FEDMA
Federation of European Data and Marketing

Position Paper
Digital & AI Omnibus Proposal

Executive summary

The EU faces an **existential competitiveness crisis** without swift or structural reforms. To reverse this trend, a new regulatory approach is needed. The aim should be for EU regulations to **support digital innovation, economic growth and competitiveness**, rather than focusing solely on restricting how data can be used, thereby slowing data and AI driven innovation, further impacting the ability of European companies to grow and compete globally. **The EU should focus on maintaining adequate levels of data protection while stimulating EU economic growth.**

Although FEDMA welcomes the omnibus initiative as a first step, at an overarching level, there is a risk that the Commission's approach to simplification may not fully seize this opportunity. Genuine regulatory simplification should not only be about easing the burden on companies' compliance departments but also be intended to meaningfully improve the conditions for enhanced competitiveness and increased growth related to digital legislation. As for this, FEDMA is presenting further suggestions such as concrete amendments.

With this said **FEDMA welcomes the European Commission's efforts to simplify the digital acquis and the AI Act**, particularly for SMEs and small mid-cap companies. The omnibus ease barriers to innovation and growth, while maintaining an appropriate level of personal data protection initiative aims to simplify legislation in order to reduce compliance costs and. To achieve this, the EU should drift away from a "tick-the-box" compliance culture and steer towards a more competitive and innovative-friendly regulatory approach. Realistic implementation timelines, clear guidance prior to enforcement and improved coordination between supervisory authorities will be key. **While many of the proposed amendments support the objective, others would benefit from improvements. To better achieve the omnibus' objective, FEDMA proposes:**

- Rebalancing more fairly the existing regulatory framework between protecting personal data and stimulating economic growth to more closely align with recital 4 GDPR
- Addressing cookie fatigue by maintaining a technically feasible and a more risk-based version of Art. 88a in the GDPR and repealing Art. 5(3) ePrivacy Directive.
- Avoiding relying on a single, centralised mechanism for automated, machine-readable user-choice signals and rather support a market-driven approach and the coexistence of various competing technological solutions developed independently or in collaboration with browser providers, which foster innovation and EU economic growth.
- Ensuring legal certainty through tech-neutral and simple identifiability criteria in the GDPR definition of personal data to support innovation.

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

- Strengthening global competitiveness through ethical AI development and streamlined GDPR, AI and cybersecurity rules.
- Readjusting the balance to protect businesses from abusive GDPR exploitation (i.e. abusive DSARs) while safeguarding legitimate compensation rights.
- Upholding strong accountability through ROPA obligations to guarantee sustainable growth in data-driven marketing.

The beneficial impacts of the above-mentioned proposals will extend beyond the data-driven marketing sector. Personalised digital advertising plays a unique role in the EU economy: 76% of SMEs report that it helps them compete with larger firms and 86% attributing their recent revenue growth directly to its use.[1] Ensuring that regulatory frameworks remain workable and oriented towards economic growth is essential to safeguarding the competitiveness of Europe's economy and the smaller companies that depend on personalised advertising to innovate and create value across the European Single Market.

More broadly, the digital economy creates unique conditions that allow small and medium-sized enterprises to compete with much larger market players. Through digital tools and data-driven solutions, SMEs can achieve meaningful market reach and performance without the scale of infrastructure, capital, or resources traditionally required. This helps level the playing field, strengthens competition, and supports a more balanced and resilient economic model, one that avoids excessive market concentration and can become a distinctive strength of the European economy in an increasingly centralised global landscape.

[1] Centre for Information Policy Leadership, 'The Impact of Digital Advertising on Europe's Competitiveness: a study on the role of digital advertising in Europe', March 2025, p.9 (weblink).

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

Overview of positions

Proposed amendments	FEDMA's position
GDPR	
Definition of 'personal data' Art. 4(1) GDPR and Art. 41a 'amended' GDPR (page 8)	**Support and require modifications** **Support and require modifications**
New definitions Arts. 4(32-38) GDPR (page 11)	**Full support**
Purpose limitation principle Art. 5(1)(b) GDPR (page 11)	**Full support**
Processing of special categories of personal data Art. 9 GDPR (page 11)	**Support and require modifications**
Abusive data subject requests Art. 12(5) GDPR (page 13)	**Support and require modifications**
Records of processing activities Art. 30(5) GDPR (page 15)	**Reject**
Notifications of personal breaches Art. 33(1) GDPR (page 13)	**Support and require modifications**
Processing of personal data in the terminal equipment Art. 88a 'amended' GDPR (page 6)	Mixed **Overall support and require modifications** **Reject §4**
Automated and machine-readable indications Art. 88b 'amended' GDPR (page 7)	**Reject**
Processing for the development & operation of AI Art. 88c GDPR (page 11)	**Support and require modifications**
ePrivacy Directive	
Confidentiality of communications Art. 5(3) ePrivacy Directive (page 6)	**Reject**
AI Act	
AI literacy Art. 4 'amended' AI Act (page 12)	**Support and require modifications**
Bias detection and mitigation Art. 4a 'amended' AI Act (page 12)	**Full support**

