WE ARE SHAPING THE INTERNET.
YESTERDAY.TODAY.BEYOND TOMORROW.

POSITION PAPER

On The REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus)

Berlin, 2 March 2026

I. Summary

eco welcomes the Digital Omnibus as an important step toward simplifying the European digital regulatory framework and strengthening legal certainty for data-driven innovation, while maintaining high standards of fundamental rights protection. In particular, eco supports the proposed clarification of the definition of personal data, the proposed changes on AI processing in articles 9 and 88 (c) as well as the transfer of the cookie related provisions from the ePrivacy Directive to the GDPR , as it introduces a more risk-based approach that reduces unnecessary over-compliance and facilitates responsible data use without weakening individual protections. eco also supports the consolidation of non-personal data legislation within the Data Act and the objective of creating a clearer horizontal framework. At the same time, merely integrating existing legal acts risks perpetuating structural complexity. A more coherent long-term architecture of the data acquis, harmonised supervision and clearer definitions remain necessary to ensure legal certainty and practical usability.

With regard to open data, eco expresses concern about the introduction of differentiated conditions and higher fees for very large enterprises, as non-discriminatory access remains essential for fostering trust-based data sharing. Stronger safeguards for trade secrets under the Data Act are welcomed but should be further strengthened to prevent misuse and security risks.

eco supports the restriction of mandatory B2G data access to clearly defined public emergencies under Chapter V, enhancing proportionality and trust. However, Chapter VI continues to raise concerns regarding unclear scope, rigid switching deadlines, interoperability requirements and the phase-out of switching charges.

The extension of certain exemptions to small mid-cap companies is welcomed, while overall regulatory complexity should remain manageable for all businesses. eco further calls for binding guidance to reduce legal uncertainty in data classification and stronger coordination of enforcement across Member States. Finally, eco welcomes simplifications in ePrivacy and cybersecurity incident reporting, while highlighting the need for robust technical implementation.

II. Detailed Assessment

- **On personal Data**

The use of data is essential for a growing number of digital business models as well as for research, innovation and the performance of public tasks. At the same time, personal data is subject to special protection due to its potentially sensitive nature. In the European Union, the General Data Protection Regulation (GDPR) governs under which conditions, and for which purposes such data may be processed. In practice, however, companies are often confronted with considerable legal uncertainty when dealing with personal data, particularly with regard to the distinction between personal, pseudonymised and non-personal data.

The Digital Omnibus addresses this issue and provides targeted clarifications to the GDPR in order to increase legal certainty and facilitate, in accordance with the SRB caselaw of the EU courts, responsible data use without jeopardising the high level of protection of fundamental rights. Specifically, the Commission proposes to further specify the definition of personal data in Article 4 GDPR. It is intended to clarify that information should only be considered personal data for a given legal entity if that entity has means reasonably likely to be used to identify the natural person concerned. eco equally welcomes the new provisions on special categories of personal data in an AI context (Articles 9(2)(k) and 9(5)), which recognise that, in the development of AI systems, exposure to special categories of data may in certain circumstances be unavoidable. This approach is consistent with relevant CJEU case law and with regulatory guidance on the processing of sensitive data in an AI context. While acknowledging that such processing must be subject to robust safeguards, eco recommends greater flexibility in the formulation of the requirements under Article 9(5). In particular, this could include explicitly recognising anonymisation as a valuable measure alongside the removal of data, as well as providing additional clarity regarding what constitutes “appropriate” organisational and technical measures. The mere theoretical possibility that another entity could identify individuals should not automatically trigger the applicability of the GDPR.

