



Position on the browser-level consent mechanism in the Digital Omnibus package – proposed alternatives and legislative recommendations

I. Executive Summary

1. We support the aim to simplify the regulatory environment and to reduce the phenomenon of “consent fatigue”.
2. However, the **browser-level consent mechanism (BLC) envisaged in Article 88b of the Digital Omnibus package will not resolve the problems that already exist**. On the contrary, it will give rise to new, significant systemic, legal and economic risks that may lead to further complication of the regulatory regime, increased interpretive uncertainty and a deterioration of conditions for the European digital market – not only for small and medium-sized enterprises (SMEs) but also for Internet users. In our assessment, the proposed solution will fail to comply with the requirements of Article 4(11), Article 6(1)(a) and Article 7 GDPR, as well as Recitals 32 and 42 GDPR, which require consent to be freely given, specific, informed and unambiguous, and given separately for each processing purpose (granular consent). The proposed solution will undermine user agency, hinder controllers’ compliance with information obligations under Articles 13 and 14 GDPR, and cause a range of risks to materialise, including risks to the open Internet funded by contextual and personalised advertising. Our position is consistent with the criticism expressed by the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) regarding the key elements of the proposed amendments.
3. **In order to eliminate the practical and regulatory problems identified by e-Izba, we recommend:**
 - deleting Article 88b and retaining the obligation for enterprises managing individual websites to collect cookie consent;
 - focusing on expanding the exemptions under Article 88a to include low-risk processing operations, in particular operations necessary for contextual advertising (without user profiling), first and third-party analytics, maintenance and security of services, fraud prevention, marketing communications to existing customers (self-marketing) and frequency capping, with reference to Article 13(2) of the ePrivacy Directive and Recital 47 GDPR; as well as reformulating the existing exemption relating to the storage of aggregated user information for the purposes of conducting statistical and analytical activities concerning the use of a website or application ad billing to also include the possibility of using third-party solutions for the exclusive purposes of the enterprise (controller);
 - confirming in Article 88a the admissibility of storing information in or accessing information from terminal equipment based on any of the legal bases provided for in Article 6 GDPR, including the legitimate interest of the controller;



- streamlining the cookie regime by repealing Article 5(3) of the ePrivacy Directive and fully integrating the “cookie rules” into the GDPR, with unified supervision by data protection authorities;
 - instead of introducing a minimum six-month period before re-requesting consent, we propose a shorter one-month period that is proportionate given evolving services and user preferences;
 - preserving the existing body of practice regarding the display of cookie banners by specifying in Article 88a the essential elements of information that should be provided to the end user before obtaining valid consent for the installation of cookies and similar technologies;
 - implementing a harmonised EU-wide cookie banner template, which will strengthen the harmonisation of rules across the European Union and eliminate the chaos currently observed in the digital market;
 - introducing uniform EU-wide UX standards for consent interfaces that raise user awareness of data processing principles and eliminate so-called dark patterns.
4. Our recommendations aim to simultaneously increase privacy protection, reduce banners where they are not needed, and maintain conditions for the competitiveness of the European digital economy and media pluralism. Available estimates indicate that centralising consent at the browser level could reduce the number of consents given by 60–65% and cause a drop in digital advertising revenues in the EU of EUR 40–50 billion annually, i.e. by 30–35%, with an additional sensitivity of EUR 600–800 million annually for every 1% decrease¹.
 5. In light of the available materials, we assess that BLC, by detaching the consent decision from the context of a specific service and controller, may not reduce the number of banners displayed, but rather transform “consent fatigue” into new forms of informational pop-ups, pressure and ambiguity for users, including through the proliferation of “pay or OK” models.
 6. We also note that, due to the centralisation of the consent mechanism on the side of browser providers, BLC may in practice strengthen the market position of the largest browser providers, which is contrary to the objectives of EU digital policy aimed at competitive balance and limiting the influence of such providers on market access conditions.
 7. We also point to the regulatory and sanctions risk on the side of controllers: should Article 88b be retained in its current wording, controllers may find themselves in a situation where simultaneous fulfilment of GDPR obligations (in particular Articles 5, 6, 7, 13) and the requirements of Article 88b is excessively burdensome, giving rise to the risk of administrative fines under Article 83 GDPR, despite acting in good faith.
 8. We also call for a full regulatory impact assessment for the proposed Article 88b, in accordance with the Better Regulation Guidelines, taking into account the impact on GDPR compliance, the competitiveness of the European digital market, media pluralism and the fundamental rights of users. The proposal requires sufficient time for the Council to properly evaluate solutions. Given the profound and disruptive potential of Article 88b, the Presidency should allow sufficient time for a rigorous and proper evaluation of the long-term consequences. A compressed negotiation timeline on Digital Omnibus carries the risk of rushed decision-making; fortunately, there is no immediate urgency, as the Parliament’s

