Clifford Chance

BRIEFING

# All aboard the Digital Omnibus?

## Highlights from the EU's Digital Simplification Package

25 November 2025

The Digital Omnibus is likely to be hard fought through the course of 2026 and has already drawn strongly contrasting responses from business organisations, consumer groups and campaigners. Several of the proposed changes are welcomed by many as supportive of innovation and competition, even as other voices raise concerns in areas such as privacy rights.

The text is likely to evolve as the proposals move through the legislative process. For businesses, this uncertainty and potential for shifting goalposts (including, potentially, unsettled positions close to the point at which certain new obligations under the EU AI Act will begin applying) mean that thoughtful and strategic choices will need to be made regarding compliance preparations and possible policy engagement approaches.

On 19 November 2025 the European Commission published the much-anticipated EU Digital Simplification Package. Also referred to as the "**Digital Omnibus**", the package is made up of two proposed omnibus laws:

- a Regulation on the simplification of the implementation of harmonised rules on artificial intelligence (the "Digital Omnibus on AI"); and
- a Regulation simplifying and consolidating parts of the EU's digital acquis, making targeted amendments to data, privacy and cyber laws ("Digital Legislation Omnibus").

Some of the key proposals of the Digital Omnibus relate to:

- facilitating use of personal data in AI training, development and operation;
- postponed entry into application for high-risk AI provisions, transitional periods for entry of certain transparency requirements for generative AI and targeted amendments to other EU AI Act provisions on oversight, AI literacy, documentation and registration;
- consent fatigue and cookie rules;
- codifying a subjective, entity-driven approach to the definition of personal data in the EU's General Data Protection Regulation (**GDPR**);
- minimising the burden on controllers for certain data subject rights under the GDPR;
- creating a single point for incident reporting under a number of EU laws, and increasing reporting thresholds and timeframes under the GDPR;
- amending and consolidating key EU laws on data access and re-use; and
- repealing the Platform-to-Business Regulation.

**Wider context**

The Digital Omnibus package is a pivotal step in the EU's push towards harmonising and streamlining its digital regulatory framework, including for AI, data access, privacy, and cybersecurity. This forms part of the EU's new "digital package", which also includes a new Data Union Strategy and a proposal for a European Business Wallet.

More broadly, the Digital Omnibus sits within a wider EU focus on enhancing competitiveness, reflected in the Competitiveness Compass, and is intended to align with the European Data Protection Board (EDPB)'s recent Helsinki Statement, which called for practical simplification of the GDPR, clearer and more usable guidance and deeper cross-regulatory cooperation to ensure greater consistency across the EU's evolving digital regulatory landscape.

**Next steps:** This is only the first step in a legislative process: the proposals will require approval from the European Parliament and the Council of the EU before they can become law. Further engagement with businesses and civil society is expected in the coming months as the Member States and Parliament consider their positions. This includes the Commission's post-adoption feedback periods on both proposals within the Digital Omnibus (both currently open until 20 January 2026) and the "Digital Fitness Check" consultation and call for evidence (open until 11 March 2026), which could result in further reform to a wide range of other EU digital legislation such as, potentially, the Digital Services Act and the Digital Markets Act.

**Organisations should analyse the potential impact of the proposed reforms and consider whether, and how, to commence or continue policy engagement given the significant uncertainty expected in the coming months as to the final outcome of the legislative process.**

In addition to monitoring the progress of the Digital Omnibus, organisations should review and track:

- the Data Union Strategy;
- the proposal for European Business Wallets; and
- the newly published Model Contractual Terms on Data Access and Use and Standard Contractual Clauses for Cloud Computing Contracts.

## What's driving the Digital Omnibus?

Proposed in the wake of the 2024 Draghi Report, which warned that the EU's complex laws were stifling innovation and EU growth, the Digital Omnibus responds to calls for a more competitive, innovation-friendly, and less burdensome digital environment. It follows a series of public consultations and calls for evidence, including a call for evidence on the Digital Omnibus which ran from September to October 2025.

According to the Explanatory Memorandum, a core objective of the Digital Omnibus is to reduce the administrative costs of compliance for businesses and public administrations by clarifying legal interplay and ensuring an innovation-friendly implementation of the EU AI Act. The Commission's supporting documents to the Digital Omnibus contain initial estimates of possible savings of up to EUR 6,055 million by 2029 from the changes proposed by the Digital Omnibus, in addition to non-quantifiable benefits such as eased compliance and enforcement due to streamlined rules.