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

Rebalancing more fairly the existing regulatory framework between protecting personal data and stimulating economic growth to more closely align with recital 4 GDPR

Although we recognize that it would be only one of many factors that need to be addressed to resolve the EU's competitiveness challenges, **a balanced regulatory framework for the use of data in marketing, innovation and business development, is crucial to achieving the goals of enhanced competitiveness and increased growth**. It also requires a new approach: a high threshold for whether new legislation is needed at all, principles-based rules rather than detailed regulation, and impact assessments that rigorously examine how proposals and existing legal frameworks affect innovation and the enterprises of the future.

Beyond reviewing legislation itself, **we must also assess how key digital laws have been implemented, particularly their practical impact on competitiveness, which is often overlooked**. Although the principles of the GDPR were designed to strike an acceptable balance between businesses' legitimate need to process data and the crucial need to protect sensitive data,[2] an inherent imbalance in its application has existed from the outset – one that has increasingly led to competitiveness issues over time. A key part of this imbalance lies in the role assigned to the European Data Protection Board (EDPB) and the fact that its guidelines, in effect, have no counterpart that takes its starting point in interpreting the GDPR through the lens of European competitiveness.

It is also worth noting that **any changes to the GDPR itself risk being ineffective should the EDPB continue in its line of expansive interpretations and restrictive-to-European-growth guidelines.** The core issue is also how the legal text itself is applied in practice. FEDMA calls on the EU to foster a more balanced regulatory approach, one that protects personal data while also enabling economic growth, in line with the spirit of Recital 4 of the GDPR. To ensure that competitiveness plays a much greater role in the interpretations, including the legitimate data needs of European businesses, we are suggesting amendments to the GDPR in either an article or a recital to rebalance the GDPR.

Sustained EU economic growth is essential to guarantee that fundamental rights can be meaningfully exercised. Economic dependency creates a vulnerability whereby citizens are compelled to compromise on their rights. A stagnating economy risks creating a citizenry forced to prioritize immediate economic survival over the protection of their personal data.

1. Proposed amendment to article 1 (add new paragraph 1a) GDPR

In protecting natural persons with regard to the processing of personal data, **the GDPR shall also ensure conditions for the competitiveness of the European economy and the freedom to conduct a business, in particular by supporting proportionate, risk-based and technology-neutral rules that enable lawful data use across the internal market.** The interpretation and application of the GDPR shall respect the principles of proportionality and legal certainty and

[2] Recital 4 GDPR.

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

shall not unduly restrict legitimate commercial activities where adequate safeguards for individuals are in place.

Building on this, procedural rules should clearly require supervisory authorities and the EDPB to demonstrate how their decisions, guidelines and recommendations uphold these principles in practice. Rather than relying solely on broad and high-level obligations, regulators could be **mandated to explicitly assess and explain proportionality, legal certainty and economic impact of their initiatives.** Providing this clarity would not only support a predictable regulatory environment but also help ensure that guidance does **not** inadvertently restrict legitimate economic activity or the freedom to conduct a business. Embedding such expectations into procedural frameworks would strengthen cooperation between regulators and industry while maintaining strong protections for natural persons.

2. A proposed new recital to GDPR

In pursuing the EU's objectives for a well-functioning internal market and sustainable competitiveness, **the GDPR shall be applied in a manner that safeguards the rights to privacy and protection of personal data of natural persons** (Articles 7 and 8 of the Charter of fundamental rights of the EU) **while equally respecting other freedoms such as the freedom to conduct a business and the freedom to provide and receive services within the Union** (Art. 16 of the Charter of fundamental rights of the EU; Art. 114 of the Treaty on the Functioning of the EU). The rules herein are risk-based and proportionate, and should not unduly impede data-driven innovation, legitimate commercial communications, or the scaling of European enterprises. Where several lawful bases are available, consent is not a default requirement for processing personal data; it is required only where expressly stated. Controllers and supervisory authorities shall interpret and apply the GDPR so as to strike a fair balance between these fundamental interests, avoiding unnecessary burdens that fragment the internal market.

