ACT Association for Competitive Technology

Digital Omnibus

Position Paper

Executive Summary

ACT welcomes the European Commission's initiative to simplify and consolidate the current EU digital framework. This objective reflects the calls made by both Draghi[1] and Letta[2] reports to ensure a legislative environment that can support small and medium-sized enterprises (SMEs) and startups to grow.

The current digital and data acquis has experienced a substantial increase during the past 10 years, with the introduction of several legislative developments that have a direct impact on small companies. We believe that simplification is the key element that will help European companies to scale and grow cross-border, by making compliance workable, predictable, and proportionate. In this respect, the Digital Omnibus represents an important step forward to ensure tangible benefits.

[1]Mario Draghi (2024), Report on the future of European competitiveness.
[2]Enrico Letta (2024), Report on the Future of the Single Market.

For these reasons, ACT shares the ambition of new simplification measures, concretely:

Artificial Intelligence Act

- Targeted simplification and streamlining measures can reduce compliance burdens for SMEs and startups developing artificial intelligence (AI) systems.
- Clear guidance on classification, risk assessment, and conformity procedures is essential to enable smaller companies to innovate confidently.
- Proportionate obligations that account for company size and risk level will help ensure the AI Act does not create insurmountable barriers to entry for European AI developers.
- Harmonised implementation across Member States is critical to prevent fragmentation and ensure a level playing field.

General Data Protection Regulation (GDPR)

- Clarifying GDPR obligations for SMEs, including definitions of personal data, pseudonymisation criteria, and proportional responses to abusive data requests reduce overcompliance and legal uncertainty.
- Risk-based adjustments to personal data breach notifications, including high-risk thresholds, extended deadlines, and common templates, improve predictability and reduce administrative burdens for SMEs.
- Harmonised data protection impact assessment requirements and consistent guidance across the EU addresses fragmentation, lowering compliance costs and enabling SMEs to focus resources on effective data protection.
- Clear rules on AI-related data processing, including the use of legitimate interests and narrowly tailored exemptions for special category data, support responsible innovation while maintaining robust consumer safeguards.

Data Act and Data Regulations

- The consolidation of the Free Flow of Non-Personal Data Regulation, the Data Governance Act, and the Open Data Directive within the Data Act, will reduce fragmentation and improving legal clarity.
- Strengthened protections for trade secrets with a clearer risk-based approach to international data sharing are essential to preserve investment incentives.
- More clearly defined thresholds for public-sector access to private data improve predictability and limit disproportionate requests.
- Increased flexibility for cloud users and providers, particularly through eased switching requirements for SMEs, addresses longstanding concerns about feasibility and compliance costs.
- Further clarification is needed on how data holders should assess and demonstrate risks related to third-country access to prevent legal uncertainty.

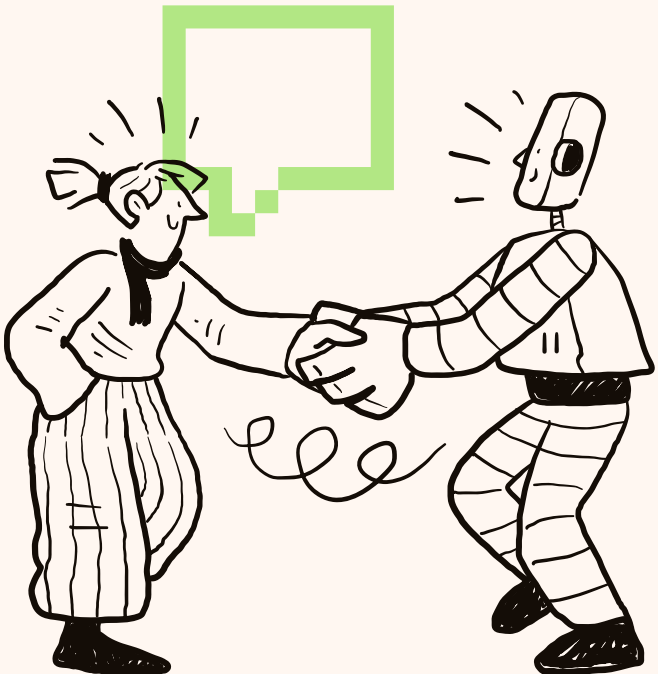
Single Reporting Mechanism and e-Privacy Directive

- The creation of a Single Reporting Mechanism operated via ENISA will allow companies to fulfil incident reporting obligations under multiple EU legal acts through a single entry point.
- Streamlining cookie consent requirements and introducing machine-readable user preferences under the revised e-Privacy Directive will reduce compliance costs while improving user experience.
- The repeal of the Platform-to-Business Regulation is a positive step toward reducing regulatory overlap, as its objectives have been largely overtaken by newer digital laws.

