March 9, 2026

Appendix to the position paper: Statement on the individual provisions in the Digital Omnibus Package

On November 19, 2025, the European Commission presented its seventh omnibus package and is seeking comments on it until March 13, 2026. This position paper comments on the proposed regulations contained therein for a "Digital Omnibus" on data, a "Digital Omnibus on AI," and a proposed regulation on European Business Wallets.[1] The proposed regulations are currently only available in English.

a) Digital Omnibus (Data): Amendments to the Data Act

Regulation	Content	Opinion
---	Integration of FFDR, DGA, Data Act, Open Data Directive in the Data Act	**Integration is generally useful**, as the system is currently unclear and there are overlaps between legal acts. However, converting the Open Data Directive into **regulatory law** is not without its problems: The Directive is about control over public sector information, its availability and reuse (Rec. 16), which may be **relevant** to **the internal and external security of Member States**. **As an alternative** to integrating the rules on data reuse in the Data Act, the **DGA provisions** on this could also be **integrated into the Open Data Directive**, leaving Member States room for maneuver in their implementation.
---	Criminal data retention is regulated separately	This makes sense, as it is **a separate issue:** access to personal data for security purposes.
Art. 1(2)(d)	Inclusion of the DGA provisions on data intermediation services/data altruism in the Data Act	The rules have **not proven effective** and should be removed without replacement. A subsequent evaluation (Art. 1(26) = Art. 49 Data Act, new version) offers no discernible added value.
Art. 1(2)(e)	Definition of 'medium-sized enterprise'/'small mid-cap'	**Multiple categories of small businesses** subject to special regulations **reduce legal clarity**. They also indicate that the rules of the Digital Omnibus continue to place an excessive burden on the economy.

[1] COM(2025) 836 final and COM(2025) 837 final.

Regulation	Content	Opinion
Art. 1(3), (4)	Introduction of a right of refusal for trade secret holders regarding data access (Art. 4(8), Art. 5(11) Data Act)	The obligation of data recipients to protect the **trade secrets** of the original data owner leads to **risks** for the data owner **that are difficult to assess**. In this respect, the agreement between the product user and the recipient constitutes a contract at the expense of third parties (the original data owner). **Legal uncertainty** due to the combination **of legal terms that are highly subject to interpretation** ("exceptional circumstances," "highly likely," "serious economic damage," "on a case-by-case basis"). **Data access** should be structured **in accordance with** the Data Act **and the EHDS Regulation**. The regulatory approach of the Data Act is fundamentally flawed.
Art. 1 (6)-(14)	Limiting data access for public authorities to cases of "public emergency" instead of "exceptional need"	This restriction **reduces the** potential **burden** on companies and appears **unproblematic** in view of the goal of competitiveness.
Art. 1 (15)	Regulations on cloud switching (Art. 23 ff. Data Act) are simplified (new Art. 31 (1a), (1b) Data Act).	**Regulatory approach is to be questioned:** In addition to storage, there is also demand for very specific services → The need for isolated switching rules in Art. 23 ff. Data Act remains unclear overall. Migration is made more difficult not so much by incompatible functionalities as by incompatible software architectures/interfaces and data formats.
Art. 1(16)	Reuse of public data subject to the proviso that access by third countries can be prevented (Article 32 Data Act)	This makes sense in order **to strengthen resilience in the EU's external relations.** **However, the wording of the provision is unclear:** references to other provisions, legal terms requiring interpretation ("minimum amount of data permissible"; "reasonable interpretation").
Art. 1(17)	Deletion of the provision on smart contracts (Art. 36 Data Act)	Makes sense as the provision is impracticable and leads to legal uncertainty (according to the EU Commission itself; COM(2025) 837 final, p. 5 and recital 16).