3. A practice-oriented tool operated by the European Commission replacing growth inhibiting EDPB guidelines by a more accessible, pragmatic and stable tool for SMEs

Other concrete measures to achieve better application of the legislation could include **avoiding the growth-limiting impact of the EDPB's mandate on SMEs by establishing a growth-stimulating, pragmatic and reliable tool for SMEs.** For instance, AI could be used by the European Commission to disseminate legislation and soft law at a lower operational cost. The objective of such a tool would be to create a more easily accessible and stable regulatory framework that support SMEs bridging the gap between the regulatory framework and their business idea.

Besides, other options could *inter alia* include **new mechanisms such as a European Commission AI-tool giving legally binding answers on how data may be used for innovation and replacing growth inhibiting guidelines from the EDPB which are effectively inaccessible unless a company has an in-house legal department.** For someone seeking to turn a business idea into reality, for start-ups or SMEs that is not an option. The Digital Omnibus is an opportunity for the European Commission to show it can follow the ethical AI development trend it contributed to launch and become more accessible to SMEs.

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

A modern and simplified EU consent framework (incl. GDPR and ePrivacy) to effectively solve cookie fatigue, empower SMEs and drive European economic growth

4. Targeted amendments under Art. 88a 'amended' GDPR, Art. 5(3) ePrivacy Directive

FEDMA welcomes the amendments that mirror Art. 5(3) ePrivacy Directive into the new Art. 88a 'amended' GDPR and we are confident that this could help addressing the widespread cookie fatigue experienced by users, provided that more amendments are introduced. For instance, this amendment requires a reassessment of Art. 5(3) ePrivacy Directive itself. **Given the GDPR's clarified relative approach to personal data,[3] the amendment categorises a large part of cookies as non-personal data for individual controllers or processors.** Maintaining a parallel consent regime under Art. 5(3) ePrivacy Directive would therefore create unnecessary duplication and perpetuate cookie fatigue.

More broadly, **EU digital legislation should regulate the risks arising from processing activities** rather than the source of the data or the specific technologies involved. Many cookies that do not involve personal data and are not widely used for tracking purposes entail minimal risks and therefore do not justify a parallel consent regime. Importantly, the risks associated with tracking arise from the processing of personal data and not from the mere use of cookies, and these risks are comprehensively regulated under the GDPR (e.g. strict requirements on profiling and behavioural advertising).

Taking into account the above mentioned, we propose to repeal Art. 5(3) ePrivacy Directive to eliminate cookie fatigue all the while preserving high standards of data protection, particularly because unauthorized access to devices remains strictly prohibited under existing legislation.[4] Article 5(3) of the ePrivacy Directive was initially and intentionally framed broadly to cover all data accessed on a user's device, based on the assumption that any such access poses a privacy risk because the involved data could include personal data, but this assumption is not accurate anymore. **If concerns around cookies and similar technologies are primarily addressed through the GDPR, which governs the processing of personal data, there appears to be little justification for maintaining such a broad, burdening and overly precautionary rule in the ePrivacy Directive.** The necessary safeguards are already provided by the GDPR framework, rendering Art. 5(3) ePrivacy Directive redundant.

FEDMA is also concerned that Art. 88a 'amended' GDPR will lead to a technology-dependent and tightly regulated "island" in the GDPR. While processing of personal data currently benefits of several legal bases (e.g., consent, legitimate interest, contractual basis), Art. 88a introduces an unworkable consent-only rule for device-level processing, denying operational realities and innovative trends. The differences between data originating from various technical

[3] Case C-413/23 P SRB (weblink).
[4] Art. 3 of Directive 2013/40 of the European Parliament and of the Council on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. The transposition deadline was in September 2015 (see Art. 16 of the same Directive).

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

sources are disappearing, and it is nonsensical to tailor rules based on those differences. For instance, future user interactions will be increasingly automated through AI-enabled devices (e.g. AI agents). **The GDPR should therefore remain tech-neutral and become more risk-based in order to strike a fairer balance between the rights of data subjects and the freedom to conduct business, in line with recital 4 GDPR.**

Beyond the conceptual concerns, Art. 88a 'amended GDPR also risks creating unintended operational constraints. It remains important that when device-level processing involves personal data which is identifiable, Art. 88a 'amended' GDPR does not unintentionally and unjustifiably narrow legitimate low-risk customer-service analytics. **As such, the distinction between low-risk and high-risk analytics (as well as anything in between, as such acknowledging that data processing occurs on a spectrum of risks) should be clearly articulated in the GDPR recitals.** Without such clarity, everyday legitimate low-risk customer analytics could become unduly overly limited, especially because of the increasingly broad and tech-specific interpretation of 'cookies' by supervisory authorities.[5]

Furthermore, we welcome the amendment in Art. 88a(3) 'amended' GDPR which allows controllers to access, without consent, personal data already stored on terminal equipment to generate aggregated audience-measurement information for their own online services. This amendment increases legal certainty and **contributes to economic growth in the EU because it allows companies to gain insights in the performance of their marketing activities.** However, in this context, it should be noted that fewer cookie banners will only materialise where organisations are able to rely on consent-free measurement and advertising routes. Given that most websites still operate standard third-party marketing stacks, consent banners are likely to remain unavoidable for a large part of the market.