However, uncertainty remains. Member States and stakeholders remain divided as to how far the changes should go, and many civil society groups have expressed concerns over the "roll-back" of rights in the proposals and the "fast-track" lawmaking procedure used, as well as scepticism regarding the degree to which the proposals will support EU competitiveness. Additionally, while the Digital Omnibus consolidates certain laws and clarifies their interactions, in some areas its approach to amending existing provisions across numerous laws in a bundled manner can increase structural complexity.

These reforms would also have significant impact beyond the EU. Many of the laws being reformed apply to non-EU organisations in certain circumstances. Additionally, some of these laws – such as the GDPR – have influenced equivalent regimes in other countries. Where Brussels goes, others may follow – potentially shaping approaches to data and AI regulation across the world.

## An overview of key proposals

### 1. EU AI Act requirements and enforcement

The Digital Omnibus on AI proposes a number of changes to the EU AI Act's requirements and enforcement framework, including those set out below.

These proposed changes to the entry into application of the EU AI Act's requirements for high-risk AI introduce a degree of uncertainty, whilst at the same time giving the prospect of additional time.

The inclusion of this proposal in the Digital Omnibus relies on the Digital Omnibus on AI being approved before the high-risk AI regime begins to take effect in August 2026 – putting significant pressure on EU lawmakers to reach an agreement.

1.1. **Timing and entry into force – Linking high-risk AI implementation to standards availability:**

To help address uncertainties caused by the delayed availability of harmonised standards, common specifications and Commission guidelines, the Digital Omnibus on AI links the timing of the entry into application of high-risk AI requirements under the EU AI Act to the availability of these standards, specifications, and guidelines. This is intended to give businesses sufficient time to better prepare for compliance.

Once the Commission confirms this availability, the EU AI Act's provisions governing high-risk AI systems would apply:

- after 6 months for 'standalone' high-risk AI systems listed in Annex III of the EU AI Act, such as those evaluating creditworthiness; and
- after one year for high-risk AI systems under specific sectoral legislation listed in Annex I of the EU AI Act, such as medical devices.

There are 'backstop' dates for the entry into force of these provisions: in the absence of any Commission confirmation that would trigger an earlier application, the EU AI Act's provisions governing high-risk AI systems would be set to apply in any event:

- from 2 December 2027 for 'standalone' AI systems listed in Annex III of the EU AI Act (which are currently due to apply from 2 August 2026); and
- from 2 August 2028 for high-risk AI systems under specific sectoral legislation listed in Annex I of the EU AI Act (which are currently due to apply from 2 August 2027).

The relevant obligations for high-risk AI systems under the EU AI Act include detailed requirements for data governance, transparency, documentation, human oversight and robustness.

Related technical amendments have been made in connection with these changes. For example, the EU AI Act already includes transition periods for certain high-risk AI systems placed on the market or put into service by the dates on which the relevant high-risk AI requirements begin to apply (i.e., currently, those placed on the market or put into service by 2 August 2026 for "standalone" high-risk AI systems and 2 August 2027 for high-risk AI under specific sectoral legislation). These transition period start dates would be adapted to align with the dates on which these high-risk AI obligations would kick in as a result of changes brought by the Digital Omnibus on AI.

1.2. **Transitional period for GenAI systems marking obligations:**

The EU AI Act sets obligations for the marking of artificially generated or manipulated content produced by generative AI systems (such as synthetic audio, video or text output). The Digital Omnibus would defer the entry into application of these obligations until 2 February 2027 for systems which have been placed on the market before 2 August 2026. This is designed to allow providers to adapt their practices, particularly as a Code of Practice is

under development to guide the implementation of transparency obligations for generative AI under the EU AI Act.

Expanding the AI Office's mandate in this way would mean a greater degree of centralisation in the supervision of AI, potentially enhancing consistency in enforcement. It would also respond to some of the EU AI Act's implementation challenges, such as the slow designation of competent authorities and conformity assessment bodies. However, following the leak of drafts of the Digital Omnibus, some voices have raised concerns around these proposals, expressing a view that the AI Office is not sufficiently independent from the Commission's wider policy agenda.

1.3. **Strengthened AI governance and supervisory powers:**

The AI Office is currently responsible for supervision and enforcement in relation to general purpose AI models (GPAI), as well as coordinating consistent enforcement of the EU AI Act across Member States. The Digital Omnibus proposes that the AI Office now have exclusive competence to oversee:

- AI systems based on GPAI developed by the same provider (excluding AI systems covered by specific sectoral legislation listed in Annex I of the EU AI Act) – where previously this was not explicitly reserved for the AI Office; and
- AI embedded in Very Large Online Platforms and Very Large Online Search Engines within the meaning of the Digital Services Act – which is not specifically addressed in the EU AI Act at present.