Regulation	Content	Opinion
Art. 1(18)	Adoption of DGA provisions on data intermediation services and data altruism	The **provisions** have **not proven effective** and, instead of the planned streamlining within the Data Act (Art. 32a ff. new version), would be better removed without replacement. A subsequent evaluation (Art. 1(26) = Art. 49 Data Act new version) offers no discernible added value.
Art. 1 para. 18	Adoption of DGA regulations on the reuse of public data	The **adoption of these provisions (Art. 32i ff. Data Act, new version) makes sense**. This will create uniform standards for public data. The **consolidation with the provisions of the Open Data Directive (Art. 32n ff. Data Act, new version)** also makes sense, but is not without problems due to the importance of the data concerned for the sovereign information management of the Member States (see above, line 1). In particular, the provisions on the **identification of "high-value datasets"** (Art. 14 Directive (EU) 2019/1024; Art. 32v Data Act, new version) also contain many legal terms that require interpretation. As a result, they contribute **little** to **legal certainty**. In any case, it would be better to comprehensively standardize the rules for public data, insofar as it can be used for statistical or scientific purposes: • Data access has so far been regulated in a fragmented manner (see also Directive 2007/2/EC; Directive 2003/4/EC); • Duplications in special regimes, such as for health data (Regulation 2025/327 – EHDS), should be reduced for greater legal clarity (e.g., regarding rights/documentation/compliance requirements).
Art. 1(18)	Inclusion of the FFDR data localization ban in the Data Act	The incorporation of **the data localization ban (Art. 32h Data Act, new version) is justifiable**, but its practical significance is likely to be limited. The removal of the FFDR provisions on codes of conduct for data sharing is justifiable due to their limited regulatory effect.

Regulation	Content	Opinion
		However, in the interests of **promoting interoperability and uniform** data formats in general, the **scope of Art. 33 ff. of** the Data Act should be **extended beyond European data spaces**.

b) Digital Omnibus (Data): Amendments to the General Data Protection Regulation (GDPR)

In anticipation of the presentation of the Digital Omnibus, Germany had submitted proposals to the European Commission for simplifying the GDPR. This **"German proposal for simplification of the GDPR"** was published by Netzpolitik.org on October 23, 2025, and was incorporated into the Digital Omnibus package following the impact assessment. It is therefore also taken into account in the following comments.

GDPR

Regulation	Content	German position	Statement
---	Summary of GDPR and e-Privacy Directive 2002/58/EC.	---	Makes generally sense.
---	---	Call for a better balance between the protected interests concerned: • General personal rights of those affected by data processing • Economic freedom/ freedom of science of data processors	Additional considerations: • Public interest in data use for the fulfillment of public interest obligations • Digital sovereignty (resilience) vis-à-vis non-EU countries; but also limits for EU industrial policy (Art. 173 TFEU)

Regulation	Content	German position	Statement
Art. 3(1)	Revised definition of "personal data" (Art. 4 GDPR):	---	Introduction of a "subjective approach" that limits the scope of the law to situations in which a person can be identified by a specific company. The new provision implements ECJ C-413/23 P – *EDSB*. However, it carries the risk that **companies** will **strategically** exclude themselves from **collecting** personal **data**, but at the same time ensure that they provide their business partners with data that may be personal (without the data subjects having a direct relationship with these other companies). In addition, the assessment of data collection under the GDPR is made more difficult by terms that are highly open to interpretation ("not [...] personal [...] where that entity cannot identify the natural person [...] taking into account the means reasonably likely to be used by that entity"). In this respect, the new provision is likely to cause **considerable difficulties** in terms of evidence in disputes. It would be **better to align** the **scope of the GDPR more closely with the relevant fundamental rights issues** and, in particular, to differentiate between government and company data processing.
---	---	Examination of **a 3-layer model** (see, for example, Wendehorst): Extensive obligations for large companies, regular obligations, reduced obligations/exceptions for SMEs and non-economic activities	**To be rejected: The need for protection of data subjects does not depend on the size of the processing company, but on the risks of processing** ("same risk – same regulation"). Data protection requirements must also be limited to what is necessary in order to be compatible with entrepreneurial freedom (Art. 16 CFR). The necessary requirements can usually be implemented better by large companies than by smaller ones. Large companies have more resources for this.

