

Data Protection Reform: Changes in the UK Data (Use and Access) Act 2025 and the EU Digital Omnibus Regulation Proposal

April 1, 2026 – The TMCA

by Ron Moscona and Sam Fitzgerald



Related People

- Ron Moscona
- Sam Fitzgerald

Related Capabilities

- Trademark, Copyright + Advertising
- Intellectual Property Litigation

Eight years on from the introduction of the GDPR, both the United Kingdom and the European Union appear to be taking on board the calls from the business community for reform and for a fairer balance between individual data protections and the need for less burdensome restrictions on businesses. In the UK, this has come in the form of the Data (Use and Access) Act 2025 (“**DUAA**”). The goal of the Act is to promote innovation and economic growth. In the EU, the Digital Omnibus Regulation Proposal (“**Digital Omnibus**”) aims at consolidating and simplifying existing, often overlapping, European data related regulation, such as the GDPR, Data Act, EU AI Act and ePrivacy Directive. The goal of the reform is to promote competitiveness and reduce compliance burdens for businesses.

Businesses operating in the UK should be aware of the new changes brought in by the DUAA and, for those also operating in the EU, it is important to be aware of the current proposals and how these differ from the DUAA. The two sets of measures are not

identical and present the beginning of a divergence in data protection regimes in the two jurisdictions. Below we discuss some of the key changes brought in by the DUAA and key proposals under the Digital Omnibus.

1. What are the Changes?

1.1 The DUAA

The commencement of the DUAA is phased; the majority of the data protection law changes came into force on 5 February 2026, and the new statutory complaints process will commence on 19 June 2026.

New recognised legitimate interests

The DUAA creates a new lawful ground at UK GDPR Article 6(1)(ea), which permits processing necessary for certain “recognised” legitimate interests, with no requirement to balance these against the rights of data subjects. Essentially, the DUAA creates a list of legitimate interests, which the UK legislature has deemed to be sufficient in all cases to justify the processing of personal data. This should help to reduce the burden on data controllers of balancing the applicable tests for the “legitimate interest” lawful grounds for processing and to reduce compliance risk. Some of the recognised categories of ‘legitimate interest’ include, among others, processing necessary to: (i) detect, investigate or prevent crime; (ii) disclose personal data to public authorities making public task requests; and (iii) safeguard vulnerable individuals.

Data subjects can still exercise a right to object to the processing of their data based on these recognised ‘legitimate interest’ categories in accordance with the existing rules under Article 21(1) GDPR (and if an objection is made, the controller has to demonstrate a “compelling legitimate interest” to justify any further processing).

Exemptions to the requirement for consent to cookies

The DUAA amended the Privacy and Electronic Communications Regulations cookies framework which, until now, required that organisations obtain the user’s consent for placing (or viewing) cookies on a device in all cases except where the cookie code is strictly necessary for providing the service or where the sole purpose of the cookie is for transmitting communications over an electronic communications network. The DUAA created a number of additional exemptions to the requirement to obtain user consent for the use of cookies, including:

- where the service provider uses the cookie for the sole purpose of collecting statistical information about visitors to its information society service (or a website through which the service is provided) to improve it;
- where the sole purpose is to enable the screens or functionalities of a website to be adapted to the preferences of the user or to allow some other enhancement of this nature; and

user (or the user's device) in response to a request for emergency assistance.

The DUAA also clarifies the original exception which applies where use of the cookie is deemed "strictly necessary". A non-exhaustive list of examples of "strictly necessary" cookies is provided in the legislation, including cookies used to ensure device security, prevent or detect fraud or technical faults, or to authenticate the identity of the user.

Controllers may now be able to redesign cookie banners to reflect these new exemption categories, reducing consent prompts for qualifying low-risk cookies.

However, fines for breaches of these rules now increase to a maximum of 4% of worldwide turnover (an increase from a maximum of £500,000 before the DUAA).

Further processing for research, archiving or statistical purposes

The DUAA introduced an important exception to the rule on 'purpose limitation', under new Articles 84A and 84B UK GDPR, which will help research institutions, commercial companies, public sector entities and other organisations engaged in scientific or statistical research to use data which was collected for one particular research purpose for other research purposes, even those unrelated to the original one. This includes where the use of the data was originally based on data subject consent.

