FEDMA
Federation of European Data and Marketing

Position on the Digital Fitness Check

The Digital Fitness Check is an opportunity to unlock Europe's innovation capacity through more effective regulation

Data has a particular role to play with regards to European competitiveness. At the moment, Europe's data economy falls behind other global regions, yet it is also precisely in this area that the EU's single market could generate substantial gains if rules are better aligned and cross-border data use is facilitated. To unlock these benefits, however, Europe needs a more coherent and innovation-friendly approach to data within a framework that fully safeguards fundamental rights. This situation is also reflected in the Draghi report, which finds that Europe's data economy remains fragmented and that cross-border data sharing between Member States is far from optimal. The report therefore calls for EU-level incentives – including simplification of the GDPR – and for harmonised standards to create a genuine single market for data. Overlapping obligations, conflicting European and national rules and redundant requirements currently create high fixed compliance costs without delivering commensurate benefits for consumers, and enforcement of the GDPR often reflects an imbalance between businesses' legitimate need to process data and the need to protect personal data. Therefore, the Digital Fitness Check is a critical opportunity to re-balance and modernise the EU's digital rulebook so that it continues to protect citizens while also enabling European companies (especially SMEs) to innovate, compete and grow both within the EU and globally primarily by improving the coherence and application of existing rules rather than creating broad new legislative layers.

a. Proportionate and risk-based rules that reduce unnecessary burdens for companies

A key priority for the Digital Fitness Check should be to ensure that consent requirements focus on situations that genuinely create privacy risks, rather than on routine, low-risk technical uses. The coexistence of the proposed amendments in the GDPR with Article 5(3) ePrivacy Directive will create a dual-consent regime that no longer reflects technological or legal realities. Many cookies are no longer personal data under the GDPR (ref. SRB ruling), yet ePrivacy still requires parallel consent. This fuels cookie consent fatigue, adds no meaningful data protection, and imposes unnecessary costs on companies. Repealing Article 5(3) ePrivacy Directive[1] and replacing it with a GDPR-based only, tech-neutral and risk-proportionate provision would maintain strong personal data protection safeguards while reducing friction for users and businesses. To ensure proportionality, low-risk activities such as frequency capping, ad-fraud

[1] Unauthorized access to devices remains strictly prohibited under existing legislation (ref. 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)).

prevention, ad-measurement and brand-safety functions should be exempted from the consent requirement in Art. 88a GDPR (digital omnibus).

Moreover, EU digital legislation should regulate the risks arising from processing activities, not the source of the data or the technology used. For instance, the obligation in Article 13(2) of the ePrivacy Directive on the right to object at the moment of data collection is outdated. A modernised approach should recognise that a company has a legitimate right to contact its own customers, provided this is done transparently and always respects the customer's choice of whether, and through which channel, they wish to be contacted. To remain future-proof, the provision should be tech-neutral and avoid tying obligations to specific devices or communication tools that may quickly become outdated.

b. Coherent legislation: one activity should be regulated by one rule only

Multiple EU instruments currently regulate the same data processing activities in parallel (GDPR, ePrivacy Directive, DMA, UCPD, EECC), often with different legal concepts and obligations. For instance, Article 22 GDPR and the AI Act apply different logics to AI-driven profiling, creating uncertainty for legitimate, economically necessary and low-risk marketing activities. The GDPR and AI Act must be aligned around a single, coherent logic for impact and risk.

The upcoming Digital Fairness Act risks re-regulating issues already covered by the GDPR and ePrivacy rules, e.g. for cookie-banners, dark-pattern consent flows are already unlawful. This redundancy would add compliance burden for businesses, especially SMEs, without improving consumer protection. The Digital Fitness Check should ensure the DFA targets genuine gaps rather than duplicating existing rules.

c. Legal certainty through streamlined definitions and legal concepts

Divergent definitions, such as when personal data qualifies as "remuneration", force companies to conduct multiple parallel assessments for the same activity. The codification of the Inteligo ruling, as well as a harmonised, modern definition of "data as value" and an explicit exclusion of non-consumer-facing data from "data as remuneration" provisions would reduce legal uncertainty and support economic growth as well as innovation.

More generally, inconsistent enforcement across Member States increases compliance costs, slows product deployment, and undermines legal certainty. For instance, the draft joint European Commission and EDPB guidelines covering Article 6(11) DMA appears to apply a broader and more absolute version of the "means reasonably likely to be used" test for qualifying personal data anonymous than the GDPR and CJEU approach to the personal data definition and anonymity. The SRB case should therefore be codified in the GDPR.

d. Innovation and economic growth enabling regulation

Some proposed EU simplification amendments are ineffective in practice, because larger companies can often pass obligations downstream through contracts, creating a *de facto* situation in which SMEs must comply fully despite legal exemptions. This risks reinforcing incumbent advantages without delivering better protection for individuals. A more sustainable approach would be to scale obligations according to the risk and impact of the processing, focusing on the depth and sophistication of safeguards rather than on categorical exemptions based solely on company size.

These structural effects are reinforced by the current enforcement culture, which often treats regulation primarily as a tool for sanctioning non-compliance. This disproportionately affects legitimate, ethical companies that invest in responsible data practices but receive no regulatory benefit from doing so. A shift toward 'supportive of ethical activities' legislation, risk-based supervision, with practical guidance and consistent interpretation across DPAs and other national authorities, would allow and even incentivise responsible innovation while maintaining high standards of personal data and consumer protection.

To address both the structural and enforcement-related issues described above, a new policy-making approach is needed. This should include a high threshold for whether new legislation is needed at all, risk-based and principle-based rules rather than detailed regulation, and impact assessments that rigorously examine how proposals and existing legal frameworks affect innovation and the entrepreneurship of the future.

e. Practical support to reduce fixed compliance costs for SMEs (but not only) and ensure a fair level playing field

SMEs face the highest burden from fragmented and duplicative rules. EU-level templates, interoperable systems and common standards would reduce fixed costs and enable companies to focus resources on innovation, product development and consumer value. For instance, Article 6(10) DMA is intended to give advertisers and publishers high-quality and continuous access to both aggregated and non-aggregated performance data. However, in practice, the data provided by gatekeepers is often delayed, degraded, and limited, preventing SMEs from fully exercising these rights in a meaningful way.

In addition to such standardised tools and interoperable systems policy makers and privacy enforcement authorities will increasingly need, in line with the OECD recommendations, to consider how the use of PETs impacts regulatory assessments under privacy and data protection frameworks, recognising their contribution to privacy protective outcomes. A good example is Singapore's IMDA PETs Adoption Guide providing clear, practical and tech-neutral guidance to accelerate PET uptake. Such guidance could be considered by the European Commission to complement Article 25 GDPR, and explicit incentives could be included in Articles 6(1)(f) and 25 GDPR.