CONFEDERATION OF INDUSTRY
OF THE CZECH REPUBLIC

PRAGUE, DECEMBER 15TH 2025

POSITION OF THE CONFEDERATION OF INDUSTRY OF THE CZECH REPUBLIC (SP ČR) ON THE DIGITAL OMNIBUS

The Digital Omnibus marks an important and long-awaited shift in the EU's approach to digital regulation. For several years, European industry — including SP ČR and our partner business federations — has been calling on the Commission to simplify rules, reduce fragmentation, and provide a more predictable regulatory framework. We therefore welcome the fact that the Commission has now presented a package that responds to many of these concerns and recognises the growing need to ease the administrative burden on companies.

From our perspective, the Digital Omnibus is not a new layer of regulation, as it is sometimes portrayed, but rather an attempt to streamline existing rules and make them more workable. This direction is both necessary and appreciated. At the same time, the proposals fall short of what is needed for simplification to be meaningful in practice. Many obligations remain unchanged, deadlines are often unrealistic, and several technical issues — long raised by industry — require clearer solutions.

Below, we outline both the elements we welcome and the areas where further improvement is essential.

1. AI Act – a positive shift, but real legal certainty still requires bigger changes

SP ČR welcomes the Commission's willingness to adjust the AI Act, in particular the effort to clarify definitions, improve classification rules, and extend certain deadlines. This reflects long-standing demands from industry.

However, the effectiveness of the AI Act still depends on conditions that are not yet in place. Obligations for high-risk systems must not be applied before harmonized standards, classification guidelines, reporting methodologies, and technical tools are available. The Commission's proposal recognises the problem, but the extensions of 12–18 months remain insufficient.

The need to seriously consider extensions also applies to Article 50 regarding the provenance and transparency of generative AI. Given that the Code of Practice is far from being finalized, the existing timeline for enforcement (August 2026 for Article 50(4)) is unrealistic. The agreed extensions should apply to new systems as well as those already on the market.

To avoid delays to the entire Omnibus, the extension of AI Act deadlines should be adopted as a separate, fast-track legislative proposal. At the same time, we welcome and strongly support the removal of the obligation to provide access to source code (Articles 74(13) and 92(3)), which would otherwise expose companies to severe IP and cybersecurity risks. Furthermore, the full exclusion of AI systems already

E-MAIL SPCR@SPCR.CZ
WEB WWW.SPCR.CZ | ADDRESS FREYOVA 948/11, 190 00 PRAGUE 9, CZECH REPUBLIC

regulated under other legal frameworks (as outlined in Annex 1) is necessary to avoid unnecessary duplication and complexity.

A further clarification is also needed concerning the distinction between B2B and B2C systems. Requirements intended for consumer protection must not be automatically applied to purely industrial or enterprise solutions.

In addition, SP ČR welcomes the postponement of certain obligations for high-risk AI systems and reporting requirements, but emphasises that the most financially and administratively burdensome elements of the AI Act remain unaddressed. It is necessary to reduce reporting obligations for non–high-risk AI systems, enable a greater degree of flexibility for high-risk conformity assessors to avoid delays, avoid double regulation of vehicles, and ensure that AI requirements for the automotive sector are adopted transparently and early enough to allow sufficient implementation time.

2. AI Act – CRA interaction: SP ČR welcomes recognition of the problem, but duplication must be removed

One of the most persistent and burdensome issues in the digital regulatory landscape — the overlap of the AI Act and Cyber Resilience Act — still requires more ambitious action.

SP ČR welcomes the Commission's acknowledgment of the need for coordination, yet the current proposals do not eliminate the duplication of conformity assessments. Companies remain at risk of undergoing two parallel audits and preparing two sets of documentation for systems that are often identical.

SP ČR considers it essential to allow joint conformity assessment for both laws. This would significantly reduce unnecessary administrative costs and allow companies to focus resources on innovation and security improvements.

3. GDPR and Data – a step toward clarity, but uniform interpretation and practical adjustments are essential

SP ČR positively notes that the Digital Omnibus includes measures that move GDPR in a more practical direction. Among the most welcome steps are:

- clarifying the definition of personal data in line with CJEU case law,
- expanding Article 9 to better support AI training and deployment,
- introducing "legitimate interest" as a legal basis for data processing in AI development.

The proposed clarification of the definition of personal data from an objective to a subjective test (i.e., data is personal only if a controller can reasonably identify a person) could bring substantial relief in borderline cases and reduce divergent interpretations by national regulators. SP ČR also welcomes the integration of cookie-related ePrivacy rules into the GDPR, as cookie consent banners have long ceased to fulfil their original purpose and primarily hinder user experience. However, further steps are needed - notably limiting the need

for consent for accessing data on end-user devices and enabling reliance on legitimate interest where appropriate. Moreover, Article 88b, which reintroduces the concept of browser-level consent, should be removed. As discussed in previous rounds of negotiations at the EU level, a browser-level consent does not meet fundamental GDPR consent requirements and will not actually address the underlying causes of consent fatigue. Instead, it will harm the overall model of the ad-supported open web.

