**SIEMENS**

# Siemens' Position on the Digital Omnibus Proposal

## The Data Act: Fragmenting Europe's Data Ecosystem, stifling AI innovation and weakening European manufacturers

On 19 November 2025 the European Commission proposed the Digital Omnibus Regulation. It was communicated as a key step to reform the EU digital rulebook by amending the Data Act and beyond. The Commission's intention with the Digital Omnibus proposal was to improve competitiveness.

However, the Digital Omnibus proposal including the Data Act does not address industry concerns and will not improve Europe's competitiveness. The Data Act and the Digital Omnibus Proposal:

- **fail to distinguish B2B from B2C, putting EU manufacturers at a competitive disadvantage and diverting AI capabilities away from Europe**
- **pose a substantial obstacle to European manufacturers' ability to innovate and develop digital business models**
- **endanger and potentially destroy trade secrets, eroding Europe's own economic security**
- **disincentivize customized Software-as-a-Service solutions**
- **place unnecessary costs and bureaucratic burden on EU manufacturers, shrinking their competitiveness**

## What the Digital Omnibus must deliver

- Exclude the B2B sector from the scope of the Data Act. Ensure contractual freedom in B2B and repeal the mandatory transfer of product data collected by the manufacturer.

- Safeguard the manufacturer's ability to use the product data collected, especially for product improvement and developing innovative digital business models.

- Allow for and safeguard adequate protection of trade secrets as defined in the Trade Secrets Directive.

- Exempt industrial SaaS offerings from rules on switching data processing services (bare minimum: exempt all customized SaaS offerings – not only customized SaaS offerings based on contracts concluded before or on 25 September 2025). Ensure that legacy contracts remain unchanged as already foreseen for SMEs. Exclude contracts provided by customers, e.g. in public tenders, from switching rules.

## Adverse consequences caused by the Data Act

**Use case I: How the Data Act cripples Europe's Industrial AI by eroding manufacturers' ability to innovate and develop digital business models.** The Data Act is actively hampering innovation in critical applications such as industrial machinery, robotics, smart grids, railway systems, and building automation, threatening Europe's industrial competitiveness and economic security.

The B2B markets in Europe have already organized data sharing with contracts efficiently and independently. The Industrial AI sector is also building various data spaces and alliances. The B2B market does not exhibit the asymmetries that may be found in B2C sectors, where providers may hold a dominant position over an individual consumer.

Although supplier and customer needs are adequately addressed in B2B by contractual mechanisms, the Data Act imposes mandatory data transfer obligations, weakening European manufacturers. Industrial players have already negotiated data access through tailored contracts. Imposing a one-size-fits-all mandatory regulation, unilaterally aimed at manufacturers, erodes their competitiveness. The Data Act's user centric architecture curtails opportunities for product and service improvement by the manufacturer. It unilaterally strengthens the user but substantially weakens the capability of the manufacturer to use data for product and service innovations or the training of industrial AI models. It thus imposes unnecessary costs and diverts critical development resources – all while failing to address any genuine legal gap.

The Data Act also creates a structural competitive disadvantage for European Industrial AI companies. While non-EU competitors freely use collected product data to train AI models, European companies face a significant disadvantage. Under the Data Act, they must individually negotiate data-use clauses, risking fragmented training datasets due to holdouts. European manufacturers also absorb significant legal costs, directly undermining EU's own competitiveness.

The Data Act applies a regulatory logic borrowed largely from consumer/personal data frameworks but treats product data even stricter than personal data. At the same time, it ignores the reality that product data can be inseparable from trade secrets of the manufacturer. Forcing transfer of these data risks hollowing out Europe's industrial knowledge base, effectively transferring hard-won competitive intelligence to third parties, including non-EU actors with no reciprocal benefit.

The Data Act Chapter 2 does not improve industrial data access and usage. It simply converts voluntary, well-functioning data sharing into a dangerous and burdensome mandatory transfer procedure.

**Use case II: How the Data Act endangers trade secrets and erodes EU's own economic security.** The Data Act includes disclosure of sensitive and R&D-intensive data, even to competitors, unless companies can meet practically impossible conditions (e.g. reporting to competent authorities, proving severe economic damage, etc.). This effectively will cause irreversible loss of trade secrets to competitors (even in third countries), damaging competitive advantages, and eroding economic security.

