November 2025

The "Digital Omnibus": Ten Key Changes to the GDPR

STEPHENSON HARWOOD

On Wednesday 19 November 2025, the European Commission ("**Commission**") published its Digital Omnibus Regulation proposal as part of its Digital Omnibus Package (the "**Digital Omnibus**").

The Digital Omnibus proposes reforms across EU data, AI and cyber legislation, aimed at simplifying existing laws and boosting innovation, whilst maintaining high standards.

The package proposes significant amendments to the EU General Data Protection Regulation ("**GDPR**"), ePrivacy Directive, Data Act, Data Governance Act and NIS2 Directive, as well as the EU AI Act.

The proposals have already provoked strong reactions, particularly from civil society. Critics have expressed concern that some of the proposed changes, including provisions on the use of personal data in AI models, risk weakening the core protections currently afforded by the GDPR.

It should be noted that the proposals are just the beginning. The details will need to be negotiated in trilogue between the EU institutions before anything comes into force. However, organisations should still monitor developments and prepare for change.

This update focuses on the proposals to amend the GDPR. For a more detailed look at the proposed changes to the EU AI Act, click on the link below:

Read our article here on The "Digital Omnibus": Ten Key Changes to AI Regulation

Our summary of the other proposed changes will follow in due course.

GDPR REFORM

The Digital Omnibus's approach to reforming the GDPR would, if passed unamended, bring about the most dramatic changes to EU data protection law since 2018.

The Commission's stated aims are for its GDPR amendments to:

+ **Reduce unnecessary compliance** by clarifying and narrowing definitions (e.g., personal data) to;
+ **Reduce** administrative burdens by simplifying information and notification requirements, especially for smaller business and those performing low-risk processing;
+ **Facilitate AI innovation** by allowing certain uses of data for AI training and operation, with safeguards.
+ **Harmonise and streamline procedures** across the EU;
+ **Address consent fatigue** by enabling technical solutions for cookie consent; and
+ **Protect fundamental rights** while supporting digital innovation and competitiveness in the EU.

WHAT ARE THE KEY PROPOSED CHANGES?

1. Re-defining personal data

The Commission proposes to amend the definition of "personal data", effectively making the question of whether data is personal data a subjective one. The changes would mean that information relating to a natural person is only considered personal data for a particular entity if that entity has the "means reasonably likely to be used" to identify the individual. This would codify elements of the recent decision in EDPS v SRB.

This narrowed definition means that pseudonymised data could fall outside of the scope of the GDPR in the hands of one entity, even if another entity could identify the individual. This aims to facilitate use of pseudonymised data, but there is concern that the test

would be complex to apply and could risk weakening data subject protections.

2. Loosening up breach notification rules

There would be a significant reduction in breach reporting administration under the proposals. Personal data breaches would only be reportable to a supervisory authority if they are likely to result in a and a list of examples for which the reporting threshold is met.

The Commission also proposes a mandated "*single entry-point*" for incident reporting under the GDPR, NIS2, DORA, eIDAS and the CER Directive, which will be managed by the European Union Agency for Cybersecurity (ENISA). The Commission's hope is that organisations can report under multiple obligations with a single submission, reducing administrative burden.

3. Legitimate interests as a basis for AI development and operation

A new provision would confirm that controllers can rely on legitimate interests as a legal basis for processing personal data when training and operating AI models. It would still be necessary to conduct a balancing test, and to demonstrate that the processing is necessary and proportionate. Legitimate interests could still not be used where consent is required by applicable law.

Giving legitimate interests a green light will provide certainty for model developers, who currently face differing views among regulators in this context. However, a number of unanswered questions remain, particularly around how to achieve meaningful transparency and how individuals can exercise their right to object to such training in practice.

4. Special category conditions for AI and biometrics

Two new Article 9 derogations to the prohibition on processing special category data are proposed. First, controllers will be able to process any special category data that remains in data sets when training AI models, provided they make efforts to identify and remove it. If removal requires disproportionate effort, they must ensure special category data is not used in outputs or disclosed to others.

Second, biometric data may be used to confirm an individual's identity, provided this is solely under their own control (for example, a user's fingerprint to unlock their device, which stays on that device).

These changes would help overcome the current challenges of processing sensitive data for AI models. However, requiring controllers to remove sensitive data from large data sets may not be enough to prevent misuse.

5. Commercial research is "scientific"

The Digital Omnibus introduces an explicit definition of "scientific research", formally clarifying that this includes any research supporting "innovation, technological development and demonstration" whether in non-commercial or commercial contexts. It also confirms that further processing of personal data for scientific purposes is automatically considered compatible with the original purpose for which the data was collected.

These changes would address the lack of certainty around what qualifies as scientific research, particularly for industry-led or commercial projects, and would reduce barriers for businesses and research organisations seeking to use personal data in research; providing a boost to innovation.