Additionally, the Digital Omnibus proposes that the AI Office can also conduct pre-market conformity assessments and tests for certain high-risk systems.

The Digital Omnibus would also remove a provision which empowered the Commission to adopt a template post-market monitoring plan, while requiring the Commission to publish guidance on that topic.

1.4. **Revised AI literacy requirements:**

Currently, the EU AI Act requires providers and deployers of AI systems to take measures to ensure a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf. Criticisms have been raised that these requirements are vague and create a compliance burden that could have been avoided through other approaches to AI literacy.

The Digital Omnibus proposes shifting the primary responsibility for AI literacy from operators to the Commission and Member States. The current horizontal duty would be replaced by a new Article 4 which instead mandates that the Commission and Member States encourage AI providers and deployers to ensure sufficient AI literacy among staff and other persons dealing with the operation and use of AI systems on their behalf, using non-binding initiatives such as training, informational resources, and best practice exchanges. This does not affect other training obligations under the EU AI Act (e.g., for deployers of high-risk AI systems).

1.5. **Streamlined registration and technical documentation requirements:**

Certain registration requirements for AI systems would be narrowed, particularly for systems regarding which the provider has concluded that it is exempted from high-risk classification under Article 6(3) of the EU AI Act (i.e., on the basis that they do not pose a significant risk of harm to the health, safety or fundamental rights of individuals). Providers would need to document their exemption assessment but would not be required to register themselves and these systems in the EU database, reducing administrative burden.

Technical documentation requirements for high-risk AI systems would be streamlined for SMEs and SMCs (previously only the case for SMEs), with the

Commission establishing a form for conformity assessment. Some existing regulatory privileges for SMEs would be extended to SMCs, including with respect to the calculation of fines. Simplified compliance for quality management systems for microenterprises is extended to SMEs.

Other amendments include a broader use of AI regulatory sandboxes and real-world testing, including the facilitation of an EU-level AI regulatory sandbox by the AI Office for AI systems based on GPAI models which are both developed by the same provider under the EU AI Act, and clarifications of the interplay between the EU AI Act and other EU legislation.

## 2. AI and privacy

Proposals focused on the interplay between privacy requirements and AI sit in both the Digital Omnibus on AI and the Digital Legislation Omnibus. These include:

### 2.1. **Facilitating AI training, testing and operation:**

The Digital Omnibus proposes confirming that 'legitimate interest' may be relied on as a legal basis under the GDPR where personal data processing is necessary for the controller's interest in the context of the development and operation of AI. However, Member States would be allowed to require consent as the legal basis and the EU could also mandate consent in other EU laws. Controllers relying on 'legitimate interest' would still be obliged to conduct a balancing test to justify the processing.

The 'residual' processing of special category personal data in training, testing, and validation datasets or AI systems and models would also be allowed, subject to safeguards. Such safeguards include having in place during the entire AI lifecycle appropriate measures to avoid processing special category personal data and, if such data is identified, to remove it. Where removal is disproportionate, the controller should effectively protect such data from being disclosed or used to infer outputs.

### 2.2. **Special category personal data for bias detection and correction in AI:**

There is also a proposal to clarify and expand the framework under the EU AI Act for allowing the processing of special categories of personal data for bias detection and correction. Currently this framework applies only to providers of high-risk AI systems, but the proposal would make it available to providers and deployers of all AI systems and models. The framework may be relied on provided that:

- no alternative (e.g. synthetic or anonymised) data can fulfil the purpose;
- technical and organisational safeguards are implemented to prevent data re-use and for data security (such as pseudonymisation, strict access controls, and deletion upon the earlier of bias correction or expiry of the data retention period); and
- the necessity of the processing is documented in records of processing activities.

Although there have been questions as to how the existing provisions operate in practice, and the expanded scope may raise additional questions (such as the degree to which AI system deployers could in any case 'correct' the AI system) the proposal to expand this framework is likely to be welcomed by many.

## 3. Privacy more broadly

There are significant proposed amendments to data protection and ePrivacy laws, including:

3.1. **Amending the definition of "personal data" and facilitating certain processing:**

The Commission proposes codifying a subjective approach to the definition of personal data under the GDPR by adding a statement that information relating to a natural person is not necessarily personal data for every other person or entity, merely because another entity can identify that natural person. It would also add: "*Information shall not be personal for a given entity where that entity cannot identify the natural person to whom the information relates, taking into account the means reasonably likely to be used by that entity*."

The proposed amendment to the definition of personal data also states that, where data is not personal for an entity because it cannot identify the individual to whom it relates, such data does not become personal for that entity merely because a subsequent recipient has means reasonably likely to be used to identify the individual. This does not appear to align with statements made in *EDPS v SRB,* but would help address some challenges arising from maintaining this position in conjunction with a subjective approach to the definition of personal data.