While the Digital Omnibus represents meaningful progress, we encourage policymakers to ensure that simplification translates into tangible reductions in administrative burden. Consolidation should not merely reconfigure existing obligations but should actively reduce duplicative reporting, clarify the interplay between different legal instruments, and provide practical tools and guidance tailored to the needs of startups and SMEs. Harmonised implementation across Member States is essential to prevent national-level divergences from undermining the framework's effectiveness.

AI Act

ACT welcomes the European Commission’s initiative to simplify and streamline implementation of the AI Act through the Digital Omnibus. As with other parts of the EU digital framework, the effectiveness of the AI Act will depend not only on its objectives, but on whether its obligations are workable, proportionate, and predictable in practice, particularly for small and medium-sized enterprises and startups. The Omnibus reflects a necessary recognition that regulatory complexity, overlapping obligations, and delayed implementation tools risk undermining innovation and competitiveness if not addressed.



The AI Act represents a significant step toward promoting trustworthy AI in Europe through a risk-based framework. ACT has consistently supported this approach, particularly where it focuses regulatory attention on genuinely high-risk uses of AI. However, early implementation signals point to legal uncertainty, delayed standards, and cumulative compliance burdens that could disproportionately affect SMEs[3] and downstream developers that integrate AI into broader products and services. In this context, the Digital Omnibus provides an important opportunity to ensure the AI Act supports innovation rather than discouraging deployment.

ACT welcomes several of the targeted simplification measures proposed under the Omnibus in relation to the AI Act. Linking the application of high-risk obligations to the availability of harmonised standards, guidance, and compliance tools is a pragmatic and necessary step.

Applying far-reaching obligations before the supporting regulatory infrastructure is in place would expose businesses, particularly smaller ones, to legal uncertainty and compliance risks they are not well positioned to manage. A phased, industry-led, standards-driven approach improves predictability and allows companies to invest in compliance with greater confidence, while maintaining accountability for high-risk uses.

ACT also supports extending SME-specific simplifications to small mid-cap companies. Many growing firms face similar resource constraints as SMEs, and abrupt transitions to full compliance obligations can discourage scaling within the EU. Simplified documentation requirements, proportionate quality management systems, and calibrated enforcement are important to ensure the AI Act does not inadvertently penalise growth or favour firms with greater compliance capacity.

ACT further welcomes the shift away from vague, horizontal obligations related to AI literacy toward a more capacity-building and guidance-based approach led by the Commission and Member States. Practical training resources and clear guidance can be more effective than ill-defined legal duties, particularly for SMEs without dedicated compliance teams. At the same time, EU-level initiatives should complement, not replace, the responsibility of organisations developing and deploying AI systems to ensure appropriate internal understanding of their technologies.

The Omnibus also introduces meaningful reductions in administrative burden through simplified documentation, registration, and post-market monitoring requirements. Reducing unnecessary reporting and allowing greater flexibility in post-market monitoring can lower compliance costs without weakening safeguards. These changes are particularly relevant for downstream developers and integrators, for whom rigid or duplicative processes can delay deployment and market entry. Simplification should, however, be accompanied by clear accountability and transparency to preserve trust and legal certainty.

[3]See https://actonline.org/the-hidden-cost-of-ai-regulations-a-survey-of-eu-uk-and-u-s-companies/.

ACT recognises the importance of clarifying lawful pathways for bias detection and correction, including where this requires the processing of sensitive data. The ability to identify and mitigate bias is central to the development of trustworthy AI. Such measures should be narrowly scoped and subject to strict necessity, data minimisation, and strong security safeguards. Alignment with existing data protection frameworks is essential to avoid fragmentation or misuse.