FEDMA does not welcome Art. 88a(4) 'amended' GDPR as the amendments on managing consent requests are technically challenging, and risk undermining the reliability of consent, the latter being a cornerstone of data-driven marketing activities. Restrictions on repeatedly requesting consent, while strengthening user control and transparency, may affect the ability of marketers to re-engage audiences. The provision prohibiting new consent requests for as long as the controller can lawfully rely on existing consent is technically unfeasible and is not anchoring into existing GDPR rules, creating legal uncertainty. This prohibition therefore needs to **be replaced by a reference to Arts. 4(11), 6 and 7 GDPR which enshrine the grounds for processing and consent rules, thereby avoiding technical issues and legal uncertainty all the while guaranteeing high data protection standards.** Besides, the six months prohibition on re-requesting consent after a refusal requires additional data storage and leads to technical issues. **We therefore propose deleting this prohibition.**

5. Targeted amendments under Art. 88b 'amended' GDPR

[5] EDPB Guidelines 2/2023 on the technical scope of Art. 5(3) of the ePrivacy Directive, adopted on the 7th of October 2024 (weblink).

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

Consent enables transparency, user trust and autonomy and ethical data use in the data-driven marketing sector and should therefore remain a core concept in the GDPR. To preserve a competitive and innovation-friendly environment for consent management, and catering to the needs of a wide range of different users, **FEDMA does not welcome Art.88b 'amended' GDPR** aiming at establishing automated and machine-readable indications of data subject's choices (e.g. browser-based consent) and urges the deletion of this amendment for several reasons:

- There is a widespread concern that relying on a single, centralised mechanism for automated consent signals would create a ***de facto* monopoly for some dominant tech providers, limiting the ability of a wide ecosystem of European businesses to build direct and trusted relationships with the end users.** Such a model would unduly negatively affect data-driven marketing companies, particularly SMEs. Such unintended consequences can only be prevented by the deletion of Art. 88b 'amended' GDPR.

- Furthermore, entrusting a small number of global technology intermediaries with the technical implementation of user-choice signals presents a strategic risk to European digital sovereignty. Current market data reveals that **over 90% of the browser market in Europe is controlled by non-EU entities**, primarily headquartered in the United States (e.g., Google Chrome, Apple Safari, Microsoft Edge)[6]. Mandating privacy controls through these platforms would effectively **outsource the guardianship of European fundamental rights to non-European jurisdictions**. This creates a paradox where the enforcement of EU data protection standards becomes dependent on technical protocols defined outside of the EU, potentially conflicting with the EU's goal of strategic autonomy and raising complex issues regarding international data transfers and extraterritorial jurisdiction.

- To build on the abovementioned, a market-driven solution would allow a **diversity of solutions**, **catering to a variety of users' expectations and needs, and the competition could raise qualitative outcomes, raising the levels of user satisfaction as well as data protection sector standards**. The sector's longstanding experience shows that users value different types of personalisation depending on context, brand, and purpose. A one-size-fits-all mechanism cannot capture this diversity of expectations and needs.

Instead of relying on a single, centralised mechanism for automated, machine-readable user-choice signals, FEDMA would support a **balanced, market-driven and multi-technical-solution developed by standalone companies or in collaboration with browser providers and taking account of the diversity of users' needs and expectations.**

Legal certainty through tech-neutral and simple identifiability criteria are key to innovation and EU economic growth

6. Targeted amendments under Art. 4(1) GDPR and 41a 'amended' GDPR

[6] The aggregate market share of US-based providers (Chrome, Safari, Edge, Firefox) consistently exceeds 90% of the European market. See, for 2025 https://gs.statcounter.com/browser-market-share/all/worldwide/2025, and, for 2024 https://gs.statcounter.com/browser-market-share/all/worldwide/2024.

