The Digital Omnibus – a package of simplification

What is the Digital Omnibus? Scope, aims and who it affects

"Simplifying, clarifying and improving the EU's digital rule-book" – this is the vision of the European Commission for adapting the EU's regulatory framework to a more volatile and competitive world. On November 19, the European Commission published the first step toward this vision, two Digital Omnibus proposals.

Two proposals, one package: Digital Omnibus vs Digital Omnibus on AI

The first proposal, simply referred to as the Digital Omnibus, aims to simplify the EU data legislative acquis (which covers the Data Act, Data Governance Act, Open Data Directive, and Free Flow of Non-Personal Data Regulation), the GDPR, the ePrivacy Directive, and certain EU cyber laws (NIS2, DORA, CER and the Digital Identity Regulation). The second, the Digital Omnibus on AI, aims to simplify the EU AI Act.

The official versions of the two Digital Omnibus proposals released on November 19 do not significantly deviate from the versions leaked a few weeks back. Initial reactions to the proposals seem to vary greatly: while activists criticise what they saw as a slashing of civil rights, other voices view the proposed changes to the GDPR, the AI Act, the Data Act, and other legislation more as a technical reform rather than fundamental policy reversal, and yet other voices claim they couldn't care less because the Digital Omnibus will not bring any changes, same-same with a new title.

Compliance may ease: Practical impact of the Digital Omnibus

In our view, the Digital Omnibus should be viewed more as a cautious and selective adjustment rather than a sweeping overhaul. The proposal addresses inconsistencies and regulations that have simply proven to not work in practice. While some amendments do make compliance easier for companies in some areas, the changes are rather targeted than comprehensive.

Which topics are affected by the Digital Omnibus?

- Artificial Intelligence
- GDPR
- e-Privacy
- Cyber security
- Data legislative acquis

Below, we outline the most relevant aspects of the proposed Digital Omnibus and their implications for companies. Given that the leaked draft has already attracted considerable attention, we also discuss the differences between the leaked versions and the official drafts. .

What are the most relevant aspects of the proposed Digital Omnibus on AI?

1 One obligation less, longer implementation periods for high-risk and transitional periods for transparency obligations

1.1 No obligation to implement AI literacy

The proposal eliminates the currently existing obligation for providers and deployers of AI systems to ensure an appropriate level of AI literacy within their company. Instead, the proposal provides that the European Commission and

the Member States shall merely encourage providers and deployers to provide a sufficient level of AI literacy.

1.2 Entry into force and application of high-risk obligations

The application date for obligations relating to high-risk AI systems shall be overhauled significantly. The applicability of these obligations shall be linked to the availability of measures to support compliance, which may include harmonised standards, common specifications and Commission guidelines. Additionally, the application date shall differ depending on whether the AI system is classified as high-risk under Article 6(2) and Annex III, or under Article 6(1) and Annex I. In any case, obligations relating to high-risk AI systems shall apply on 2 August 2028 at the latest or 2 August 2030, if the AI system is intended to be used by public authorities.

1.3 New grace periods for high-risk

The application of the grace period under Art. 111 (2) AI Act shall be clarified. The grace period should cover broader categories of types and models of high-risk AI systems, and not each individual unit of that high-risk AI system. Additionally, the Omnibus replaces the fixed 2 August 2026 cut-off for the grace period with a dynamic cut-off tied to the actual date of application of Chapter III under Article 113 (triggered by the Commission's decision), while retaining the 2 August 2030 compliance deadline for systems intended for public authorities.

1.4 New grace period for transparency obligations

The draft proposes an extended grace period for some transparency obligations: Providers of generative AI systems, including General-Purpose-AI-models (GPAI-models), placed on the market before 2 August 2026 must comply with Article 50(2) AI Act by 2 February 2027 instead of 2 August 2026. Under Article 50(2) AI Act, AI-generated or manipulated audio, image, video and text content must be marked in a machine-readable format and detectable as artificially generated or manipulated by this point in time.

❷ Procedural simplifications

2.1 Relief for registration requirements

Providers of AI systems shall no longer be required to register AI systems referred to in Art. 6 (3) AI Act given that those systems may be exempt from the classification as high-risk AI systems under certain circumstances even if they are used in a high-risk area. The providers of such AI systems shall only be required to document their respective assessment of the AI system in question.

