

Warsaw, 20 March 2026

Position of the Union of Entrepreneurs and Employers (ZPP) on the Digital Omnibus Package

- **The ZPP supports the move towards simplifying European digital regulations, but this simplification must be genuine, proportionate and adapted to the realities of the modern digital economy.**
- **The proposed provisions on browser-level consent, in particular Article 88b, raise fundamental concerns, as they may weaken the competitiveness of European businesses, especially SMEs, without any demonstrated benefit to users.**
- **For the ZPP, this is not a technical issue nor one limited to the digital advertising sector. It is a solution that could have a real impact on the entire online sales ecosystem, including online shops, marketplaces, payment service providers, analytics, security, marketing and sales support tools.**
- **The ZPP calls for the abandonment of the mandatory, centralised browser-level consent model under Article 88b and for the focus of the reform to shift towards modernising Article 88a, so as to limit excessive consent requirements where the risk to the user is low and processing is justified, proportionate and necessary for the functioning of digital services.**
- **The ZPP supports a relative approach to the definition of personal data, the extension of standards to PETs, the clarification of the definition of scientific research, and the narrowing of the overly broad interpretation of special categories of data.**

The Union of Entrepreneurs and Employers, representing over 21,000 member companies operating in Poland and the region, the vast majority of which are small and medium-sized enterprises, welcomes the direction of work on the Digital Omnibus package. Simplifying European digital regulations, increasing their consistency and reducing excessive regulatory burdens are necessary and justified objectives from the perspective of the European Union's competitiveness.

At the same time, we emphasise that simplification must not mean creating new, rigid mechanisms which, in practice, will prove costly for the market, difficult to implement and unconvincing from the user's perspective. Good digital law should solve real regulatory problems, rather than merely shifting them from one level to another.

From this perspective, we are particularly critical of the proposal contained in Article 88b concerning browser-level consent. This mechanism is presented as a response to the phenomenon of so-called ‘consent fatigue’, but in practice it may lead to the centralisation of consent management at browser level, a weakening of the relationship between the business and the user, a decline in the effectiveness of legitimate marketing and analytical activities, and a restriction on the potential for the development of digital services, particularly among SMEs.

For the ZPP, this is not a narrow or sector-specific issue. Browser-level consent could affect the entire online sales ecosystem, encompassing not only the largest platforms but also online shops, retail businesses, digital service providers, technology partners, security systems, analytical and marketing tools, and thousands of businesses that use digital solutions to acquire customers and build a competitive advantage. Smaller businesses will be particularly hard hit, as they lack the scale and resources of the largest players, yet are dependent on an efficient, proportionate and predictable regulatory environment.

Areas supported

1. Definition of personal data, Article 4(a)

The ZPP welcomes the attempt to codify a relative approach to personal data. This is in line with a modern, risk-based understanding of data protection and is important from a business perspective.

If the controller does not have reasonable means to re-identify an individual, the data should not automatically be treated as personal data in relation to that entity. This approach enhances legal certainty, reduces excessive formalism and creates real incentives to invest in pseudonymisation and secure data processing architectures.

2. Pseudonymisation standards and PETs, Article 41a

The ZPP supports granting the Commission the power to clarify standards in the area of pseudonymisation. This is a necessary step towards greater regulatory predictability.

At the same time, we note that limiting this mandate solely to pseudonymisation is too narrow. The modern technological ecosystem is also developing other privacy-enhancing technologies, such as on-device processing, differential privacy and synthetic data. The legal framework should cover a broader category of PETs, rather than just a single risk mitigation method. Only then will the regulation be truly technology-neutral and resilient to rapid progress in the field of AI and data.

Areas requiring clarification

1. Definition of scientific research, Article 4(b)(38)

The ZPP supports broadening the definition of scientific research to also include technological development, applied research and privately funded research. This is an important direction from the perspective of building a competitive digital economy in Europe.

