

## Response to consultation

# Protecting EU data and privacy rights in the Digital Omnibus

## Why it matters to consumers

The EU digital rulebook has been designed to protect consumers' data and privacy in the new digital economy. At the core of it, there is a careful balance of interests which the EU's Digital Omnibus now risks overturning. This balance should be protected and even strengthened to protect consumers' fundamental rights and freedoms. The proposed reform of the General Data Protection Regulation (GDPR) goes beyond simplification and will expose consumers to unnecessary risks and compromise essential protections, including the right to effective judicial remedy, and erode trust in digital products and services.

**Published** | February 2026

**Contact** | [digital@beuc.eu](mailto:digital@beuc.eu)

**Reference** | BEUC-X-2026-011

**Document coordinator** | Cláudio Teixeira, Stefano Rossetti

**Credit** | Photo by lersan8910 from iStockPhoto

The European Consumer Organisation ([BEUC](https://www.beuc.eu)) is the largest organisation promoting the general interests of Europe's consumers. Founded in 1962, it proudly represents more than 40 independent national consumer organisations from over 30 European countries. Together with [our members](#), we inform EU policies to improve people's lives in a sustainable and fair economy and society.

### **BEUC, The European Consumer Organisation**

Bureau Européen des Unions de Consommateurs AISBL | Der Europäische Verbraucherverband  
Rue d'Arlon 80, B-1040 Brussels • Tel. +32 (0)2 743 15 90 • [www.beuc.eu](http://www.beuc.eu)  
EC register for interest representatives: identification number 9505781573-45



*Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EISMEA. Neither the European Union nor the granting authority can be held responsible for them.*

## TABLE OF CONTENTS

<b>1. A too restrictive and subjective definition of personal data .....</b>	<b>6</b>
<b>2. Implementing acts must not redefine pseudonymisation.....</b>	<b>7</b>
<b>3. The new definition of "scientific research" should be rejected .....</b>	<b>8</b>
<b>3.1 No purpose limitation for scientific research .....</b>	<b>9</b>
<b>3.2 Exemption from the obligation to inform users .....</b>	<b>9</b>
<b>4. Uncontrolled data use for AI purposes .....</b>	<b>10</b>
<b>4.1 Legitimate interests as default managing AI systems .....</b>	<b>10</b>
<b>4.2 Management of AI systems based on special categories of data .....</b>	<b>11</b>
<b>5. Unjustified limits to right of access to data .....</b>	<b>12</b>
<b>6. Data processing exceptions for SMEs .....</b>	<b>13</b>
<b>7. Automated individual decision-making only when necessary .....</b>	<b>14</b>
<b>8. Single-entry point for data breaches .....</b>	<b>15</b>
<b>9. New cookie rules that hardly apply to cookies.....</b>	<b>15</b>
<b>9.1 Uncertain application .....</b>	<b>16</b>
<b>9.2 Clearer exceptions and stronger safeguards are needed .....</b>	<b>16</b>
<b>9.3. The case for contextualised advertising.....</b>	<b>17</b>
<b>10. Browser signals for cookie preferences .....</b>	<b>18</b>

## Summary

---

The EU's simplification agenda is an opportunity to streamline processes, improve the application and enforcement of digital rules and make it easier for consumers to exercise their rights. However, simplification should not be a cover for deregulation. Despite earlier assurances, the Digital Omnibus proposal on the GDPR goes far beyond "targeted modifications".<sup>1,2</sup> Instead, it weakens longstanding consumer protections regarding data and privacy by reopening the General Data Protection Regulation (GDPR) and the ePrivacy Directive.

We regret that the proposed changes lack adequate justification and evidence, based on an inclusive consultation of stakeholders and a dedicated impact assessment, as required by the Better Regulation principles.<sup>3</sup> Relevant stakeholders also did not have the opportunity to comment on key aspects of the reform beyond the cookie revisions,<sup>4</sup> such as the new restrictive definition of personal data, AI-exemptions, or limits to the right of access. It is especially worrying that these changes, which are now central to the proposal, are closely aligned with Big Tech's own policy positions.<sup>5</sup>

If implemented, these changes will make it more difficult for consumers to protect their data from unlawful processing and to challenge possible violations. Strong safeguards and clear definitions are essential to ensure that consumer rights are protected. Moreover, despite the claims that the present reform aims to increase European competitiveness, it actually risks undermining it, compromising the compliance efforts already made by responsible businesses<sup>6</sup> while favouring dominant, mostly non-European companies consolidate their dominance of the EU market at the expense of European consumers, SMEs and startups.