In this context, ACT notes the Joint Opinion of the European Data Protection Board and the European Data Protection Supervisor[4], which supports efforts to streamline AI Act implementation while underscoring the need to maintain robust protections for fundamental rights. The Opinion reinforces that simplification should clarify obligations and support SMEs.

While ACT supports the overall direction of these simplification efforts, their impact will depend on consistent and careful implementation. Simplification measures must be operational in practice and not offset by informal expectations, fragmented national interpretations, or overlapping obligations under other EU legislation, including data protection, cybersecurity, and product safety rules. Clear guidance, harmonised templates, and consistent enforcement across Member States are critical to delivering meaningful benefits for SMEs.

ACT also emphasises that trust, security, and the protection of intellectual property are foundational to a functioning AI ecosystem. Measures intended to improve transparency or data access must be calibrated to avoid weakening cybersecurity or exposing sensitive business information. For smaller developers in particular, consumer trust and secure platforms are key enablers of competition.

In conclusion, ACT supports the Commission's efforts through the Digital Omnibus to make the AI Act more proportionate and predictable. Aligning obligations with risk, implementation capacity, and real-world development practices is essential for Europe's AI ecosystem to remain competitive. Simplification should reduce administrative burden while preserving trust and legal certainty for businesses of all sizes. With careful execution and coordinated oversight, the Omnibus can help ensure the AI Act achieves its objectives without placing disproportionate strain on SMEs.

[4]https://www.edps.europa.eu/press-publications/press-news/press-releases/2026/edpb-and-edps-support-streamlining-ai-act-implementation-call-stronger-safeguards-protect-fundamental-rights_en.

GDPR

ACT supports the Commission's efforts to simplify the EU acquis to advance innovation and improve regulatory clarity for SMEs. As the backbone of the digital economy, SMEs depend on regulatory certainty and practical rules to responsibly innovate and compete. In this context, the Digital Omnibus offers a welcome opportunity to improve clarity, consistency, and proportionality in the application of digital regulations in a manner that promotes effective data protection for SMEs.

Clarifying the scope of personal data under the GDPR is an essential step toward more predictable and effective compliance. For instance, clarifying that information is not necessarily personal data if a given entity cannot reasonably identify the individual in question can reduce legal uncertainty and help organisations avoid over compliance in low-risk contexts. Further, the proposal's inclusion of language enabling the Commission and European Data Protection Board (EDPB) to develop criteria for assessing when pseudonymised data constitutes personal data can provide SMEs with clearer, more consistent guidance.

ACT appreciates the inclusion of clearer safeguards allowing controllers to either refuse requests or charge reasonable fees for abusive data access requests. While ACT fully supports the rights conferred by the GDPR, small businesses operating with limited resources often do not have the requisite staff, time, or capacity to respond to excessive or abusive requests. Clarifying that small businesses may refuse or charge reasonable fees for abusive requests will enable SMEs to focus on legitimate requests without diverting disproportionate resources away from day-to-day operations.

The clarifying language in Article 13 detailing the circumstances under which controllers must repeat disclosures to data subjects is a welcome development that will reduce legal burdens for SMEs. In its current form, Article 13 offers limited guidance on when renewed disclosures are necessary, which may inadvertently lead SMEs to repeat information as a precautionary compliance measure. Providing clearer guidance for when disclosures must be repeated can reduce duplication, especially in low-risk contexts, and help alleviate administrative burdens on SMEs.

ACT welcomes changes to the personal data breach notification requirements in the GDPR. Limiting notifications to supervisory authorities to cases where a personal data breach is likely to result in a high risk will meaningfully reduce unnecessary administrative burdens and avoid excessive reporting of low-risk incidents with limited impact. Further, the extension of the notification deadline from 72 to 96 hours offers SMEs additional time to assess incidents accurately and respond appropriately without undue time pressure. The development of common templates for personal data breach notifications and a list detailing the circumstances in which a breach will likely present high risks will also aid in effective breach responses. Together, these measures promote proportionate, risk-based breach reporting, cooperation, and transparency without imposing excessive or ineffective burdens on SMEs.