To support the application of this updated, more subjective definition, the proposal would also empower the Commission – in close cooperation with the EDPB – to adopt implementing acts specifying the technical means and criteria to determine when pseudonymised data can be considered no longer personal data for a given entity. These acts would be developed on the basis of an assessment of the state of the art and would set out criteria or categories to help controllers and typical data recipients assess the risk of re-identification in practice. Controllers could rely on the application of such criteria as an element in demonstrating that re-identification is not reasonably likely. In parallel, the EDPB announced that it will hold an information session on 12 December 2025 to review its guidelines on anonymisation and pseudonymisation in light of the recent CJEU judgment, and industry has called for a harmonised, practical framework (including potential certification schemes).

Other proposed amendments include:

- allowing for processing of biometric data when it is necessary for confirming the identity of data subjects and where the biometric data or means needed for such verification is under the sole control of the user (e.g. on-device facial recognition), as a derogation to the Article 9 GDPR restrictions for special category data;
- adding a definition of "scientific research", including any research which supports innovation, such as technological development and demonstrations, subject to certain requirements – this includes an express statement that it may include research that aims to further a commercial interest; and
- clarifying that further processing for scientific or statistical purposes is compatible with the initial purpose of processing, irrespective of compatibility considerations in Article 6(4) GDPR.

These changes to the definition of personal data could have a significant impact on whether entities fall under the scope of the GDPR at all, as well as on data breach assessments.

The recitals to the Digital Omnibus state that the changes would reflect the approach taken in recent CJEU case law. The recent Case C 413/23 P, *EDPS v SRB*, will be foremost in mind, which recently confirmed the principle that pseudonymised data should not necessarily be considered personal data for a data recipient. There will likely be much discussion in the coming months regarding how this will apply in particular situations (e.g., any possible impact of the nature of the data recipient and its relationship to the data discloser) and how it may impact GDPR requirements such as those relating to controller-to-processor contracts and restricted international transfers of personal data.

The clarifications around "scientific research" are not dissimilar to those introduced recently by the UK's Data (Use and Access) Act 2025 (**DUAA**). They will encourage a broad interpretation of this concept and are likely to be read with interest by organisations pursuing AI development and other forms of innovation. The provisions regarding biometric data anticipate and seek to bolster expanding use of digital verification.

3.2. **Consent fatigue and cookie rules:**

Proposed changes would include:

- confirming the integration into the GDPR of the ePrivacy rules on processing personal data in the terminal equipment (devices) of individuals, meaning that the one-stop-shop mechanism would apply and primary supervisory competence would shift to the company's lead supervisory authority;
- introducing a conditional consent exemption for certain first-party, aggregated analytics and audience measurement cookies and confirming consent exemptions for security-related cookies and cookies for delivery of user-requested services;
- clarifying that access to or storage of information in the terminal equipment continues to require consent (subject to a limited set of exemptions). However, these clauses are written such that the subsequent processing of personal data lawfully obtained from terminal equipment is not captured within these consent requirements, and the recitals to the Digital Legislation Omnibus indicate that such subsequent processing should be governed by the GDPR and may rely on any lawful basis under Article 6 (including legitimate interest);
- reducing consent fatigue by stipulating that where someone has given consent, a controller shall not make a new request for consent for the same purpose for a certain period. If someone has declined consent, a new request for consent for the same purpose should not be made for at least six months; and
- requiring controllers to ensure that their online interfaces are able to interpret automated and machine-readable indications of user preferences in relation to cookies and similar technology (consent / objection signals, e.g. via browser / device), with harmonised standards to be set by European standardisation bodies. The obligation would apply six months following publication of the harmonised standards, and there would be a presumption of compliance where the standards are followed. Media service providers would be exempted on the basis that advertising revenue is indispensable for independent journalism.

The proposed eventual move to universal settings-based mechanisms for user preferences is intended to reduce the need for repeated consent banners but has already raised concerns around loss of user control to differentiate cookie preferences depending on the relevant website or platform and the security of the consent management platform.

3.3. **Harmonising DPIAs:**

The EDPB would be required to develop EU-wide lists of processing activities requiring, or not requiring, a data protection impact assessment (**DPIA**), replacing the current disparate national lists. The EDPB would also be required to develop a common methodology and template for conducting DPIAs.

3.4. **Data Subject Access Requests (DSARs):**

Where the right of access is abused by an individual, including where a DSAR is submitted for purposes other than protecting their data or where they excessively use the right of access with the intent of causing damage or harm to the controller, the controller would be able to treat the request as "manifestly unfounded or excessive" and may therefore reject the DSAR or charge a reasonable fee for handling it.