2.2 Pre-market conformity assessments

For AI systems under Art. 75(1) AI Act that are high-risk and subject to third-party assessment under Art. 43 AI Act, the Commission may organise and carry out pre-market tests and conformity assessments or entrust notified bodies to act on its behalf to verify that the system complies with the AI Act.

2.3 "Once-only"-applications

Conformity assessment bodies may use a single application and a single assessment to obtain designation under both the AI Act and the Union harmonisation legislation listed in Annex I, Section A, where such a procedure exists in the sectoral law.

For high-risk AI systems covered by existing product regulation (Annex I, Section A, such as radio equipment devices and similarly regulated products), the sectoral product conformity assessment remains the primary route, and the AI Act Chapter III, Section 2 requirements become part of that assessment. Thus, notified bodies that are already notified in the primary route shall have the additional power to assess compliance with the rules regarding high-risk AI.

2.4 Expanded rules for AI sandboxes and real-world testing

In addition to national sandboxes, the AI Office may establish sandboxes at Union level for AI systems falling under Article 75(1) AI Act. This scope includes (i) AI systems based on GPAI models where both the system and the model are developed by the same provider, excluding AI systems related to products covered by Union harmonisation legislation listed in Annex I, and (ii) AI systems that constitute or are integrated into a designated very large online platform or very large online search engine.

Real-world testing outside sandboxes shall be extended beyond Annex III to high-risk AI systems under Annex I, Section A. For high-risk AI systems under Annex I, Section B, real-world testing may take place on the basis of a voluntary agreement concluded between the Commission and interested Member States.

❸ (More) Power for the AI office

According to the draft, the AI Office will get more power when it comes to the surveillance of GPAI models and „Very Large Online Platforms" (VLOPs, as defined in the DSA). In order to exercise these competences, the AI Office shall have "all the powers of a market surveillance authority". To support this, there will be an implementing act defining the enforcement powers and procedures for the exercise of such powers. Adopting the supervisory and enforcement system of the Digital Services Act, the AI Office shall become the market surveillance authority under the AI Act where an AI system qualifies as a VLOP or a VLOSE or is embedded into one.

4 Data processing

Under Art. 10 (5) EU AI Act providers of high-risk AI systems may process sensitive data for bias detection. This exception shall be expanded to AI models and other AI systems.

5 Facilitation for small and middle-sized enterprises

The AI Act already imposes lower requirements on small and medium-sized enterprises ("SME"), i.e. companies with fewer than 250 employees and less than EUR 50 million turnover. The proposal now includes additional relief for small and mid-cap enterprises („SMC"), i.e. companies with fewer than 750 employees and an annual turnover of less than EUR 150 million, such as facilitated procedures and lower fines.

What are the most relevant aspects of the proposed Digital Omnibus with respect to the GDPR, e-Privacy and the various cyber laws?

According to the European Commission, the proposed Omnibus provides a series of targeted amendments to simplify the GDPR and clarify some of its provisions, to overhaul the so-called cookie rules in the ePrivacy Directive and to establish a single-entry point for incident related reporting obligations.

1 Definition of personal data

The definition of personal data in Art. 4 (1) GDPR shall be refined to reflect the most recent CJEU decisions by clarifying that information is not necessarily personal data for every other person or entity, merely because another entity can identify the natural person. Furthermore, it shall be clarified that information shall not be personal for a given entity where that entity cannot identify the natural person to whom the information relates, and such information does not become personal for that entity merely because a potential subsequent recipient has the means reasonably likely to be used to identify the natural person. In fact, these amendments do not bring about a substantive change since the clarification is in line with the current CJEU interpretation of "personal data" anyhow.

Unlike the leaked draft of the Digital Omnibus, the official version no longer contains clarification relating to the definition and qualification of sensitive data.

2 Specifications on data subject rights

Amendments to Art. 12 shall clarify that the right of access under Art. 15 GDPR may not be misused in the sense that the data subject abuses it for purposes other than the protection of their data, e.g., where the access request is made to subsequently demand the payment of compensation or to merely cause damage or harm. In recent years, a certain practice had become established of making access requests under Article 15 GDPR unspecific and broad and thus not easy to comply with particularly in an employment context, thereby building up bargaining power in labour law disputes. Yet, the specification will likely not bring relevant improvements because it will be easy for the data subject to hide the real purposes and also, the examples stated in the draft are currently already acknowledged by the EDPB in its guidelines to be misuses of the right to data access.