ACT supports the harmonisation of data protection impact assessment (DPIA) requirements across the EU. By empowering the Board to develop lists of processing operations that do and do not require a DPIA, a common template, and a common methodology, the Digital Omnibus addresses longstanding fragmentation and legal uncertainty arising from divergent approaches at the Member State level. For SMEs, inconsistency in privacy and data protection obligations can lead to defensive overcompliance, unnecessary costs, and increased administrative burden. Harmonising the framework at the EU level can reduce these burdens, improve legal certainty, and enable organisations to focus resources on maintaining strong safeguards for consumers' data.

Provisions addressing the application of the GDPR to the development and operation of AI systems will offer much-needed clarity for SMEs. Providing greater certainty around the use of the legitimate interests' legal basis for processing personal data necessary for the development and operation of AI systems can help SMEs innovate responsibly and preserve the existing balancing of interests and safeguards under the GDPR.

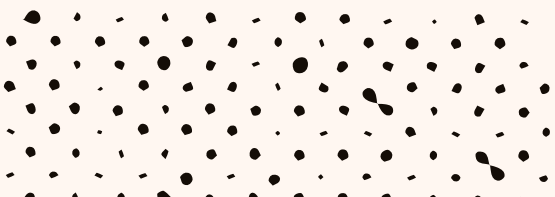
Further, ACT supports the inclusion of a narrowly tailored exemption addressing the residual processing of special categories of data in the development and operation of AI systems, including in the context of bias detection, testing, and mitigation. Such processing should remain subject to robust technical and organisational safeguards to ensure that efforts to improve fairness and trustworthiness in AI systems do not create new risks to consumers' rights.

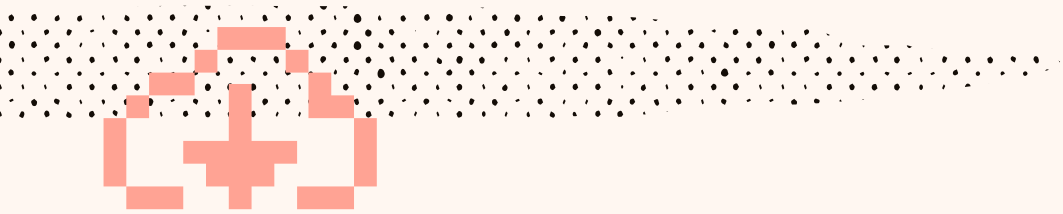
In conclusion, the Commission's efforts to improve clarity, reduce legal uncertainty and administrative burdens, and maintain strong protections for consumers will help SMEs continue to innovate and compete effectively in the digital economy. To ensure these benefits are realised in practice, policymakers should prioritise consistent interpretation, clear guidance, and harmonised implementation. ACT welcomes the opportunity for continued engagement towards workable regulations that enable SMEs to innovate responsibly and protect consumer data effectively.

DATA ACT

This section sets out our assessment of the proposal regarding the data regulations, highlighting the changes introduced, the elements we support, and areas where we believe further ambition or clarification is needed.

The Digital Omnibus brings together and amends core elements of the EU data framework, notably the Free Flow of Non-Personal Data Regulation, the Data Governance Act, and the Open Data Directive, within the scope of the Data Act. A first important change concerns the protection of trade secrets. The proposal strengthens safeguards for data holders by allowing them to refuse data sharing where there is a demonstrable high risk of leakage to third countries with insufficient protections. This introduces a clearer and more realistic risk-based approach to international data sharing.





A second key change relates to public-sector access to private-sector data. Government access is more tightly circumscribed, with the threshold raised from a broad notion of ‘exceptional need’ to clearly defined public emergency situations. This improves predictability for companies and limits the risk of disproportionate or open-ended access requests.

The proposal also addresses data flows and the re-use of public-sector data. It codifies the prohibition of unjustified localisation requirements for non-personal data and further harmonises the conditions under which public-sector data may be re-used. In this context, it allows public bodies to charge higher fees for re-use by large enterprises, reflecting differences in economic capacity and potential market impact.

Finally, the Digital Omnibus introduces changes to cloud-related rules and contractual obligations. It eases requirements for switching between cloud service providers, particularly for SMEs, and removes highly prescriptive smart contract obligations. The overall approach shifts away from detailed technical mandates towards greater flexibility and outcome-oriented regulation.