3.5. **Exception for privacy notices:**

Privacy information would not be required in certain circumstances, provided that the organisation (controller) can reasonably assume that the

individual already has the necessary information and the organisation does not carry out certain types of transfer, automated decision-making or high-risk processing. This is intended to apply, for example, in clear, direct and non-complex relationships where only a minimal amount of personal data is processed and the organisation's processing operations are not data intensive. This exception – which would apply even where the data is directly collected from the individual – is intended to cover low-risk, straightforward situations such as simple service relationships or membership management by associations or sports clubs.

3.6. **Clarification on significant automated decision-making (ADM):**

The Digital Omnibus proposes to clarify that even if a decision could be made by non-automated means, this does not prevent an entity from relying on the 'contractual necessity' ground for undertaking significant ADM under Article 22 GDPR (which is one of a limited number of legal bases available for such ADM). This would provide clarity that may support the further roll-out of ADM in connection with the provision of goods and services and customer onboarding. However, many businesses may have been hoping for reform more akin to the UK's DUAA, which will allow reliance on 'legitimate interest' for significant ADM that is not based on special category data.

**4. Cyber incidents and security**

Commission officials have described incident reporting obligations in this context as the "low-hanging fruit" of simplification: today, the same event can often trigger multiple overlapping notifications, using different templates and timelines.

By introducing a single reporting channel, the SEP aims to reduce duplication, ease administrative burden for organisations and improve coherence across overlapping cybersecurity and incident-reporting frameworks.

One of the most important parts of the Digital Omnibus is the reform of cyber incident reporting, which intends to reduce duplication across the GDPR, the Network and Information Security Directive (**NIS2**), the Critical Entities Resilience Directive (**CER**), the Digital Operations Resilience Act (**DORA**) and other instruments.

4.1. **A single reporting point for incidents:**

There is a proposal to establish a single-entry point (**SEP**) to be developed by ENISA for organisations to simultaneously fulfil incident reporting obligations to regulators under multiple legal acts including the GDPR, NIS2, DORA, CER, eIDAS Regulation and certain sectoral frameworks such as the network code on cybersecurity aspects of cross-border electricity flows (NCCS) and the relevant instruments for the aviation sector. At the same time, the separate breach-reporting requirement for communications service providers under the ePrivacy Directive is removed as obsolete.

The SEP embodies a "report once, share many" system, under which:

- entities would submit incidents through a single EU-level interface;
- the SEP then routes the notification to the competent authorities under each regime;
- ENISA operates as a mere technical conduit and will not access the content of notifications, unless expressly foreseen in the relevant legal act; and
- substantive reporting obligations would remain unchanged, except where explicitly amended (notably GDPR timelines and thresholds).

4.2. **Synergies with the CRA:**

Proposals include a requirement for ENISA to develop the SEP taking into account the single reporting platform established under the CRA, which is expected to be operational by September 2026, when CRA reporting

Despite this streamlining objective, some practical questions remain – particularly as the Digital Omnibus does not expressly limit the number of competent authorities that may receive a report routed through the SEP. In practice, the "report once, share many" system could still result in notifications being distributed to multiple authorities across different regimes, and it is not yet clear how this will reduce, rather than merely centralise, the complexity that organisations face today. The degree to which there ends up being further alignment between the SEP and the single reporting platform under the CRA will also be an aspect to monitor.

obligations kick in. The CRA single reporting platform – used for notifications of actively exploited vulnerabilities and severe incidents involving products with digital elements – is intended to serve as a reference point for the SEP: although the SEP may ultimately be a distinct system, the Commission expects that it could build upon the CRA platform, to the extent possible.

The Digital Omnibus also clarifies that a notification of a severe incident pursuant to Article 14(3) of the CRA shall also constitute reporting of information under NIS2, reinforcing cross-regime coherence. This synergy with the CRA is therefore part of a broader effort to minimise duplicative reporting and support consistent treatment of incidents involving products with digital elements.

4.3. **Harmonised templates and information requirements:**

There is a proposal to (i) empower the EDPB to develop a common EU template for GDPR breach notifications, for consideration and formal adoption by the Commission and (ii) allow the Commission and ENISA to align templates and data fields across NIS2, DORA, CRA and other instruments to the extent possible.

Where existing frameworks (such as DORA) already contain detailed, standardised incident-reporting templates, the Digital Omnibus encourages re-use and adaptation. DORA's templates are therefore expected to provide insights and best practices for the SEP, though some differences will remain necessary given the distinct scope and objectives of each underlying regime.