BEUC welcomes certain elements of the proposal, such as the Single-Entry-Point for incident reporting to improve information sharing and make enforcement more efficient. We also cautiously welcome the provision on browser signals to strengthen consumer consent. However, several aspects still require clarifications to ensure that both a high level of protection for consumers' data and privacy rights and a regulatory level playing field for EU businesses remains in place.

---

<sup>1</sup> European Commission, 'Summary Conclusions of the Implementation Dialogue on the Application of the GDPR', 16 July 2025, [https://commission.europa.eu/get-involved/events/implementation-dialogue-application-general-data-protection-regulation-commissioner-michael-mcgrath-2025-07-16\\_en](https://commission.europa.eu/get-involved/events/implementation-dialogue-application-general-data-protection-regulation-commissioner-michael-mcgrath-2025-07-16_en)

<sup>2</sup> European Commission, 'Simpler EU digital rules and new digital wallets to save billions for businesses and boost innovation\*', [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_25\\_2718](https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2718) (accessed 18 December 2025)

<sup>3</sup> European Commission, 'Better Regulation', [https://commission.europa.eu/law/law-making-process/better-regulation\\_en](https://commission.europa.eu/law/law-making-process/better-regulation_en)

<sup>4</sup> See "Background Note" shared by the Commission before the Reality check on the Cookie Policy Framework under Article 5(3) ePrivacy Directive on 15 September, 14:00-16:30 CET.

<sup>5</sup> Corporate Europe Observatory, 'Article by article, how Big Tech shaped the EU's roll-back of digital rights', 14 January 2026, available at <https://corporateeurope.org/en/2026/01/article-article-how-big-tech-shaped-eus-roll-back-digital-rights>

<sup>6</sup> The Commission's own estimates admit that the reform could add over 80 billion Euros a year in annual compliance costs, far more than what it would cut. The Economist, 20 November 2025, Can Europe's deregulation drive actually deregulate anything? <https://www.economist.com/europe/2025/11/20/can-europes-deregulation-drive-actually-deregulate-anything>

## BEUC RECOMMENDATIONS

- 1** The undue restriction the definition of personal data should be rejected.
- 2** The empowerment of the Commission via implementing acts to define the concept of personal data is disproportionate and should be rejected.
- 3** Reject the new definition of “scientific research” or, at the very least, clearly redefine it to avoid misuse.
- 4** The use of ‘legitimate interest’ for authorising AI systems to process data should not be allowed.
- 5** The processing of sensitive data for AI development should not be allowed.
- 6** The restrictions on consumers’ right to access data should be rejected.
- 7** The use of automated decision making should be allowed only when necessary.
- 8** Support the single-entry point for data breaches and similar incidents, provided it does not result in lower reporting requirements.
- 9** Ensure the requirement for consent remains applicable to cookies, and better clarify the applicable criteria for exceptions.
- 10** Support and clarify the new approach of introducing browsers signals into the GDPR.

# 1. A too restrictive and subjective definition of personal data

The Commission proposes to change the definition of “personal data” in Article 4 GDPR,<sup>7</sup> restricting the definition of personal data under the guise of “aligning” the GDPR with the latest case law of the EU Court of Justice. Yet the Commission proposal is based on a single, selective ruling - *EDPS v SRB* from September 2025.<sup>8</sup>

BEUC considers that this selective approach **redefines** the concept of personal data in an **extremely restrictive and subjective way**. In February 2026, the European Data Protection Supervisor (EDPS) and the European Data Protection Board (EDPB) issued a joint opinion pointing out that the current proposal “does not accurately reflect and clearly goes beyond” the original meaning of the ruling.<sup>9</sup>

In short, under the Commission proposal, any information element that does not **immediately** identify a person would fall outside the definition of personal data. For example, most online activity rely on cookies, hashed email values, device IDs and similar identifiers. Under the new definition, these elements risk no longer being considered as personal data, which means that the GDPR would no longer apply.