We strongly support the Commission’s overall direction. The effort to simplify and consolidate the regulatory framework is a significant step towards reducing overlap between instruments and improving legal clarity for businesses operating across borders. In particular, stronger protection for trade secrets is essential to preserve incentives to invest in data generation and voluntary data sharing.

Additionally, merging the Data Governance Act, Free Flow of Non-Personal Data Regulation, and parts of the Open Data Directive into the Data Act directly addresses longstanding calls from the startup community to reduce fragmentation. Innovation requires rules that are not just clear on paper, but actually usable in practice. This consolidation would be a meaningful step towards that goal.

We also welcome the more proportionate and clearly delimited approach to public-sector access to data, which is now anchored in well-defined public emergency scenarios. The explicit reaffirmation of the free flow of non-personal data across the EU is another positive element that remains fundamental to the functioning of the Digital Single Market. In addition, greater flexibility for cloud users and providers, especially through eased switching requirements for SMEs and the removal of rigid smart contract rules, responds to long-standing concerns about feasibility and compliance costs.

Despite these positive elements, the proposal could be further strengthened in several areas. In particular, clearer guidance is needed on how data holders should assess and demonstrate risks related to third-country access. Without additional clarification, there is a risk of legal uncertainty and divergent interpretation across Member States. We encourage the institutions as they negotiate the file, clear, practical guidance with concrete criteria for risk assessment, including safe harbours and presumptions that enable startups to make confident compliance decisions without extensive legal resources.

More emphasis should also be placed on preventing new administrative burdens. Regulatory consolidation should result in fewer and lighter compliance obligations in practice, rather than a reconfiguration of existing ones. The Omnibus should more explicitly guard against duplicative reporting, notification, or documentation requirements.

The proposal could also go further in supporting international data flows, especially for non-personal and mixed datasets. Stronger alignment with global practices and greater interoperability would enhance legal certainty while remaining consistent with EU standards. In parallel, additional targeted support for SMEs and mid-sized companies would be welcome, including clearer exemptions, standard contractual tools, and practical implementation guidance.

A central Issue remains the Interaction between the Data Act and the GDPR. While the Data Act formally operates without prejudice to the GDPR, companies in practice continue to struggle to determine which rules apply in specific situations. Businesses are often required to assess whether datasets are personal, non-personal, or mixed, and to reconcile diverging obligations under the two regimes, particularly in the context of data access and sharing.

As highlighted in recent legal analysis, this uncertainty frequently leads companies to adopt overly conservative compliance strategies, defaulting to full GDPR-level obligations in order to mitigate legal risk. This approach increases compliance costs and can discourage lawful and beneficial data sharing, especially for smaller app developers.

In this respect, the Digital Omnibus should go further in delivering genuine simplification. Consolidating the data acquis should not only bring instruments together formally but also clarify responsibilities and remove overlaps in substance. Clearer guidance on the practical interplay between the GDPR and the Data Act, especially for mixed datasets and data-sharing obligations, would significantly improve legal certainty.

Finally, the Digital Omnibus is a welcome and constructive attempt to rationalise the EU data framework. With targeted refinements to enhance clarity, proportionality, and openness to international data flows, it has the potential to significantly improve data sharing and re-use while safeguarding legitimate commercial and public interests.

e-Privacy Directive, Single Reporting Mechanism, and P2B Regulation

ACT strongly supports the creation of a Single Reporting Mechanism, operated via European Agency for Cybersecurity (ENISA), which allows companies to fulfil their incident reporting obligations under multiple EU legal acts through a single entry point. This one-stop mechanism reduces administrative burdens, particularly for SMEs and startups, while ensuring timely and coherent reporting across EU legislation. By providing a single framework for compliance, the mechanism also facilitates the fulfilment of administrative reporting requirements, accelerating businesses, and ensuring more regulatory clarity.

ACT also welcomes the Commission's recognition of the challenges posed by cookie and consent fatigue. In this context, the revision of the e-Privacy Directive will introduce measures to streamline consent requirements and enable machine-readable user preferences, and reduce administrative burdens for businesses while improving user experience. Simplifying consent procedures helps SMEs and startups comply more efficiently and ensures that users are not overwhelmed by repetitive and unclear prompts, creating a more rational and user-friendly digital environment.

