FEDMA
Federation of European Data and Marketing

Position Paper: Digital/Data Omnibus

Aligning cookie rules with actual risk and technological reality: operationalising Article 88a GDPR

Data-driven marketing practices cover a wide spectrum of practices, many of which entail low-risk personal data processing, are privacy-preserving, and fully embed in EU fundamental rights. Yet, the current legal framework and the omnibus legal framework are complicated, technology-specific and ambiguous. This leads to legal uncertainty and fragmented interpretation, ultimately stifling innovation and economic growth.

Today, an outdated-and poorly understood legal framework applies two legislations to the use of cookies and similar technologies, consisting of:

(i) one legislation (ePrivacy Directive) for the access to terminal equipment; and
(ii) one legislation (GDPR) for the subsequent processing of personal data.

The lack of a coherent legal framework and a clear and explicit articulation between these two practical operations have resulted in over-reliance on consent, sub-optimal protection of privacy rights and inconsistent enforcement. In addition, there is a widespread misconception that any interference with privacy necessarily entails high risk, despite the existence of sophisticated legal and technical safeguards and processing activities that are designed to be low risk from the start. This complexity and legal uncertainty disproportionately affect SMEs, which often lack the legal and technical resources to navigate fragmented interpretations and inconsistent enforcement.

Therefore, this position paper argues for a single, **coherent and risk-based legal framework under Article 88a(1) GDPR** that clearly articulates the conditions for accessing terminal equipment with the assessment of the lawfulness of subsequent processing under Article 6 GDPR. Simplification is conditional on the **repeal of Article 5(3) in the ePrivacy Directive**.

Besides, an optimal and high privacy protection standard cannot be realized by the omnibus "purpose-free" rule on access to terminal equipment followed by a purpose-based processing rule**.** Today, purpose limitation, necessity and proportionality already apply at the point of collection, and as such, treating access to terminal equipment as a separate, purpose-free event adds complexity without improving fundamental rights protection. **Instead of two-layered and complex rules, access to terminal equipment should always be "purpose-based" and therefore be seamlessly articulated with and justified by purpose-based processing**.

Furthermore, for a limited and clearly defined set of low-risk processing activities that deliver consumer benefits while preserving individuals' rights, **Article 88a(3) GDPR**, as proposed in the Digital Omnibus, **should allow reliance on appropriate GDPR legal bases without systematically requiring consent for access to terminal equipment and subsequent processing**. At the same time, all such processing must remain **fully subject to the GDPR's**

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

safeguards. This approach is particularly justified where strong safeguards apply under other legal bases, notably legitimate interest, which entails robust accountability, necessity and balancing assessments. A clearer, risk-based articulation between access to terminal equipment and GDPR lawfulness will also be particularly beneficial for SMEs.

This position paper proposes a set of non-cumulative risk indicators that establish a rebuttable presumption that a data processing activity is low risk under the GDPR (section I), some wording suggestions for the omnibus amendments (section II) and low risk data processing examples in the field of direct marketing (section III). Moreover, this position paper includes an overview table of the current legal framework, the omnibus legal framework as well as the legal framework FEDMA proposes in this position paper (annex).

I. What should be considered as low-risk personal data processing?

Below a list of non-cumulative indicators[1] that should establish a rebuttable presumption[2] that a data processing activity is low risk under the GDPR:

- No sensitive data or highly personal data that due to its nature, scope or context is likely to result in risks to the fundamental rights of natural persons as described in recitals 75 and 76 GDPR and no inference of sensitive characteristics or highly personal data[3]
- No cross-context processing, except where the processing is strictly limited to measuring the audience of an online service, as defined in Article 2(16) of Regulation (EU) 2024/1083, for the sole purpose of generating aggregated information about the usage of that online service, and where such processing is carried out by the provider of the online service itself, or by a joint controller or processor acting on its behalf and under its instruction.
- Clear and limited purposes aligning with expectations of an average user
- Strong technical and organisational safeguards, such as short retention periods
- No use of profiling for minors[4]

[1] A list of cumulative indicators could become too rigid and exclude legitimate low risk data processing activities, weakening the simplification effect and limiting cost savings for companies. It also follows the same EDPB logic as in its Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.

[2] Where a processing operation demonstrably fulfils some indicators, it should generally be presumed to fall within the scope of low-risk data processing, without prejudice to a context-specific assessment. This presumption may be rebutted where specific circumstances indicate higher risks for individuals, in which case additional safeguards or a different legal assessment may be required.