¹ Assessing the socio-economic impact of browser-level consent in the EU, prepared by the Consultancy Group, https://cms.implementconsultinggroup.com/media/uploads/articles/2026/Gone-in-one-click/260325_Gone-in-one-click.pdf [accessed 05.05.2026]



position remains pending until February 2027. It is essential for the Council to use this time to collaboratively explore more viable, effective alternative solutions that avoid unnecessary economic disruption

II. Brief description of the problem

The essence of the problem that the Digital Omnibus package concerning BLC is intended to solve is the excessive burden on users caused by banners relating to the installation of cookies and similar technologies on their terminal equipment, and the resulting decrease in the quality of consent decisions, which has been aptly diagnosed as “consent fatigue.” The Commission’s proposed solution in the form of a centralised BLC mechanism shifts the act of giving consent from the level of “user – specific controller” to the browser interface. This mechanism assumes that browsers will transmit automated, machine-readable preference signals (consent signals) that would be binding on all providers of information society services operating in the EEA. However, the proposal does not sufficiently specify: (i) the scope of processing purposes covered by a single signal, (ii) the method of configuring user preferences and its granularity, (iii) the scope and nature of obligations incumbent on browser providers (whether they are controllers, processors or entities performing quasi-public functions), (iv) the legal effect of the signal (whether it replaces consent within the meaning of Article 4(11) GDPR or constitutes a rebuttable presumption), (v) the rules of liability for incorrect reading, transmission or interpretation of the signal. In practice, this effectively means “blanket” consent or refusal relating to an unlimited number of heterogeneous online services that differ in terms of controller identity, purposes, categories of recipients, legal bases and security practices. The proposal envisages a minimum six-month binding period for refusal, which, given the realities of the rapidly evolving digital world and changing user preferences, is a very long period.

A critical consequence of implementing the proposed solution is the detachment of consent from the context in which the user typically assesses the value and risk of a given service, and also builds trust in the controller. This is contrary to the requirement of “specific,” “informed” and “unambiguous” consent, given separately for each processing purpose, arising from Article 4(11), Article 6(1)(a) and Article 7 GDPR, as well as from Recitals 32 and 42 GDPR. This requirement has been confirmed in the established case law of the CJEU, which affirms that consent must be active and specific in relation to a defined purpose, and that the burden of demonstrating the informed nature of consent rests on the controller. As a consequence, a reduction in users’ real agency must be expected, because a global browser-level choice does not reflect the differentiated attitudes towards brands, types of content and monetisation models, which is confirmed by the observation that users do not make uniform privacy decisions across all services. Additionally, the browser is unable to provide the user with information about the identity of every specific controller, all purposes and categories of recipients across millions of websites, let alone guarantee actual fulfilment of the information obligation under Articles 13 or 14 GDPR in the relationship with a specific publisher. In practice, controllers may be forced to continue maintaining their own interfaces to fulfil information obligations, meaning that the number of banners may not decrease in a manner commensurate with the declared objective of the reform.

From the market perspective, the proposed solution does not sufficiently distinguish between high-risk and low-risk processing operations, subjecting both personalised advertising profiling and essential operations accompanying contextual advertising, as well as measurement provided by third-party solutions, to a single regime. From a cross-border perspective, the risk of user confusion should also be noted, as BLC signals will be legally effective only within the EEA, while outside it they will remain de facto optional, potentially rendering browser-based choices ineffective (this will occur without user intervention).



