POSITION PAPER

What SMEs expect from the Digital Omnibus

Key messages

- The digital Omnibus must strike the balance between simplifying compliance, streamlining obligations and ensuring competitiveness.
- Therefore, the Data Act should not be watered-down and the Commission should focus on a strong enforcement of the legislation.
- While SMEunited does not see the need to reopen the GDPR, targeted measures to simplify compliance could benefit SMEs, such as more guidance, proportionate information obligation, clarification of notification of personal data breach and for the designation of a data protection officer.
- GDPR and AI use must follow a risk based approach, with rules proportionate to the risks and size of the companies, especially for the smallest companies that do not have a dedicated legal department for compliance.
- AI guidelines must be practical, proportionate, and implementable for SMEs.
- Additionally, some provisions of the AI Act could be clarified such as record-keeping and technical documentation, high-risk system obligations and conformity assessments.
- Simplification of the Cyber Resilience Act should include pre-filled documentation templates.
- The CRA should allow SMEs to self-declare lower risk based on pre-defined, objective criteria.
- The EC should work on the interoperability between different standards to reach simplification of documentation requirements.
- Since all the pieces of legislations in digital policy are deeply linked, EC should consider the establishment of 'holistic' helpdesks for the Data Act, AI Act, GDPR and CRA. These desks should work as single national points of contact (*one-stop shop*) for businesses, coordinated with ENISA, the competent authorities and business organisations, capable of providing integrated technical and legal support.
- The creation of a single document platform (an interoperable "digital business file" for all standards) could avoid duplication and bring clarity among market operators.
- SMEs in the value chains have a weak contractual position towards large businesses, which often pass on compliance costs to them. The Omnibus should make sure obligations are proportionate and provide for ad hoc provisions prohibiting contractual clauses that unduly transfer responsibility.
- The Omnibus proposal should align definition across the different pieces of legislation and ensure they are not open to different interpretation at national level.

SMEunited | Rue Jacques de Lalaingstraat 4, B-1040 Brussels | +32 2 2307599 | info@smeunited.eu | **www.smeunited.eu**
EU Transparency Register: identification number 55820581197-35 | VAT BE 0441.251.911

Introduction

SMEunited welcomes the Commission objective to rationalise the obligations arising from different pieces of legislation in the field of digital policy. This is key to boost innovation and competitiveness of EU businesses, as highlighted in the Draghi report.

However, it is worth noting that much can be done not only with some legislative revisions but also and especially through a proportionate implementation of the existing provisions. This process entails the solution of several horizontal issues that have a huge impact on the ability of economic operators to comply with the different regulations and directives.

Guidelines, templates and simplifications are more than needed. Nevertheless, SMEs also request that the Commission or national authorities publish official binding or presumptive compliance models, including European open source tools for mandatory documentation. These tools should have legal value as presumptions of compliance, not just recommendations.

What is more, there is currently no concrete discussion on the possibility to foresee vouchers, incentives or contributions to support compliance, training and audit costs. Member States are therefore required to activate specific funds for the digital compliance of SMEs (as was the case for GDPR or CE marking) and to include regulatory sandboxes for testing and support, with appropriate funding.

The EU should work on binding common EU criteria, harmonised glossaries, and, above all, European monitoring of national implementation to ensure a level playing field.

I. Ensuring access to data and proportionate data protection

1. Guarantee strong implementation of the Data Act

The Data Act is a landmark regulation that strengthens SMEs and fosters open, competitive markets. Its full potential can only be realized through consistent, uncompromised and proportionate implementation. SMEunited together with other business organisations published a joint statement in September detailing how watering-down the Data Act would negatively impact competitiveness and undermine its core strength: enforceable rights, fairness, procedural justice, and legal clarity. These principles are essential to Europe's long-term resilience and innovation. Signatories of the joint statement are also notably calling for timely and practical guidance as well as for the promotion of the standard contractual clauses.

The European Commission must therefore:

- Reject any attempts to make data sharing voluntary
- Maintain binding reporting obligations on trade secret and cybersecurity exemptions, keeping the burden of proof with the data holder and ensuring robust, accessible review mechanisms.

- Guaratee a SME-friendly implementation ensuring the interoperability of data and systems. Smaller businesses also need capacity building to comply with the Data act, e.g. for the purchase of systems of data storage and management.

Data Act obligations apply only to readily available data, not to internal product data. The risk of reverse-engineering intellectual property from such data is minimal, and the Data Act itself introduces strong safeguards (Art. 5(9–11)) to protect trade secrets and sensitive business data.