[3] This indicator is coherent with Art. 26(3) of the Digital Services Act. This provision prohibits platforms to present ads based on profiling using sensitive data as per Art. 9 GDPR, indicating that this activity does not align with fundamental rights. Besides, the concept of "highly personal data" is broader than the prohibition under Art. 26(3) of the Digital Services Act. As such, the exclusion of highly intrusive personal data and related inferences removes key risk factors identified in recitals 75 and 76 GDPR, thereby significantly reducing the likelihood and severity of impacts on fundamental rights and supporting a presumption of low-risk processing.

[4] This indicator is consistent with Art. 28(2) of the Digital Services Act which prohibits platforms from presenting ads on their interface based on profiling using personal data of minors. This prohibition indicates that the use of personal data of minors for profiling cannot be reconciled with the protection of fundamental rights.

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

- No profiling involving automated decision making that produces legal or similarly significant effects
- No reuse of user profiles for a different purpose
- No creation of persistent user profiles
- No systematic monitoring across services of users over time

How does a rebuttable presumption contribute to the European Commission simplification agenda?

Establishing a rebuttable presumption of low-risk data processing simplifies compliance and supervisory practice, reduces administrative burden and legal uncertainty for routine low-risk activities, lowers compliance costs for companies, and allows both controllers and DPAs to focus resources on genuinely high-risk data processing to preserve high standards of fundamental rights protection.

II. Wording suggestions

Three types of wording suggestions were considered:

Option A:

- Insert a new Article 88a(3)(e) containing a closed and carefully drafted list of low-risk data processing activities (e.g., contextual advertising, ad fraud prevention, brand safety, frequency capping).
- Add risk indicators and a rebuttable presumption of low risk in a new recital 76a, after the recitals on the risk-assessment framework (recitals 75, 76).
- Amend recital 76 to clarify that a risk assessment may conclude that risks to rights and freedoms are high, medium, or low.

Option B: only amend Article 88a(3) to include risk indicators and a rebuttable presumption that data processing including some of those indicators are low risk, without listing any specific activities in the text (provisions or recitals).

Option C:

This amendment would also benefit of the incentivisation of effective age assurance tools. Age assurance and verification tools are sometimes criticised due to concerns about effectiveness, proportionality and impacts on young people's freedom online. However, where age verification systems are developed in line with high technical standards, supported by competent public authorities, and combined with effective enforcement, they can serve as an important safeguard to prevent the profiling of minors. Such systems may therefore contribute to a differentiated, risk-based approach, particularly where they enable providers to reliably exclude minors from data processing activities that would otherwise raise heightened risks under the GDPR.
In some Member States, national authorities have assessed age verification systems against detailed criteria and allowed their use in regulated contexts, illustrating that public interest-oriented standards can provide legal certainty while enhancing the protection of minors. See one example here.

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

- Clarify in Article 88a(1) GDPR the conditions under which access to terminal equipment may take place, while explicitly clarifying the lawfulness of subsequent processing which continues to be assessed under Article 6 GDPR.
- Insert option B: amend Article 88a(3) to include risk indicators and a rebuttable presumption that data processing including some of those indicators are low risk without listing any specific activities.
- Add a new recital 40a that: (i) provides a non-exhaustive list of examples of processing likely to be low risk (as in option A), and (ii) states key guiding principles:
  (a) the purpose of personal data processing is central to determining the appropriate safeguards and conditions;
  (b) the GDPR is technology-neutral (rules apply regardless of the technical means used);
  (c) where processing is presumed low risk under Article 88a(3)(e), reliance on legitimate interests is generally available subject to the usual safeguards.

After due consideration, FEDMA supports option C because it fits best to the approach that the legal assessment should be driven primarily by the purposes of personal data processing activities and their level of risk. This option is the most flexible and sustainable one, because the operative provision is not sector or activity specific. Furthermore, it refers to legal bases that guarantee strong company accountability and fundamental rights safeguards and clarifies how the legal basis for processing under Article 6 GDPR interacts with the rules on access to terminal equipment under Article 88a. Besides, it leaves enough room for interpretation by anchoring key guiding principles, limiting legal uncertainty.

While option A, by anchoring the "low risk" concept directly in recital 76, avoids its misreading, namely that "high risk" is the default, it could also lead to future pressure to expand the list of activities in Article 88a(3). This will ultimately lead to revisions of the GDPR provisions as practices and technologies evolve, together with the risks to fundamental rights.

Option B follows the GDPR logic (just as option C), and the absence of sectoral exemptions avoids political discussions, but the lack of interpretative guidance, particularly on the interaction with Article 6 GDPR also leaves a lot of room for interpretations, potentially leading to divergent interpretations and legal uncertainty.

Below option C. The wording suggestions for options A and B are available upon request.