The derogation in Article 13 GDPR relating to transparency obligations shall be expanded to situations where the processing is not likely to result in a high risk (Article 35 GDPR) and where there are reasonable grounds to assume that the data subject already has the information about the controller's identity and contact details and the processing purposes. Presumably, mainly small businesses with rather one-dimensional data processing activities will benefit from these derogations; for larger companies, comprehensive data protection notices will remain necessary. Further derogations from transparency obligations shall be granted in case of scientific research if the provision of the information is impossible or would involve a disproportionate effort.

3 Legal basis for sensitive data in the context of AI

Article 9 (2) GDPR shall be amended by a new lit. k) that shall permit the processing of sensitive data in the context of the development and operation of an AI system or an AI model, subject to further conditions, such as appropriate technical and organisational measures to avoid the collection and further processing of sensitive data. Where, despite such safeguards, the controller identifies sensitive data in the training or testing data set or even in the AI system or AI model, such sensitive data shall be removed. If such removal requires disproportionate effort, the controller shall take other measures to protect such data from being used to produce outputs, from being disclosed or otherwise made available to third parties. The European Commission explains that sensitive data may residually exist in the training, testing or validation data sets or be retained in the AI system or the AI model, although the sensitive data are not necessary for the purpose of the processing. This amendment to Art. 9 GDPR shall prevent the disproportionate hinderance of the development and operation of AI in this context. This amendment would in fact bring legal certainty to a highly debated question. Member State Courts including those in Germany have handed down differing

judgements on the permissibility to use personal data for AI training including on whether and how to comply with Art. 9 GDPR in this context.

4 Legitimate interest in the context of AI

A new Art. 88c GDPR shall specify how the legitimate interests pursuant to Article 6 (1) lit f) GDPR can be leveraged as a legal basis for the development and operation of AI systems. It shall not provide a blanket legal basis in the AI context, though. Instead, where the processing is necessary for the interests of the controller in the context of development and operation of an AI system or AI model, such processing may be pursued for legitimate interests within the meaning of Article 6 (1) lit f) GDPR, where appropriate, except where other Union or national laws explicitly require consent, and where such interests are overridden by the interests, or fundamental rights and freedoms of the data subject, in particular where the data subject is a child. Any such processing shall require appropriate technical and organisational measures and safeguards, in particular for data minimization and protection against non-disclosure of residually retained data in the AI system or AI model, on transparency, and on an unconditional right to object to the processing of the personal data.

5 Automated decision-making

Art. 22 GDPR shall be amended by clarifying that decisions based solely on automated processing are allowed when specific conditions as currently provided in Art. 22 GDPR are met, thereby moving away from the current language referring to a data subject right concept. It shall also be clarified that when assessing whether a decision is necessary for entering into, or performance of, a contract, it shall not be required that the decision could be taken only by automated processing. This amendment would have an impact on AI-based decision making as automated decision making would also be permitted in the contract-scenario if a manual decision were also theoretically possible.

6 Data breach notification obligations and single-entry point for incident reporting

In order to reduce the burden on controllers, the threshold for notifications to the regulator in case of a personal data breach shall be aligned with that of communicating the personal data breach to the data subjects, i.e., only if the breach is likely to result in a high risk to the rights and freedoms of the data subjects. The notification period shall be extended from 72 hours to 96 hours. In particular, the introduction of the high-risk threshold for the reporting obligation could have a huge impact because in reality, low-risk incidents happen quite frequently.

Furthermore, a single-entry point for incident reporting shall be developed and offered. The European Commission states that several horizontal or sectoral EU laws require the notification of the same event to different authorities using different technical means and channels. The single-entry point for incident reporting shall allow entities to fulfil reporting obligations under NIS2 Directive, GDPR, DORA, Digital Identity Regulation, and CER

7 ePrivacy and Cookies

The Digital Omnibus proposal restructures the legal framework for cookies by recalibrating the relationship between the ePrivacy Directive and the GDPR. In future, the ePrivacy Directive shall no longer govern the processing of personal data of natural persons in relation to terminal equipment; such processing will fall entirely under the GDPR. To this end, the Digital Omnibus shall insert a clarifying subparagraph into Article 5(3) ePrivacy and introduces a new Article 88a GDPR, which sets out when storing or accessing information in terminal equipment (including cookies) is lawful without consent.