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

We welcome the streamlining of the definition of personal data in line with the recent SRB ruling[7] (C-413/23 P), which codifies the relative approach to identifiability and thereby enhances legal certainty across the EU. This legislative development will allow for better results when training AI, which will boost innovation in the EU economy. Besides, the amendment creates space for the adoption of Privacy Enhancing Technologies (PETs)[8], such as pseudonymisation, benefitting companies and consumers alike. PETs operationalise core GDPR data protection principles (such as data minimisation and privacy-by-design) in business systems, thereby strengthening regulatory resilience, and embed safeguards into the way data is collected, used and stored. As highlighted by the OECD[9], PETs have proven successful in safeguarding privacy and personal data protection by enabling data utility while protecting confidentiality and trust in processing. In line with the OECD recommendations, policy makers and privacy enforcement authorities will increasingly need to consider how the use of PETs impacts regulatory assessments under privacy and data protection frameworks, recognising their contribution to privacy-protective outcomes.[10] A good example is Singapore's IMDA PETs Adoption Guide providing clear, practical and tech-neutral guidance to accelerate PET uptake.[11] **By embedding PETs into the Digital Omnibus, the European Commission not only reinforces trust but also unlocks innovation potential, ensuring that privacy and (international) competitiveness advance hand in hand.**

To strengthen the amendment in Art. 4(1) GDPR, we call for recital 26 GDPR to be aligned not only with the recent SRB ruling, but above all with the tech-neutral character of the GDPR. A tech-neutral GDPR is essential to foster innovation, growth and competition in the EU, because rigid technological prescriptions risk stifling innovation and burdening companies with outdated compliance models. For instance, recital 26 GDPR refers to the 'singling out' technique, which nowadays does not necessarily lead to identifiability when state-of-the art solutions are used. Yet, the 'singling out' technique remains a key method to underpin many legitimate processes that feed European economic growth. By remaining technology-neutral, the GDPR also becomes future-proof against evolving technology and guarantees consistent legal application, allowing businesses to carry innovation through to market, benefitting the society as a whole and guaranteeing a competitive spot in international markets. More concretely, we suggest deleting the following struck through words in recital 26: 'To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used~~, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly~~'. **Ensuring recital 26 reflects both legal certainty and technological neutrality will**

[7] Case C-413/23 P SRB (weblink)
[8] Privacy Enhancing Technologies are an umbrella term to designate multiple tools used to improve security, maintain user privacy, through an additional layer of protection, for instance, by minimising the amount of data processed by third parties.
[9] OECD report Emerging Privacy Enhancing Technologies: Current Regulatory and Policy Approaches, March 2023, pp. 4–5, 8–9 (weblink).
[10] OECD report Emerging Privacy Enhancing Technologies: Current Regulatory and Policy Approaches, p. 39.
[11] Infocomm Media Development Authority, 'Privacy Enhancing Technologies adoption guide', 2026 (weblink).

safeguard data subject rights while enabling the deployment of increasingly advanced technologies and practices that drive Europe's digital competitiveness.

In addition, we welcome the mandate in Art. 41a 'amended' GDPR for an implementing act to **specify criteria** for determining when data resulting from pseudonymisation is no longer considered personal data. Establishing EU-wide criteria will provide legal certainty, which is a key driver of economic growth, by enabling flexibility, innovation and cross-border data exchange. **We stress that the criteria must be simple and unambiguous in their implementation, ensuring that all companies can apply them:**

- **effectively (i.e., meet the objective of the GDPR);**
- **efficiently (i.e., without additional cost or effort); and**
- **consistently (i.e., the same application across the EU).**

This is particularly important for SMEs, which have fewer resources and must be able to rely on clear, accessible rules to remain competitive in the digital economy.

Notwithstanding the aforementioned, it is equally important that **Art. 41a's mandate for an implementing act remains focused on principles rather than prescribing specific technical 'means' for determining when pseudonymised data may no longer constitute personal data for certain entities.** Such an approach would preserve flexibility and avoid unintentionally constraining innovation. This provision should therefore focus on tech-neutral and subjective factors (given the relative approach codified in Art. 4(1) GDPR), such as 'available resources, legal rights, available technology in a data recipient and costs and time necessary to implement mitigating measures by a data recipient'. We propose to add the mentioned factors in Art. 41a explicitly. **Besides, we stress that the assessment of anonymity or pseudonymisation must be a realistic risk-based evaluation, reflecting actual risks and operational circumstances and relying on empirical evidence.** Such an approach will encourage the use of PETs and other mitigating measures, consistent with a risk-based framework, while ensuring that companies (and particularly SMEs) can implement solutions effectively and competitively.