The Digital Omnibus furthermore proposes amendments to Article 22. Lenders may rely on Article 22(2)(a), which allows automated decision-making where it is necessary for entering into, or the performance of, a contract between the data subject and the data controller. eco considers that it should be clarified that Article 22(2)(a) is not limited to the narrow act of concluding or performing a contract, but also covers pre-contractual decision-making processes, including the involvement of third parties acting on behalf of the contractual partner, provided that such activities are directly linked to a potential contractual relationship. Corresponding examples in the recitals would support a harmonised and practical application.

eco further considers that the proposed changes to Article 22, enabling automated decision-making subject to appropriate safeguards, provide important flexibility and legal certainty to support AI-driven innovation, particularly in a B2B context, including use cases such as agentic AI and AI-powered Know-Your-Customer (KYC) verification tools.

eco supports efforts to harmonise Data Protection Impact Assessment (DPIA) processes under Article 35 GDPR, in particular through the establishment of a single EU-level approach instead of divergent national lists. Greater harmonisation would reduce administrative burden for organisations operating across multiple Member States and help address existing fragmentation in the application of DPIA requirements. The clarifications regarding data subjects' information rights and data access requests under Articles 12, 13 and 15 GDPR, are also welcomed by eco. From the perspective of the Internet Industry these clarifications can help to reduce abusive access requests and unjustified compensation claims. In this context, further clarification at EU level would be beneficial, in particular by explicitly recognising that organisations should only be required to conduct reasonable and proportionate searches when responding to data subject requests.

- **Acknowledging AI and Sensitive Data**

eco also supports the new concept of scientific research (Article 4(38)), which clarifies that the GDPR provisions on academic research also apply to projects involving commercial participation. This is fully consistent with Recital 159 of the GDPR.

eco supports the objective of creating greater clarity regarding Data Protection Impact Assessments (DPIAs), as well as achieving EU-wide consistency on the circumstances under which they are required. At the same time, eco emphasises that DPIA methodologies and templates should remain non-binding rather than prescriptive. Otherwise, this could create additional costs for controllers who would need to adjust their existing frameworks and would limit their ability to tailor DPIAs to the specific characteristics of individual processing activities. Therefore, eco proposes not to include such templates in an Implementing Act.

- **On the Data Acquis**

In its draft, the Commission proposes to consolidate legislation on non-personal data within the Data Act. In particular, the Data Governance Act (DGA), the Free Flow of Data framework and the Open Data Directive are to be integrated into the Data Act, while certain outdated provisions of these instruments are to be repealed without replacement. The current data regulatory framework is fragmented, consisting of European regulations such as the Data Act and the Data Governance Act as well as numerous sector-specific rules. In addition, overlaps with the GDPR create further uncertainty. From the perspective of the internet industry, a clear horizontal framework is needed that operates across sectors, is technologically neutral and avoids double regulation. Equally important is a streamlined and unified supervisory structure with clearly defined responsibilities to enable

coherent decisions and provide legal certainty for companies. eco therefore fundamentally supports the Commission's initiative.

It is also positive that the Commission focuses on non-personal data in this context. Mixing different types of data would dilute the systematics and undermine the added value of the data framework for practical data use.

However, from the perspective of eco, the opportunity could have been used to rethink the data acquis more fundamentally. Merely integrating three existing legal acts into the structure and logic of the Data Act may not achieve the desired simplification effect. Rather, there is a risk that existing complexity and demarcation issues will simply be transferred into a new regulatory framework. Against this background, the association recommends developing a clearer and more coherent overall structure of the data acquis in the medium term, which more transparently reflects the functional interdependencies between the various regulatory areas. This applies in particular to the interaction between rules governing the provision and re-use of public sector data, where overlaps and differing logics between open data and protected data still exist. Further clarification is also needed with regard to inconsistent definitions of key concepts such as "data holder" or "user", as well as the tension between the protection mechanisms for trade secrets provided under the Data Act and the simultaneously far-reaching data access and sharing obligations, notably in B2B and B2G contexts

- **On Open Data**

The proposal introduces the possibility for public sector bodies, under Article 32q, to set different conditions and charge higher fees for the re-use of data by very large enterprises, including undertakings designated as gatekeepers under the Digital Markets Act. From the perspective of the internet industry, this differentiation raises concerns. Conditions for data re-use should remain non-discriminatory and innovation policy should not be limited to specific categories of market participants.