Obtaining a new consent will not be required if it would not be possible or would require disproportionate efforts. In addition, the obligation to inform data subjects of the new purpose of processing will also be exempted. Other conditions and safeguards also apply. Within the limitations of the new rules, however, this new exemption should be highly relevant, for example, when dealing with patient data or consumer data collected for research purposes and the researcher has no practical means by which to seek further consent for the use of the data for new research purposes and no practical way of informing the data subjects of the additional processing.

Data Subject Access Request ("DSAR") changes

There is a new right for data controllers to request clarification after they receive a DSAR, under the new UK GDPR Article 12A, and to effectively then pause the timeframe for responding to the request. Data controllers can request clarification where they "reasonably require" further information to identify the relevant personal data required by a DSAR, for example where they hold "a large amount of information concerning a data subject". Under the new article 15(1A), controllers will only be required to undertake "reasonable and proportionate searches" for the personal data of data subjects. This could in many cases considerably reduce the burden of responding to a DSAR.

New right to complain

The DUAA inserts Article 164A to the Data Protection Act 2018 ("**DPA**") introducing a new right to complain to a data controller where a data subject believes the manner in which their information is used breaches data protection legislation. Data controllers will

now be required to establish a formal data protection complaints process, acknowledge a complaint within 30 days and respond in full “without undue delay”. This measure will commence on 19 June 2026.

In practice, complaints are likely to be made to data controllers in the same circumstances (and probably often at the same time) as when a data subject makes a DSAR. Whilst the new complaints procedure may add to data controllers’ compliance burden, it could potentially provide an alternative to making complaints to the regulator (i.e., the Data Commissioner). This may be designed primarily to relieve pressure from the regulator, but for data controllers that receive complaints, it should be easier to respond to a data subject complaint than to an investigation by the Data Commissioner which may be instigated in response to a complaint. In any event, organisations will need to update their procedures and IT systems to address the requirement to respond to data subject complaints.

Automated decision-making

A “solely automated decision” is a decision with “no meaningful human involvement”. Under new Articles 22A-22D, UK GDPR, solely automated decisions – which were generally prohibited by GDPR with very limited exceptions – are now permitted, albeit subject to certain safeguards being put in place. A clear notice will have to be given to data subjects who will still have a right to contest the automated decision making, make representations and seek human intervention in such decisions. However, there are various limitations to the right to use automatic decision making and data controllers would need to develop their processes and systems to meet the requirements of the new rules.

Data transfer changes

Under GDPR, strict rules apply to the transfer of personal data to other jurisdictions unless the jurisdiction into which the data is imported is recognised as providing adequate protection to the data and the privacy rights of individuals.

Schedule 7 of the DUAA introduces a new “data protection test” which asks whether the level of protection secured by the laws of the foreign jurisdiction is “not materially lower” than the standard of the protection provided for data subjects in the UK. It will be a matter for the UK Government to apply the test when considering the recognition of other jurisdictions as having adequate protection to data and privacy rights.

New powers for the ICO

The DUAA will replace the ICO (i.e., the current Information Commissioner’s Office) with the “Information Commission”. It is yet to be seen how this will affect regulatory activity, but it is generally seen as a measure to reduce the role of the regulator.

The DUAA introduces new investigation powers which would help the Information Commission to investigate serious complaints of breaches of the data protection rules.

These include powers to obtain information from data controllers and processors, a power to require staff and management to make themselves available for interviews and a power to require a controller or processor to appoint an independent third party to prepare a report for the Commissioner about an issue of interest to an investigation.

1.2 The Digital Omnibus

The Digital Omnibus was published by the European Commission on 19 November 2025, and will likely undergo changes during the legislative process in the Council of the European Union and the European Parliament throughout 2026. The European Commission has already launched a consultation on a “Digital Fitness Check” to evaluate the cumulative impact of EU digital regulations on competitiveness and consumer protection. The consultation ended on 11 March 2026.