Regulation	Content	German position	Statement
			It would be **better to align** the **scope of the GDPR more closely with the relevant fundamental rights issues** and, in particular, to differentiate between government and company data processing.
Art. 3(2)	Feedback of the principle of purpose limitation (Art. 5(1)(b) GDPR) to the purpose limitation rule in Art. 6(4) GDPR	---	Clarification makes sense.
Recital 30 f.	Data use for AI training should be recognized as a "legitimate interest."	Safe harbor for setting up AI systems in compliance with the GDPR.	**The Digital Omnibus refrains from amending the wording of the law (Art. 6(1)(f) GDPR). The regulation is therefore insufficient to create legal certainty.** This would also require rules on the use of copyright-protected content and trade secrets for the training of AI models.
Art. 3(3)	Restriction of protection for specially protected data (Art. 9 GDPR) for cases involving the training of AI models and the processing of biometric data for identity verification	Access to specially protected data (Art. 9 GDPR) should (only) be simplified in emergency situations (e.g., pandemic).	The **exemption** of the use **of** specially protected data **for AI training purposes** serves to protect entrepreneurial freedom (Art. 16 CFR) in the development of innovative AI products, but **severely restricts the protection of fundamental rights for data subjects.** The **requirement** that appropriate **technical and organizational measures** must be taken to minimize the collection of relevant data and to protect such data (Art. 9(5) GDPR, new version) **is not sufficient.** In addition, the legal position of data subjects would have to be strengthened, e.g., by a presumption rule with regard to damages. Compatibility with Articles 7 and 8 of the Charter of Fundamental Rights of the European Union is therefore doubtful. With this provision, the EU legislator is failing to fulfill its **duty to protect** consumers from **the risk of exploitation**.

Regulation	Content	German position	Statement
			The **use of biometric data** should be limited to cases where the data is under **the sole control of the person concerned**. The provision appears reasonable. The **German proposal is sensible.**
Article 3(4)	Restriction of free information about data collection from the data subject or elsewhere (Article 12(5) GDPR).	Restriction of abusive requests for information (Art. 15, 57 GDPR).	The **Digital Omnibus** regulation restricts the right to free information for abusive requests for information, with the burden of proof for abuse lying with the data processor. The **regulation appears reasonable.** The German proposals, on the other hand, are too cumbersome.
Art. 3(5)	Limitation of information about data collection from the data subject (Art. 13(4) GDPR) within the framework of existing legal relationships and where information is already available to the data subject.	Reduction of information obligations (Art. 13 GDPR): Companies should only provide relevant information on their own websites.	**The Digital Omnibus rule set** restricts the right to information in cases where the data subjects do not need the information to exercise their rights. The regulation contains many legal terms that require interpretation ("clear and circumscribed relationship"; "activity that is not data-intensive"; "reasonable grounds") and therefore seems **hardly practicable.** It would be better to simply have the data subjects contribute to the costs of providing the information. **The German proposal is problematic because of the risk of manipulation.** If anything, relevant information should be provided on trustworthy third-party websites. The **exceptions** (disclosure to third parties; special vulnerability) **outline fundamental rights limits.** These exceptions should therefore be mandatory in principle.
Art. 3(6)	Restriction of free information about data collection for scientific purposes	---	The regulation **restricts the possibilities for using data for scientific purposes.** It contains many legal terms that require interpretation ("disproportionate effort"; "seriously impair"; "appropriate measures") and therefore appears to **be impractical**. It would be