However, it should be clarified that the contribution to the advancement of knowledge and social welfare cannot be understood in isolation from the realities of innovative activity. In practice, many research and development activities deliver social benefits through the implementation of new products, services and technological solutions. One must not create the impression that research activities require the public disclosure of methodologies or results in a manner that would undermine the protection of trade secrets and know-how.

2. Special categories of data and bias mitigation, Article 9

The ZPP supports a more pragmatic approach allowing the processing of special categories of data for the purpose of detecting and mitigating bias in AI systems. Without such a possibility, it is difficult to build systems that are truly fair and non-discriminatory.

At the same time, it is necessary to clarify when data should be considered as ‘revealing’ special categories of data. An overly broad interpretation, whereby ordinary behavioural data becomes sensitive data merely because it is theoretically possible to draw conclusions from it, cannot be accepted. Such an interpretation undermines the protective purpose of Article 9. We therefore support the approach whereby data should be considered to ‘reveal’ special categories only where such information is explicitly and manifestly disclosed, or where the controller deliberately uses it to draw such conclusions.

Areas requiring changes

1. Article 88a: the provisions on access to data on end devices must be substantially modernised

The ZPP supports the very aim of greater consistency between the GDPR and the existing ePrivacy regime. The current fragmentation of the law has for years led to excessive complexity, interpretative chaos and disproportionate burdens on businesses.

This does not mean, however, that it will suffice to transfer the existing logic of the cookie rules to the GDPR almost unchanged. In its current form, Article 88a still relies on

assumptions from a different era of the internet and does not correspond to the way modern digital services operate.

The biggest problem lies in maintaining an overly rigid structure, in which the lawfulness of operations depends essentially on consent or on a very narrowly defined notion of necessity. Such a model does not reflect how online shops, security systems, analytical tools, anti-fraud mechanisms, service performance measurement or user journey optimisation actually function in practice.

The ZPP calls in particular for:

1. Greater alignment of Article 88a with the GDPR framework

Provisions concerning access to data on end devices should be integrated into the legal framework provided for in Article 6 of the GDPR. Maintaining a separate, more restrictive regime solely for the moment of data access is no longer convincing, either from the perspective of user protection or from the perspective of legal consistency. In particular, it should be permitted to base such operations on a legitimate interest, provided that the conditions under the GDPR are met and appropriate proportionality is maintained.

2. Expanding the list of exceptions to the consent requirement

The list of exceptions should be explicitly extended to include, at a minimum, the prevention of fraud and abuse, the maintenance of the security and integrity of services, performance measurement and basic service analytics, as well as A/B testing and activities aimed at improving the functioning and usability of the service. These are fundamental functions for modern digital services. Without them, businesses, particularly SMEs, are unable to effectively develop services, improve the user experience, enhance payment security or verify whether a particular solution performs better or worse.

3. Explicit consideration of privacy-enhancing technologies

If a business operator employs solutions that effectively reduce the risk to the user, the law should reward this. This applies in particular to recognised PETs, such as on-device processing or other technologies that limit the scope and sensitivity of data. There is no justification for the legal system to require the same level of formalisation of consent in high-risk situations as in situations where the risk has already been technically mitigated. Such a model discourages investment in more privacy-friendly solutions.

4. Moving away from a model based on an abundance of consent notices

An excessive number of prompts does not mean greater user protection. In practice, it leads to fatigue, automatism and a decline in the quality of decisions made. Users do not gain real control if they are constantly asked for consent even for low-risk operations, without which the service cannot develop safely and meaningfully. This model hits

smaller entities particularly hard, as they lack the resources of the largest platforms yet must meet the same requirements.

2. Article 88b: browser-level consent is a disproportionate and risky solution for the market

The ZPP opposes the mandatory binding of controllers to automated, machine-readable signals of consent or objection generated at browser level.

We understand the intention behind this proposal. Reducing ‘consent fatigue’ and simplifying consent interfaces is a goal worth discussing. However, the proposed mechanism does not address the problem appropriately. Rather than improving the quality of consent, it shifts the focus from the user–service provider relationship to the browser infrastructure level, creating new legal, economic and competitive risks.