The Data Act, as currently structured, risks undermining the very industrial innovation it claims to foster. By mandating overly broad data-transfer obligations, the Act erodes the incentive to invest in data-generating devices and AI development. Why invest heavily in Industrial AI and data if competitors can access the data via the Data Act? This creates a chilling effect on R&D investment, precisely when Europe needs to accelerate its Industrial AI capabilities to compete others. Rather than strengthening European industry, the Data Act risks turning Europe's industrial data into “free supply” at the expense of European innovators.

Robust protection of trade secrets as defined in the Trade Secrets Directive is paramount for investment and economic security, which is best achieved through B2B contractual and technical agreements rather than the Data Act’s approach.

**Use case III: How the Data Act creates unnecessary burden and stifles the adoption of smart systems.** Optimizing modern trains and buildings requires deploying and using thousands of sensors. Yet, the Data Act imposes an unsustainable burden: for each sensor signal, companies must continuously validate capture methods, metadata, scope, and secure access. Scaling this across tens of thousands of products means millions of discrete reviews, including separation of personal and non-personal data, demanding constant engineering, cybersecurity, and legal resources. This diverts critical talent from innovation and safety, making the obligation operationally and economically unfeasible. The inevitable outcome is fewer sensors, leading to less smart and less efficient infrastructure.

**Use case IV: How the Data Act impedes (custom-made) industrial SaaS solutions and discourages R&D.** The Data Act’s mandatory cloud switching rights are severely damaging to customized industrial SaaS. These solutions are built on long-term models, and imposing short-term switching rights fundamentally undermines their technical architecture and commercial viability. This interference with contractual freedom eliminates business planning certainty, directly discouraging crucial investments in complex industrial solutions and inhibiting innovation, as providers cannot guarantee amortization of high initial costs. Compounding this, the Act's vague definition of 'data processing service’, with only non-binding European Commission guidance introduces significant legal, technical, and economic risks. Further, the explicit exemption for SMEs from the obligation to adapt contracts concluded before or on 25 September 2025 should be enlarged to companies of all sizes.

## Concluding Remarks

- The B2B market has already organized data sharing. Maintaining contractual freedom in the B2B sector is essential for the EU to maintain its competitiveness. The mandatory data transfer in B2B must be repealed to allow for balanced agreements.
- The rights of the manufacturer to use data to improve products and develop new and innovative service concepts must be safeguarded.
- The protection for trade secrets must be drastically enhanced maintaining the level of protection that the Trade Secrets Directive guarantees. We reiterate our request to exempt data that is a trade secret or from which a trade secret can be derived from any data transfer obligations.
- The rules on switching data processing services shall be amended as laid out in the Annex below to clarify definitions and scope of applicability. Industrial SaaS offerings (bare

minimum: all customized SaaS offerings) shall be excluded from Chapter VI. Legacy contracts shall stay unchanged. Contracts provided by customers, e.g. in public tenders, shall not be subject to switching rules.

For our concrete proposals on the Digital Omnibus, explaining how our recommendations can be incorporated into the legal text, please refer to the Annex starting on the next page.

## Annex: Siemens' concrete proposals on the Digital Omnibus

<table>
<tr><td colspan="2">Article 1 Amendments to Regulation (EU) 2023/2854</td></tr>
<tr><td>Commission's proposal</td><td>Siemens' concrete amendments</td></tr>
<tr><td>1. Article 1 is amended as follows:<br>(a) […]<br>(b) in paragraph 2, the following points are added:<br><br>'(g) Chapter VIIa applies to personal and non-personal data;<br>(h) Chapter VIIb applies to any non-personal data;<br>(i) Chapter VIIc applies to personal and non-personal data, namely the following:<br>(i) documents held by public sector bodies of Member States as referred<br>(1) to in Article 32i(1), point (a) or by public undertakings as referred<br>(2) to in Article 32i(1), point (b);<br>(ii) research data as referred to in Article 32i(1), point (c);<br>(iii) certain categories of protected data as referred to in Article 32i(1), point (a).'<br>[…]</td><td>1. Article 1 is amended as follows:<br>(a) […]<br>(b) in paragraph 2,<br><br>(1) point (a) is replaced by the following:<br><br>'Chapter II applies to data, with the exception of content, concerning the performance, use and environment of connected products and related services; Chapter II does not apply in business-to-business relations;<br><br>(2) point (e) is replaced by the following:<br><br>Chapter VI applies to any data and services processed by providers of data processing services; Chapter VI does not apply in business-to-business relations;<br><br>(3) the following points are added:<br><br>'(g) Chapter VIIa applies to personal and non-personal data;<br>(h) Chapter VIIb applies to any non-personal data;<br>(i) Chapter VIIc applies to personal and non-personal data, namely the following:<br>(i) documents held by public sector bodies of Member States as referred<br>(1) to in Article 32i(1), point (a) or by public undertakings as referred<br>(2) to in Article 32i(1), point (b);<br>(ii) research data as referred to in Article 32i(1), point (c);<br>(iii) certain categories of protected data as referred to in Article 32i(1), point (a).'</td></tr>
</table>