Such an approach would be **extremely dangerous for consumers**. In an online environment where increasingly vast amounts of personal data are collected, shared, and repurposed in a continuous flow between different market players, the re-identification of personal data has practically become the norm: despite “anonymised”, vast amounts of data are now easily reconnected and traced back to real individuals. For this reason, such identifiers have consistently been treated as personal data under the GDPR as individuals can be re-identified when data is shared or enriched by other parties.<sup>10</sup>

The proposed change would create a loophole for **many controllers and undermine GDPR enforcement**.<sup>11</sup>

Moreover, this change would drastically reduce protections for consumers. Individual consumers would not only have to prove the existence of a violation of the GDPR but also

---

<sup>7</sup> The Commission proposes adding a new paragraph to Article 4(1), GDPR: “information does not become personal for that entity merely because a potential subsequent recipient has means reasonably likely to be used to identify the natural person to whom the information relates.”

<sup>8</sup> CJEU, 4 September 2025, C-413/23, *EDPS v SRB (Concept of personal data)*.

<sup>9</sup> EDPB/EDPS Joint Opinion 2/2026 On the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus), p. 10.

<sup>10</sup> The EDPB has clarified that the cookie ID itself could be used to prove a user’s digital identity and exercise the rights provided by the GDPR. EDPB, ‘Guidelines 01/2022 on data subject rights - Right of access (Version 2.1)’, 28 March 2023, see p. 25.

<sup>11</sup> Already in 2014, the European Data Protection Supervisor (EDPS) warned that “companies may consider most of their data to be non-personal datasets, but in reality, is now rare for data generated by user activity to be completely and irreversibly anonymised”. See, EDPS, Preliminary opinion, Privacy, and competitiveness in the age of big data: the interplay between data protection, competition law and consumer protection in the Digital Economy, (March 2014), see p. 9.

prove that the data in question is to be considered **personal data**. In practice, consumers would be **confronted with a disproportionately higher burden of proof**,<sup>12</sup> which would prevent them from litigating GDPR violations effectively.

### Recommendation

The definition of personal data is crucial in defining the scope of the EU data protection rules and **should remain flexible**. If the definition is too narrow, companies can avoid GDPR rules by claiming data is not personal. This change goes beyond a mere “targeted amendment”: it hits substantive requirements of the GDPR, weakening privacy protections while increasing risks and undermining trust for consumers.

BEUC therefore recommends **rejecting this change and preserve the current definition** under the GDPR. Any changes to this definition should explicitly reaffirm that **pseudonymous identifiers remain personal data** where they can reasonably be linked to individuals, directly or indirectly, by **any actor** in the processing ecosystem.

## 2. Implementing acts must not redefine pseudonymisation

Following the proposal for a new, more restrictive and subjective definition of personal data, the Commission also proposes a new Article 41a GDPR which would empower it to adopt **implementing acts to define when pseudonymised data no longer qualifies as personal data**.

The definition of personal data is a core element of the EU data protection framework determining the scope of consumer rights. Any attempt to modify this legal definition through an implementing act risks legal uncertainty and weakens consumers protection, especially given the risks of re-identification. Unlike a regulation, an implementing act cannot reliably define whether specific data is personal data. Implementing acts have a limited role to specifying technical details and cannot be an alternative to the clear, objective legal definition in the GDPR.

Moreover, unlike delegated acts, **implementing acts are not subject to ex post control by the European Parliament**, significantly limiting democratic oversight. Following the experience with the **Digital Services Act**, where the EU’s Court of Justice (CJEU) expressly found that key elements of the supervisory fee regime should not have been adopted with “implementing decisions but in a delegated act”, BEUC cautions **against repeating a similar approach**.

---

<sup>12</sup> If the GDPR does not apply, consumers will not be able to exercise their rights, including the right to access the data. As a result, it becomes impossible for them to verify whether a certain piece of data is personal or not.