Our main concerns are as follows:

1. User preferences are contextual, not universal

A user may wish to make different decisions on a local online shop’s website, on a booking platform, and again on a social media site. A single, general browser signal does not reflect this reality. As a result, browser-level consent may lead not to greater user autonomy, but to its simplification and impoverishment.

2. The mechanism weakens the direct relationship between the business and the customer

Yet it is precisely this relationship that forms the foundation of e-commerce and modern online sales models. It enables the development of services, the testing of solutions, the conduct of marketing activities, the building of conversion rates, and the financing of product development. When the decision regarding consent is shifted to the browser level, companies—especially smaller ones—lose the ability to manage this relationship in a manner that is proportionate and tailored to their service.

3. Article 88b could have a significant impact on the entire online sales ecosystem

This solution goes far beyond online advertising. It will affect e-commerce, marketplaces, performance marketing tools, analytics providers, personalisation systems, payment operators, security tools and thousands of SMEs that rely on digital customer acquisition for their growth. For small and medium-sized enterprises, the ability to measure the effectiveness of their activities, improve conversion rates, personalise their offerings, detect fraud and develop functionality is not a luxury. It is a prerequisite for competing with larger players. A poorly designed browser-level consent system could, in practice, deprive them of some of the tools essential to running their businesses.

4. Browser-level consent need not necessarily reduce the number of consent prompts

There is a serious risk that the proposed mechanism will not eliminate banners, but will add another layer of uncertainty to them. If consent given at browser level does not, in practice, meet the requirements of specificity, awareness and a link to a specific processing purpose, service providers will still be forced to display their own messages for some operations.

5. The proposal creates a risk of decision-making becoming concentrated among browser providers

Mandatory browser-level consent effectively strengthens the role of a few infrastructure providers who design interfaces, define how choices are presented, and influence how users understand their decisions. This is particularly sensitive from a competition perspective, as some of these entities also operate in adjacent markets, including digital advertising and other internet services. Such a model may lead to new distortions of competition and the emergence of new gatekeepers at the infrastructure level.

6. The proposed solution has not been preceded by a sufficient regulatory impact assessment

Such a significant change, which could reshape the architecture of consent and the functioning of digital services, should be preceded by a thorough analysis of the legal, technical, security and economic impacts.

7. Article 88b also raises legal doubts regarding the validity of consent

Under the GDPR, consent must be freely given, specific and informed. Replacing individual consents with general browser signals may undermine the requirement to link consent to a specific purpose of processing. As a result, the proposed system may, paradoxically, facilitate mass opt-outs, but make it more difficult to obtain legally valid, active consent where it is actually required.

ZPP's legislative proposals

The ZPP supports the Digital Omnibus as an attempt to streamline and modernise the European digital framework. However, for this package to genuinely serve competitiveness, innovation and user protection, it must be refined in key areas.

- maintaining the direction of changes regarding the relative definition of personal data,
- extending the standards of Article 41a to PETs as well,
- clarifying the definition of scientific research so that it also covers technological development and market innovation,

- narrowing the excessively broad interpretation of special categories of data in Article 9,
- bringing Article 88a more fully into line with the legal basis set out in Article 6 of the GDPR,
- extending the exceptions to the consent requirement to include low-risk and necessary operations related to security, analytics, performance measurement, fraud prevention and service improvement,
- explicitly prioritising privacy-enhancing technologies,
- abandoning the mandatory, centralised browser-level consent model in Article 88b,
- conducting a thorough regulatory impact assessment for the proposed changes regarding browser-level consent.

For the ZPP, this is a matter of real economic significance. We represent over 21,000 member companies, the vast majority of which are SMEs. It is these companies that will feel the effects of poorly designed consent mechanisms, restrictions on reaching customers and disruptions to the functioning of the open internet most acutely. We therefore call for the Digital Omnibus to be shaped in such a way that it simultaneously protects fundamental rights, supports innovation and does not undermine the competitiveness of European business.