| | |
|---|---|
| | [...] |
| *Justification: The changes proposed in the Digital Omnibus would introduce ambiguities and even contradictions with existing provisions. The uniform application of Chapters II and VI to both B2B and B2C contexts, combined with an overly simplified view of industrial data sharing, creates significant legal and technical uncertainty. Consequently, companies may be incentivized to design their products in a less data-sharing manner, thereby undermining the very objectives of the Data Act. The promotion of the voluntary nature of data sharing should serve as the default standard in B2B.*<br><br>*The Data Act's rules on switching "data processing services" may technically and economically be feasible for Infrastructure as a Service (IaaS) or in a B2C context. However, this is not true for Software as a Service (SaaS) in B2B contexts. SaaS offerings are usually highly customized, deeply integrated, and lack easy portability. To avoid stifling innovation, cloud switching obligations should not apply to the B2B context – at least should be limited to IaaS, explicitly excluding SaaS.*<br><br>Any recitals and further parts of the Data Act shall be adapted as necessary to reflect the proposed amendments of Article 1 (b) (1) and (2). | |

| ***Article 1 Amendments to Regulation (EU) 2023/2854*** | |
|---|---|
| **Commission's proposal** | **Siemens' concrete amendments** |
| 2. Article 2 is amended as follows:<br><br>(a) the following points (4a), (4b) and (4c) are inserted: [...]<br>(b) point (13) is replaced by the following: [...]<br>[...] | 2. Article 2 is amended as follows:<br><br>(a) the following points (4a), (4b) and (4c) are inserted: [...]<br>**(b) point (8) is amended as follows:**<br><br>**"**"data processing service" means a digital service that is provided to a customer and that enables ubiquitous and on-demand network access to a shared pool of configurable, scalable and elastic computing resources of a centralized, distributed or highly distributed nature ~~that~~ **if and insofar the digital service itself is elastic,** can be rapidly provisioned and released with minimal management effort or service provider interaction.<br>**Digital services provided in a SaaS delivery model shall only be considered as Data Processing Services if the main purpose of such service is the provision of access to computing resources other than those used to enable access to and use of the application.""** |

| | |
|---|---|
| | (~~b~~ c) point (13) is replaced by the following: [...]<br>[...] |
| *Justification: "Data processing service" is very loosely defined, leading to legal risks due to interpretation; to extensive technical and contractual measures if interpreted broadly, even for digital services not intended to be covered; and to compliance violations and economic risks if interpreted narrowly. The EU Commission rightly confirms that Chapter VI applies only to data processing services, where the digital service itself, incl. SaaS, can be rapidly provisioned or released with minimal management effort or service provider interaction (see FAQ 58a). Incorporating the EU Commission's clarification (FAQ 58a) into the definition or, at minimum, adapting the Recitals to address this critical gap for the industry is needed. Furthermore, a genuine advance in legal certainty, simplification, and innovation-friendly regulation would require exempting PaaS and SaaS from the scope of Chapter VI for all companies, regardless of their size.* | |