2. Data Governance Act

SMEunited already raised the challenges faced by SMEs when it comes to notifications and record keeping procedures. In order to strike a balance between protection and simplification, SMEunited suggests the following:

- **Obligations of data intermediation services providers (Art.11-12)**

These obligations should be come with more guidance for SMEs. Additionally, the legislation should provide for proportionate administrative costs for SMEs.

- **Provisions regarding data altruism organisation registration (Chapter IV)**

The obligations to maintain records, notify changes, and undergo regular assessments are perceived as excessive and complex for SMEs. Simplification could involve risk-based tiering of obligations based on the scale and nature of data use.

3. Simplify GDPR compliance

SMEunited welcomes the proposed exemption from maintaining a record of processing activities, as included in the Omnibus IV package. However, a genuine application of the risk-based approach should replace the current information obligation with a right to information on request. Customers seeking specific details must of course receive them, but imposing blanket obligations to provide unsolicited legal and technical details is unnecessary and excessive.

Further adjustments are necessary to ensure a consistent risk-based approach. SMEunited published in June proposals to simplify SMEs compliance with the GDPR. These proposals notably include:

- More guidance and support from public authorities (for example on Art. 35 GDPR on the so-called 'whitelist')
- Proportionate information obligation: Articles 13 and 14 impose information obligations that are disproportionate, especially for low-risk processing activities. The volume and complexity of required disclosures, such as legal bases, retention periods, or extensive rights explanations, are often disproportionate to the actual risk and interest to the customer.

- Clarification of article 30: The obligations under Article 30 are often unclear, leading to excessive and sometimes redundant documentation, especially for low-risk data processing activities. To improve this situation it is important to clarify and limit record-keeping obligations to situations where data processing is a core business activity. SMEs should be provided with simplified templates by public authorities and with clear criteria to determine when full documentation is required are necessary.
- Clarify notification of personal data breach: Article 33 does not come either with a clear definition of what 'risk' means in this context nor with clear criteria to notify after 72 hours.
- Proportionality for the designation of a data protection officer: Article 37 is too rigid for SMEs, who should be able to appoint a DPO according the nature and scale of their data processing.

GDPR and AI Use

The same principle must apply to AI-related data processing. Where risks are minimal, companies should be able to use low-risk AI-related data.. This clarity is essential to enable SMEs and craft enterprises to deploy AI in practice.

That means:

- The use of "legitimate interest" as a legal basis must be more clearly defined and reinforced to justify key AI applicationsfor low-risk processing safeguarded by techniques such as pseudonymisation, reliance on legitimate interest must be sufficient
- where re-identification is technically impossible, the data must no longer be classified as personal data.

II. Foster AI adoption by SMEs

1. AI Act guidelines

The upcoming Digital Omnibus must decisively eliminate all uncertainties between the AI Act and the GDPR. For SMEs in particular, legal clarity is essential. Without it, the use of key technologies such as open-source AI models will remain out of reach for many businesses.

A central element will be the guidelines foreseen in **Article 96 of the AI Act**, to be issued by the European Commission. These guidelines must be practical, proportionate, and implementable for SMEs. Above all, they must prevent additional or unforeseen burdens for small businesses and crafts.

Clarity is urgently required on issues such as:

- **Defining "substantial modifications"**: It must be made explicit which types of system changes do not qualify as substantial modifications.

- **Ensuring flexibility in conformity assessments:** AI providers must retain sufficient flexibility to adapt and further develop their systems in day-to-day business, without triggering costly and repeated reassessments.

Equally important, the Article 96 guidelines must explicitly recognise that fine-tuning AI systems, through the use of company-specific or customer data to optimise performance within the intended purpose, constitutes legitimate use. **Businesses that adjust AI systems to their workflows or that perform adaptation or fine-tuning activities on behalf of third parties using data provided to them must not be reclassified as "providers."** The responsibility for conformity assessments must remain with the manufacturers. Only in cases of a fundamental change of purpose or independent, substantial redevelopment should legal responsibility shift to the business itself.

2. Clarifying AI Act provisions

On top of the guidelines, some of the provisions of the AI Act could be clarify to support compliance and foster AI adoption.

Record-keeping and technical documentation (Article 11)

High-volume documentation can overwhelm small developers, especially SMEs who do not have a dedicated legal and engineering compliance team. Standardised templates and interoperable reporting tools could lighten the burden.

Article 11 could be adapted to include support tools such as:

- pre-filled documentation templates, with sector-specific examples
- standardised documentation toolkits in open source or under EU license.