Regulation	Content	German position	Statement
			better to simply require applicants to contribute to the costs of providing the information.
Art. 3(7)	Limitation of the right not to be subject to automated data processing (including profiling) (Art. 22(1) GDPR)	---	The **provision restricts legal protection.** However, it takes into account the fact that in practice, the right exists only on paper anyway. It appears **reasonable.**
Art. 3(8)	Extension of the deadlines for reporting breaches; uniform reporting office and transitional regime; forms (Art. 33 GDPR).	Necessary simplification of the reporting of breaches; replacement of the 72-hour deadline with a deadline of 3 working days (Art. 33 GDPR).	The provisions of **the Digital Omnibus facilitate legal protection** for data subjects and **tend to reduce the administrative burden.** Thus, they appear reasonable.
Art. 3(9)	Clarification of the necessity and requirements for data protection impact assessments (Art. 35 GDPR)	---	The provision provides for standardization ("common template"), but uses terms that require interpretation with regard to the requirements to be specified. In the interest of legal clarity, it would be useful if at least the **sectors** in which **data protection impact assessments** are to be **carried out** were **defined**.
Art. 3(10)	Authorization of the EU Commission to adopt delegated legislation with regard to pseudonymization	Clarification: Anonymized data are not personal data – but anonymization is the processing of data worthy of protection.	The provision in the Digital Omnibus cannot create legal certainty: the **removal of the personal reference is a question of fact. The provision should be rejected.** The **German proposal, on the other hand**, is **useful for clarifying the term "data processing."**
---	---	In Art. 42 ff. GDPR, more scope should be given to certifications, in particular through the possibility of manufacturer/supplier	The Digital Omnibus has not taken up the **German proposal**. Nevertheless, the proposal appears to be **sensible.**

Regulation	Content	German position	Statement
		certification, rather than holding processors solely liable.	
	---	Additional regulations on youth/consumer protection.	The German proposals were not taken up in the Digital Omnibus, but appear sensible.
	---	Guidelines for data protection in archiving.	
	---	Facilitation of data use for R&D if the specific purpose of use is not yet known at the time of data collection.	

c) GDPR and ePrivacy Directive (Directive 2002/58/EC)

Regulation	Content	Opinion
Art. 3(15); Art. 5(2)	Restriction on the placement of cookies and similar items on users' end devices; in this respect, new rules in Articles 88a and 88b GDPR are based on the previous Article 5(3) of Directive 2002/58/EC.	The fact that the **Digital Omnibus** does not merely provide for an opt-out for tracking cookies, as previously reported in the press, is to be welcomed. **Tracking cookies are problematic in terms of general terms and conditions and data protection law.** Their use should be restricted in the long term in favor of more privacy-friendly technologies, such as a decision screen in the web browser (cf. Art. 88b (6) GDPR) . However, it should be noted that central control of consent, e.g., via a web browser, is **difficult to implement** because consent is granted for specific purposes. The proposed regulations should therefore be reviewed in order to achieve a fair balance between the interests of intermediary services, the advertising industry, and consumers as holders of fundamental rights.

Regulation	Content	Opinion
		Apart from that, consideration should be given **to integrating Directive 2002/58/EC into the GDPR as a whole** for the sake of legal clarity**.**
Art. 5(1)	Deletion of Art. 4 Directive 2002/58/EC	The provision to be deleted sets out requirements for the security of data processing, but is likely to be superseded by Article 25 GDPR and Directive 2022/2555 (NIS 2).

d) Digital Omnibus (Data): Amendments to the NIS 2 Directive

Provision	Content	Opinion
Articles 6-9	Single point of contact for IT security incidents (NIS2 Directive, eIDAS Regulation, Critical Entities Regulation, DORA; GDPR)	The provisions of **the Digital Omnibus facilitate legal protection** for those affected and **tend to reduce the administrative burden.** They therefore appear reasonable.

e) Digital Omnibus on AI: Amendments to the AI Regulation

Regulation	Content	Opinion
---	The Digital Omnibus on AI is intended to remove implementation difficulties that could jeopardize the effective start of application of the main provisions of the AI Regulation (COM(2025) 836 final, p. 2).	**Amendments to the AI Regulation are not sufficient to create legal certainty and reduce bureaucratic burdens.** To achieve this, it would be necessary, in particular, to eliminate the duplication of obligations/liabilities under the AI Regulation on the one hand and the GDPR/AVMD/DSA/Directive on unfair commercial practices, etc. on the other in relation to the generation of AI outputs. Furthermore, under the current AI Regulation**, almost all relevant risks** are considered **potentially systemic** (except for Art. 51 ff.). A distinction should be made here in order to take greater account of the market significance of the respective application.