Moreover, the absence of a clear legal definition of "very large enterprise" creates legal uncertainty and risks unintended effects across the wider data ecosystem. Allowing differentiated licensing conditions may also lead to license incompatibilities, thereby limiting the ability of all stakeholders, including SMEs and civil society, to combine public sector data with other data sources to develop innovative datasets.

Rather than introducing differentiation mechanisms, policymakers should prioritise interoperable and widely recognised standard licensing models, such as Creative Commons CC0 or CC BY, in order to preserve legal certainty, usability and a level playing field in the European data economy.

- **On trade secrets in context with the Data Act**

The Commission proposes changes to the Data Act itself in the Digital Omnibus package, in particular concerning the protection of trade secrets, the chapter on

smart contracts and the provisions for providers of data processing services. eco already pointed out during the adoption of the Data Act that adjustments would be necessary in order to maintain the attractiveness of investments in data collection and processing.

The draft amends Chapter II of the Data Act to prevent the leakage of trade secrets to third countries without an adequate level of protection. Specifically, Article 4(8) allows data holders to refuse disclosure of trade secrets to a user where there is a high risk of unlawful acquisition, use or disclosure to third countries or entities under their control that are subject to jurisdictions with weaker protections than those available in the Union. The same wording is included in Article 5(11) regarding disclosure to third parties. From the perspective of the internet industry, stronger protection of trade secrets is welcome. However, eco considers the proposal not to go far enough. While we agree that the objectives of the Data Act are important, they should be balanced by equally important standards to maintain the integrity of both security and trade secret information. We recommend introducing appropriate limitations to ensure that these rights do not result in access to data by malicious actors seeking to exploit security vulnerabilities or misuse confidential commercial information.

- **On Chapter V Data Act**

The draft proposal introduces significant amendments to Chapter V of the Data Act, which governs the obligation to make data available to public sector bodies. In its original form, the Data Act allowed public authorities to request access to data not only to respond to public emergencies or, under strict conditions, for statistical purposes where other data sources were insufficient, but also more broadly for the performance of tasks carried out in the public interest. Taken together, these provisions granted public sector bodies far-reaching rights to request access to data held by private entities.

Such a broadly framed scope risked significantly increasing the number of data access requests and imposing substantial administrative and operational burdens on companies, particularly given the relatively low threshold for justification. At the same time, the framework lacked sufficiently precise and enforceable safeguards regarding how public authorities must handle accessed data, notably with respect to data security, personal data protection and the safeguarding of trade secrets and intellectual property rights. This created legal and economic risks for data holders and could ultimately discourage data generation, retention and investment. In addition, the power asymmetry inherent in B2G data sharing risked placing companies in an unequal negotiating position, as public authorities could rely on mandatory access provisions in voluntary data-sharing discussions.

Against this background, the restriction introduced by the Digital Omnibus, which limits mandatory data access under Chapter V to clearly defined public emergencies, is welcome. This narrowing strengthens legal certainty, enhances proportionality and helps restore trust in B2G data sharing as an exceptional instrument rather than a general policy tool.

- **On Chapter VI Data Act**

The Commission's draft also proposes amendments to Chapter VI of the Data Act, which establishes obligations for providers of data processing services and aims to facilitate switching between providers. Chapter VI sets out rules on contractual termination, data portability and interoperability to reduce lock-in effects and strengthen user choice. In addition, it regulates so-called "switching charges", i.e. fees incurred by users when changing providers, which are to be progressively restricted and fully abolished by 2027.

eco already highlighted potential shortcomings of Chapter VI during the legislative process of the Data Act, and one of the most fundamental issues remains insufficiently addressed by the Digital Omnibus. In particular, the definition of "data processing services" continues to lack sufficient clarity and differentiation. As currently formulated, it may cover a wide range of heterogeneous service models with fundamentally different technical and organisational characteristics. This creates ongoing legal uncertainty and risks imposing obligations that are not appropriate to the respective business models. A clearer delineation of the scope of affected services and providers is therefore urgently required.

