing for a new purpose will be expressly permitted where there is data subject consent, where the new processing is for research, archiving or statistical purposes, or where certain other criteria are met (e.g. national security or legal obligations); and (iii) the controller does not need to inform the data subject of the new processing if it would be impossible or involve a disproportionate effort (taking into account factors such as the number of data subjects, the age of the data and other safeguards applied). This enactment of previous guidance in legislation will give welcome certainty.
- **Subject Access Requests.** A number of amendments to the UK GDPR's data subject access request ("DSAR") regime have been introduced, in particular that: (i) a controller's one-month response period only begins on receipt of all reasonably requested information from the data subject; and (ii) the controller is only required to provide information based on a reasonable and proportionate search (putting existing guidance on a statutory footing). Although not radically changing existing market practices, these amendments will further insulate controllers from the burdens of DSARs.
- **International Data Transfers.** The Act lowers the standard for the UK to approve third countries for international data transfers under its adequacy regulations, requiring that the other jurisdiction's protections are "not materially lower" than those in the UK (rather than the EU GDPR's "essentially equivalent" requirement). This gives the UK more freedom (even if incremental) to expand the range of recognised jurisdictions to which personal data may be transferred without additional safeguards (versus the current, EU-aligned, list). Whilst this raises optimism for allowing further frictionless international data transfers from the UK, this will be of limited benefit if a transfer also includes EU personal data.
- **PECR Penalties.** In contrast to the reduction in obligations elsewhere, the Act has increased the penalties for breaches of the Privacy and Electronic Communications Regulations (EC Directive) 2003 ("PECR")<sup>4</sup> to align with those in the UK GDPR (i.e., increasing from a maximum of £500,000 to a maximum of the greater of £17,500,000 and 4% of global turnover). This represents a significant step up in potential penalties relating to, in particular, direct marketing activities, aligning with the proposals for the EU's e-Privacy Regulation (which has been stuck in a legislative limbo for many years). The result is that data controllers should take additional care to ensure that their direct marketing activities are compliant with PECR.
- **Cookies/Tracking Technologies.** The exceptions to use of cookies and other tracking technologies without data subject consent under PECR have been expanded where: (i) strictly necessary (e.g. for security, fraud detection, fault finding, authentication and maintaining details of selections); (ii) used for analytics for the purpose of website improvement; (iii) required to optimise website appearance; or (iv) required for geolocation to provide emergency assistance. These additional exceptions will provide website owners access to an increased scope of data to secure and optimise their websites.

---

<sup>4</sup> Available here: <https://www.legislation.gov.uk/ukxi/2003/2426/contents>

- **Access to Data.** The Government has been granted broad powers to implement legislation requiring data holders (i.e., businesses providing goods or services that store that data) to correct that data and/or make it available to the data owner (customer or business), or a third party nominated by the data owner, upon request. The scope of data covered includes data stored on the goods or services and information about the goods and services themselves (including terms of use, performance, prices, etc.). The legislation may require the data holder to make the data available in certain formats and/or to provide assistance in relation to such data access (with regulatory bodies to set appropriate standards and access methods). The Act envisages that failure to comply with these new regulations could result in fines, requirements to change business practices and criminal offences in certain cases (e.g., fraud, misleading information or obstruction of enforcement). The intention of these provisions is to allow the UK to implement further smart data schemes (following the success of its Open Banking initiative) that seek to improve data interoperability, similarly to the EU's Data Act.
- **ICO Reforms.** Finally, the ICO will be replaced by the Information Commission, with a mandate to consider broader public interests in exercising its powers (including innovation and competition). It remains to be seen to what extent this shift in policy will materialise in the form of pro-business guidance and enforcement activity.

### Conclusion

After months of speculation and press coverage (particularly surrounding the Parliamentary battle between the House of Commons and House of Lords), the cumulative contents of the Act are rather meagre. Although there have been some changes that will be welcomed by businesses in the UK (in particular, the reduction in administrative burden for data subject access requests and expanded rights to utilise tracking technologies), the increase in enforcement power for marketing-privacy breaches in PECR will require businesses to take a detailed look at their direct marketing and tracking technology activities, and the deferral of the discussion on a number of topics such as AI transparency obligations and interoperability of connected devices creates more uncertainty. UK businesses will need to monitor how the UK privacy regulator (in its new form) and Government implement these deferred topics and exercise their delegated powers.

This uncertainty is exacerbated by the expiry of the EU's adequacy decision for the UK on 27 December 2025 (which has already been extended once). The UK's adequacy status is essential to facilitating smooth data flows with the EU and could cause significant disruption if not renewed. The UK Government appears to have taken this into account in its relatively moderate departures from the EU GDPR, but it remains to be seen how the European Commission will react.

The main result of the Act is that businesses which operate in both the UK and EU will need to consider how to concurrently comply with the relevant provisions under the UK GDPR, EU GDPR, PECR and national e-privacy legislation in EU member states. A prudent approach could be to adopt the most stringent set of rules (primarily those in the EU) to reduce the cost of diverging internal privacy functions. However, to the extent that there is internal bandwidth (especially if those businesses are already operating in other diverging jurisdictions such as the U.S.), businesses may choose to benefit from the differences in legislation (e.g., increasing the use of automated decision-making, legitimate interests and cookies, where permitted).

Finally, and although the Act was not intended to regulate use of AI, a great amount of legislative time was taken up in debating the inclusion of AI transparency obligations (particularly with respect to training data) in reaction to significant pressure from the creative industry (which pushed for businesses to be required to publicly disclose what copyright protected works are used to train AI). The Government ultimately rejected any substantive reform in this area but agreed to publish an economic impact assessment regarding its proposed text and data mining exception reforms, as well as a report on the use of copyright works in the development of AI systems, within nine months of the Act coming into force. This deferral will be frustrating for those in all industries, as uncertainty remains regarding whether and how protected works can be used in the AI ecosystem. Diary reminders will be set for March 2026 to assess the outcome.

\* \* \*

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

**John Patten**  
+44-20-7367-1684  
[jpatten@paulweiss.com](mailto:jpatten@paulweiss.com)

**Georgina Hoy**  
+44-20-7601-8743  
[ghoy@paulweiss.com](mailto:ghoy@paulweiss.com)

**Alex Zapalowski**  
+44-20-7367-1697  
[azapalowski@paulweiss.com](mailto:azapalowski@paulweiss.com)

*Associates Charlie Burrell and Ali Fazeli-Nia contributed to this Client Memorandum.*