Personal data

The Digital Omnibus includes an important proposal to amend the definition of personal data under GDPR Article 4(1). The proposed change would codify the recent decision of the Court of Justice of the European Union (“**CJEU**”) in Case C-413/23 P EDPS v SRB, by clarifying that information is not personal data for a given entity where that entity does not have the “means reasonably likely to be used” to identify the natural person to whom the information relates.

This means that where data is received by a company or organisation after it has been coded or “pseudonymised” it will no longer be deemed “personal data” unless the recipient has the means to reidentify the individuals.

It has long been recognised that the risk to privacy interests where data is properly pseudonymised is negligible and the requirement to comply with GDPR rules in relation to such data is an unnecessary burden. This change would correct that anomaly.

Controller’s information requirements

Articles 13 and 14 GDPR set out the general rules requiring data controllers to provide data subjects with information on the processing of their personal data (the “processing notification” requirement). A new proposal under the Digital Omnibus would establish that Article 13 will not apply in certain situations where the data is collected in a “clear and circumscribed relationship”, the activity of data controllers is not “data intensive” or “high risk” and where there are reasonable grounds to believe the data subject already has the specified information. This does not affect the processing notification requirement applicable (under Article 14 GDPR) where personal data is not collected directly from the data subject.

Scientific research

The Digital Omnibus proposal provides a new definition for ‘scientific research’ (Article 4 GDPR), clarifies that further processing for scientific purposes is compatible with the initial purpose of processing (Article 5(1)(b) GDPR), and clarifies that scientific research

constitutes a legitimate interest within the meaning of Article 6(1)(f) GDPR. These changes would have similar benefits for the use of personal data in scientific research as the changes introduced under the DUAA.

Artificial Intelligence

Another proposal in the Omnibus would reduce the legal uncertainty concerning the use of personal data for AI development. It is proposed to expressly recognise that legitimate interests (Article 6(1)(f) GDPR) provide a lawful basis for processing personal data where such processing is necessary in the controller's interest to develop and operate an AI system, provided it is appropriate, satisfies the balancing test and does not override the freedoms and rights of individuals. The proposal suggests certain conditions or exceptions, for example where EU or member state laws explicitly require consent. There may also be further safeguards where the 'legitimate interest' basis applies, such as strict data minimisation obligations, requirements to protect against residual disclosure or unintended output of personal data, greater transparency, and that individuals may have an unconditional right to object. This amendment will clarify that controllers of personal data may be able to rely on legitimate interests for AI training, testing and activities while still retaining appropriate safeguards. The clarification would be welcome by AI developers particularly those developing general purpose LLMs that rely on training models with large amounts of data which may include sporadic elements of personal data for which it is unrealistic, in practice, to obtain data subject consent and no other "lawful basis" under GDPR applies.

A related proposal would permit residual processing of special category data in limited circumstances where it is necessary for AI development and operation. This will be permitted under strict conditions, such as a requirement to remove such data once it is identified and to protect such data from being used to infer outputs, being disclosed or otherwise made available to third parties. Again, this is likely to be important particularly in the context of general purpose LLMs where the training of the model does not focus necessarily on specific categories of data but since large amounts of data are used for model training, small elements of data falling under the special categories may be used.

Right of access

Currently, data subjects (those whose personal data is processed by a controller or processor) have the right to obtain from the data controller confirmation as to whether or not their personal data is being processed, and have access to that data. Organisations have often complained of receiving repeated and strategically motivated requests, including for information gathering purposes in litigation (rather than genuine data protection concerns). The Omnibus proposes to amend GDPR Article 12 so that a data controller can either reject a data subject's right of access request or charge a reasonable fee, where the data subject is abusing the right of access provision. An example of an abuse as such would be when a data subject intends to cause the controller to refuse an access request in order to claim compensation, possibly under the threat of bringing a claim for damages.