In conclusion, any changes affecting the definition of personal data must remain in the scope of the GDPR and be subject to a full legislative scrutiny. Frequent or fragmented adjustments to the criteria for pseudonymisation would lead to **legal uncertainty for consumers, businesses, and enforcement authorities alike**, weakening effective enforcement and trust in the GDPR framework.

### Recommendation

BEUC recommends that this **proposal is rejected**. Delegating fundamental assessments to **implementing acts instead of primary legislation** risks undermining the effectiveness and clarity of EU data protection rules, compromising legal certainty and weakening the level of protection for consumers.

Any changes to the **scope of personal data should remain clearly defined in the GDPR itself** and be subject to a full democratic scrutiny.

## 3. The new definition of "scientific research" should be rejected

The proposal introduces a new definition of "scientific research" (Art. 4(38) GDPR), which would include any research which can "also" support innovation, should it:

1. Contribute to existing knowledge or to apply existing knowledge in new ways.
2. Have been conducted with the *aim* of contributing to growing society's *general knowledge*.
3. Adhere to ethical standards in the *relevant research area*.

Additionally, scientific research under the GDPR would **no longer be considered incompatible with the controller's commercial interests**.

This definition is **excessively broad** and **lacks legal clarity**. Core concepts (e.g. "existing knowledge", "technological development", and "growth of society") are left undefined or subjective, allowing organisations to label many activities as scientific research. Additionally, the definition fails to specify what ethical standards are, which can vary widely across fields and cultures, leaving researchers without a consistent framework.

The new definition should be **rejected or, at the very least, be reconsidered**. Data processing should only occur when there is a **clear, significant and defined public interest**, with prior approval from data protection authorities to ensure proper oversight.

### 3.1 No purpose limitation for scientific research

The above changes should be read together with the proposed changes to Art. 5(1)(b) GDPR, which **would allow further data processing for scientific research independently of the conditions** stated in the GDPR which currently regulate secondary processing (Art. 6(4) GDPR).

**In practice**, this would **remove the principle of purpose limitation for scientific research** (i.e. data can only be used for the express purpose it was collected for). Should this change be implemented, it could allow companies (e.g. AI developers) to carry out **unlimited additional data processing** under the cover of “research”, including for commercial interests, while avoiding key GDPR safeguards and **increasing the risk of misuse**.

### 3.2 Exemption from the obligation to inform users

The proposal also adds another exemption whereby a company processing data for scientific research is **no longer required to inform the user** (new Art. 13(5) GDPR), when the act of informing users is considered 1) not possible, 2) to take too much effort, or 3) to hinder the research objectives.

Allowing such broad exemptions from privacy policy obligations under the justification of scientific research activities is disproportionate, creating an unacceptable lack of transparency and oversight that would allow for the unfettered exploitation of all kinds of consumer data for profit, at the **cost of increased privacy risks and undermining of consumer trust**.

#### Recommendation

**The new definition of “scientific research” is disproportionality broad and concerningly vague and** would no longer be limited by the principles of transparency and purpose limitation. This would risks opening the door for private companies to claim research activities while pursuing their own commercial interests.

**BEUC recommends rejecting this definition entirely. At the very least, the definition should be radically reformed:** vague references (i.e. “societal growth”) should be removed or precisely defined. Research exemptions must not become a loophole for extensive commercial data reuse at the expense of consumer rights.

Further processing for research purposes **should only be allowed in case of high public interest** and remain subject to the compatibility assessment and robust safeguards.

## 4. Uncontrolled data use for AI purposes

The proposal contains several different changes to the GDPR which will impact the interplay between data processing and the **development and operation** of AI systems. First, a new provision will allow data processing based on the controller's legitimate interests. Second, another amendment to Art. 9 GDPR would, in practice, allow the processing of special categories of data for AI deployment.