Furthermore, transferring rules concerning personal data stored on terminal equipment to the GDPR generates a “splitting” of the regime for the same files and technical identifiers, resulting in overlapping legal bases, multi-track supervision and increased legal uncertainty. In particular, there is a risk of parallel jurisdiction of national ePrivacy authorities and data protection authorities, a lack of a uniform cooperation mechanism between these authorities, divergent sanctions regimes, and consequently a risk of conflicting decisions in individual Member States. The Digital Omnibus package was intended to simplify the rules for processing data using information installed on terminal equipment, and the multiplication of legal regimes contradicts these objectives.

Independently of the above, it should be noted that the proposed BLC mechanism is based on the assumption of the dominant role of the web browser as the main point of access to digital services, which does not correspond to contemporary market realities. A significant part of user interactions with information society services now takes place through mobile applications, connected devices and artificial intelligence-based interfaces, in which the browser no longer serves as the main intermediary. Basing the consent regime on a browser-based model is therefore a structurally inadequate solution for the actual shape of the contemporary digital ecosystem, and an attempt to extend BLC logic to other distribution channels would replicate the same problems identified in relation to browser providers, deepening the market asymmetry in favour of entities controlling the system layer of terminal equipment.

III. Proposed solutions and legislative recommendations

1. Deletion of Article 88b and expansion of Article 88a

As a first step, we recommend abandoning the BLC mechanism by deleting Article 88b and focusing legislative efforts on strengthening and specifying Article 88a, so as to introduce a balanced, risk-based model of consent given in the context of a specific website or application and exemptions that distinguish between high-risk and low-risk operations and naturally limit the number of banners to cases in which user choice matters most.

Only by deleting Article 88b and departing from the proposed BLC solution will it be possible to build on the existing body of practice and cookie banner standards, improving them rather than replacing them with a new mechanism of questionable interpretive clarity.

The main problem associated with retaining the proposed BLC mechanism is the detachment of the consent stage for storing information on terminal equipment from the specific service (website/application) to which that information relates. This results in users having to make a choice – acceptance or refusal of information storage – that will apply to a variety of online services, differing in terms of controller identity and the purposes for which such information is installed on the device. Consequently, consent given through BLC will lack the elements of “specificity” and “awareness” on the part of the user, as it will be blanket in nature, which is contrary to the requirements of Article 4(11) and Article 7 GDPR and to the EDPB Guidelines 05/2020 on consent, which clearly emphasise the need to obtain separate consent for each processing purpose (granular consent). Given that websites or applications are to read the automated and machine-readable indications of choices made by data subjects regarding the processing of personal data on natural persons’ terminal equipment, it is difficult to see how a user will encompass within their consent a specific processing purpose pursued by a given online service. Additionally, web browsers do not possess the tools to verify the actual practices of individual entities, creating scope for abuse and improper use of data. The



proposed solution also conflicts with the principle of privacy by design and privacy by default expressed in Article 25 GDPR, as it shifts the burden of designing privacy protection mechanisms to an entity (the browser provider) that is not a data controller within the meaning of Article 4(7) GDPR and does not have knowledge of the purposes of individual processing operations.

Moreover, the timing of the fulfilment of the information obligation by a given website or application under the proposed solution may also be delayed, since the giving or refusal of consent will be centralised, while the relevant processing to which such a choice relates will differ in terms of entities and subject matter. Controllers will, as a rule, have difficulty fulfilling their information obligations, and consequently may need to maintain some form of banner purely for informational purposes. Thus, the proposed solution will not reduce the number of information banners displayed.

The fulfilment of the information obligation under Article 13 GDPR must take place no later than the moment of collection of personal data. The centralisation of consent in the browser, which by its very nature does not have knowledge of the identity of all controllers, purposes and categories of recipients at individual publishers, structurally prevents fulfilment of this requirement. This is contrary to the principle of transparency expressed in Article 5(1)(a) GDPR and to the Guidelines of the Article 29 Working Party (endorsed by the EDPB) on transparency.