High-risk system obligations (Title III, chapter 2)

Requirements around risk management, data governance, transparency, and human oversight are extensive. **Modular compliance pathways or exemptions for SMEs (already partially introduced) could be extended or clarified**.

Therefore, we suggest to:

- allow SMEs to self-declare lower risk based on pre-defined, objective criteria (e.g., no impact on fundamental rights, limited user base).
- create regulatory sandbox routes to allow safe testing before full compliance kicks in.

Conformity assessments and notified bodies (Art. 43-44)

SMEunited expresses concerns around cost, complexity, and availability of notified bodies. Streamlined or simplified procedures for systems with proven lower risk profiles would help.

For an SME with one or two AI products, the cost of assessments can outweigh revenue, making it unsustainable. Therefore, we suggest the following:

- Allow for **shared compliance services**, e.g. using AI assurance providers or trusted third-party sandbox environments
- **waivers or fast-track assessments for low-complexity, low-volume low-risk systems**
- EU or national voucher schemes for SMEs to cover conformity costs.

III. Support cybersecurity compliance

1. Cyber Resilience Act

SMEunited supported the adoption of the Cyber Resilience Act (CRA). Harmonised rules for digital products create incentives and trusts for entrepreneurs. Nevertheless, the Digital Omnibus is the occasion to assess reporting obligations introduced by the CRA.

Vulnerability handling and notification requirements (Articles 11–12)

SMEs are required to monitor, manage, and report product vulnerabilities within 24 hours of being aware of an actively exploited vulnerability. However, most SMEs do not have the capacity to run 24/7 threat monitoring systems or maintain a Computer Security Incident Response Team (CSIRT). To simplify, here are a few ideas:

- **Exemptions or longer timelines for low-risk products by SMEs**
- A shared, centralised vulnerability reporting platform (or helpdesk) managed by ENISA or national authorities for support to SMEs.
- **Clear guidance on thresholds**: when is a vulnerability "actively exploited" or "severe" enough to require reporting.

Conformity assessments (Chapter III)

The CRA requires extensive assessments even for non-critical digital products unless the product qualifies for self-assessment, which is not be clearly defined. Even for self-assessment heavy documentation is required.

Conformity assessments are perceived as disproportionately heavy, especially for non-critical products. **Greater use of self-assessment or harmonised standards for low-risk categories could support SMEs compliance.**

Therefore, we suggest to:

- allow broader self-assessment pathways for SMEs offering non-critical or niche products
- develop pre-approved compliance templates for typical SME product categories
- clarify and promote use of harmonised standards to streamline the process.

Documentation and technical files (Art. 23)

The CRA require extensive internal documentation and a declaration of conformity before placing products on the market. SMEunited believe **extensive documentation obligations could be streamlined**, especially when cumulative with sectoral or existing ISO standards. We notably suggest to

- Develop standardised documentation kits or pre-filled forms for typical SME devices.
- Accept existing certifications or documentation to avoid duplication (e.g. for cybersecurity controls already certified under another framework). Allow pre-market compliance support through national authorities as an SME helpdesks.

IV. Simplify compliance with the ePrivacy Directive

The uncertainty in application and "consent fatigue" regarding cookies and web tracking will not be alleviated by new regulations, especially since no "one size fits all" approach can be found for such a technically complex issue.

On the one hand, the current legal requirements for the lawful use of tracking have been fundamentally adjudicated by the ECJ and the EU supervisory authorities, and on the other hand, they have also been comprehensively explained by the European Data Protection Board. If no explicit simplification of the current provisions is planned, such as an extension of the legitimate interest to include (third-party) analysis options or the expansion of the permitted grounds for technically necessary technology, we believe that new regulations on this issue are not sensible.

To effectively support SMEs on the ground, SMEunited request the Commission to provide SMEs with simple templates for cookie consent tools or sample privacy policies for a variety of standardised use cases that not only companies but also consumers can rely on. This would increase the transparency of these technologies, which are generally difficult to understand, and reduce errors in use.

It would also be worth **considering extending the "privacy by default" principle pursuant to Article 25 of the GDPR to manufacturers/providers of templates, such as website templates or newsletter distribution systems**, as a kind of product safety regulation. If these were already delivered in the most data protection-friendly version and with default settings, some practical problems would be eliminated. Non-technically savvy companies typically use such tools and are unaware of the specific impact of their functions.

Brussels, 16 October 2025

For more information, please contact:
Sophia Zakari
Director Enterprise Policy & Legal Affairs
E: s.zakari@smeunited.eu