4.4. **Changes to GDPR breach reporting:**

Two key changes are proposed for GDPR breach notification:

- **Higher reporting threshold**: Only personal data breaches likely to result in a "high risk" to individuals would need to be notified to data protection authorities. This aligns the controller's duty to notify authorities (currently under Article 33 GDPR) with the existing duty to notify affected individuals (Article 34 GDPR): both would apply only where a breach poses a high risk to data subjects' rights and freedoms.

  Notifications would be submitted through the SEP using a new EDPB-standardised template. The EDPB will also draw up a common list of scenarios typically considered high risk. Both the template and the list will be reviewed at least every three years.

- **An extended timeframe:** The period for notifying authorities would be extended from "without undue delay and where feasible not later than 72 hours" to "without undue delay and where feasible not later than 96 hours", in each case from becoming aware of a reportable breach.

**5. Data access and use**

5.1. **Amending and consolidating various EU data laws:**

The Digital Omnibus would consolidate the provisions of the Data Act, the Free Flow of Non-Personal Data Regulation, the Data Governance Act, the Open Data Directive and introduce targeted amendments.

The Data Governance Act (**DGA**), Open Data Directive and Free Flow of Non-Personal Data Regulation would be repealed except for:

While these proposals to consolidate and amend the provisions of the Data Act, the Free Flow of Non-Personal Data Regulation, the DGA and the Open Data Directive are intended to simplify the legislative landscape for data access and re-use, the Digital Omnibus' consolidation and amendment of provisions across numerous laws introduces its own structural complexity, requiring organisations to invest resources in understanding potential implications of the amendments and engaging with its progress.

- **Data intermediation services and data altruism:** DGA requirements applicable to data intermediation services and data altruism would be amended and moved to the Data Act. The mandatory regime for data intermediation services under the DGA would be replaced by a voluntary regime in the Data Act. Legal separation requirements for data intermediation services and other value-added services would be replaced by functional separation requirements. Reporting obligations for data altruism organisations would be reduced.
- **Public sector data:** DGA rules on re-use of protected public sector data and Open Data Directive rules for accessible public sector information would be moved to the Data Act and merged into a single new chapter with common principles and aligned terminology (including clear distinction between "data" and "documents"). The merged framework would: introduce clearer provisions for secure processing environments, anonymisation and pseudonymisation; retain and refine safeguards for trade secrets, intellectual property, and personal data as well as maintain third-country transfer protections; and introduce mechanisms enabling public sector bodies to set out different conditions and provide higher fees for the re-use of data and documents by very large companies, such as those designated as gatekeepers under the Digital Markets Act.
- **Data localisation prohibition:** The Free Flow of Non-Personal Data Regulation's prohibition on data localisation within the EU would be moved to the Data Act. The main rule would remain unchanged: Member States would not be permitted to require non-personal data to be stored or processed within their territory unless the localisation measure is necessary for public security or specifically required by EU law. Member States would still be required to notify the Commission of new data localisation requirements, but the obligation to maintain national single information points listing these measures would be removed. This consolidation of non-personal data provisions within a single instrument is intended to support the free flow of non-personal data within the EU by preventing national data-localisation obligations that would otherwise fragment the internal market. Rules on international access and transfers (which address situations where third-country access would conflict with EU or Member State law) would continue to apply (see below).
- **International access to non-personal data:** The DGA's rules governing international access to non-personal data (including requirements to assess and protect against foreign governmental access that would conflict with EU or Member State law) would be moved to, and consolidated within, the Data Act. Data re-users would have to take measures to prevent transfers or foreign government access that would conflict with EU or Member State law. Re-users transferring certain categories of protected non-personal data (e.g., non-personal confidential data, and data protected by IP rights) to third countries would also have to inform the relevant public body, obtain necessary permissions, and commit contractually to confidentiality and IP protections, including accepting EU court jurisdiction.

5.2. **Other amendments to the Data Act:**

In addition to changes mentioned above, other amendments to the Data Act would include:

Many data holders will wish to review their processes for responding to data access requests in order to take account of enhanced protections for trade secrets when the Digital Omnibus is closer to final form, and give thought to their interim approaches.