We also noted the current placement of Art. 41a 'amended' GDPR within the GDPR itself, situated between provisions on certification (Art. 42) and codes of conduct (Arts. 40, 41). **This implementing act addresses the definition of personal data, and therefore, we believe that its natural and logical place is directly within Art. 4(1), which sets out that definition.** In the context of transfers, while pseudonymisation is often categorized as a technical and organisational measure under Article 32, the specific purpose of this provision is to determine the legal status of the data relative approach (i.e., whether it remains 'personal data'). Ensuring that EU law remains accessible and easy to navigate is essential for all stakeholders. Embedding Art. 41a 'amended' GDPR in the 'definitional section' (i.e. chapter I GDPR) would strengthen legal certainty and ensure that businesses, regulators, and citizens can navigate the GDPR with clarity.

Lastly, while Art. 41a 'amended' GDPR foresees close cooperation between the European Commission and the EDPB in preparing the implementing act, we believe that a more transparent and practice-oriented approach would further strengthen the process. The EDPB's core mandate

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

is to ensure consistent application of the GDPR and to issue opinions, advice and guidance.[12] **In this context, it may be more appropriate for the EDPB to contribute through an independent, practice-informed advice in line with Art. 70(1)(b) GDPR rather than through direct involvement in drafting the implementing act. At the same time, closer engagement with industry stakeholders would allow the European Commission to draw on operational expertise and established risk-management practices.** This would respect institutional roles, enhance transparency, and support the development of criteria that are both workable and aligned with real-world needs.

7. Targeted amendment under Art. 4(32-38) and Art. 5(1)(b) GDPR

We welcome the alignment of the same definitions across different legislations, which provides clarity in data use and contributes to greater legal certainty. Besides, the new definition on 'scientific research', which includes research that support innovation and aim to further a commercial interest, together with the amendments in Art. 5(1)(b) GDPR, are particularly valuable. The amendments will enable companies to gain insights necessary to improve and market their products and services effectively. Moreover, it gives companies the flexibility to choose between carrying out studies inhouse or to outsource these to external specialised research companies. **This clarity ultimately supports economic growth and fosters research and innovation that are both responsible and practically relevant.** A minor drafting refinement could be considered: replacing the phrase "independent of" with "notwithstanding" or "regardless," which may provide greater legal consistency.

Fostering global competitiveness through ethical AI development and streamlined GDPR, AI and cybersecurity rules

8. Targeted amendments under Art. 9 and Art. 88c GDPR

FEDMA welcomes the two additional processing grounds for special categories of personal data in Art. 9(2) GDPR. When combined with the safeguards proposed in Art. 88(c) 'amended' GDPR (i.e., appropriate organizational, technical measures and safeguards for the rights and freedoms of the data subject), together with the existing security obligations in Art. 5(1)(f) GDPR, these provisions provide legal certainty while ensuring that sensitive data can be processed responsibly and in a manner proportionate to the risks involved. **This legal certainty allows companies, including SMEs, to develop new products, improve services, and invest confidently in data-driven development while maintaining high standards of data protection.**

The above-mentioned amendment is even further strengthened by the added fifth paragraph in Art. 9 GDPR. This paragraph aims at balancing the protection of special categories of data that could inadvertently flow into the pool of data used for training an AI system. While it is for the industry to figure out ways to prohibit the disclosure of such data to third parties, we believe it a realistic approach to close the regulatory gap between the essential protection of special

[12] Art. 70 GDPR.

categories of personal data and the practical reality that such data can inadvertently end up in AI training sets. **An important drafting refinement could be considered, namely 'remove such data' should be complemented by 'from the AI output' to ensure clarity regarding the intended scope of the obligation**.

FEDMA welcomes the amendment in Art. 88c 'amended' GDPR explicitly allowing processing for legitimate interests when necessary, in the context of the development and operation of an AI system, mainly because it will open room for innovation all the while guaranteeing strong accountability for companies, ultimately leading to sustainable EU economic growth. Unlike consent which can be collected in a formalistic and procedural way, legitimate interest requires controllers to undertake rigorous and documented (risk) assessments, laying the ground for targeted safeguards for the data subjects' GDPR rights. As a result, processing on the basis of legitimate interest mandates robust accountability and aligns seamlessly with the GDPR's risk-based approach. However, introducing an unconditional right to object in Art. 88c 'amended' GDPR would go beyond the GDPR's existing framework and risks imposing disproportionate burdens on businesses, particularly SMEs. In line with the spirit of recital 4 GDPR, any new rights introduced in Art. 88c should respect the principle that data protection is not an absolute right and must be balanced with the freedom to conduct business. **A more proportionate approach is to apply the same balancing test established in Art. 21 GPDR and directly refer to that provision in Art. 88c 'amended' GDPR.**

9. Targeted amendments under Arts. 4 and 4a 'amended' AI Act

We welcome the clarification in Art. 4a of the amended AI Act according to which the mere processing of special categories of data does not in itself constitute discrimination. This amendment provides much-needed legal certainty and supports the responsible development of AI systems that rely on sensitive data for legitimate and socially beneficial purposes. We are committed to advancing methods and deploying PETs to address the associated challenges in a responsible and innovative manner.

