Position Paper

Digital Omnibus – Data Aspects

January 2026

AFME broadly welcomes the European Commission's proposals in relation to data policy under the Digital Omnibus initiative. In particular, we are supportive of the Commission's intention to consolidate and streamline data rules, as well as to clarify and tailor existing requirements to ensure they are fit-for-purpose also for AI training and development. We are also highly supportive of specific proposals to provide simplification for EU-based companies, such as the proposed extended deadline and higher threshold for data breach notifications.

In this context, we have identified key issues under the GDPR that may benefit from further clarifications, such as e.g. the definition of personal data, the definition of anonymous data, data subject rights, and data restrictions. Clarifications on these topics will ensure that the Digital Omnibus delivers on its policy objectives of simplification.

GDPR Issues List

- **Definition of Personal Data**: the proposal seeks to clarify that data will not be considered personal from the perspective of an entity when that entity cannot identify the natural person to whom the information relates taking into account the means "reasonably likely to be used" by the same entity. This may potentially apply to pseudonymised data (e.g., Jack Doe becoming John Smith) but also to data that can be considered "partial" (e.g., IP address with the last octet removed) because in both cases the receiving entity might not have the additional information needed to identify the natural person(s). Therefore, we request clarification on how the new definition of personal data might apply to such scenarios. Also, while this provision comes from a ruling by the Court of Justice of the European Union, its practical interpretation and implementation may require companies to perform an additional assessment on a case-by-case basis. Therefore, we support further regulatory guidance, as envisaged by the newly proposed Art. 41.a GDPR, to provide clarifications on the actual implementation of the new definition of personal data.
- **Definition of Anonymity from the Controller's Perspective**: we request clarification on the point at which data should be regarded as anonymous from the perspective of the data controller. Specifically, we seek guidance on whether the definition of anonymous data may apply where the controller shares data that is pseudonymised at the controller's level but is considered anonymous by the receiving third party; or whether data must be fully anonymised at the controller's level to ensure that individuals cannot be identified by any party involved.
- **Use of Legitimate Interest for Anonymization:** we request clarification on when and under which conditions data controllers may invoke legitimate interest as a basis for processing personal data with the aim of anonymising it, particularly when the primary goal of utilising anonymized data is commercial.
- **Restrictions under Article 23 of the GDPR:** we request clarification on whether data controllers can invoke the restrictions in Article 23 of the GDPR to withhold

Association for Financial Markets in Europe
London Office: Level 10, 20 Churchill Place, London E14 5HJ, United Kingdom T: +44 (0)20 3828 2700
Brussels Office: Rue de la Loi 82, 1040 Brussels, Belgium T: +32 (0)2 883 5540
Frankfurt Office: c/o SPACES – Regus, First Floor Reception, Große Gallusstraße 16-18, 60312, Frankfurt am Main, Germany T:+ 49 (0)69 710 456 660
www.afme.eu

Company Registration No: 6996678 Registered Office: Level 10, 20 Churchill Place, London E14 5HJ
AFME is registered on the EU Transparency Register, registration number 65110063986-76

certain information from data subjects when those subjects ask whether any authority has requested their information. For example, in the banking sector, if authorities request information about individuals during ongoing investigations, certain national laws prohibit banks from disclosure[1]. Additionally, authorities often specifically instruct data controllers not to inform subjects about such investigations. However, there are situations where these instructions for non-disclosure are not given, and the investigations may not be directly related to crimes covered, e.g., by money laundering laws. In such cases, the bank may be aware of an investigation, and disclosing any information could potentially compromise the judicial process.

- **Data Subjects Rights**
    - **Access Requests**: we support a clear definition and examples of use cases that would qualify as unfounded or excessive (e.g. to access data to be used for ongoing legal proceedings instead of going through official channels, ask for the IP address used to access a service). .We also propose explicitly amending art. 15 GDPR to acknowledge within art. 15 itself that overly broad and/or undifferentiated access requests could be disregarded on the ground of their excessiveness (rather than simply stating it in Recital 35 of the Digital Omnibus)."
    - **Obligation to Inform Data Subjects on Data Processing**: regarding the controllers' obligation to inform data subjects about the processing of their personal data and the removal of this obligation in situations where there are reasonable grounds to assume the data subject already possesses the information, we support further guidelines with practical examples to clarify the conditions under which this assumption of prior knowledge is valid. Specifically, we would appreciate clarifications on whether publishing the information on the entity's website is sufficient, and on whether knowledge can be presumed when the data subject is the direct source of the data.
- **Derogations under Article 49 sec. 1 of the GDPR:** whilst not explicitly covered by the Digital Omnibus, we would highly welcome a sectoral exemption for large-scale data transfers to third countries (without an adequacy decision) applicable for the financial industry, in particular when it comes to transmitting EU personal data from banks located in the EU to service providers located in third countries, e.g. in conjunction with rendering custody services in those countries. In such scenarios, it would be more efficient to rely upon the Art. 49 derogations rather than concluding EU Standard Contractual Clauses with the third country data recipients. However, in view of recital 111 of the GDPR, data transfers on the grounds of the derogations available under Article 49 sec. 1 (b), (c) and (e) of the GDPR may take place "where the transfer is occasional and necessary in relation to a contract (…)". In general, although the derogations relating to the performance of a contract may appear to be broad, they are being limited by meeting the criteria of "necessity" and, more importantly, of "occasional transfers". Reference is made to the Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 as of 25 May 2018 issued by the EDPB (pages 8 ff.). This has the negative consequence of impeding any large-scale data transfers to third country recipients in the normal course of business, as those data transfers are not "occasional transfers". Also, where data transfers present minimal risk - such as those involving small datasets, non-sensitive information, or intra-group flows - the European Commission could consider establishing a legislative threshold to determine when supplementary measures are required. As possible solutions, transfers falling below such a threshold could rely on internal risk assessments and baseline security controls, while transfers exceeding the threshold could remain subject to the full requirements set out in Chapter V of the GDPR.

[1] For example, German law prohibits banks from disclosing this information to data subjects as specified in Article 47 of the Money Laundering Act (GwG)