- **reinforcing the protection of businesses' trade secrets:** To protect data holders against serious economic damage or unlawful acquisition, use or disclosure of trade secrets, data holders would be allowed to refuse to share their trade secrets with entities subject to third-country jurisdictions offering weaker or non-equivalent protection than the EU, including entities established in the EU that are under the direct or indirect control of such third-country entities. Data holders would be able to refuse such disclosure on a case-by-case basis, subject to justifying their decisions on the basis of objective elements (e.g., the enforceability of trade-secret protection in the relevant third country or the nature and level of confidentiality of the data requested). Data holders would also be required to notify the competent authority in such a case;
- **narrowing the circumstances in which a data holder may have to disclose information to public sector bodies and other authorities**: The scope of business-to-government data sharing requirements would be narrowed from "exceptional need" to "public emergencies" (including to help mitigate or recover from public emergencies), with clearer procedures for requests, compensation, and safeguards for trade secrets and personal data. For instance, personal data could be requested only where the provision of non-personal data would be insufficient to address the public emergency and subject to appropriate technical and organisational measures to ensure their protection;

The proposed amendments to the Data Act's 'cloud switching' requirements also contain related points, presumably intended as clarificatory, which introduce ambiguities as they appear to not entirely align with existing Data Act provisions, including regarding the termination of agreements. These will require further attention and clarification during the forthcoming discussions.

- **reducing the 'cloud switching' requirements in certain circumstances:** Lighter regimes are introduced for (i) custom-made data processing services (i.e., services that are "not off-the-shelf and would not function without prior adaptation to the needs and ecosystem of the user") and (ii) SME and SMC data processing service providers, in both cases in relation to non-IaaS services, under contracts concluded before or on 12 September 2025. Most of the Data Act Chapter VI provisions that aim to facilitate switching between data processing services would not apply in these specific cases (with the exception of the obligations to reduce and ultimately remove switching and egress charges); and
- **smart contracts for data sharing:** The Digital Omnibus would remove Article 36 of the Data Act on essential requirements regarding smart contracts executing data sharing agreements. This removal aims to address legal uncertainties arising from the lack of harmonised standards and clear definitions of key concepts, which could otherwise impede the development of innovative business models.

**6. Repeal of the Platform-to-Business Regulation**

The Platform-to-Business (P2B) Regulation would be repealed, as its provisions would largely be covered by the Digital Services Act and the Digital Markets Act. This would help clarify compliance requirements for online intermediary service providers. However, cross-references to the P2B Regulation in other EU laws would remain valid until those acts are amended and, in any case, no later than 31 December 2032 (e.g., rules on restrictions and suspensions of online intermediation services, complaint-handling systems for business users and enforcement provisions).

Businesses should assess what these potential changes could mean for them, consider whether any aspects warrant policy engagement and closely monitor the progress of the Digital Omnibus. Notably, there is a post-adoption feedback period of 8 weeks on both proposals within the Digital Omnibus (both currently open until 20 January 2026).

Some aspects of the text are likely to change through the legislative process and businesses will need to make thoughtful, strategic choices regarding how the potential changes proposed in the Digital Omnibus may impact their compliance preparations.

**Data Union Strategy**

Pillar 1: flagship initiatives to address current limitations in access to critical datasets, insufficient infrastructure for large-scale AI development, and the need for trusted environments, such as data labs that connect European data spaces with the AI ecosystem.

Pillar 2 initiatives are reflected in the Digital Omnibus. Additional efforts will focus on building a future-proof data framework, enabling "one-click compliance" and supporting Data Act compliance.

Pillar 3: plans to, in Q2 2026, issue guidelines assessing the treatment of EU entities by third countries and to develop an anti-data leakage toolbox to address localisation demands, market exclusion, insufficient safeguards, or other forms of unjustified treatment. Further targeted measures to be developed by Q3 2026 to protect sensitive EU non-personal data.

## How it becomes law – the road ahead for the Digital Omnibus

The Digital Omnibus will require approval from the European Parliament and the Council of the EU before it can be passed into law. Once the Digital Omnibus is agreed, the majority of its provisions would enter into force three days after its publication in the Official Journal of the EU (OJEU). There would be transitional periods for certain rules such as:

- those relating to settings-based mechanisms for cookie preferences (48 months following entry into force of the Digital Legislation Omnibus) and to moving cookie compliance to the GDPR (six months following entry into force of the Digital Legislation Omnibus); and
- the new single-entry point should start being used within 18 months from the entry into force of the Digital Legislation Omnibus. The Commission can extend the application of the revised rules to 24 months from entry into force if it does not find that the single-entry point is functioning properly.

The legislative process is expected to include much debate on the proposed changes to landmark legislation, in particular with regard to amendments to the GDPR and the ePrivacy Directive. At the same time there is widespread recognition of the need to reduce legislative complexity, simplify compliance, address timing issues for EU AI Act implementation and, more broadly, foster innovation.