FEDMA's wording suggestion

Key:
- In **bold** is added text
- In ~~strike through~~ is text to be deleted

Recital 40a: This Regulation is based on a technology-neutral, risk-based and purpose-oriented approach to the processing of personal data. The lawfulness of processing depends on the pursuit of a specific and legitimate purpose and on the assessment of risks to the rights and freedoms of natural persons, taking into account the

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

nature, scope, context and purposes of the processing. Where processing of personal data in the terminal equipment of natural persons takes place, and some indicators suggest that the likelihood and severity of risks to the rights and freedoms of natural persons are limited, other legal bases than consent, as per Article 6 of this Regulation, can be considered appropriate. For instance, where processing is strictly limited to the measurement of a service explicitly requested by the data subject, such processing will, in principle, be likely to result in low risks for individuals. Furthermore, processing activities necessary for carrying out the transmission of an electronic communication over an electronic communications network, for providing a service explicitly requested by the data subject, or for maintaining or restoring the security, integrity or availability of such a service or the terminal equipment used for its provision, such processing will, in principle, be likely to result in low risks for individuals. Similarly, contextual advertising, frequency capping aimed at preventing excessive user exposure to the same advertisement, ad fraud detection, ad measurement, brand safety measures preventing the placement of advertisements alongside illegal or harmful content may be considered as pursuing legitimate purposes and, where appropriately safeguarded, are in principle, likely to result in low risks for individuals.

Article 88a(1): Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person is only allowed when that person has given his or her consent, in accordance with this Regulation~~.~~ **unless otherwise permitted under paragraphs 2 and 3 of this article and without prejudice to Article 6 of this Regulation.**

Article 88a(3): Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person without consent, and subsequent processing, **and where the processing relies on a legal basis under Article 6 of this Regulation other than consent,** shall be ~~lawful to the extent it is necessary for any of the following:~~ **presumed to be likely to result in low risks to the rights and freedoms of natural persons where one or more of the following indicators are demonstrated:**

~~(a) carrying out the transmission of an electronic communication over an electronic communications network;~~

~~(b)providing a service explicitly requested by the data subject;~~

~~(c)creating aggregated information about the usage of an online service to measure the audience of such a service, where it is carried out by the controller of that online service solely for its own use;~~

~~(d)maintaining or restoring the security of a service provided by the controller and requested by the data subject or the terminal equipment used for the provision of such service.~~

a) **The processing does not involve special categories of personal data within the meaning of Article 9 of this Regulation nor highly personal data that due to its nature, scope or context is likely to result in risks to the fundamental rights of natural**

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

persons and does not enable inference of sensitive characteristics or highly personal data;

b) **The processing does not involve cross-context processing, except where the processing is strictly limited to measuring the audience of an online service, as defined in Article 2(16) of Regulation (EU) 2024/1083, for the sole purpose of generating aggregated information about the usage of that online service, and where such processing is carried out by the provider of the online service itself, or by a joint controller or processor acting on its behalf and under its instruction;**

c) **The purposes of the processing are specific and limited and align with the reasonable expectations of the data subject in the given context;**

d) **Effective technical and organisational measures are implemented to minimise risks, including, where appropriate, short retention periods;**

e) **The processing does not involve profiling of minors;**

f) **The processing does not involve profiling or automated decision-making producing legal effects concerning the data subject or similarly significantly affecting them within the meaning of Article 22 of this Regulation;**

g) **User-level data or profiles are not reused for purposes that are incompatible with the original purpose of collection;**

h) **The processing does not result in the creation or maintenance of persistent user profiles over time;**

i) **The processing does not involve systematic monitoring of data subjects across services over extended periods.**

Art. 88(3a): The presumption of low risk established under paragraph 3 may be rebutted where, in light of the specific circumstances of the processing, it is likely to result in higher risks to the rights and freedoms of natural persons.

III. Illustrative examples

a. Frequency capping to avoid user over-exposer to ads

Why frequency capping benefits users/consumers?

Frequency capping enhances user experience by preventing excessive ad repetition without relying on tracking, profiling, or behavioural monitoring. It can therefore also protect consumers from annoyance, pressure, and cumulative negative effects, while reducing rather than increasing risks to their rights and freedoms.

Technical description: a small, first-party cookie associated with a specific service or website is placed on the user's terminal equipment. The cookie contains only a campaign-specific counter, indicating how many times a specific advertisement has been shown.

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

The data stored are limited to:

(i) a campaign identifier
(ii) a numerical counter
Concretely: “ad X seen Y times”.