Regulation	Content	Opinion
---	Announcement of 13 further guidelines to clarify the AI Regulation and facilitate its application	**A multitude of supplementary guidelines does not contribute to legal certainty and ease of application.** The need for such guidelines indicates a failed regulatory approach in the AI Regulation. The guidelines also increase the implementation effort to an extent that is likely to be manageable only by larger companies.
Art. 1 (1), (3)	Extension of privileges for small businesses (SMC in addition to SME).	**Multiple categories of small** businesses subject to special regulations **reduce legal clarity**. They also indicate that the rules of the AI Regulation continue to place an excessive burden on the economy even after the Digital Omnibus on AI. In any case, it would be **better** to have an exception that removes the regulation for **small-scale use of AI**, regardless of the size of the company.
Art. 1 (4)	Revised version: Instead of requirements for AI competence in Art. 4 AI Regulation, now support for AI education (AI literacy).	The provision contains only a vague requirement that fails to take into account that, on the one hand, the EU Commission has no educational mandate and, on the other hand, the Member States already have all the necessary legal powers to promote AI education (Art. 4(1), Art. 5(1), (2) TEU)**.** The provision has **no discernible added value.**
Article 1(5), (7)	Authorization to use personal data within the meaning of Art. 9 GDPR (see Recital 6) for AI training instead of the previous Art. 10(5) AI Regulation (Art. 4a AI Regulation, new version).	The provision defines **narrow conditions** under which special categories of personal data may be accepted for the identification of bias. It is based on terms that require interpretation ("exceptionally process"; "suitable safeguards"). The provision contributes only to a limited extent to additional legal clarity.
Art. 1(6), 14	New regulation on self-assessment as an operator of non-high-risk AI (Art. 6(4), 49(2) AI Regulation).	The new provision **reduces the procedural burden** because **it eliminates** the need for **registration in an EU database.** It is to be welcomed.
Art. 1(8)	Requirements for the technical documentation of high-risk AI systems (Art. 11(1) subparagraph 2).	The **documentation requirements** of the AI Regulation are problematic overall: they are very extensive and also **deviate from general market regulation law** , according to which government agencies only intervene in the market in cases of abuse and concrete imminent danger. Rather, the obligations enable close monitoring, as is the case, for example, in financial supervisory law, where systemic risks

Regulation	Content	Opinion
		must be averted. With regard to high-risk AI systems, however, the revised provision, including the limitations for small businesses, is **reasonable**.
Art. 1 (9)	Size-dependent requirements for quality management systems (revised Art. 17(2) AI Regulation)	The **regulation is unclear** because it defines requirements in relation to a goal that is itself value-dependent ("respect the degree of rigour and the level of protection required to ensure compliance").
Art. 1(10)-(15)	Various amendments to notifications, conformity assessments, and practical guidelines (Articles 28-30, 43, 50 of the AI Regulation).	The changes serve to **simplify administration** and speed up procedures. In this respect, they are to be welcomed.
Art. 1(16)	Monitoring of guidance documents: sub-delegation to the EU Commission (Art. 56(6) CRR).	The provision can contribute to **more effective supervision**, if deemed necessary, and increases the transparency of the supervisory system for market participants. In this respect, it is to be welcomed.
Art. 1 (17)-(19)	Authorization for AI real-world laboratories at EU level; further regulations on AI real-world laboratories (Art. 57(3a) AI Regulation, new version).	The need for **AI regulatory sandboxes** (Art. 57 et seq. AI Regulation) arises solely from the fact that AI in the EU is subject to extensive special monitoring, with obligations that nevertheless overlap with other rules (GDPR, consumer protection law, etc.). In this respect, the market significance of AI is not sufficiently taken into account, depending on the intended use, if the risks are regulated as (at least potentially) systemic risks. The regulations on AI regulatory sandboxes thus **demonstrate** the existing **overregulation.**
Art. 1 (20)	New regulation on testing high-risk AI systems under real conditions outside regulatory sandboxes (Art. 60a new version of the AI Regulation).	The provision is **at odds with the regulatory approach of the AI Regulation**, which regulates AI systems according to their (potentially systemic) risk and only provides for regulatory sandboxes, and these only at the Member State, regional, or local level—i.e., with limited impact in the event of risk realization. The provision is also **already outdated due to developments:** In recent years, AI models for general use – albeit not defined high-risk AI systems – have been rolled out on the market. Although widespread use **to test and improve systems under**