The Omnibus introduces certain adjustments to the switching regime, notably by extending Article 31 to include exemptions for data processing services whose core functionalities are largely tailored to the specific needs of an individual customer. While this clarification is welcome, the fundamental issue of rigid transition periods remains unresolved. Switching processes, especially in complex environments, vary significantly in duration and complexity. Prescriptive deadlines do not sufficiently reflect this reality. A more appropriate approach would be to require providers to complete switching without undue delay attributable to the provider.eco is concerned that the current language introducing limits on fees collected upon termination of IaaS services in Article 31(1b) could restrict EU customers' access to fixed-term agreements and discounted pricing models, including bulk or minimum purchase arrangements. This provision appears to deviate from the original intent of the Data Act, particularly as reflected in Recital 89, which does not differentiate between types of data processing services. eco understands that it was not the intention to introduce such a prohibition and therefore encourages policymakers to address this issue during the negotiation process by removing the reference excluding IaaS services at the end of Article 31(1b).

Furthermore, eco considers that the interoperability requirements under Chapter VI remain highly far-reaching and may significantly interfere with existing business models. Excessive standardisation aimed at achieving functional equivalence risks weakening competition by driving service convergence instead of fostering innovation and differentiation. eco also recommends a thorough evaluation of the planned repository of harmonised standards and common specifications. Given that digital services continuously evolve and disruptive innovations frequently introduce entirely new service categories that render older technologies obsolete, careful

consideration is required when selecting open interoperability specifications in order to establish a framework that remains future-proof.

- **On the exemptions for SMCs**

In its current form, the Data Act provides certain reliefs and exemptions for SMEs. The Commission intends to extend these reliefs to small mid-cap companies (SMCs) so that more companies can benefit from these provisions. eco generally welcomes the fact that the Digital Omnibus introduces targeted relief for SMCs and aligns them with SMEs in selected areas. Many digitally driven growth companies exceed SME thresholds at an early stage while continuing to face similar resource and structural constraints. At the same time, such exemptions also indicate a high level of regulatory complexity that affects all companies and undermines Europe's innovation capacity. eco therefore emphasises the importance of keeping regulatory requirements overall at a level that remains manageable for all companies.

- **Reducing Legal Uncertainty**

In Data Classification eco supports the Commission's objective of simplifying data use and relieving Europe's data and AI economy from bureaucracy and legal uncertainty, both of which remain major obstacles to growth. However, the proposed measures do not address all relevant challenges faced by companies in practice. In particular, the legally secure differentiation between personal and non-personal data remains one of the most significant barriers to efficient data use despite certain clarifications in the Digital Omnibus. While the refinement of the definition of personal data is a step in the right direction, it is insufficient to eliminate persistent legal uncertainty. The assessment of whether identification is possible using means "reasonably likely to be used" continues to be interpreted differently by supervisory authorities and leads to precautionary over-application of the GDPR.

eco therefore advocates the development of binding, practical guidance on anonymisation and certain forms of pseudonymisation, as well as positive lists of typical data types and use cases that clearly qualify as non-personal data. Such clarification would reduce compliance costs and facilitate data reuse, particularly for data-driven innovation and AI applications, while strengthening data protection by allowing resources to be focused on genuinely high-risk processing activities.

According to Art. 40 GDPR, associations and organisations should be encouraged to develop codes of conduct that specify the application of the GDPR. Currently, the codes of conduct approved by the supervisory authorities do not offer sufficient legal certainty. Class actions and individual court rulings can call approved codes of conduct into question, which can lead to years of legal uncertainty. Approved codes of conduct need to be given greater legal weight. Codes of conduct should, as a rule, establish a presumption of the lawfulness of data processing, and compliance with them should lead to a stronger privilege under the law regarding liability and fines (Art. 82 & 83 GDPR).

- **On Measures for a Genuine European Data Single Market**

From the perspective of eco, the lack of uniform interpretation and enforcement of European data rules remains a key obstacle to effective data use within the internal market. Despite the harmonisation ambition of existing legislation, divergent national interpretations and supervisory practices, especially at the intersection of the GDPR, the Data Act and sector-specific rules, continue to create legal uncertainty and fragmented compliance requirements. The Digital Omnibus addresses this issue only partially. To fully unlock the potential of a European data single market, stronger mechanisms for binding coordination between competent authorities at EU level are required. This includes consistent and practical guidance with clear authority, a stronger role for European bodies in interpreting key concepts, and more efficient dispute resolution mechanisms between national authorities. Coordinated enforcement priorities and common supervisory frameworks should also be considered in order to avoid diverging regulatory expectations and uneven application of the rules across Member States.