Retaining Article 88b, including the proposed “media” exception, will lead to an unjustified differentiation of obligations among various participants in the digital market. This differentiation raises concerns under the principle of equal treatment arising from Article 20 of the EU Charter of Fundamental Rights and the proportionality test required under EU law for differentiating the legal position of comparable market participants, as the drafters have not provided a convincing justification for distinguishing the category of media service providers, nor for preferential treatment of browser providers based on size criteria. The exception provided for media service providers effectively enables them to continue independently collecting consent under the existing rules despite BLC signals, which undermines the fundamental objective of the reform – namely reducing “consent fatigue” – and its justification does not appear consistent with respect to other categories of online services. The EDPB and EDPS have also been critical of this exception, additionally noting that advertising and tracking activities in the media environment are often carried out not only by the media entity itself but also by third parties present on the website or in the application. Moreover, it is unclear why only media service providers should be covered by this exception, which – apart from the additional regulatory complications – creates unequal conditions for various entities operating in the digital economy.

Analogous reservations arise concerning the exemption provided in Article 88b of certain obligations for browser providers that are SMEs, which leads to unjustified preferential treatment on the browser provider market based on the criterion of enterprise size. The EDPB and EDPS have also indicated the lack of a convincing justification for differentiating the positions of individual market participants in this regard.

We therefore call for the expansion of the catalogue of exemptions in Article 88a to include low-risk and operationally essential operations, including:

- **contextual advertising without profiling,**
- **first and third -party analytics,**
- **content frequency capping (particularly for contextual advertising),**



- **measurement of advertising campaign effectiveness and ad billing based on aggregated information carried out on the controller's behalf by third parties,**
- **operations for the maintenance and security of services, including the detection of cyber threats and ensuring their technical performance, which constitute a basic and expected ancillary service accompanying the use of the service;**
- **fraud prevention and detection, including the prevention of account takeovers and securing transactions or ad fraud prevention which directly serve the protection of users themselves;**
- **marketing communications to existing customers (self-marketing), the admissibility of which is already supported by Article 13(2) of the ePrivacy Directive (providing for an opt-out mechanism) and Recital 47 GDPR, which recognises direct marketing as a legitimate interest of the controller.**

Expanding the catalogue of exemptions will relieve users of unnecessary interactions with cookie banners while maintaining rigorous consent requirements for operations posing a high risk to user privacy, such as personalised profiling. Such a model shifts the focus from managing the symptoms of fatigue in the form of cookie banners to removing the root cause of the problem, namely excessive reliance on consent in cases of low risk and high technical necessity for the functioning of the open Internet. The effectiveness of achieving this goal through our proposed solution will depend on the simultaneous introduction of an exemption from the requirement for layered fulfilment of the information obligation, allowing simple notification of data processing within the general information obligation, e.g. via a privacy policy.

Furthermore, in our assessment, **it is necessary to specify standards for consent interfaces on the controller's side in Article 88a itself or in implementing acts and harmonised standards, including the introduction of uniform, easily understandable elements and minimum UX requirements, so that the European standard eliminates dark patterns** while preserving the contextuality and informativeness of consent. In particular, the scope of presented purpose categories, a simple opt-out mechanism per category, transparent information on the storage period and the duration of consent, and the ability to easily modify choices from the service interface at any time should be defined, making consent more "living" and embedded in the user–publisher relationship. These recommendations are consistent with the diagnosis that the reduction of banners should result from limiting the consent requirement where its added value for privacy protection is low, rather than from centralising the signal at the expense of legality and user agency. Such a result can only be achieved by specifying in Article 88a the concrete conditions that must be met for consent to be lawful and for the user's choice to be informed, while simultaneously introducing a model banner template. The introduction of a uniform standard for collecting consent/refusal while ensuring a uniform level of information about the purposes and principles of processing to which such a choice is to relate will enable genuine harmonisation of the rules governing the digital market in this regard and shape user experiences in a clear and comprehensible manner regardless of the individual characteristics of the user.

Complementarily, we call for Article 88a to explicitly confirm that the storage of information on terminal equipment or access to such information remains permissible on the basis of any of the legal bases provided for in Article 6 GDPR, including the legitimate interest of the controller (Article 6(1)(f) GDPR), subject to a balancing test taking into account the rights and reasonable expectations of data subjects. This will enable the construction of a unified, coherent GDPR-



based regime in which consent is not treated as the sole or default basis for the lawfulness of processing in every situation, but rather as one of several equivalent instruments selected appropriately to the nature of the operation. This solution will increase legal certainty for controllers, limit the phenomenon of parallel application of inconsistent legal bases to the same operations and – contrary to concerns – will not lower the level of data protection, as all other guarantees arising from the GDPR will be maintained.