Regulation	Content	Opinion
		real-world conditions is still **not the legal norm, it is in practice an essential part** of the development and refinement of AI systems.
Art. 1 (21), (23)	Exceptions to quality management system requirements for small businesses; consultation (Art. 63(1), Art. 70(8) AI Regulation, new version).	These provisions are again **necessary because the AI Regulation**, with its approach that does not differentiate between potential system risks, **can lead to disproportionate requirements** in individual cases**.** Instead of a rule based on company size, it would also be **better** in this context to withdraw the regulation for **small-scale use of AI**, **regardless of company size**.
Art. 1(25), (26)	Concentration of responsibilities for market surveillance at EU level; cooperation between authorities (Art. 75, 77 AI Regulation).	The amendments serve to **simplify** administration and, if deemed necessary, can contribute to **more effective supervision**. In this respect, they are again to be welcomed.
Art. 1(27), (28)	Codes of conduct and guidelines for small businesses (Art. 95, 96(1) CSR)	Instead of a regulation based on company size, the **extent to which AI technology is used** in the company should once again be **the decisive factor**. For all companies with only limited use of AI, regulatory support in the form of simplified guidelines/codes of conduct is equally useful.
Art. 1(29)	Extension of enforcement and sanction rules to additional small businesses (Art. 99 AI Regulation)	The provision continues to regulate only **sovereign enforcement** by authorities of the Member States. It is open with regard to civil law protection. This causes **legal uncertainty as** to **the relevance** of the requirements of the AI Regulation **in civil law relationships**.
Art. 1 (30), (31)	Postponement of the date of application of the AI Regulation (Art. 111, 113 AI Regulation).	**The provisions are to be welcomed if only because of the AI Regulation's misguided regulatory approach. It would be better if the regulation were withdrawn altogether and new provisions adopted that strike a better balance between risk protection and the promotion of innovation.**

f) Proposed regulation on EU wallets for businesses (European Business Wallets)

Regulation	Content	Opinion
Art. 2	Scope: Provision and acceptance of European Business Wallets and suitable holder identification data; use of European Business Wallets.	The European Business Wallet should be usable not only for companies, but also for data transfers in the context of research and development.
Art. 6 (1)	Functions of European Business Wallets	The provision makes sense, especially insofar as interaction between European Business Wallets and European Digital Identity Wallets must be ensured. However, suitable identity functions should also be created for research and development.
Art. 7(2)	Providers of European Business Wallets must be based in the EU.	The provision is reasonable in order to ensure legal enforcement vis-à-vis providers and thus their trustworthiness.
Art. 9(1)	Use of uniform identifiers assigned by a company	In addition to companies, research institutions should also be able to acquire a uniform identifier. The possibility of identity management via European business wallets may additionally be relevant in the context of research and development outside an entrepreneurial context.
Art. 9(2)	Assignment of a unique identifier on the basis of an implementing act	In addition to the unique identifiers assigned by Member States in accordance with the provisions implementing Directive 2017/1132, identifiers developed by international organizations such as the GLEIF Legal Entity Identifier should also be recognized as "unique identifiers" valid throughout the Union.
Art. 10(4)	Directory of European Business Wallet holders	In addition, there should be a freely accessible register providing information on restrictions on the use of signatures issued using a European Business Wallet.

* * *