Data breach notifications to supervisory authorities

The Omnibus includes a proposal to simplify data breach reporting requirements and reduce the burden on controllers. GDPR Article 33 would be amended so that data controllers are only required to notify supervisory authorities and data subjects of data breaches if there is a “high” risk to the rights and freedoms of natural persons. Additionally, the proposed change would extend the notification deadline from 72 to 96 hours and require use of a European-level Single Entry Point for notifying breaches, which would streamline such incidents. There would also be a common EU notification template and list of high-risk scenarios to be reviewed every three years.

Cookies

Currently, both the ePrivacy Directive and GDPR contain rules regarding cookies. The Omnibus contains a proposal to move the rules on accessing or storing information through cookies from the ePrivacy Directive into the GDPR.

The goal of some of the proposals is to address the growing problem of consent fatigue and ineffective cookie banners and modernise the current ePrivacy framework. The EU Commission proposes to update the rules on storing information or on gaining access to information stored on devices. The changes will allow users to reject or accept all cookies with the click of one button and if they opt for the former, data controllers will have to wait 6 months before asking the user for consent again.

In addition, the proposal will clarify a list of situations where cookies can be used without the consent of the data subject, namely carrying out the transmission of an electronic communication over an electronic communications network, provision of services explicitly requested by a user, a website operator carrying out analytics where the data is only used for aggregated audience measurement (such as measuring page visits) and maintaining or restoring the security of the provided service.

2. The UK DUAA Versus the EU Digital Omnibus – Side by Side Comparison of Proposed Changes

Topic	UK DUAA changes	EU Digital Omnibus proposed changes
Personal data definition	No change.	Amend the definition of personal data under GDPR Article 4(1) to codify the recent CJEU decision <i>P EDPS v SRB</i> , clarifying that information is not personal data for a given entity where that entity does not have the “means

		reasonably likely to be used” to identify the natural person to whom the information relates.
Legitimate interests	Introduces new “recognised legitimate interests”, which allows processing without a balancing test against the data subject’s rights and a legitimate interests assessment.	In the context of AI, controllers can process data to develop and operate AI systems by relying on legitimate interests, subject to the outcome of a standard balancing test, any relevant consent rules and other safeguards.
Special category personal data	Gives the Secretary of State the authority to widen the scope of special category data.	Maintains that special category data should generally not be used when operating or developing AI systems, but residual processing of special category data may be permitted in such instances however the controller must “effectively protect without undue delay such data from being used to produce outputs, from being disclosed or otherwise made available to third parties”.
Pseudonymisation	No proposed change.	In certain circumstances, pseudonymised data would no longer constitute personal data for certain entities. The Commission would provide further details of such circumstances via implementing acts.
Cookies	Introduces new exemptions for cookie consents, for example	Emphasises the concept of “consent fatigue” and introduces an option where

	when cookies are used to prevent and detect fraud.	users can refuse consent requests via the click of a button.
Data Subject Access Requests	Establishes a standard of “reasonable and proportionate” searches for controllers to limit the scope of searches for DSARs. It also introduces a pause mechanism where data controllers require additional information.	Focuses on “abusive” and “excessive” access requests. It introduces a provision where a data controller can reject “abusive” requests or charge a fee. It reduces the controller’s burden of proof for showing that a DSAR is “excessive”.
Data breaches	No substantive change unless you are a provider of public telecommunication services, which are now required to report personal data breaches to the ICO without undue delay, and where feasible, no later than 72 hours of becoming aware of the breach (rather than within 24 hours currently).	The Omnibus extends the deadline for a data controller to report a breach to 96 hours, introduces a single reporting point and raises the supervisory authority notification threshold to “high risk”.
Data transfers	Replaces the “essential equivalence test” for assessing the adequacy of a third country’s data protection regime to a new test of “not materially lower” than the standard of the protection provided for data subjects in the UK	No changes.
Automated decisions	The existing default prohibition on solely automated decisions with legal or similarly significant effect is removed provided that the data is not special category data. Whether a	Focuses on how to interpret “necessity” when assessing whether an automated decision is necessary for entering into, or performance of, a contract between the data

	process is “solely automated” is clarified to mean a decision with no “meaningful human involvement”.	subject and a data controller. The assessment of “necessity” does not require that the decision could be taken only by solely automated processing.
--	---	---