2. Repeal of Article 5(3) of the ePrivacy Directive

As a second step, **we propose streamlining the regulatory environment concerning the storage of information on terminal equipment by repealing Article 5(3) of the ePrivacy Directive and transferring all requirements contained therein to the GDPR provisions** regarding the provision of information, including the purpose of storage and the right to withhold/withdraw consent. This will enable the full integration of cookie and similar technology rules into the GDPR, eliminating parallel, partially overlapping legal regimes for the same operations, and will simplify data processing rules. It will also ensure a unified supervisory system by data protection authorities, without prejudice to terminal equipment users. This solution responds to EDPB/EDPS criticism regarding the risk of fragmentation and interpretive uncertainty, and strengthens predictability for enterprises operating cross-border.

In order to regulate cases where information stored and retained on terminal equipment does not constitute personal data, we propose the addition of a further paragraph to Article 88a, providing that:

„Where information stored and retained on terminal equipment does not constitute personal data, paragraphs 1 to 4 above shall apply mutatis mutandis, and the competent supervisory authority shall be the supervisory authority responsible for fulfilling the tasks and exercising the powers conferred upon it in accordance with this Regulation in the territory of its Member State.“

Consequently, at the national level, we call for the repeal of Article 399 of the Electronic Communications Law, which constitutes the implementation of Article 5(3) of the ePrivacy Directive. Maintaining the national provision after the repeal of its EU basis would lead to the further entrenchment of a parallel, fragmented legal regime for the same processing operations, contrary to the objectives of the Digital Omnibus package. An amendment to Article 400 of the Electronic Communications Law will also be necessary insofar as that provision refers to the aforementioned provision.

3. Shortening the consent retention period

We recommend **shortening the proposed period for respecting refusal and acceptance of consent to one month instead of the proposed six months**. Specifying a concrete period for respecting a given consent or refusal should be coupled with the requirement to provide users with simple tools for revoking or changing their decision ad hoc, which do not require lengthy identification. Implementing such a solution better reflects the dynamics of consumer behaviour and the principle of data minimisation expressed in Article 5(1)(c) GDPR, according to which data (including cookie preferences) should be stored for no longer than is necessary for the purposes of processing. We are aware that shortening the consent retention period could theoretically increase the frequency of user exposure to banners; however, in our assessment, this effect will be more than offset by the simultaneously proposed expansion of the catalogue of exemptions in Article 88a (section III.1), which will structurally limit the number of situations requiring the display of a banner. The proposed shorter period will reduce the technical pressure for persistent user tracking and will make it easier for controllers to adapt



their practices to purposes where the user's choice may change rapidly with context and trust in a specific website or application publisher.

5. Benefits for business, the economy and consumers

The legislative direction we propose will achieve the goal of reducing “consent fatigue” by limiting the consent requirement to operations posing a genuine risk to privacy, which will naturally reduce the number of banners without compromising the principle of legality and contextuality of user choices.

For enterprises, particularly SMEs, the expansion of exemptions to include contextual advertising and ancillary operations will maintain the foundations for effective customer acquisition and content monetisation, limiting cost pressure and the risk of revenue declines that under the BLC scenario would reach 30–35% of current advertising revenues in the EU.

For the media market, departing from BLC and eliminating sectoral exceptions will foster more competitively neutral conditions and the maintenance of media pluralism, which is protected by Article 11 of the EU Charter of Fundamental Rights and Regulation 2024/1083 (European Media Freedom Act), because the value of advertising inventory will not be artificially depressed by the inability to carry out basic measurement and validation operations.

SMEs, which constitute 99% of European enterprises, are the most exposed to the negative effects of BLC, as they do not possess their own extensive first-party data bases and rely more heavily on digital advertising tools for customer acquisition and retention. Smaller enterprises cannot afford untargeted advertising – they must precisely reach users in their market segment, which requires cookie-based personalisation. Automated browser signals may in practice prevent many entities from reaching new users and developing their business based on existing marketing models.