Consent nonetheless remains the general rule, with Article 88a(3) GDPR providing an exhaustive list of low-risk purposes for which storage or access is permitted without consent. As Recital 44 makes clear, any subsequent processing for other purposes must be assessed under the ordinary GDPR framework, including the strict conditions for relying on legitimate interests.

The envisaged exemptions of the new Article 88a GDPR for low-risk purposes are narrowly drafted and limited to (i) transmission of communications, (ii) the provision of services explicitly requested by the data subject, (iii) the creation of aggregated audience measurements for the provider's own online service, and (iv) maintaining or restoring the security of a service provided by the controller or the terminal equipment used for that service. Article 88a(4) additionally tightens the handling of consent by requiring one-click refusal, prohibiting renewed requests while consent is still valid, and imposing a six-month "cooling-off" period after a refusal for the same purpose.

Article 88b adds a technical layer by requiring that consent, refusal and objections can be expressed through automated and machine-readable means and must be respected by controllers, while obliging non-SME browser providers to implement the necessary technical capabilities. A limited carve-out for media service providers relieves them only from these technical duties, without establishing an explicit legal basis for processing. In practice, considerable uncertainty is likely to remain: the exemptions in Article 88a(3) are narrow, the continued relevance of ePrivacy persists, and many providers currently rely on cookie banners to meet

transparency obligations. Combined with the time needed to develop and deploy interoperable technical standards for machine-readable consent, a rapid and frictionless end to the current "cookie banner" landscape appears unlikely.

In addition, the Digital Omnibus proposes the repeal of Article 4 of the ePrivacy Directive. Hence, security and personal data breach obligations for providers of publicly available electronic communications services will instead be governed coherently under the GDPR and the NIS2 Directive.

8 P2B regulation

In the interest of simplification of EU law in the field of online intermediaries and online platforms and given the overlap with the DSA and the DMA, the P2B Regulation shall be repealed, with certain provisions to remain temporarily in application.

What are the most relevant aspects of the proposed Digital Omnibus with respect to the data legislative acquis?

Moreover, the proposed Digital Omnibus provides for a consolidation of the data legislative acquis: The Open Data Directive (Directive (EU) 2019/1024), the Regulation on the Free Flow of Non-Personal Data (Regulation (EU) 2018/1807) and the Data Governance Act (Regulation (EU) 2022/868) shall be consolidated into the Data Act. The Data Act is thus becoming more than ever a potpourri of various regulatory aspects without a comprehensive and harmonized theme.

1 Clarification of definitions

Beyond the consolidation, the draft Digital Omnibus contains numerous clarifications for definitions currently used in the Data Act. For example, the key terms ('data user,' 'data holder,' 'public emergency') are to be harmonised and clarified. In fact, particularly the definition of the data holder, had been criticised as flawed from the outset.

2 Stronger protection of trade secrets

Furthermore, the protection of trade secrets will be further strengthened by allowing data owners to refuse disclosure if this could result in sensitive information being transferred to third countries with an inadequate level of protection or could compromise the EU's essential security interests. At this point, conflicts between companies vying for data are to be expected more than ever. Other changes are likely to have a rather minor immediate impact on organisations, such as the restriction of the access rights for public authorities to cases of 'public emergency', moving away from the initial permission ground of 'exceptional necessity'.

The switching obligations under Section 26 et seq. of the Data Act shall also be slightly amended. In particular, customised services are exempt from the interoperability requirements in existing contracts and small and mid-cap companies (up to 750 employees) shall be permanently exempt from additional obligations.

What comes next?

The typical politics in Brussels – in order for the Digital Omnibus to become law, not only the European Commission but also the European Parliament and the Council of the EU must agree to these proposals. Given the reactions to the drafts to date, it is unlikely that the proposals will be adopted in their current form. Either there will be lengthy negotiations that may take months, if not years, before the proposals will – with whatever further amendments – be adopted, or the trilogue negotiations will limit the Omnibus Package to certain key aspects they consider important to agree on a quicker timeline, leaving other aspects out for now. What those key aspects will be, that is something we can only guess at.