### 4.1 Legitimate interests as default managing AI systems

Firstly, the proposal **would allow any data processing used to train or run AI systems to rely solely on the controller's legitimate interests** (new Art. 88c GDPR). This change risks enabling large-scale data use for AI without consent of users in an unprecedented and unjustified manner. More concerningly, the wording is extremely vague and ultimately fails to clearly define the scope of such activities, creating legal uncertainty and ultimately disrupting the fine balance of the GDPR between innovation, consumer protection, and fundamental rights.

In practice, **there would be no limit to the volume or categories of personal data that AI systems could process**. For example, the controller could use data previously provided by users, such as social media posts, or private communications, as well as data obtained from third parties. Similar practices from AI operators are not new: concerns about AI systems collecting and processing sensitive information of consumers' lives continue to receive **widespread criticism** by the European public.<sup>13,14,15</sup>

BEUC recalls that **consumers remain the most vulnerable link in the AI data processing chain**, for whom it is very difficult to fully understand or anticipate such downstream uses and the potential negative implications when they consent to their data being collected.

Although the proposal contains a provision that **gives users a right to object to such processing**, the process in practice **seems disproportionately complex and overly burdensome** for the average consumer **to freely exercise its rights**, often requiring them to navigate complex user flows and require the use of complex online forms.<sup>16</sup> In practice, this means that consumers will **find significant, deterring barriers to the exercise of their right to object**.

---

<sup>13</sup> CNIL, 'IA : Meta entraînera ses systèmes d'IA avec les données des utilisateurs européens dès fin mai 2025', <https://www.cnil.fr/fr/meta-entrainement-ia-donnees-utilisateurs>

<sup>14</sup> Netzpolitik.org, 'Object Now or Be Silent Forever', 20 May 2025, <https://netzpolitik.org/2025/meta-ki-jetzt-widersprechen-oder-fuer-immer-schweigen/>

<sup>15</sup> eDiario.es, 'Meta pausa la inteligencia artificial que iba a entrenar con fotos y comentarios de Instagram y Facebook', 14 June 2024, [https://www.eldiario.es/tecnologia/meta-pausa-inteligencia-artificial-iba-entrenar-fotos-comentarios-instagram-facebook\\_1\\_11450417.html](https://www.eldiario.es/tecnologia/meta-pausa-inteligencia-artificial-iba-entrenar-fotos-comentarios-instagram-facebook_1_11450417.html)

<sup>16</sup> The Journal, Facebook will soon use your photos, posts and other info to train its AI. You can opt out (but it's complicated), 28 May 2024, <https://www.thejournal.ie/facebook-data-ai-6391876-May2024/>

Finally, we note that both European or national law may derogate from this rule and actually require controllers to obtain consent in a case-by case approach. This could create significant fragmentation and allow for fundamentally different approaches between Member States, with consumers being subject to different levels of protection depending on the Member State.

### Recommendation

BEUC recommends that the proposed change is **rejected**, given the problematic impact on the fundamental rights of consumers. This change could **weaken privacy protections or limit redress for unfair practices for consumers**. A thorough impact assessment considering the actual effects of the changes should be carried out.

## 4.2 Management of AI systems based on special categories of data

A new provision would also **allow for the development and operation of AI systems based on sensitive data**. To manage the risks of using sensitive data in AI systems, controllers must adopt two types of safeguards. First, remove sensitive data from the AI system as soon as possible. Second, if this is not feasible, they must make sure that sensitive data does not appear in the AI's output.

In practice, this still allows **sensitive personal data to be processed by technologies that are not yet fully understood, controlled, or reliably constrained**. AI developers would gain access to categories of data that have so far remained, at least in principle, **off limits**. Yet this sensitive data could now be used by AI systems supporting decisions with clear impact on consumers' fundamental rights (e.g. supporting decisions by insurance companies, banks, and credit institutions to define policy prices, risks, or creditworthiness).

This raises clear concerns that unfettered access to sensitive data for such operations could have negative impacts on vulnerable consumers, such as leading to **discrimination, exclusion, and unfair treatment of consumers**<sup>17</sup>.