While FEDMA supports ethical and responsible AI development, AI literacy obligations should be implemented in a practical and proportionate manner. Clearer and less burdensome AI literacy requirements than those currently envisaged in the AI Act would be welcome, provided they remain effective. Rather than introducing AI literacy as a standalone obligation, it could be embedded within the human oversight requirement, not only for high-risk systems (i.e. Art. 14 AI Act) but also for other AI systems, in order to stimulate broader uptake by companies.

For marketing teams, this means focusing on awareness, responsible use and basic risk assessment of AI-enabled tools, rather than formalised training requirements detached from operational reality. At the same time, a general obligation to promote AI literacy could be maintained at Member State level, encouraging companies to invest in appropriate upskilling without imposing rigid, one-size-fits-all compliance duties. Such a balanced approach better supports innovation, especially for SMEs, while remaining aligned with the risk-based logic of the GDPR and the AI Act.

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

10. Targeted amendments under Art. 33(1) GDPR

FEDMA welcomes the amendments in Art. 33(1) GDPR which **better align personal data breach notifications in several legislations** (e.g., GDPR, NIS2[13]). FEDMA also supports the clarification that notification is required only where a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, as **this raises the threshold for controllers and reduces unnecessary notifications while maintaining strong protection for individuals**. However, FEDMA foresees that the reference to 'high risk' resulting from a personal data breach could lead to difficulties, particularly for SMEs, because the GDPR does not define this concept. While reliance on existing guidelines[14] and national guidance provides for some steering, the existing fragmentation due to interpretative differences, difficulties (relating to the time pressure under which a human-centric assessment must be completed) and legal uncertainty will remain. A particularly concerning situation arises when supervisory authorities in the Member States adopt an overly broad interpretation of the concept of "high risk", effectively requiring controllers to notify both authorities and affected individuals even in cases where, on a reasonable assessment, such risk does not in fact exist. In practice, these assessments are often overly simplified and binary in nature, reflecting an excessive and frequently insufficiently justified level of precaution. Linking the concept of "high risk" for breach notification to the existing and well developed DPIA framework could improve consistency and reduce uncertainty, particularly for SMEs.

Readjusting the balance to protect businesses from abusive GDPR exploitation (i.e. abusive DSARs) while safeguarding legitimate compensation rights

11. Targeted amendments under Art. 12(5) GDPR

The original purpose of Art. 12(5) GDPR was to ensure that data subjects who suffer harm are appropriately compensated, a principle FEDMA fully supports. While we recognise and share this intention, practices developed over the years and experience has shown that the **practical application of this provision has, at times, come to diverge from its initial objective.** The proposed amendment (and the obvious effort by the European Commission to address abusive claims) is therefore a positive and timely development.

At the same time, we remain concerned that the current wording may not fully safeguard well-intentioned companies that act responsibly and cause no harm from individuals seeking to exploit 'a well-documented practice of abusive claims'. Such abusive claims not only impose unnecessary burdens on organisations but also risk undermining the credibility and effectiveness of legitimate compensation requests. **We believe that a more *balanced***

[13] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (weblink).
[14] EDPB Guidelines 9/2022 on personal data breach notification under GDPR (weblink).

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

approach is essential to protect both data subjects' rights and the integrity and fairness of the existing framework. We therefore propose the following:

- We welcome the amendment clarifying that this also applies to requests under Art. 15 GDPR where a data subject abuses the rights conferred by the GDPR for purposes other than the protection of their personal data. However, we remain concerned that the current wording may not sufficiently address the unfair impact this provision continues to have on well-intended and responsible companies. **In line with existing caselaw,[15] we therefore propose to refine the description of the manifestly unfounded or excessive requests by explicitly referring to the data subject's "abusive *intention*", indicative of *bad faith*. This should be understood as a situation where there is a lack of genuine interest in the personal data or where the request is instrumentalised for purposes unrelated to data protection, such as exerting coercive leverage over the controller or pursuing an ulterior aim detrimental to the integrity of the GDPR framework,** alongside the "excessive character" already laid down in Art. 12(5) GDPR.
- In addition to the explicit mention in Art. 12(5) GDPR, we propose to add the following sentences to recital 59 **to safeguard against fragmented interpretations in Member States and overly broad interpretations which could undermine legitimate compensation claims:** within the context of manifestly unfounded or excessive requests, which implies acting in bad faith, an abusive intention refers to a situation in which a data subject exercises a right under this Regulation in a manner that exceeds the limits of normal exercise of that right for a purpose unrelated to the protection of their personal data, or to artificially or explicitly cause disruption. This includes scenarios where the request is used as a tool for coercion, to obtain a settlement unrelated to actual data protection harms, or where the request is part of a coordinated commercial campaign designed to burden the controller rather than to genuinely exercise data protection rights. Notwithstanding the aforementioned, where the exercise of a right supports a legitimate compensation claim provided for in this Regulation, it should **not** be regarded as an abusive intention.
- FEDMA also welcomes the lower threshold for the controller who must demonstrate that there are reasonable grounds to believe that a request is excessive.