Osborne Clarke will continue to monitor the legislative process and publish detailed analyses and updates on further developments in the legislative process for the Digital Omnibus here.

Find more information here:
Digital Omnibus Landingpage

Get in touch with our experts

Gereon Abendroth
Partner
T +49 221 5108 4332
gereon.abendroth@osborneclarke.com

Ulrich Bäumer
Partner
T +49 221 5108 4168
ulrich.baumer@osborneclarke.com

Dr. Lina Böcker
Partner
T +49 221 5108 4434
lina.boecker@osborneclarke.com

Konstantin Ewald
Partner
T +49 221 5108 4106
konstantin.ewald@osborneclarke.com

Julia Kaufmann
Partner
T +49 89 5434 8068
julia.kaufmann@osborneclarke.com

Dr. Flemming Moos
Partner
T +49 40 55436 4054
flemming.moos@osborneclarke.com

Dr. Tobias Rothkegel
Partner
T +49 40 55436 4090
tobias.rothkegel@osborneclarke.com

Dr. Jens Schefzig
Partner
T +49 40 55436 4058
jens.schefzig@osborneclarke.com

Adrian Schneider
Partner
T +49 221 5108 4370
adrian.schneider@osborneclarke.com

Dr. Hendrik Schöttle
Partner
T +49 89 5434 8046
hendrik.schoettle@osborneclarke.com

Dr. Marc Störing
Partner
T +49 221 5108 4266
marc.stoering@osborneclarke.com

Claire Bouchenard
Partner
T +33 1 84 8 24530
claire.bouchenard@osborneclarke.com

Robert Briske
Partner
T +49 30 7262 18164
robert.briske@osborneclarke.com

John Buyers
Partner
T +44 20 7105 7105
john.buyers@osborneclarke.com

John Davidson-Kelly
Partner
T +44 20 7105 7024
john.davidson-kelly@osborneclarke.com

Rafael Garcia Del Poyo
Partner
T +34 91 576 44 76
rafael.garciadelpoyo@osborneclarke.com

Chloe Deng
Partner
T +44 20 7105 7188
chloe.deng@osborneclarke.com

Grégoire Dumas
Counsel
T +33 1 84 8 24548
gregoire.dumas@osborneclarke.com

Georgina Graham
Partner

T +44 117 917 3556
georgina.graham@osborneclarke.com

Gianna Hendriks
Associate

T +31 20 702 8642
gianna.hendriks@osborneclarke.com

Mary Lawrence
Partner

T +44 117 917 3512
mary.lawrence@osborneclarke.com

Roderick Nieuwmeyer
Partner

T +32 2 515 9423
roderick.nieuwmeyer@osborneclarke.com

Olgierd Swierzewski
Partner

T +48 502 198 010
olgierd.swierzewski@osborneclarke.com

Joanne Zaaijer
Partner

T +31 20 702 8622
joanne.zaaijer@osborneclarke.com

Paul Harris
Partner

T +44 20 7105 7441
paul.harris@osborneclarke.com

Ashley Hurst
Partner

T +44 20 7105 7302
ashley.hurst@osborneclarke.com

Gianluigi Marino
Partner

T +39 02 5413 1769
gianluigi.marino@osborneclarke.com

Will Robertson
Partner

T +44 117 917 3660
will.robertson@osborneclarke.com

Mark Taylor
Partner

T +44 20 7105 7640
mark.taylor@osborneclarke.com

Guohua Zhang
Partner

T +86 21 6279 8808
guohua.zhang@oclegalchina.com

About Osborne Clarke

Osborne Clarke is an international legal practice with over 2,800 employees at 26 locations worldwide, including more than 280 lawyers in Berlin, Hamburg, Cologne and Munich. With the claim "Helping you succeed in tomorrow's world", extensive industry knowledge through networking and outstanding expertise in the digital transformation of business models, Osborne Clarke advises and represents companies, entrepreneurs and investors in all practical business law issues focusing not only on our chosen sectors but also on the three key topics of digital transformation, decarbonisation and urban dynamics.