---

<sup>17</sup> MLex, 'Instacart questioned by New York AG on algorithmic pricing', 8 January 2026, available at: <https://www.mlex.com/mlex/articles/2428120/instacart-questioned-by-new-york-ag-on-algorithmic-pricing>

## Recommendation

BEUC recommends keeping the **strict prohibition** on processing special categories of personal data **under Article 9 GDPR, without introducing a new AI-specific exception** for the processing of special categories of personal data for the development and operation of those systems.

The **use of sensitive data**, such as biometric or socio-economic information, in AI systems poses systemic risks of discrimination, misuse and irreversible harm to consumers. The existing technical safeguards and organisational measures remain **insufficient to guarantee such data is protected** once integrated into AI systems, particularly in the medium and long term.

## 5. Unjustified limits to right of access to data

The proposed changes to the GDPR would allow the data controller to refuse, or even charge for, data access requests when they unilaterally consider that such requests are **not aimed at exercising rights under the GDPR**.

For example, a consumer who finds an error in their credit profile (e.g. a loan wrongly attributed to them) may need to use their right of access to correct the mistake. If such a request is deemed outside the GDPR, the provider could refuse or decide to charge the consumer. As a result, **consumers could face higher loan rates or be denied financial services due to inaccuracies** that they cannot easily rectify or effectively challenge.

Consumers may find themselves unable to access data to investigate unfair manipulation by online platforms (e.g. personalised pricing) or wrongly attributed information. This makes it harder to spot and stop unfair or discriminatory practices.

By making **access requests more difficult or costly for consumers**, the changes could **erode consumer agency, transparency, and fair treatment**.

## Recommendation

BEUC recommends that this **proposed change is rejected**. The right of access is a stand-alone fundamental right under the EU Charter of Fundamental Rights. The right to access is a key transparency tool and a precondition for the effective exercise of other rights, including the **right to an effective remedy under Art. 47 of the Charter**.

Introducing additional limitations in a context of increasing information asymmetry between consumers and data-driven companies would significantly **weaken the practical enforceability of consumer and data protection rights**.

## 6. Data processing exceptions for SMEs

The proposed changes to Article 13 GDPR aim to reduce the administrative burden on small and medium-sized enterprises (SMEs). However, **the text is not limited to SMEs**.

**To qualify, a company must meet several conditions:** the controller-user relationship must be “clear and circumscribed”, the processing must not be “data-intensive”, and the controller must have “reasonable grounds” to assume the user already knows who is using their data, for what reasons and under which legal basis.

**However, none of these concepts are defined**, creating potential loopholes and uncertainty. Expecting small businesses – like a doctor’s office or market research firm – to interpret these criteria without legal support is unrealistic. This may increase, rather than reduce, their burden.

The exemption also **does not apply if the company shares data with third parties**, transfers data internationally, uses **automated decision-making** (including profiling), or handles **high-risk data**. Since even very small businesses rely on third-party tools like email or cloud services, the **exemption would rarely apply** in practice.

### Recommendation

The proposed exemptions for SME controllers regarding data processing **risks falling short of helping either SMEs or consumers**. Yet it introduces a significant degree of legal uncertainty and potential loopholes.

**BEUC therefore recommends rejecting the proposed changes to Art. 13 GDPR** to ensure that any simplification of the GDPR preserves the consumers' right to clear, accessible and predictable information about the processing of their personal data.

## 7. Automated individual decision-making only when necessary

The GDPR includes a general ban on certain types of automated individual decision-making (AIDM). However, the proposal adds the key verb “may”, which could suggest a general possibility for AIDM. Keeping the original wording would better preserve consumers' right not to be forcibly subject to these decisions.

On top of that, the current GDPR text **allows AIDM when the automated processing is necessary for entering into or performing a contract**. The proposal adds a sentence saying that AIDM will be allowed, **regardless** of whether the decision could be taken in another way. Using the words “necessary” and “regardless” in the same sentence can generate confusion without adding much to the provision.

Concerning the rights to contest the automated decision-making, BEUC welcomes that the provisions under Art. 22(3) GDPR remain unchanged, given its fundamental importance for consumers to obtain information and actively seek redress.<sup>18</sup>

### Recommendation

**BEUC recommends rejecting both changes to Art. 22 GDPR and revert to the original wording**. The proposal ultimately fails to add clarity to this provision and would only contribute to further legal uncertainty. The current Art. 22 GDPR is a clearer and more unambiguous provision that adequately protects the general right of the individual not to be subject to this type of decision.