| ***Article 1 Amendments to Regulation (EU) 2024/1689*** | |
|---|---|
| **Commission's proposal** | **Siemens' concrete amendments** |
| - | **2A. in Article 3 paragraph 1 is replaced by the following:**<br><br>Connected products shall be designed and manufactured, and related services shall be designed and provided, in such a manner that product data and related service data, including the relevant metadata necessary to interpret and use those data, are, by default, easily, securely, ~~free of charge,~~ in a comprehensive, structured, commonly used and machine-readable format, and, where relevant and technically feasible, directly accessible to the user. |
| *Justification: Mandating free data access would undermine investment incentives, distort competition, and unfairly shift costs, whereas fair compensation ensures proportionate, FRAND-based, and sustainable data sharing.* | |
| 3. in Article 4, paragraph 8 is replaced by the following:<br><br>'8. In exceptional circumstances, where the data holder who is a trade secret holder is able to demonstrate that, despite the technical and organisational measures taken by the user pursuant to paragraph 6 of this Article, it is highly likely to suffer serious economic damage from the disclosure of trade secrets or that the disclosure of trade secrets to the user | 3. in Article 4,<br>**(1)** paragraph 1 is replaced by the following:<br><br>Where data cannot be directly accessed by the user from the connected product or related service, data holders shall make readily available data, as well as the relevant metadata necessary to interpret and use those data, accessible to the user without |

| | |
|---|---|
| poses a high risk of unlawful acquisition, use, or disclosure to third country entities, or entities established in the Union under the direct or indirect control of such entities, which are subject to jurisdictions offering weaker or non-equivalent protection compared to that under Union law, that data holder may refuse on a case-by-case basis a request for access to the specific data in question. That demonstration shall be duly substantiated on the basis of objective elements, such as the enforceability of trade secrets protection in third countries, the nature and level of confidentiality of the data requested, and the uniqueness and novelty of the connected product. It shall be provided in writing to the user without undue delay. Where the data holder refuses to share data pursuant to this paragraph, it shall notify the competent authority designated pursuant to Article 37.'; | undue delay, of the same quality as is available to the data holder, easily, securely, ~~free of charge,~~ in a comprehensive, structured, commonly used and machine-readable format and, where relevant and technically feasible, continuously and in real-time. This shall be done on the basis of ~~a simple request through electronic means where technically feasible~~ **fair, reasonable and non-discriminatory terms analogous to Article 8 and 9.**<br><br>**(2)** paragraph ~~8~~ **6 to 9** is replaced by the following:<br><br>**"Trade secrets shall be preserved and do not have to be disclosed. Data from which trade secrets may be retrieved shall not be subject to disclosure, unless the data holder and the user have reached an agreement on necessary measures to preserve their confidentiality and implemented those."**<br><br>~~'8. In exceptional circumstances, where the data holder who is a trade secret holder is able to demonstrate that, despite the technical and organisational measures taken by the user pursuant to paragraph 6 of this Article, it is highly likely to suffer serious economic damage from the disclosure of trade secrets or that the disclosure of trade secrets to the user poses a high risk of unlawful acquisition, use, or disclosure to third country entities, or entities established in the Union under the direct or indirect control of such entities, which are subject to jurisdictions offering weaker or non-equivalent protection compared to that under Union law, that data holder may refuse on a case-by-case basis a request for access to the specific data in question. That demonstration shall be duly substantiated on the basis of objective elements, such as the enforceability of trade secrets protection in third countries, the nature and level of confidentiality of the data requested, and the uniqueness and novelty of the connected product. It shall be provided in writing to the user without undue delay. Where the data holder refuses to share data pursuant to this paragraph, it shall notify the competent authority designated pursuant to Article 37.';~~ |

| | |
|---|---|
| | **(3) paragraph 13 is replaced by the following:**<br><br>A data holder ~~shall only~~ **is entitled to** use any readily available data that is non-personal data ~~on the basis of a contract with the user~~. A data holder shall not use such data to derive insights about the economic situation, assets and production methods of, or the use by, the user in any other manner that could undermine the commercial position of that user on the markets in which the user is active.<br><br>**(4) paragraph 14 is replaced by the following:**<br><br>Data holders ~~shall not~~ **may** make available non-personal product data to third parties for **legitimate** commercial or non-commercial purposes.~~, other than the fulfilment of their contract with the user.~~ |

*Justification:*

1. *Mandating free data access would undermine investment incentives, distort competition, and unfairly shift costs, whereas fair compensation ensures proportionate, FRAND-based, and sustainable data sharing.*