6. Right to refuse DSARs made for "unrelated purposes"

The Commission proposes an amendment to Article 12 of the GDPR to allow controllers to refuse, or instead opt to charge for, a data subject rights request made for purposes unrelated to the protection of the requester's data, on the grounds that such request is unfounded or excessive. While such requests can be extremely burdensome, there is no information given about how controllers are expected to judge whether a rights request has been made for unrelated purposes.

7. No need for "obvious" privacy notices

The Commission proposes to remove the Article 13 duty on controllers to provide privacy notices when collecting data directly from an individual where there are reasonable grounds to assume that individuals already know the controller's identity, the purpose of processing the personal data, and the legal basis for the processing. This would not apply where there were certain risk factors such as overseas transfers, automated decision-making, or high-risk processing.

This proposal should remove the need for "check box" privacy notices where the controller is simply receiving low-risk data in order to provide a service directly to a customer who is well aware of the processing.

8. Solely ADM is still "necessary" even with a human alternative

The Commission proposes that solely automated decisions producing legal or similarly significant effects on individuals would still be permitted on the grounds that they are "necessary" for entering into a contract with the data subject, even if the decision could have been taken by a human. This would still be subject to the right to obtain human oversight.

This proposal reflects the reality of how ADM is now used – while it would often be technically possible for a human to be in the loop, this is often not cost effective.

9. DPIA standardisation

The Commission's proposals require the EDPB to develop lists giving examples of the types of processing that would and would not be subject to the Data

Protection Impact Assessment ("**DPIA**") requirements. The EDPB must also develop a common template and methodology for conducting DPIAs.

This will be welcome news to controllers who struggle to know when the DPIA requirement is engaged. If executed well, it should also streamline how DPIAs are undertaken. There is always a risk that the template and methodology will create additional burdens, especially for organisations that have established DPIA processes in place.

10. Reducing cookie fatigue

A key aim of the Digital Omnibus is to reduce the "consent fatigue" experienced by users who encounter voluminous cookie banners. A new provision in the draft prevents a controller from making a new request for cookie consent for the same purpose for a period of at least six months, if a data subject has already rejected cookies. This would, presumably, itself require the setting of a consent preference cookie.

The Digital Omnibus proposes to move provisions on cookies and similar technologies that use personal data to under the GDPR, instead of the e-Privacy Directive. This would bring maximum fines in line with GDPR limits. It would also permit use of cookies without consent where necessary for providing a service explicitly requested by the data subject, aggregated audience measurement, or security.

The proposals pave the way for cookie consent preferences to be set from a device level, rather than through a banner. These would need to be respected by controllers, except for media services providers.

SUMMARY AND COMPARISON TO DUAA

We have prepared the following handy table of the ten key changes proposed to the GDPR, their impact and their potential departure from UK data protection law as reformed by the Data (Use and Access) Act 2025.

Click here for the Data Protection team's Latest News & Insights

TEN KEY CHANGES TO THE GDPR: IMPACTS AND COMPARISONS WITH THE UK

TOPIC	CURRENT POSITION UNDER GDPR	OMNIBUS PROPOSALS	IMPACT OF CHANGE	DEPARTURE FROM UK DATA PROTECTION LAWS?
Definition of Personal Data	Article 4: "*any information relating to an identified or identifiable natural person* [...]"	Adds in the "means reasonably likely" test of Recital 26 GDPR and position from CJEU case law (EDPS v SRB):	Confirms that pseudonymised data will only be personal data for those with the means reasonably likely to identify the natural person.	Yes. This CJEU decision is persuasive (but not binding) on the UK so this marks a divergence from the UK position.
Legitimate interests as a basis for AI training	Use of legitimate interests for AI training lacks clear guidance and is inconsistently applied.	Confirms legitimate interests may be used as a basis for processing data in AI training, subject to certain safeguards.	Provides certainty for AI model developers but questions remain around individuals' rights.	Yes. Marks a divergence from the position in the UK, where there is no equivalent provision.
Exemptions for special category data (AI and biometrics)	Article 9(2). Processing of special category data only permitted in limited circumstances, creating challenges for AI training and biometric authentication.	Processing of special category data in AI training permitted if appropriately safeguarded. Use of biometric data for ID verification permitted (if under data subject's control).	Relaxes restrictions on AI training and biometric authentication. Supports innovation, but practical compliance with safeguards may be challenging.	Yes. Marks a divergence from the position in the UK, where there is no equivalent provision.
Definition of scientific research	Article 4. No explicit definition of "scientific research" or clear rules on further processing for scientific purposes (which may not yet be known).	New definition of "scientific research" which covers commercial purposes. Further processing for scientific purposes is deemed compatible with the original purpose.	Reduces compliance burden and will likely encourage innovation, especially in healthcare and tech sectors.	No. More closely aligned to the wider definition of "scientific research" and related changes introduced by the Data (Use and Access) Act 2025 ("DUAA"), due to commence in January 2026. See our summary of the DUAA here.
Right of access abuse	Article 12(5). Controllers can refuse or charge fees for access requests if requests are unfounded or excessive.	Adds that controllers can refuse or charge for access requests if used for purposes other than data protection, or if requests are unfounded or excessive.	Prevents abuse of data subject rights; reduces administrative burden.	Yes. Marks a divergence from the position in the UK., where there is no equivalent provision.