The cookie does not contain and cannot be used to infer data relating to the user’s identity, browsing history, interests, preferences, or behaviour across websites or applications, and it is not reusable for other advertising or analytics purposes.

The data is processed exclusively to limit ad repetition within a short timeframe and is automatically deleted once that purpose is fulfilled.

Why it is low risk

- Purpose is limited to ad delivery optimisation
- No inference of interests or preferences
- No significant impact on users’ rights
- No behavioural targeting, persistent profiles, cross-service tracking
- It benefits the user by improving his/her online experience

Key safeguards

- Short retention periods
- No possible reuse for other purposes
- No enrichment or reuse of data

b. Fraud and invalid traffic detection for advertising integrity

Recital 47 GDPR explicitly recognises that the processing of personal data for fraud prevention constitutes a legitimate interest of the data controller. Besides, the EDPB Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR further clarify the recital (paragraphs 100-108). Article 88a(3) GDPR should be building on the existing recognition that fraud prevention constitutes a legitimate interest so as to avoid conflicting with recital 47 GDPR.

Why fraud and invalid traffic detection benefit users/consumers?
Fraud and invalid traffic detection protects users from abusive or deceptive online practices and supports the integrity and reliability of digital services. At the same time, by ensuring that advertising financed by companies is effectively delivered to human users rather than automated traffic, these measures also help avoid waste of resources and support more accurate and accountable advertising outcomes, without increasing data collection or user exposure.

Technical description: when an advertisement is requested for delivery on a website, limited technical signals[5] are processed in real time to assess whether the interaction is likely to originate from a human user or from automated or fraudulent activity. Where necessary, a

[5] Non-content, non-behavioural indicators that relate to the technical characteristics of an interaction (such as abnormal request patterns or automation indicators), and do not involve observation of user behaviour over time or across services.

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

short-lived, first-party technical cookie may be used to distinguish legitimate traffic from invalid traffic within the same service or session.

The data stored are limited to a technical assessment outcome (concretely: "human" or "bot"). This processing does not involve data relating to the user's identity, browsing history, interests, preferences, or behaviour across websites or applications.

Data are retained for very short periods, typically limited to the duration strictly necessary to detect and mitigate fraudulent activity, and are automatically deleted once that purpose is fulfilled.

This processing is functionally and organisationally separated from advertising delivery, analytics, or targeting processes.

Why this is low risk

- Legitimate purpose linked to security and system integrity
- No commercial or behavioural exploitation of user data
- Strong alignment with reasonable user expectations
- No behavioural advertising, interest inference, profiling for commercial purposes

Key safeguards

- Use of technical signals
- No reuse for marketing or targeting purposes

c. Ad measurement techniques to assess reach, delivery, and effectiveness

Why ad measurement benefits users/consumers?

Privacy-preserving ad measurement allows transparency and accountability in digital advertising by assessing campaign performance at an aggregated level, without tracking or profiling individuals. It avoids unnecessary data collection while ensuring that advertising resources support genuine user interactions rather than ineffective delivery.

Technical description: when an advertisement interacted with (for example, by clicking on it or completing a purchase), a measurement signal[6] is generated to record that the event occurred. Where access to the user's terminal equipment is necessary, a short-lived, first-party event counter may be used solely to enable aggregation. The measurement process is designed so that individual level data are not retained or exploited, and results are produced exclusively in aggregated or anonymised form.

Depending on the processes, the data processed may include:

(i) an event indicator
(ii) a campaign identifier
(iii) a short-lived counter enabling aggregation

[6] Recording that an ad was clicked or viewed, so totals can be counted across a campaign, without identifying or tracking people.

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

Concretely: “Ad X was clicked on Y times”

This processing does not involve data relating to the user’s identity, browsing history, interests, preferences, or behaviour across websites or applications. The processed data does also not allow for profiling.

Raw event-level data are retained only for a very short period, strictly necessary to generate aggregated metrics and the aggregated data in the report does not contain personal data.

Why this is low risk

- Focuses on aggregate outcomes, not individual behaviour
- No decision-making affecting individual users
- No individual level behavioural profiling, targeting decisions based on personal behaviour

Key safeguards

- Aggregation and/or privacy enhancing technologies
- Short retention periods
- Strict purpose limitation

d. Context-based assessment to avoid placing ads next to harmful or inappropriate content

Why brand safety measures benefit users/consumers?
Context-based brand safety measures help protect users from being exposed to inappropriate, harmful, or misleading advertising by ensuring that ads are shown only in suitable content environments.

Technical description: before or at the moment an advertisement is displayed, the content of a webpage (such as text, metadata, page category, or content labels) is analysed to determine whether it is suitable for advertising placement.