---

<sup>18</sup> See BEUC Position Paper, Consumers' right to explanation under AI decision making, January 2026, available [here](#).

## 8. Single-entry point for data breaches

BEUC welcomes the proposed **introduction of a single-entry point for incident reporting obligations**, empowering the EU Cybersecurity agency ENISA to receive and share reporting under multiple legal acts. This centralisation at EU level to ensure appropriate coordination and information sharing at the European level between regulators has been consistently supported by BEUC and was a key recommendation for the Cyber Resilience Act in 2022.<sup>19</sup>

The **“report once, share many” principle** has the potential to ensure effective communication and data-sharing between EU regulators, secure information flow about security incidents and allow more effective market monitoring and enforcement.

However, we caution that **single reporting obligations should not translate into less reporting obligations: centralisation should not create a backdoor for lowering reporting requirements** or the disclosing of fewer elements than is currently required by the various regulations concerned.

### Recommendation

**BEUC welcomes the introduction of a single-entry point for incident reporting obligations.** However, we caution that single reporting should not translate into less reporting and lower protection for consumers.

## 9. New cookie rules that hardly apply to cookies

The proposal adds a new Art. 88a to the GDPR, requiring controllers to obtain **users’ consent before storing or accessing personal data. The proposal includes exceptions** such as technical needs, providing a requested service, audience measurement, or the security of communications. It also introduces a “Reject All” button for cookies that remains valid for six months once clicked.

---

<sup>19</sup> BEUC, ‘The Cyber Resilience Act proposal’, [Position paper], 23 January 2023, available at [https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-006\\_The\\_Cyber\\_Resilience\\_Act\\_Proposal.pdf](https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-006_The_Cyber_Resilience_Act_Proposal.pdf)

## 9.1 Uncertain application

However, **it is unclear if this new article will effectively apply to cookies**. The proposal introduces a narrow definition of personal data<sup>20</sup> that may exclude pseudo-anonymous data (which potentially includes cookies). If so, the consent requirement would no longer cover them. This undermines the goal of strengthening consumers' choice and is likely to result in **costly and time-consuming legal disputes between consumers and data controllers**.

In more detail, the proposed coordination between the e-Privacy and GDPR regime **risks rendering Article 88a GDPR ineffective in practice**. The main issue arises from the distinction between 'information' under the e-Privacy Directive and 'personal data' under the GDPR. The proposed GDPR's restrictive definition of personal data, which will most likely exclude pseudo-anonymous data like device identifiers and cookie values from the definition of personal data, will have negative impacts on the new Art. 88a GDPR.

Going forward, if cookies are not consistently considered personal data, and Article 88a applies only to personal data, **then its application to cookies would be limited or largely excluded**. This would be a **concerning outcome for a provision intended to strengthen consumers' freedom of choice and ensure effective privacy protection**.

Moreover, this lack of clarity is likely to result in **numerous costly and time-consuming legal disputes between consumers and data controllers** on a case-by-case basis.

## 9.2 Clearer exceptions and stronger safeguards are needed

The proposed new Art. 88a(3) GDPR contains a list of processing operations for which consent is not needed. Controllers will not have to seek consent to (a) carry out the transmission, (b) provide a service explicitly requested by the user, (c) maintain or restore the security of such service, and (d) perform audience measurement.

The scope of the exceptions mentioned above is sometimes **unclear**. The **law should provide criteria to define which data is needed for the provision of the service or for security purposes**. For the security exception, controllers should be required to carry out and be able to document a balancing test anytime a security measure is implemented.

The concept of audience measurement should also be clarified. Moreover, **additional safeguards should be put in place to avoid risk of abuse by controllers**. First, cookie values should be generic enough to avoid singling-out individual users. Second, analysis should only be possible in aggregated form. Third, there should be a clear ban to any

---

<sup>20</sup> As discussed above, see BEUC recommendation in Section 1.

further processing or transferring of the data. Finally, users should always be able to opt-out of audience measurement.