## Related developments

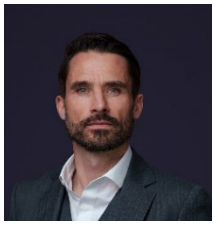
Organisations will want to review other connected developments and consider any policy engagement appetite, including for:

- **Data Union Strategy:** The Digital Omnibus was published as part of the EU's new "digital package" which also includes a new Data Union Strategy and a proposal for a European Business Wallet. The Data Union Strategy identifies three priority areas (Pillars) for EU action: (1) scaling up and improving access to data for AI; (2) streamlining data rules; and (3) strengthening the EU's global position on international data flows.
- **European Business Wallets:** This legislative proposal would establish a framework for the provision of European Business Wallets. It seeks to streamline cross-border business operations by introducing a secure, interoperable digital identity, document, and exchange system for companies and public authorities.
- **Model Contractual Terms on Data Access and Use and Standard Contractual Clauses for Cloud Computing Contracts:** On the same day as the Digital Omnibus package proposal was published, the Commission also published its highly anticipated (non-binding) model contractual terms regarding data access and use and (non-binding) standard contractual clauses for cloud computing contracts under the Data Act.
- **Digital Fitness Check:** The Commission has also launched a public consultation and call for evidence to further evaluate existing EU digital legislation. This is the second stage of the Commission's plan to simplify and streamline the EU's digital rules. The consultation is open until 11 March 2026 and relates to, among other things, an assessment of how different laws work together, identifying overlaps and inconsistencies in legal definitions, requirements, scope and supervision. This evaluation is a key step toward further potential simplification of EU digital regulations.

# Authors

**Dessislava Savova**
Partner, Head of Continental Europe Tech Group, Paris

Dessislava.Savova@cliffordchance.com
+33 1 4405 5483



**Alexander Kennedy**
Knowledge Director – CE Tech Group, Paris

Alexander.Kennedy@cliffordchance.com
+33 1 4405 5184

**Rita Flakoll**
Knowledge Director – Global Tech Group, London

Rita.Flakoll@cliffordchance.com
+44 207006 1826

**Alexandre Balducci**
Lawyer, Paris

Alexandre.Balducci@cliffordchance.com
+33 1 4405 5137

**Blanche Barbier**
Lawyer, Paris

Blanche.Barbier@cliffordchance.com
+33 1 4405 8290

**Kelly Cannon**
Lawyer, Paris

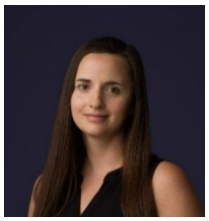
Kelly.Cannon@cliffordchance.com
+33 1 4405 5350

**Eliot Cohen**
Lawyer, London

Eliot.Cohen@CliffordChance.com
+44 207006 2966

**Simon Davis**
Senior Associate, London

Simon.Davis@cliffordchance.com
+44 207006 4468



**Orsolya Gondos**
Senior Associate, Amsterdam

Orsolya.Gondos@cliffordchance.com
+31 20 711 9414

**Wided Kaidouchi**
Lawyer, Paris

Wided.Kaidouchi@cliffordchance.com
+33 1 4405 5955

**Alexandre Manasterski**
Counsel, Paris

Alexandre.Manasterski@cliffordchance.com
+33 1 4405 5971

**Grégory Sroussi**
Counsel, Paris

gregory.sroussi@cliffordchance.com
+33 1 4405 5248

# Other contacts

**Anna Carrier**
Head of EU Tech Policy, Brussels

Anna.Carrier@cliffordchance.com
+32 2 533 5048

**Jonathan Kewley**
Partner and Co-Chair of the Global Tech Group, London

Jonathan.Kewley@cliffordchance.com
+44 207006 3629

**Holger Lutz**
Partner, Frankfurt

Holger.Lutz@cliffordchance.com
+49 69 7199 1670

**Andrei Mikes**
Counsel, Amsterdam

Andrei.Mikes@cliffordchance.com
+31 20 711 9507

**Patrice Navarro**
Partner, Paris

Patrice.Navarro@cliffordchance.com
+33 1 4405 5371

**Milena Robotham**
Partner, Brussels

Milena.Robotham@cliffordchance.com
+32 2 533 5074

**Katrin Schallenberg**
Partner, Paris

Katrin.Schallenberg@cliffordchance.com
+33 1 4405 2457

**Phillip Souta**
Global Director of Tech Policy, London

Phillip.Souta@cliffordchance.com
+44 207006 1097

**Herbert Swaniker**
Partner, London

Herbert.Swaniker@cliffordchance.com
+44 207006 6215

**Andrea Tuninetti Ferrari**
Counsel, Milan

Andrea.Tuninettiferrari@cliffordchance.com
+39 02 8063 4435

cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