[15] Opinion of Advocate General Szpunar for case C-526/24 Brillen Rottler GmbH & Co. KG v. TC, paragraphs 44 to 50 in which the Advocate General explains that, while access requests can legitimately support damage claims, they become abusive if the data subject's only intention is to provoke a refusal and exploit GDPR rights for purposes unrelated to data protection (weblink). The opinion refers to previous caselaw, e.g. : case C-416/23 Österreichische Datenschutzbehörde v. F R, paragraph 50, specifying that the manifestly unfounded or excessive character of a request under Art. 57(4) GDPR is not only characterised by its repetitiveness (i.e. the number of requests during a specific period), because the supervisory authority, having regard to all the relevant circumstances of each case, also needs to demonstrate an abusive intention on the part of the person who submitted the request (weblink). In its opinion, the Advocate General Szpunar specifies that because both provisions (i.e., Arts. 57(4) and 12(5) GDPR) use identical wording and serve the same purpose, the same interpretation applies (ref. paragraph 40 of the opinion - weblink). Crucially, access requests become abusive and demonstrate bad faith if the data subject's intention is not to obtain the personal data, but solely to provoke a refusal, disrupt operations, or exploit GDPR rights for coercive purposes unrelated to data protection.

- **EU law has consistently treated compensation as a non-punitive mechanism, as confirmed by recent CJEU case law[16] under Art. 82 GDPR, which requires data subjects to demonstrate actual and certain material or non-material damage as a result of the GDPR infringement.** We therefore recommend codifying the caselaw by adding one sentence: 'for the avoidance of doubt, a data subject shall be entitled to compensation only where they demonstrate that they have suffered actual and certain material or non-material damage as a result of the controller's action or inaction that constitutes an infringement of the GDPR'. Besides, CJEU caselaw[17] also confirmed that administrative fines are punitive instruments while distinguishing administrative fines from compensation.

- Similarly, collective redress mechanisms, while valuable for ensuring access to justice, **may risk taking on a punitive character when aggregated claims amplify even modest individual damage, making careful calibration important to preserve their compensatory purpose.** To support this balance, further calibration measures would be welcome, for example, ensuring that collective redress actions remain grounded in an individualised assessment of actual harm[18] so that aggregated claims do not inadvertently assume a punitive effect.

Simplifying the GDPR ROPA obligations need to go hand-in-hand with strong accountability to guarantee sustainable growth in data-driven marketing

12. Targeted amendments under Art. 30(5) GDPR

While FEDMA approves the intention of the European Commission to reduce the GDPR compliance burden for SMEs in Omnibus IV, **FEDMA does not welcome the threshold increase in Art. 30(5) GDPR.** Fewer companies will be obliged to fulfil the record of processing activities (ROPA), thereby significantly increasing the legal risk for SMEs. More concretely, compliance checks will be difficult or impossible without a record of processing activities, which significantly undermines the accountability of businesses. **We therefore propose to erase this amendment from Omnibus IV.**

***

[16] Case C-340/21 VB v. Natsionalna agentsia za prihodite, paragraphs 83 to 86 (weblink). Case C-741/21 GP v. juris GmbH, paragraphs 42, 43, 64 (weblink). Case C-667/21 ZQ v. Medizinischer Dienst der Krankenversicherung Nordrhein, Körperschaft des öffentlichen Rechts, paragraphs 110, 111, 118 (weblink). Case C-687/21 BL v. MediaMarktSaturn Hagen-Iserlohn GmbH, paragraphs 67 to 69 (weblink).

[17] Case C-300/21 UI v. Österreichische Post AG, paragraphs 42 and 58 (weblink). See also Opinion of Advocate General Campos Sanchez-Bordona, paragraphs 39, 49, 52 (weblink). Case C-456/22 VX v. AT, paragraphs 21 to 23 (weblink).

[18] Case T-354/22 Thomas Bindl v. European Commission paragraphs 54, 196 to 198 (weblink).

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