- **On the e-privacy Directive**

eco appreciates the Commission's intention to partially integrate provisions equivalent to Article 5 of the ePrivacy Directive into the GDPR through the proposed new Articles 88a and 88b. However, the proposed simplification may fall short in the light of existing uncertainties regarding the practical application of data protection rules. The Digital Omnibus presents a timely opportunity to ajdust the ePrivacy framework by integrating the majority of its provisions into the GDPR, for example those relating to traffic data processing, or, where appropriate, aligning them with other relevant legislative instruments such as the European Electronic Communications framework and the evolving digital networks regulatory landscape. While the ePrivacy framework continues to play an important role in safeguarding the security and confidentiality of electronic communications, eco the integration of its provisions in the GDPR a solid approach for consolidation and an important step in clarifying data protection rules for both citizens and businesses. eco particularly values the security requirements established under the current framework, which remain essential to ensuring the confidentiality of electronic communications. At the same time, technological and regulatory developments, including the establishment of cybersecurity and telecommunications frameworks at EU level, have reduced the relevance of certain legacy provisions and support the case for further streamlining and modernisation.

Regarding the proposed Article 88a, which constructively aims to reduce consent fatigue, eco notes that the current exemptions from consent requirements for processing personal data on terminal equipment remain too narrow. At a minimum, the exemption for security purposes should explicitly cover security-related processing, fraud prevention, and necessary software updates. eco further considers that additional low-risk processing activities could be included in order to more effectively achieve the objective of reducing consent fatigue while maintaining a high level of user protection.

- **On Cybersecurity related incident reporting**

eco explicitly welcomes the proposed simplifications in the field of cybersecurity, in particular the introduction of a Single Entry Point (SEP) for incident reporting. The "report once, share many" principle represents an important step towards avoiding duplicate and overlapping reporting obligations under multiple EU cybersecurity and digital resilience frameworks, thereby significantly reducing administrative burdens for companies. For digitally active companies operating cross-border, a central, secure and standardised reporting channel can enhance legal certainty, improve report quality and increase reporting willingness.

At the same time, eco considers that further improvements are needed in the practical design of the Single Entry Point. The system should be technically robust, highly available and user-friendly, and should be accompanied by clear guidance on the classification of reportable incidents. eco also regrets the absence of liability protection mechanisms, which would be essential to build trust and ensure that companies feel comfortable sharing incident-related information in good faith. In addition, eco recommends extending the scope of the Single Entry Point to also cover incident and vulnerability reporting obligations under the Cyber Resilience framework in order to ensure a truly streamlined reporting environment.

From the perspective of the internet industry, the need to align the definition of 'main establishment' across EU cybersecurity and digital legislation is further emphasised. This would help to reduce regulatory fragmentation and enable companies to base their compliance structures on the location that is most relevant to their cybersecurity expertise and operational setup. The number of employees in a specific Member State should not automatically determine regulatory competence if relevant cybersecurity capabilities are located elsewhere.

Finally, eco calls for the streamlining of audits and conformity assessments across EU cybersecurity legislation through mutual recognition mechanisms and the development of common assessment tools. Avoiding repetitive and overlapping audit requirements would reduce unnecessary compliance costs for companies and ultimately benefit end-users, while maintaining a high level of cybersecurity across the European Union.

About eco: With approximately 1,000 member companies, eco (international.eco.de) is the leading Association of the Internet Industry in Europe. Since 1995, eco has been highly instrumental in shaping the Internet, fostering new technologies, forming framework conditions, and representing the interests of its members in politics and international forums. eco has offices based in Cologne, Berlin and Brussels. In its work, eco primarily advocates for a high-performance, reliable and trustworthy ecosystem of digital infrastructures and services.