The repeal of the Platform-to-Business (P2B) Regulation is also an important step forward to reduce fragmentation and compliance uncertainty, since its objective has been largely overtaken by new digital laws.

While the Digital Omnibus represents an important step forward, ACT believes that its implementation must carefully consider the different capacities and needs of startups and SMEs. Simplification should be practical and tailored, ensuring that smaller businesses are not disproportionately burdened. A one-stop reporting system should cover all relevant EU-wide obligations, allowing companies to report incidents once and meet all legal requirements simultaneously. Clear timelines and harmonised documentation standards are essential to avoid conflicting obligations and ensure timely compliance without exposing businesses to unnecessary risk.

Harmonised implementation across Member States is also crucial. Even with a consolidated framework, national-level divergences could undermine its effectiveness and create uncertainty for smaller businesses. Clear guidance and coordinated national application of EU rules will ensure that the framework supports innovation rather than creating additional barriers. Simplification should extend beyond legal texts to include practical guidance, templates, and digital tools that are accessible and usable by SMEs and startups, reflecting the fact that smaller companies have limited resources to comply.

Moreover, updates to the e-Privacy Directive that clarify rules on storing and accessing data on users' devices are essential. Streamline consent requirements and enabling machine-readable user preferences will simplify compliance for SMEs while improving the digital experience for users. The Platform-to-Business (P2B) Regulation is also welcomed for promoting transparency and fairness on online platforms. Ensuring that these obligations are proportional to company size is critical to maintaining a dynamic and competitive digital ecosystem where smaller platforms can thrive, while complying with a flexible and simplified reporting system.

Finally, we encourage the inclusion of robust monitoring and review mechanisms to assess the real-world impact of the Digital Omnibus on data sharing, competition, and innovation. Such mechanisms would allow for timely adjustments where objectives are not being met or unintended consequences arise.

In conclusion, ACT strongly supports the Commission's efforts to simplify and consolidate the EU digital framework through the Single Reporting Mechanism and cookie consent streamlining. However, simplification must go hand-in-hand with proportionality and predictability for startups, mid-sized companies, and SMEs. One-size-fits-all rules risk undermining innovation and competitiveness. Policymakers should prioritise harmonised national implementation, provide practical support and guidance to smaller businesses, and ensure that simplification reduces administrative burdens without compromising safety, transparency, or fairness. By doing so, the Digital Omnibus can become a true enabler of a competitive European digital economy.

CONCLUSION

The Digital Omnibus is a welcome and necessary initiative to rationalise the EU digital framework. By consolidating overlapping instruments and streamlining compliance processes, it has the potential to create a more navigable regulatory environment that supports innovation and cross-border growth.

ACT strongly supports the Commission's efforts to simplify data regulations, establish a Single Reporting Mechanism, streamline cookie consent requirements, and repeal redundant legislation. These measures respond directly to longstanding concerns raised by the startup and SME community about regulatory complexity and compliance costs.

The interaction between different legal frameworks, particularly between the GDPR and the Data Act, requires further clarification to prevent legal uncertainty and overly conservative compliance strategies that discourage beneficial data sharing. Clear, practical guidance with concrete criteria for risk assessment, including safe harbours and standardised tools, would enable startups to make confident compliance decisions without extensive legal resources.

Across all areas, AI regulation, data protection, data sharing, and incident reporting, the key challenge is ensuring that simplified frameworks are practical and proportionate for SMEs. This means going beyond legal consolidation to provide accessible implementation tools, harmonised standards, and flexibility that accounts for differences in company size and capacity.

We also encourage the inclusion of robust monitoring and review mechanisms to assess the real-world impact of the Digital Omnibus on data sharing, competition, and innovation. Such mechanisms would allow for timely adjustments where objectives are not being met or unintended consequences arise.

By prioritising practical implementation, proportionate obligations, and genuine simplification, the Digital Omnibus can become a true enabler of a competitive European digital economy. ACT remains committed to working constructively with policymakers to ensure that the final framework supports the growth and success of European SMEs and startups while maintaining high standards of protection for users and businesses alike.