### 9.3. The case for contextualised advertising

In its recent joint opinion on the Digital Omnibus, the EDPB and the EDPS suggest that the EU legislators should **consider introducing an additional exception in Art. 88a(3) GDPR for contextualised advertising** (i.e. personalised ads based on the content or the browsing experience the consumer is currently viewing, rather than relying on their personal data or past browsing history).

BEUC **supports** the possibility of a less harmful alternative to surveillance-based advertising. Contextualised advertising distinguishes itself from surveillance-based advertising, which requires a questionable ecosystem based on the sharing and exploitation of millions of consumers data to deliver effective personalised ads. BEUC has consistently expressed that personalisation that exploits a consumer’s situational or permanent vulnerability should be prohibited.<sup>21</sup>

However, **this possibility should also be explored with caution**. Contextualised advertising is not free of possible misuse, and measures supporting it should come with **strong safeguards for users’ privacy**. For example, users’ data should be deleted immediately after the browsing session is closed (so-called session cookies could be the standard here). Moreover, any type of data collection and processing for contextualised advertising purposes should be kept within what is strictly necessary and in respect of the data minimisation principle.

#### Recommendation

The **new definition of personal data risks being ineffective** and create legal uncertainty for both consumers and controllers. **BEUC strongly recommends** avoiding this scenario by **reconsidering this change** and **reverting to the existing definition** to keep pseudonymous data fully within the scope of the GDPR.

The scope of application of **exceptions to the rule of consent are still unclear** and should be clarified. We further recommend introducing **additional safeguards to limit the risk of abuse by controllers**.

Finally, **BEUC supports the introduction of an exception for contextualised advertising**, in line the recent EDPB and EDPS joint opinion, as a clear position against intrusive forms of marketing. We further recommend considering a **ban on surveillance-based tracking**.

---

<sup>21</sup> Regarding personalised advertising, BEUC’s Norwegian member Forbrugerrådet and German member vzbv have pointed out that the massive tracking, profiling and categorisation of consumers using thousands of keywords such as “eating disorder”, “speculative investments” and “fragile senior” can be used by businesses to target individual vulnerabilities and to discriminate certain individuals, which may cause individual harm and societal risks as illustrated by the Cambridge Analytica scandal. See, BEUC, Towards the Digital Fairness Act, p. 21 (available [here](#))

## 10. Browser signals for cookie preferences

**In general terms, BEUC welcomes the introduction of browser-level privacy signals** (new Art. 88b, GDPR) that requires data controllers to allow consumers to give or withdraw consent for the use of tracking technologies (e.g. cookies) through automated tools, including their browser settings, and to respect their choices.

This could allow consumers to set their preferences at browser level, with browsers sending automatic, machine-readable signals to websites. Clear standards would also define what different types of tracking entail, giving consumers a consistent and meaningful way to express their preferences. This is an opportunity to give consumers meaningful control over what they agree to.

Still, the proposal could be improved. We lay out three specific concerns:

1. The proposed wording for the new Art. 88b(1) risks allowing a **dangerous form of automated consent** given for one type of processing to be **automatically extended to similar situations**, undermining the requirements of free, specific, and informed consent. Users should be able to reject potential tracking requests by default unless indicated otherwise by them.
2. The proposal raises **concerns about the ability of standardisation bodies** to address complex issues regarding fundamental rights (e.g. FRIAs) as it fails to establish a clear legal framework for these bodies to operate. Moreover, it is unclear why there are separate timeframes for implementation (e.g. controllers have 24 months to implement the rules, while browsers and device manufacturers are given 48 months).

In the proposed wording for Art. 88b(3), **media service providers will not have to respect refusal signals**, but the text gives **no clear justification for this exception**. Access to quality information should not require more invasive tracking mechanisms.

### Recommendation

**BEUC welcomes the new approach**, as the proposed change would allow for better, more stable consumer choice and for potentially improved control of their data.

However, the **timely adoption and descriptions of technical specifications** is necessary to clarify potential uncertainties in interpretation.

END