2. *In the age of economic security, trade secrets are one of the most important values for companies to remain competitive. Forcing companies to share their trade secrets, as the current wording still foresees, undermines the very purpose of the EU regulations to keep European companies competitive against other players. The Digital Omnibus proposal's effort to extend trade secret protection as a preventive safeguard against third-country regimes is insufficient to ensure robust trade secret protection. Once disclosed, trade secrets are irreversibly lost, eliminating the competitive advantage of EU-based companies. Disclosure potentially causes severe economic harm and allows third parties to exploit proprietary knowledge. Strong protection is therefore essential to safeguard investments and preserve Europe's competitiveness and the EU's economic security. The requirement for trade secret owners to demonstrate a high likelihood of serious economic damage from disclosure or a high risk of unlawful disclosure to a third country remains overly burdensome and unpragmatic. Data that is itself a trade secret or from which a trade secret can be derived must be exempted from any data sharing obligations under the Data Act to preserve the competitive advantage of EU-based companies.*

3. *Data Act's mandatory data-sharing obligations* largely duplicate existing B2B contractual mechanisms, *where industrial players have long negotiated data access and licensing through tailored contracts — creating friction, legal uncertainty, and compliance costs without filling any*

| |
|---|
| *genuine legal gap. This also creates a structural competitive disadvantage for European Industrial AI companies. Non-EU competitors freely use machine data to train AI models, while European companies must negotiate data-use clauses, risk fragmented training datasets, and absorb significant legal costs. This directly undermines the EU's own goal of fostering a competitive data economy. Finally, the Data Act applies a regulatory logic borrowed from consumer data frameworks, ill-suited to machine-generated industrial data embedded in intellectual property and trade secrets. Forcing access without adequate safeguards risks transferring hard-won competitive intelligence to third parties, including non-EU actors, with no reciprocal benefit.* |

| ***Article 1 Amendments to Regulation (EU) 2024/1689*** | |
|---|---|
| **Commission's proposal** | **Siemens' concrete amendments** |
| 4. in Article 5, paragraph 11 is replaced by the following:<br><br>'11. In exceptional circumstances, where the data holder who is a trade secret holder is able to demonstrate that, despite the technical and organisational measures taken by the third party pursuant to paragraph 9 of this Article, it is highly likely to suffer serious economic damage from the disclosure of trade secrets or that the disclosure of trade secrets to the third party poses a high risk of unlawful acquisition, use, or disclosure to third country entities, or entities established in the Union under the direct or indirect control of such entities, which are subject to jurisdictions offering weaker or non-equivalent protection compared to that under Union law, that data holder may refuse on a case-by-case basis a request for access to the specific data in question. That demonstration shall be duly substantiated on the basis of objective elements, such as the enforceability of trade secrets protection in third countries, the nature and level of confidentiality of the data requested, and the uniqueness and novelty of the connected product. It shall be provided in writing to the third party without undue delay. Where the data holder refuses to share data pursuant to this paragraph, it shall notify the competent authority designated pursuant to Article 37.'; | 4. ~~in~~ Article 5~~, paragraph 11~~ is **deleted in its entirety**; ~~replaced by the following:~~<br><br>~~'11. In exceptional circumstances, where the data holder who is a trade secret holder is able to demonstrate that, despite the technical and organisational measures taken by the third party pursuant to paragraph 9 of this Article, it is highly likely to suffer serious economic damage from the disclosure of trade secrets or that the disclosure of trade secrets to the third party poses a high risk of unlawful acquisition, use, or disclosure to third country entities, or entities established in the Union under the direct or indirect control of such entities, which are subject to jurisdictions offering weaker or non-equivalent protection compared to that under Union law, that data holder may refuse on a case-by-case basis a request for access to the specific data in question. That demonstration shall be duly substantiated on the basis of objective elements, such as the enforceability of trade secrets protection in third countries, the nature and level of confidentiality of the data requested, and the uniqueness and novelty of the connected product. It shall be provided in writing to the third party without undue delay. Where the data holder refuses to share data pursuant to this paragraph, it shall notify the competent authority designated pursuant to Article 37.~~'; |
| *Justification: Third-party data sharing under Article 5 is especially critical regarding trade secret protection and involves significant practical burdens, including the conclusion of multiple contracts and technical measures to exchange data with parties outside existing customer relationships. Users are already entitled under Article 4 to request access to their data from data holders, which enables them to share such data with third parties. At least in the B2B environment, there is consequently no need for the burdensome indirect data sharing mechanism in Article 5.* | |