In addition, SP ČR welcomes the newly introduced exceptions allowing processing of special categories of personal data for AI development based on legitimate interest. To ensure innovation remains compatible with GDPR principles, innovation itself should be explicitly recognised as a legitimate purpose within the proportionality test.

However, these improvements will only work if they are interpreted uniformly across all Member States. Without binding guidance, Europe risks ending up with 27 interpretations - a situation that would further erode legal certainty rather than strengthen it. To avoid further fragmentation of the EU Single Market, the provision enabling national laws to override the GDPR should be removed.

SP ČR further recommends extending Article 9(2) to allow processing of special categories of personal data based on a contract. Similarly, GDPR should incorporate a "proximity criterion" for incidental sensitive data and introduce a broader exemption for innovation in the public interest beyond AI-specific cases - a change necessary for applications such as autonomous driving, which rely on imagery where persons may be visible yet not identifiable.

Regarding incident reporting under GDPR, it is important that the unified system (SEP) enables submission of detailed explanations, acknowledges that data-breach incidents often require broader documentation than cybersecurity events, and allows holding-level reporting where incidents affect an entire group.

4. Single-Entry Point (SEP) – Necessary Functionality, Holding Reporting, and Harmonization

SPČR strongly welcomes the creation of a single incident-reporting interface. This is one of the most significant simplification measures in the entire Omnibus. For the SEP to deliver on its purpose, it should:

- permit single reporting for entire holding structures where appropriate,
- allow companies to report via their main establishment,
- ensure legal protection for companies submitting incident notifications,
- be fully compatible with the CRA reporting platform,
- support the detailed information required for GDPR incidents.

From an NIS2 perspective, a unified reporting portal administered by ENISA — following the principle *“report once, share many times”* — would bring major administrative and financial relief. This aligns with the broader goal of reducing fragmentation across NIS2, GDPR, DORA, eIDAS, and CER regimes.

These principles should be explicitly reflected both in the operative text and in the recitals so that Member States implement them consistently.

5. Data Act – Need for Clarification, Protection of Business Data, and Legal Certainty

SP ČR considers the consolidation of open data rules within the Data Act to be a positive step. The specific relief measures for SMEs and small mid-caps are also welcome.

At the same time, SP ČR welcomes the narrowing of B2G data obligations to crises explicitly defined in the Data Act and the strengthened exclusion of trade secrets from mandatory data sharing.

To make the new framework workable, SP ČR considers it necessary to:

- exclude B2B data, as already today, manufacturers and customers negotiate data usage rights on an equal footing, and in the B2B context, the Data Act would mean a massive implementation effort, binding unnecessary resources,
- clarify that obligations to provide open data apply only to datasets explicitly defined as reusable under the Data Act,
- ensure that individualized SaaS services are not subject to mandatory B2B data sharing and rules on switching data processing services,
- provide explicit criteria for determining which datasets from connected products fall within the scope of the Data Act (or address this through Commission guidance),
- refine the definition of "data holder" to avoid circular reasoning and ensure that legal responsibility aligns with actual control over access to data,
- simplify the pre-contractual information obligations to what is truly relevant for users,
- and avoid duplication by removing redundant provisions, such as Article 20a of the RED III Directive.

6. Cybersecurity – Need for Deeper Harmonization and Realistic Deadlines

The Omnibus introduces improvements in incident reporting but does not address the structural problem of fragmented cybersecurity regulation. NIS2, DORA, and the CRA still impose overlapping, sometimes inconsistent obligations.

Conclusion:

SP ČR welcomes the Digital Omnibus as an encouraging step towards long-needed simplification. The Commission’s recognition of industry concerns — including clearer definitions, unified reporting, support for research, and elimination of unnecessary burdens — is a significant achievement and should be acknowledged as such.

At the same time, the proposals require further refinement to ensure that simplification becomes a reality, not just an intention. In particular, SP ČR emphasises the need for:

- a rapid, stand-alone extension of AI Act deadlines,
- elimination of duplication via joint conformity assessments,
- uniform interpretation of GDPR across all Member States,
- protection of TDM exceptions for research and innovation,
- a technically robust and holding-level-capable SEP,
- clear and realistic rules for the Data Act,
- deeper harmonisation of cybersecurity regulation.

Only a pragmatic, coherent, and business-friendly digital framework will allow European companies to innovate, compete globally, and make digitalisation a true driver of Europe's economic strength.