Information obligations	Article 13(4). Controllers exempt from Article 13 obligation if the individual already has the information.	Controller exempt from Article 13 obligation where there are reasonable grounds to assume that the data subject already has the information. The same exemption also applies to scientific research.	Reduces administrative burden on Controller to provide information. Reduces repetitive notifications for low-risk / non-data intensive processing.	Yes. However, under the DUAA it will be possible to re-use personal data for scientific research without providing privacy information, if it "is impossible or would involve disproportionate effort".
Automated decision-making ("ADM")	Article 22. Default prohibition on solely automated decision with legal or similarly significant effects lifted unless certain exemptions apply.	Automated decisions are allowed if necessary for a contract between the individual and controller, even if a human could make the decision.	Increases legal certainty for automated processing.	Yes. The DUAA will apply a relaxation of rules applicable to decisions made solely by ADM (except if using special category data) that extends beyond necessity for a contract, making it permissible to rely on legitimate interests.
Breach notification rules and single-entry point for reporting	Article 33. 48 hours to report to Supervisory Authority (unless unlikely to result in a risk to the rights and freedoms of natural persons). Reporting under various regulations (NIS2, DORA, GDPR) in different ways.	96 hours to report to a supervisory authority if breach is likely to result in a high risk to the rights and freedoms of natural persons. Single reporting mechanism and template for multiple regulations.	Increases time for controllers to report data breaches and reduces reports to the supervisory authority only (i.e. with no data subject notification). Streamlines administrative burden on reporting across a range of regulations.	Yes. Dual-regulated organisations will have different time periods to report breaches which affect both UK and EU data subjects. Certain reports would be UK only where increased threshold not met. UK controllers have multiple reporting obligations.
DPIA requirements	Article 35. DPIA required where processing is likely to result in a high risk to rights and freedoms of natural persons.	EDPB to create lists of processing which does require a DPIA and processing which does not. EDPB to create a common template and methodology.	Support organisations in understanding where DPIA requirement is engaged.	No. It may reduce administrative burden providing the examples and template are designed to give practical support to controllers.
Cookie consents	ePrivacy Regulation (PECR in the UK). Consent required to place cookies on a user's device (unless required for communication transmission or necessary to provide the requested service).	Consent not required for existing exceptions, along with aggregated audience information and to maintain security of a controller-provided service. Machine-readable preference regime at a device level to be developed. Cookie rules brought under the GDPR.	Reduce "consent fatigue" with cookies and ensure data subjects have genuine choice over their preferences.	In some areas. The UK retains the ePrivacy Directive position by virtue of the PECR rules. However, we note that the DUAA has recently introduced exemptions to the consent rules for 'low risk' cookies and has also aligned maximum fines with those under the UK GDPR. This covers some of the amendments made by the Digital Omnibus

OUR TEAM

KATIE HEWSON
Partner

+ 44 20 7809 2374
katie.hewson
@stephensonharwood.com

JOANNE ELIELI
Partner

+ 44 20 7809 2594
joanne.elieli
@stephensonharwood.com

ELISE DUFOUR
Partner

+33 1 88 99 10 64
elise.dufour
@stephensonharwood.com

BORIANA GUIMBERTEAU
Partner

+ 33 01 44 15 82 03
boriana.guimberteau
@stephensonharwood.com

SARAH O'BRIEN
Managing associate

+ 44 20 7809 2481
sarah.o'brien
@stephensonharwood.com

BOBBIE BICKERTON
Managing associate

+ 44 20 7809 2140
bobbie.bickerton
@stephensonharwood.com

ALISON LLEWELLYN
Senior knowledge lawyer

+ 44 20 7809 2278
alison.llewellyn
@stephensonharwood.com

MATTHEW ANGELL
Associate

+ 44 20 7809 2669
matthew.angell
@stephensonharwood.com

TATIANA CORDILHA GHELFENSTEIN
Associate

+ 44 20 7809 2887
tatiana.ghelfenstein
@stephensonharwood.com

JONATHAN HOWIE
Associate

+ 44 20 7809 2337
jonathan.howie
@stephensonharwood.com

MONICA MYLORDOU
Associate

+ 44 20 7809 2242
monica.mylordou
@stephensonharwood.com

JOSEPH SAMUELSON
Associate

+ 44 20 7809 2117
joseph.samuelson
@stephensonharwood.com

KATIE-CLAIRE LLOYD
Associate

+ 44 20 7809 2018
katie-claire.lloyd
@stephensonharwood.com

FREDERIQUE ALLIER
Associate

+33 1 88 99 10 36
frederique.allier
@stephensonharwood.com

THE LEGAL 500 UK, 2025

"The team's practical, actionable advice makes them unique - they combine deep technical knowledge with business savvy in a way that provides unmatched value to their clients."