Where necessary to enable this assessment, a short-lived, first-party contextual indicator may be processed at page level. This processing is limited to the content environment and does not involve observing or recognising the user.

Depending on the processes, the data processed may include:

(i) a content category (e.g. “adult content”)
(ii) a simple label that shows whether the page is suitable for ads (e.g. “brand safe” or “not brand safe”)
(iii) a temporary, technical “yes” or “no” signal attached to a page or viewing session used only to decide whether an ad may be shown in that content environment

This processing does not involve data relating to the user’s identity, device, browsing history, interests, preferences, or behaviour across websites or applications. The processed data does also not allow for profiling or behavioural monitoring of users.

Any data is deleted once the add placement decision was made.

Why this is low risk

- Targets webpage content, not users
- No processing of behavioural data
- Clear and transparent purpose
- No tracking, profiling, behavioural monitoring

Key safeguards

- Context-based classification
- No user identification
- No retention of user-level data

e. Contextual advertising based on page content (rather than on the user's past behaviour or interests over time)

Why contextual advertising benefits users/consumers?
Contextual advertising ensures that ads shown to users are relevant to the content they are viewing which avoids the creation of user profiles and prevents cross-context data use, while still supporting a coherent and non-intrusive advertising experience.

Technical description: when a user loads a webpage or opens an app, the content environment (such as the article text, headline) is analysed in real time to determine which ads are relevant to that context.

Where access to the user's terminal equipment is technically necessary, this may involve reading a short-lived, first-party contextual flag or page-level indicator, linked only to the current page view or session and not to the user.

Depending on the processes, the data processed may include:

(i) a content category or keyword (e.g. "travel", "sports", "news")
(ii) page-level or session-level contextual flag (e.g. "topic = travel")
(iii) a short-term tag used only while the page is open, to decide which ads can be shown on that page (e.g. if the page is about sports → show sports-related ads; if the page contains news about a tragedy → do not show commercial ads)

This processing does not involve data relating to the user's identity, browsing history, interests, preferences, or behaviour across websites or applications. The processed data does also not allow for profiling.

The data exists only for the duration of the page view or session and is deleted once the ad placement decision is made.

Why this is low risk

- Ads target content, not individuals
- No tracking of user behaviour across services or over time

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

- No profiling or behavioural surveillance
- No cross-context tracking, persistent user profiling, behavioural targeting

Key safeguards

- Real-time or short-term processing
- No storage of user-level interaction history
- Clear separation from behavioural advertising systems

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

FEDMA
Federation of European Data and Marketing

Annex 1: overview table on legal frameworks for cookie consent

Table key:
- : brief description of the rules
▲: articulation between rules on access to terminal equipment and the rules on subsequent processing
■ : role of other legal bases than consent under the GDPR

Type of rule	Today's legal framework	The legal framework in the omnibus proposal	FEDMA's position
Access to terminal equipment	Article 5(3) ePrivacy Directive: - consent per default ▲the access rule does not provide for a legal basis for processing	Article 5(3) ePrivacy Directive and Article 88a GDPR: - consent per default - limited non-consent-based access, depending on practices ▲ ambiguous interpretation possible because Article 88a can be read as implicitly legitimising processing	Article 88a GDPR: - consent per default - non-consent-based access if processing is low risk to the fundamental rights of the user ▲ explicitly clarified that the access rule **does not** provide for a legal basis for processing which continues to be regulated under Article 6 GDPR
Subsequent processing	Article 6 GDPR: - consent is asked once more for processing ■ the other legal bases than consent are available, in theory, but often sidelined	Article 6 GDPR, however the articulation with Article 88a is not explicit: - implicit whether consent should be asked once more for processing ■ availability of other legal bases is uncertain	Article 6 GDPR, the subsequent processing is articulated with the access rule: - any legal basis under Article 6 GDPR ■ explicit availability of other legal bases than consent if access is permitted and risks are low
Level of privacy and fundamental rights protection	High but rigid, outdated and stifling innovation and economic growth	Intended to be high but the ambiguity will have the effect of weakening protection	High and structured because there is a consent rule for intrusive access while upholding strong business accountability and

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

			privacy safeguards for all processing activities
Enforcement	Fragmented across Member States	Inconsistent interpretation by DPAs is likely	Improved legal certainty and simplicity leading to more consistent enforcement. Further support could consist of sector-developed guidance on typical processing purposes and safeguards, developed in line with Articles 40 and 41 GDPR and subject to appropriate regulatory oversight. Such guidance could assist in the practical application of Article 88a in articulation with Article 6 GDPR, which is particularly helpful for SMEs.

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org