Consumers, in turn, will derive tangible benefits in the form of more understandable, contextual consent interfaces with uniform informational elements across the entire EU, as well as greater transparency regarding the duration of consent and data storage, facilitating genuine privacy management without excessive barriers to using services.

Limiting the consent requirement for low-risk operations and short decision validity periods with an easy option to modify will reduce cognitive and economic pressure, and will limit the need for publishers to resort to “pay or OK” models, which under the BLC scenario are an anticipated consequence of declining advertising revenues. As a consequence of introducing BLC, a “two-tier” Internet would emerge, in which quality content would be available only to those who can afford numerous subscriptions, undermining the democratic value of the open Internet. Many independent publishers would simply cease to exist, and access to pluralistic information would be restricted. In summary, this may have critical consequences for freedom of information, freedom of expression, democracy and the freedom to share pluralistic ideas.

Preserving contextual advertising and basic advertising campaign effectiveness measurement functions while protecting against profiling without consent will ensure better proportionality and user agency, as well as greater predictability for business.

In macroeconomic terms, limiting the risks of a drastic decline in consent rates, the scale of which under BLC is forecast at 60–65%, will prevent the loss of EUR 40–50 billion annually in EU advertising revenues and secondary effects in the form of rising consumer prices and reduced access to free content. European enterprises will retain greater independence from global platforms with their own data ecosystems, which will support long-term competitiveness



CHAMBER OF DIGITAL ECONOMY

and innovation consistent with the principle of *privacy by design* expressed in Article 25 GDPR.

The Chamber of Digital Economy
Łucka 18/76,
00-845 Warsaw

KRS: 0000474028
NIP: 701-039-19-22
REGON: 146832492

Phone: +48 506 577 824
biuro@eizba.pl
www.eizba.pl

poświadczenie złożenia podpisów i pieczęci elektronicznych

Certyfikat dla dokumentu o Autenti ID: 78ca7347-6653-46bd-91b3-94ffe9ab6967
utworzonego: 2026-05-06 16:58 (GMT+02:00)

Dokument przekazany do podpisu przez Izba Gospodarki Elektronicznej biuro@eizba.pl, został zabezpieczony pieczęcią elektroniczną Autenti przed wprowadzeniem nieautoryzowanych zmian.



2026-05-06 16:58 (GMT+02:00)

Patrycja Staniszevska

patrycja.staniszevska@eizba.pl

Izba Gospodarki Elektronicznej

NIP: 7010391922 | Prezes Zarządu



**Podpis elektroniczny
zabezpieczony pieczęcią Autenti**

Uwierzytelnienie: e-mail

Powód: Podpisanie dokumentu

Adres IP: 2a00:f41:1816:a2e0:0:49:9e94:fc01

2026-05-06 17:43 (GMT+02:00)

Autentyczność oraz integralność podpisanego dokumentu przed wprowadzeniem nieautoryzowanych zmian została zabezpieczona pieczęcią elektroniczną Autenti.



2026-05-06 17:43 (GMT+02:00)

Niniejszy dokument stanowi poświadczenie wykonania usługi zaufania, w tym złożenia podpisów elektronicznych, zgodnie z zasadami opisanymi w Polityce.

Osoby podpisujące dokument złożyły podpisy elektroniczne zgodnie z zasadami opisanymi w Polityce Usług Zaufania Autenti dla podpisów elektronicznych Autenti oraz obsługi podpisywania dokumentów (dostępnej na: <https://autenti.com/pl/regulaminy>) oraz oświadczyły, że znają i akceptują treść podpisywanego dokumentu a także potwierdziły poprawność i prawdziwość danych służących do złożenia podpisu elektronicznego.

W ramach składania podpisów elektronicznych przeprowadzono uwierzytelnienie podpisujących.

Usługa została wykonana zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Rozporządzenie eIDAS).

Karta podpisów stanowi poświadczenie Autenti w zakresie realizacji poszczególnych usług zaufania, zgodnie z zasadami ich świadczenia oraz definicjami zawartymi w Polityce.