***Article 1 Amendments to Regulation (EU) 2024/1689***

| **Commission’s proposal** | **Siemens’ concrete amendments** |
|---|---|
| 15. in Article 31, the following paragraphs 1a and 1b are inserted:<br><br>‘1a. The obligations laid down in Chapter VI, with the exception of Article 29, and in Article 34 shall not apply to data processing services other than those referred to in Article 30(1), where the majority of features and functionalities of the data processing service has been adapted by the provider to the specific needs of the customer, if the provision of such services is based on a contract concluded before or on 12 September 2025.<br><br>The provider of such data processing services shall not be required to renegotiate or amend a contract for the provision of those services before its expiry if that contract was concluded before or on 12 September 2025. Any contractual provision contained in that contract that is contrary to Article 29(1), (2), or (3) shall be considered null and void.<br><br>1b. A provider of a data processing service may include provisions on proportionate early termination penalties in a contract of fixed duration on the provision of data processing services other than those referred to in Article 30(1).<br><br>Where the provider of data processing service is a small and medium-sized enterprise or a small mid-cap, the obligations laid down in Chapter VI, with the exception of Article 29, and in Article 34 shall not apply to data processing services other than those referred to in Article 30(1), if the provision of such services is based on a contract concluded before or on 12 September 2025.<br><br>Where the provider of a data processing service is a small and medium-sized enterprise or a small mid-cap, the provider shall not be required to renegotiate or amend a contract for the provision of a data processing service other than those referred to in Article 30(1) before its expiry if that contract was concluded before or on 12 September 2025. Any contractual | 15. in Article 31, the following paragraphs 1a~~, and~~ 1b **and 1c** are inserted:<br><br>‘1a. **Without prejudice to Article 2 (8) specifying all other characteristics of a data processing service,** ~~T~~the obligations laid down in Chapter VI~~, with the exception of Article 29, and in Article 34~~ shall not apply to data processing services other than those referred to in Article 30(1), where the majority of features and functionalities of the data processing service has been adapted by the provider to the specific needs of the customer~~, if the provision of such services is based on a contract concluded before or on 12 September 2025~~.<br><br>~~The provider of such data processing services shall not be required to renegotiate or amend a contract for the provision of those services before its expiry if that contract was concluded before or on 12 September 2025. Any contractual provision contained in that contract that is contrary to Article 29(1), (2), or (3) shall be considered null and void.~~<br><br>1b. A provider of a data processing service may include provisions on proportionate early termination penalties in a contract of fixed duration on the provision of data processing services other than those referred to in Article 30(1).<br><br>~~Where the provider of data processing service is a small and medium-sized enterprise or a small mid-cap, t~~**T**he obligations laid down in Chapter VI~~, with the exception of Article 29, and in Article 34~~ shall not apply to data processing services ~~other than those referred to in Article 30(1)~~, if the provision of such services is based on a contract concluded before or on 12 September 2025.<br><br>~~Where the provider of a data processing service is a small and medium-sized enterprise or a small mid-cap, t~~**T**he provider shall not be required |

| | |
|---|---|
| provision contained in that contract that is contrary to Article 29(1), (2), or (3) shall be considered null and void.'; | to renegotiate or amend a contract for the provision of a data processing service ~~other than those referred to in Article 30(1)~~ before its expiry if that contract was concluded before or on 12 September 2025. ~~Any contractual provision contained in that contract that is contrary to Article 29(1), (2), or (3) shall be considered null and void.';~~<br><br>**1c. Chapter VI shall not apply in cases where the contract is not provided by the data processing service provider, but (i) by the customer, e.g. in the context of a public tender, or (ii) is negotiated by the parties.';** |

*Justification: Siemens supports the exemption of "custom-made" services from the Chapter VI switching rules for "Legacy Contracts" (pre-Sept 12, 2025), acknowledging that Chapter VI should only cover rapidly provisioned, non-customized services. To eliminate inconsistency and undue burden, this exemption must apply to all contracts. We recommend:*

- *Article 31 (1a): Extend the "custom-made" exemption to contracts signed on or after September 12, 2025, aligning with the EU Commission's understanding expressed in FAQ 58a.*
- *Article 31 (1b) (second and third paragraphs): Universalize the SME exemption for Legacy Contracts for all companies, regardless of their size, aligning with the understanding that Legacy Contracts are already exempt. Otherwise, this creates legal uncertainty and unjustifiably burdens larger companies, which manage far more contracts (often from public tenders) and face broader regulatory challenges, undermining competitiveness.*
- *Article 31 (Extension): Clarify Chapter VI's non-applicability to customer-provided or individually negotiated contracts.*